

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛТАВСЬКА ДЕРЖАВНА АГРАРНА АКАДЕМІЯ

Кафедра менеджменту

ДЯЧКОВ ДМИТРО ВОЛОДИМИРОВИЧ

*Управлінські аспекти
інформаційної безпеки:
теорія, методологія, практика*

МОНОГРАФІЯ

Запоріжжя – 2019

УДК 005.004 – 049.5 : 338.43 (477)
ISBN 978-966-2672-51-0

Рецензенти: А. Л. Баланда, д.е.н., професор, професор спеціальної кафедри Навчально-наукового інституту перепідготовки та підвищення кваліфікації кадрів Служби Безпеки України Національної академії Служби безпеки України;
Ю. Е. Губені, д.е.н., професор, академік Академії економічних наук України, завідувач кафедри підприємництва, торгівлі та біржової діяльності Львівського національного аграрного університету;
А. М. Михайлов, д.е.н., професор, завідувач кафедри менеджменту Сумського національного аграрного університету

Дячков Д. В. Управлінські аспекти інформаційної безпеки: теорія, методологія, практика : монографія. Запоріжжя : Вид-во «Інтр-М», 2019. 424 с.

Рекомендовано до друку Вченою радою Полтавської державної аграрної академії від 29 листопада 2019 р. (протокол №7)

У монографії обґрунтовано теоретичні, методологічні засади та розроблено практичні положення щодо управління інформаційною безпекою підприємств агропродовольчої сфери. Узагальнено теоретичні основи управління інформаційною безпекою в умовах цифровізації. Систематизовано понятійно-категоріальний апарат інформаційної безпеки підприємства. Розроблено організаційно-функціональну модель управління інформаційною безпекою підприємства. Сформовано організаційні основи створення віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу. Адаптовано модель системи менеджменту інформаційної безпеки підприємства агропродовольчої сфери. Запропоновано модифікацію моделі захисту інформації підприємства на основні технології «глибинного захисту». Розроблено методичний підхід до визначення стратегії управління інформаційною безпекою підприємств агропродовольчої сфери. Актуалізовано політику інформаційної безпеки на основі концепції інформаційної культури. Спрогнозовано результативні показники діяльності підприємств агропродовольчої сфери України на основі інтегрального показника рівня інформаційної безпеки.

Розрахована для викладачів, аспірантів, магістрів, а також для наукових працівників і тих, хто цікавиться питаннями забезпечення інформаційної безпеки та управління підприємствами агропродовольчої сфери.

ISBN 978-966-2672-51-0

© **Дячков Д. В.**

Д 99

ЗМІСТ

ВСТУП.....	6
РОЗДІЛ 1. УПРАВЛІНСЬКІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ.....	10
1.1. Парадигми розвитку цифрової економіки та цифрового менеджменту.....	10
1.2. Сутність інформаційної безпеки підприємства.....	28
1.3. Сучасні моделі управління інформаційною безпекою підприємства...	48
Список використаних джерел до розділу 1.....	67
РОЗДІЛ 2. ДІАГНОСТИКА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ АГРОПРОДОВОЛЬЧОЇ СФЕРИ УКРАЇНИ	84
2.1. Характеристика стану і визначення тенденцій розвитку агропродовольчої сфери України.....	84
2.2. Оцінка зовнішніх та внутрішніх факторів впливу на систему управління інформаційною безпекою аграрних підприємств України.....	103
2.3. Аналіз рівня інформаційної безпеки підприємств агропродовольчої сфери України	123
Список використаних джерел до розділу 2.....	146
РОЗДІЛ 3. МЕТОДОЛОГІЧНІ ПІДХОДИ ДО ОЦІНЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ АГРОПРОДОВОЛЬЧОЇ СФЕРИ УКРАЇНИ.....	157
3.1. Методичні підходи до оцінювання інформаційної безпеки підприємств агропродовольчої сфери.....	157
3.2. Методологічні підходи до інтегральної оцінки рівня інформаційної безпеки підприємств агропродовольчої сфери України.....	176
3.3. Прогнозування інтегрального показника рівня інформаційної безпеки підприємств агропродовольчої сфери України	203
Список використаних джерел до розділу 3.....	221
РОЗДІЛ 4. ОПТИМІЗАЦІЯ ОРГАНІЗАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ АГРОПРОДОВОЛЬЧОЇ СФЕРИ УКРАЇНИ.....	228
4.1. Формалізація організаційних засад створення віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу....	228
4.2. Створення системи менеджменту інформаційної безпеки підприємства агропродовольчої сфери України.....	244

4.3. Адаптація моделі захисту інформації підприємства агропродовольчої сфери.....	262
Список використаних джерел до розділу 4.....	279
РОЗДІЛ 5. СТРАТЕГІЧНІ НАПРЯМИ ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ АГРОПРОДОВОЛЬЧОЇ СФЕРИ УКРАЇНИ.....	288
5.1. Розробка стратегій управління інформаційною безпекою підприємств агропродовольчої сфери України.....	288
5.2. Формування політики інформаційної безпеки підприємства на основі концепції інформаційної культури	307
5.3. Прогнозування результативних показників діяльності підприємств агропродовольчої сфери на основі рівня інформаційної безпеки.....	322
Список використаних джерел до розділу 5.....	338
ВИСНОВКИ.....	344
ДОДАТКИ.....	350

СПИСОК СКОРОЧЕНЬ І УМОВНИХ ПОЗНАЧЕНЬ

АПС – агропродовольча сфера;

БД – база даних;

ВВП – валовий внутрішній продукт.

ІБ – інформаційна безпека;

ІКТ – інформаційно-комунікаційні технології;

ІС – інформаційна система;

НДДКР – науково-дослідні та дослідно-конструкторські роботи;

НТП – науково-технічний прогрес;

ОПР – особа, що приймає рішення;

ПЗ – програмне забезпечення;

СІБ – система інформаційної безпеки

СМІБ – система менеджменту інформаційної безпеки.

ВСТУП

Загальносвітовою тенденцією є трансформація суспільства, яка відбувається в умовах посилення глобалізаційних процесів, зростання сфери послуг і нематеріального виробництва, впливу інформаційно-комунікаційних технологій на процеси розвитку науково-технічного прогресу, у тому числі масштабного, глибинного й динамічного проникнення інформаційних технологій в усі сфери життєдіяльності особи, суспільства, суб'єктів господарювання й держави. Передові інформаційно-комунікаційні технології покликані вирішувати важливі проблеми цифрових розривів наступних поколінь, оскільки оператори мереж та користувачі змушені адаптувати свої бізнес-моделі для використання можливостей цифрової трансформації. Тому нагальними питаннями є аналіз тенденцій розгортання і використання передових інформаційно-комунікаційних технологій

Сучасна агропродовольча сфера перебуває в епіцентрі цифрових інноваційних трансформацій, базисом яких є процеси автоматизації, інформатизації, цифровізації управлінських і виробничих бізнес-процесів. Цифрові технології, робототехніка, біоінженерія, сенсорні технології, аналітика великих даних, які застосовують вітчизняні суб'єкти аграрного ринку, сприяють прийняттю оперативних і релевантних управлінських рішень з метою збільшення обсягів виробництва, підвищення якості та конкурентоспроможності продукції, зменшення її собівартості, формування продовольчого потенціалу тощо. Для побудови ефективної системи захисту інформації необхідно використовувати комплексний підхід, який ґрунтується на реалізації стратегії та політики інформаційної безпеки, формуванні системи менеджменту інформаційної безпеки підприємства, що, в свою чергу, зумовлює необхідність розроблення методології оцінки та діагностики інформаційної безпеки, формалізації організаційних засад формування системи інформаційного захисту, визначення оптимальної моделі захисту інформації та підтверджує актуальність цього дослідження.

Проблемам розвитку аграрного сектора України та аналізу загроз інформаційній безпеці підприємств агропродовольчої сфери присвячена частина доробок вчених світової та вітчизняної наукової спільноти, зокрема В. Аранчій, І. Арістової, Л. Березіної, В. Болека, С. Зефірова, М. Зось-Кіора, С. Івка, П. Макаренка, О. Качана, Є. Міщука, Д. Новака, О. Сазонця та інших.

Управлінським аспектам інформаційної безпеки присвячені наукові праці таких вітчизняних і зарубіжних учених: С. Ілляшенка, Р. Калюжного, С. Ковтуна, А. Козаченко, Б. Кормича, Т. Лепейко, В. Ліпкана, І. Маркіної,

В. Морозової, С. Мочерного, І. Панаріна, О. Пузиренка, Н. Реверчука, Є. Родіна, С. Смірної, О. Сороківської, О. Теренина, В. Ярочкіна та інших.

Віддаючи належне теоретичній і практичній цінності зазначених наукових здобутків, доцільно відзначити дуалістичність поглядів на цей процес: з одного боку, – обов’язковість вимог національних уповноважених органів (стандарти, нормативи, процеси ліцензування), з іншого – розуміння власником аграрного бізнесу та керівництва підприємства необхідності та можливості впровадження комплексних механізмів захисту інформації. Недостатнє розв’язання проблем актуалізації понятійно-категоріального апарату, політики, стратегії, організаційного забезпечення та системи менеджменту інформаційної безпеки, удосконалення методичних і методологічних підходів до оцінювання та прогнозування рівня інформаційної безпеки, модифікації моделей управління інформаційною системою та захистом інформації зумовило вибір теми, мети й завдань дослідження.

Мета монографії полягає в обґрунтуванні теоретичних, методологічних засад і розробці практичних положень щодо управління інформаційною безпекою підприємств агропродовольчої сфери.

Для досягнення поставленої мети було сформульовано і виконано наукові завдання, що визначили структуру монографії:

- узагальнити парадигми розвитку цифрової економіки та цифрового менеджменту;
- систематизувати понятійно-категоріальний апарат інформаційної безпеки підприємства;
- розробити сучасні моделі управління інформаційною безпекою підприємства;
- надати характеристику стану і визначити тенденції розвитку агропродовольчої сфери України;
- здійснити оцінку зовнішніх та внутрішніх факторів впливу на систему управління інформаційною безпекою аграрних підприємств України;
- проаналізувати рівень інформаційної безпеки підприємств агропродовольчої сфери України;
- узагальнити методичні підходи до оцінювання інформаційної безпеки підприємств агропродовольчої сфери;
- обґрунтувати методологічні підходи до інтегральної оцінки рівня інформаційної безпеки підприємств агропродовольчої сфери України;
- здійснити прогнозування інтегрального показника рівня інформаційної безпеки підприємств агропродовольчої сфери України;

- формалізувати організаційні основи створення віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу;
- створити систему менеджменту інформаційної безпеки підприємства агропродовольчої сфери України;
- адаптувати модель захисту інформації підприємства агропродовольчої сфери;
- розробити стратегії управління інформаційною безпекою підприємств агропродовольчої сфери України;
- сформулювати політику інформаційної безпеки підприємства на основі концепції інформаційної культури;
- спрогнозувати результативні показники діяльності підприємств агропродовольчої сфери на основі рівня інформаційної безпеки;

Об'єктом монографічного дослідження є процес управління інформаційною безпекою підприємств агропродовольчої сфери України.

Предметом монографічного дослідження є теоретичні, методологічні та практичні засади управління інформаційною безпекою підприємств агропродовольчої сфери України.

Теоретичним і методологічним підґрунтям монографії є положення сучасної безпекології та менеджменту, наукові праці вітчизняних і зарубіжних учених, присвячені питанням УІБ суб'єктів аграрної сфери.

Міждисциплінарний і багатоаспектний характер наукової проблеми зумовив застосування комплексу таких методів: історичного, логічного, онтологічного аналізу – для висвітлення трансформації наукових парадигм цифрової економіки та цифрового менеджменту; теоретичного узагальнення, морфологічного та етимологічного аналізу – для систематизації понятійно-категоріального апарату інформаційної безпеки; систематизації та формалізації – для побудови організаційно-функціональної моделі та формування системи менеджменту інформаційної безпеки підприємства агропродовольчої сфери; економіко-статистичних – для визначення тенденцій розвитку агропродовольчої сфери України; економіко-математичних, факторного аналізу, анкетування, опитування, ранжування – для побудови факторної моделі ризиків та оцінки інформаційної безпеки, картування впливу зовнішніх і внутрішніх факторів на виникнення загроз інформаційній безпеці; порівняльного аналізу, групування – для удосконалення методичних і методологічних підходів до оцінювання та діагностики інформаційної безпеки підприємств; аналізу ієрархій, модифікованої головної компоненти, регресії, найменших квадратів,

експоненціального прогнозування, експертних оцінок – для обґрунтування методології оцінювання та прогнозування інтегрального показника рівня інформаційної безпеки підприємств; узагальнення, системного аналізу, порівняльного аналізу – для формалізації віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери», модифікації моделі захисту інформації та актуалізації політики інформаційної безпеки підприємств; матричних – для розробки стратегії управління інформаційною безпекою підприємств; прогнозування, кореляційно-регресійного аналізу, рейтингового – для прогнозування результативних показників діяльності підприємств; графічного – для відображення даних у найбільш інформативній формі.

Теоретичною та нормативною основою монографії були нормативні та правові акти, офіційна інформація Державної служби статистики України, Міністерства інформаційної політики України, Міністерства цифрової трансформації України, Державної служби спеціального зв'язку та захисту інформації України, а також наукова вітчизняна та зарубіжна література й інші довідкові матеріали. В дослідженні були використані документи підприємств агропродовольчої сфери, дані з інтернет-джерел, опрацьовані автором, власні первинні та аналітичні матеріали досліджень, результати анкетування.

Позитивною стороною монографії є системність та логічність побудови, простота та доступність викладення матеріалу, наявність прикладів та ілюстративного матеріалу.

Сподіваємося, що запропонована монографія стане ще одним кроком до наукового вирішення проблем формування ефективної системи управління інформаційною безпекою підприємств агропродовольчої сфери, а також буде корисною широкому колу викладачів, керівників і фахівців сучасних підприємств, здобувачів вищої освіти економічних та управлінських спеціальностей закладів вищої освіти.

РОЗДІЛ 1

УПРАВЛІНСЬКІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ

1.1. Парадигми розвитку цифрової економіки та цифрового менеджменту

Технологічні зміни, що характерні для ХХІ століття в частині «зрощування» телекомунікаційних технологій та інновацій, зумовили введення в науковий обіг понять «цифрові технології», «цифрова адженда», «цифрова економіка». Сьогодні цифрова економіка є одним з найважливіших чинників економічного зростання та формування нової якості життя. Лідери світової економіки розглядають цифровізацію як першочерговий напрямок інноваційного розвитку виробничо-економічних систем різних рівнів та інструмент забезпечення конкурентних переваг у довгостроковій перспективі. Тому, цифрова економіка є сферою нових надзвичайних можливостей, яка водночас вимагає застосування нових підходів до її організації та управління. Поряд з цим потребують подальшого наукового опрацювання й трансформації певні звичні категорії та напрямки економічної науки.

Сучасні інформаційно-комунікаційні технології суттєво змінюють існуючі соціально-економічні та суспільні відносини, у зв'язку з цим формується нове – інформаційне суспільство та, відповідно, новий етап економічного розвитку – становлення цифрової економіки. Незважаючи на існуючі схожі характеристики та властивості економіки в її традиційному розумінні та цифрової економіки, остання має особливості та значні переваги, які актуалізують її дослідження з погляду інтересу наукової спільноти, а тому її вивченню присвячені доробки В. Апалькової [15], Ю. Бажала [21], С. Бермана [180], Н. Борецької [26], Д. Бразевича [28], Дж. Брокмана [182], С. Веретюка [33], А. Герасимової [28], С. Дятлова [55], О. Заварицької [28], Г. Карчевої [83], Л. Кіт [86], Т. Лепейко [192], Л. Мановича [194; 195; 196], Д. Огородної [83], В. Опенька [83], В. Пілінського [33], М. Пората [203].

Одним із ключових напрямів розвитку держави, а відповідно, й інших суб'єктів макро- та макрорівня, є соціально-економічний розвиток. Упровадження цифрової економіки є важливим етапом розвитку суспільства, що дає змогу розширити інформаційний простір, використовувати

інтелектуальний потенціал і знання людини, створюючи фактори стабільного безпечного соціального середовища в майбутньому. Отже, проблематика становлення та поширення цифрової економіки є актуальною не скільки в теоретичній, скільки в практичній площині.

Розвиток інформатизації на тлі світових глобалізаційних процесів створює передумови для прискореного становлення цифрової економіки. Проте це насамперед пов'язано з економічною нерівністю, що виникає між розвиненими країнами та країнами, що розвиваються, через значну різницю темпів зростання обсягів та номенклатури товарів і послуг, що надаються за допомогою інформаційно-комунікаційних технологій. Тому для становлення та розвитку цифрової економіки держави перш за все необхідно сформувати відповідний рівень інформаційної економіки [199].

У процесі розвитку інформаційної економіки України в законодавчій базі закріпилися основи її розвитку. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [6], Розпорядження КМУ «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» [10], Розпорядження КМУ «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації» [9], ініціативи, проекти «цифровізації» України до 2020 р. – усі вони власне й визначають поле становлення та розвитку цифрової економіки України [217] та містять лише стратегічні напрями діяльності без конкретизації методів, способів і набору інструментарію.

Відповідно до Стратегії розвитку інформаційного суспільства в Україні, одним із головних пріоритетів України є розвиток інформаційного суспільства, в якому сукупність суспільних відносин у різних сферах людської діяльності (політика, економіка, освіта, культура, дозволя, особисте життя тощо) існує на основі широкого використання сучасних інформаційних і комунікаційних технологій, що дозволяє кожному створювати інформацію та накопичувати знання, мати вільний доступ до них, надає можливості для їх розповсюдження та використання задля соціального прогресу та особистісного інтелектуального зростання [10].

Основною метою цифровізації відповідно до пропонованої концепції є цифрова трансформація існуючих і формування нових галузей економіки, трансформація сфер життєдіяльності. А власне процес цифровізації економіки являє собою механізм економічного зростання завдяки здатності технологій позитивно впливати на ефективність, результативність, вартість і якість економічної, громадської та особистої діяльності [9].

Вищезазначене обґрунтовує необхідність проведення онтологічного аналізу понять «інформаційна економіка» та «цифрова економіка» (Додаток А) та їх взаємозалежності.

Онтологічні основи використання поняття «інформаційна економіка» започатковані 1933 р., у наукових працях Ф. Махлупа, який увів поняття «індустрія знань», що передбачає поєднання п'яти секторів інформаційної діяльності суспільства, таких як інформаційні технології та інформаційні послуги, засоби масової інформації, освіта, наукові дослідження та новітні розробки [109; 193].

Загалом термін «інформаційна економіка» спочатку трактувався на основі концепції первинного та вторинного інформаційних секторів, які доповнювали основні традиційні чотири сектори економіки [184]. Первинний інформаційний сектор охоплює сферу інформаційних послуг, а також виробництво обладнання, необхідного для впровадження інформаційних технологій. Концепція первинного інформаційного сектора передбачає, що вартість інформаційних продуктів і послуг слід включати до ВВП. Вторинний інформаційний сектор охоплює виробництво «неінформаційних» товарів і послуг для інформаційного сектора. Отже, М. Порат об'єднав в інформаційній економіці як галузь інформаційного обслуговування, так і галузі, що забезпечують функціонування первинного інформаційного сектора [203, с. 70].

На початку ХХІ ст. парадигма інформаційної економіки передбачала, що у всіх існуючих соціально-економічних явищ є спільна основа – стійка інформаційна структура. Також різні економічні явища, їх форми вираження та кількісні характеристики можуть бути описані як сукупність інформаційних компонентів [55].

Пізніше інформаційна економіка пов'язувалася в першу чергу з економікою знань, яка передбачала використання знань для економічного розвитку. Вважалося, що інформація та знання використовуються для виробництва конкурентоспроможної продукції, що і забезпечує економічний розвиток. Відповідно, проблеми отримання та застосування знань – один із предметів дослідження інформаційної економіки. Також слід зауважити, що економіка знань відрізняється від інформаційної економіки, оскільки основним ресурсом останньої є інформація, продуктом – інформація та знання, тоді як основним ресурсом економіки знань є знання, а основним продуктом – інтелектуальний капітал [41].

Підсумовуючи вищезазначене, доцільно зауважити, що інформаційна економіка базується на інформації та знаннях як виробничому ресурсі, передбачає інформаційне виробництво, використовує інформаційні технології, які забезпечують передачу знань. Тобто інформаційна економіка

включає створення та використання інформаційних ресурсів у структурованому інформаційному просторі, а також забезпечує можливості продукування інтелектуального капіталу та інновацій, і таким чином впливає на економічні процеси та суспільно-економічні відносини.

Онтологія цього поняття відповідно до поглядів різних учених дає змогу визначити, що воно пройшло еволюційний шлях розвитку:

спочатку інформаційна економіка визначалася як тип економіки, де переважна частка ВВП забезпечується діяльністю з виробництва, обробки, зберігання та передачі інформації і знань (1966 р.);

на етапі її становлення та закріплення інформаційна економіка визначалась як кластер галузей, що виробляють сучасні бази даних і засоби, що забезпечують їх функціонування й застосування (1978 р.);

на етапі розвитку інформаційну економіку трактували як економіку, яка враховує передумову, що інформація має не тільки соціально-економічну цінність, але і вимагає інформаційного ринку, на якому можливий інформаційний обмін (2014 р.);

на етапі трансформації вважалося, що інформаційна економіка відокремлено не існує, а є економікою в її класичному визначенні, різні сфери якої в тій чи тій мірі пронизані цифровими інформаційно-комунікаційними технологіями (2018 р.).

Трансформаційні процеси, пов'язані зі становленням інформаційної економіки, в Україні супроводжувались певними особливостями, такими як:

формування нових виробничих сил, які докорінно перетворили матеріально-технічну базу виробництва через упровадження процесів автоматизації інформаційних ресурсів, використання комп'ютерної техніки та її інтеграцію з глобальною мережею Інтернет;

трансформування характеру праці, що зумовило виникнення нового виду діяльності – інформаційної діяльності, а отже, нових форм праці – дистанційних (електронна комерція, аутсорсинг технологій тощо);

упровадження елементів інформаційних систем та інформаційних технологій у виробництво, комерцію, сферу послуг, що разом з глобальною мережею Інтернет створило базис для розгортання діяльності сітьових підприємств, віртуальних корпорацій;

поява інформаційної індустрії (унаслідок вищеперелічених особливостей), що утворилась шляхом злиття ІТ-індустрії, індустрії зв'язку (комунікації), сфери акумулювання інформаційних ресурсів, баз і банків даних тощо.

На думку переважної більшості теоретиків, поява цифрової економіки є еволюційним етапом саме інформаційної економіки, яка набула нових

якостей завдяки розвитку інформаційно-комунікаційних технологій і цифровізації економічних, соціальних, виробничих та інших процесів у суспільстві.

Як справедливо зазначають Н. Борецька та Л. Петренко, єдиного терміна досі не існує. Так, поряд із поняттям «цифрова економіка» часто використовуються такі, як «електронна економіка», «економіка додатків», «новий технологічний уклад світу», «креативна економіка», «API-економіка» тощо. При цьому важливо підкреслити, що переважна частина європейського та американського наукових співтовариств усе частіше вживає термін «цифрова економіка» [26].

Цифрову економіку у найпростішому вигляді визначають як економіку, що базується на цифрових комп'ютерних технологіях. Цифрову економіку також іноді називають інтернет-економікою, новою економікою, або веб-економікою [91].

Провідні фахівці вважають, що до терміна «цифрова економіка» існує два підходи.

Перший підхід – «класичний»: цифрова економіка – це економіка, заснована на цифрових технологіях, яка характеризує виключно сферу електронних товарів і послуг (телемедицина, дистанційне навчання, продаж медіаконтенту тощо) [33; 137; 200; 208].

Другий підхід – розширений: «цифрова економіка» – це економічне виробництво із використанням цифрових технологій [34; 51; 72; 73; 84; 86; 206; 207; 218].

Онтологія розвитку трактування цифрової економіки схожа на еволюцію поняття «інформаційна економіка»:

починаючи від її зародження, цифрову економіку розглядали як процес виробництва, продажу та постачання продукції шляхом використання комп'ютерних мереж (1995 р.);

на етапі становлення – від визначення цифрової економіки як інтеграції підтримуючої цифрової інфраструктури, електронного бізнесу та електронної комерції (2001 р.) до її визначення як формування мережі господарюючих суб'єктів, які створюють і обмінюються цифровими активами (віртуальними активами) завдяки поширенню та розвитку Інтернету (2009 р.);

на етапі розвитку цифрову економіку розглядають як трансформацію сфер традиційної та інформаційної економік завдяки перенесенню на цифрову платформу інформаційних ресурсів і знань із метою їх подальшого розповсюдження та використання (2017 р.), а також як формування системи соціально-економічних і культурних відносин завдяки використанню цифрових інформаційно-комунікаційних технологій (2018 р.);

етап трансформації цифрової економіки передбачається упродовж 2023–2025 рр.

Враховуючи особливості розглянутих понять «інформаційна економіка», «цифрова економіка» та суміжних понять «економіка знань», «веб-економіка», «електронна економіка», «економіка додатків» і спираючись на проведені дослідження зарубіжних і вітчизняних авторів, визначено еволюційний порядок формування цифрової економіки (рис. 1.1).

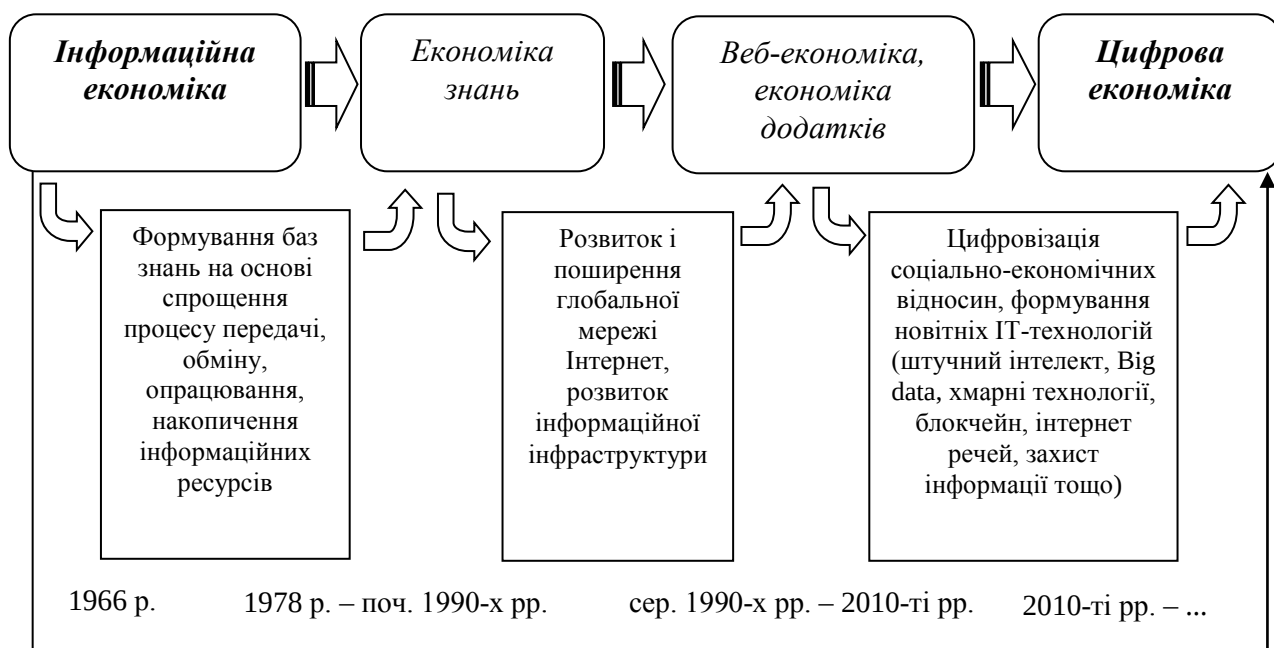


Рис. 1.1. Еволюція формування цифрової економіки [авторська розробка]

Отже, цифрову економіку в межах цього дослідження пропонується розглядати не як окремий революційний етап розвитку економіки, а як трансформацію інформаційної економіки, зумовлену розвитком ІТ-сфери, формуванням інформаційно-комунікаційної (згодом цифрової) інфраструктури, появою штучного інтелекту, віртуалізацією міжнародних ринків і, отже, зміною інформаційної культури соціально-економічних відносин у суспільстві, що надало змогу виділити основні елементи та напрями цифровізації традиційної економіки.

Узагальнення етапів еволюції інформаційної економіки та нормативно-правових актів у сфері інформатизації та цифровізації дозволило визначити основні етапи становлення інформаційної, зокрема і цифрової економіки в Україні (рис. 1.2).

В умовах сьогодення цифрова економіка України є базисом розвитку систем державного управління, економіки, бізнесу, соціальної сфери та

суспільства загалом, а її безпека є основою національної безпеки, соціальної безпеки, а також конкурентоспроможності вітчизняних підприємств, організацій та установ.

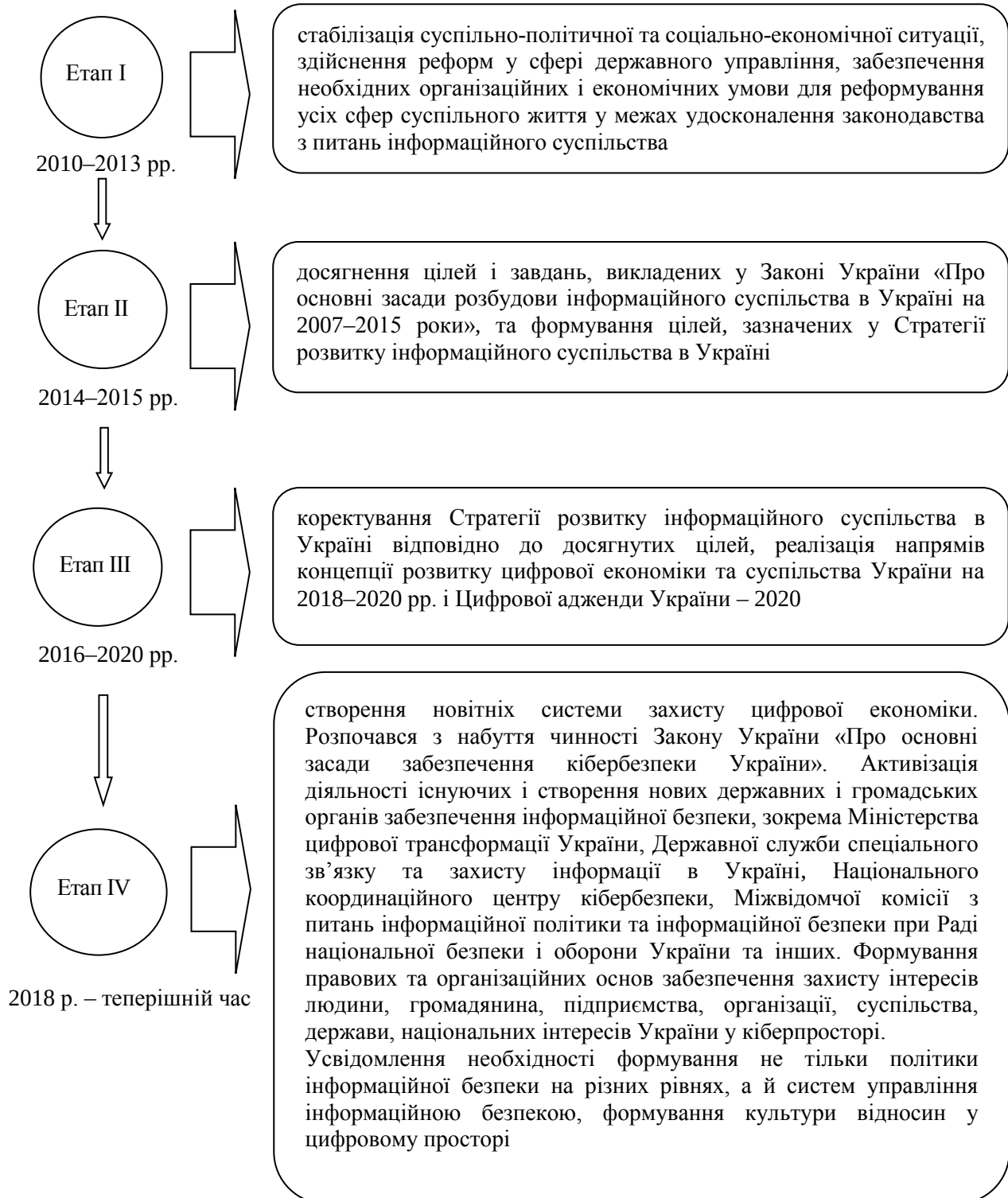


Рис. 1.2. Етапи становлення та розвитку інформаційної економіки в Україні [розроблено на основі 5; 6; 9; 10; 217]

З метою розвитку цифрової економіки України, її подальшого перетворення в новітні форми трансформації економічного устрою необхідна

ефективна державна підтримка забезпечення належних умов функціонування, її захисту на макро- та макрорівні, стимулювання її розвитку, а також подолання «цифрового розриву». Тому основою концепції «цифровізації» України має стати формування новітньої форми «цифрових взаємовідносин» тріади «особа – підприємство – держава», що в свою чергу передбачає необхідність розробки та розвитку нових наукових парадигм управління ними. Парадигми управління минулого століття характеризувалися вибором прямолінійних повільних рішень. Проте сучасне динамічне середовище стає все більш залежним від безлічі груп факторів, більш інтегрованим, а тому і більш складним і нелінійним. В епоху цифровізації завдяки сучасним цифровим ІТ-технологіям можна «перевіряти» ефективність найбільш оптимальних управлінських рішень за допомогою засобів віртуалізації, переконавшись, що ці рішення не матимуть негативних соціальних і економічних наслідків, а також втілювати їх у реальному управлінському чи виробничому бізнес-процесі.

Теоретики і практики менеджменту давно звернули увагу, що основою управлінської діяльності, яка за своєю суттю є інтелектуальною, є інформація, яка має ряд особливостей:

- вона є первинною стосовно інших видів ресурсів;
- не зникає (не витрачається) в процесі споживання (використання інформації в управлінському процесі);
- у процесі обміну або розповсюдження не передається повністю, тобто залишається і у передавача, і в отримувача (і в інформаційній системі, і в користувача – особи, яка приймає рішення);
- є неподільною;
- її можливо узагальнювати, результатом чого є отримання метайнформації;
- на відміну від інших ресурсів, практично невичерпна [128; 153; 205; 216].

Усе більше зростає роль інформаційних ресурсів та інформаційно-комунікаційних систем як основи формування нового «цифрового» суспільства, інфраструктурою якого є інтелектуальний комп'ютеринг. Цифрова трансформація суспільства призводить до переформатування всіх типів суспільних відносин, у першу чергу управління.

Зазначене зумовлює актуальність трансформації класичної парадигми менеджменту, сформульованої Ф. Тейлором, А. Файолем, Р. Емерсоном, Е. Мейо, Д. Макклелландом та іншими науковцями, оскільки вона обмежувалася положеннями управління в матеріальному світі. Створений віртуальний світ цифрових можливостей є новітнім інструментом «випереджаючих» технологій управління та дозволяє попередньо «відпрацювати» можливі рішення на віртуальних платформах і цифрових

моделях із метою передбачення не тільки локальних наслідків прийняття управлінських рішень, але й цивілізаційних [205].

Слід визнати, що в парі «менеджмент» – «цифровізація» саме менеджмент є первинним, оскільки спочатку необхідно удосконалити управління, підвищити якість кадрового потенціалу, а потім – впроваджувати стандарти цифрового управління, бо інакше виникає загроза управлінської відсталості. У законі Мерфі зазначається, що «помилятися властиво людині, але остаточно все заплутати може тільки комп'ютер» [213]. Тобто цифровізація менеджменту – це зовсім не панацея, що дозволяє «списати недоробки» розвитку менеджменту підприємства, це своєрідне випробування ступеня зрілості системи менеджменту.

Основною умовою формування та реалізації цифрового менеджменту є цифрове середовище, яке зародилось у 80-х рр. XX ст. Саме в цей період відбувся перехід від «аналогових» електронних носіїв інформації до «цифрових», з'явився широкий доступ до персональних комп'ютерів і глобальної мережі.

1992 р. у ряді статей The New York Times «Вири пам'яті, хвилі суперечок» Дж. Маркоф, Дж. Брокман [182] та «Про мову» В. Сефір уперше офіційно вжито неологізми digital (дослівно означає «цифрове середовище») і digerati (дослівно означає «...людина, здатна до маніпуляції та обробки цифрової інформації») [205].

Аналіз цифрового середовища дозволяє виділити два основні теоретичні підходи до визначення цього поняття.

Перший підхід – технологічний, що розглядає цифрове середовище як відокремлену технологію і простір об'єктів. Найбільш типовими визначеннями, характерними для цього підходу, є:

цифрове середовище – середовище логічних об'єктів, яке використовується для опису (моделювання) інших середовищ (зокрема економічного, електронного та соціального) через математичні закони [209];

цифрове середовище – електронна технологія, яка використовує дискретні значення, зазвичай один і нуль, для створення, зберігання і обробки даних. У цифровому середовищі дані передаються і зберігаються у вигляді рядків з нулів і одиниць, кожен із яких згадується як біт. Ці біти групуються в байти для представлення даних, наприклад, цифр, літер, зображень або звуків [216];

цифрове середовище включає весь континуум комп'ютерних і мережних технологій. Базовими компонентами макроструктури глобального цифрового середовища в такому разі є:

системи та мережі телекомунікацій, перш за все Інтернет – web 1;
сегмент соціальних мереж і платформ – web 2;
найбільш розповсюджений останніми роками сегмент мобільних додатків (смартфони, планшети тощо) – web 3;
платіжно-розрахункові мережі на кшталт PayPal, SWIFT, Bitcoin;
сегмент вбудованих спеціалізованих процесорів різних об'єктів виробничої, соціальної, міської інфраструктури (інтернет речей), а також вбудованих чипів медичних імплантів, іграшок, одягу (бодінет), з'єднаних за допомогою Інтернету з керуючими центрами [145].

Другий підхід – медійний, що розглядає цифрове середовище як цифрове відображення медійної платформи і технологій спілкування, до того ж медіа розглядаються досить широко. Так до сучасних медіа належать не тільки засоби масової інформації, а й основні аспекти соціального та культурного життя, міжособистісні відносини, перекладені в цифрову технологію. Цей підхід передбачає, що цифрові технології відкривають кордони між творцем і споживачем контенту, призводять до злиття процесів виробництва та управління [185].

У рамках цього підходу сформувалися два теоретичні напрями дослідження цифрового середовища – техноцентризм і антропоцентризм. Представники обох напрямів поділяють думку про злиття просторових процесів з цифровими технологіями [76; 186; 194; 195; 196; 204].

Так один із представників «техноцентристів» Л. Манович визначає цифрове середовище як нове середовище, де всі політичні, соціальні, культурні процеси слід розглядати крізь призму логіки комп'ютерних програм: «Програми (software) – це інтерфейс між нашою уявою і світом: універсальна мова, на якій говорить весь світ, і універсальний двигун, що приводить світ в рух» [76; 194; 195; 196]. Цю ідею Манович розвиває за допомогою поняття cultural transcoding в книзі «Мова нових медіа» [194] і в роботі «Програмне забезпечення бере керування на себе» [195; 196].

Представники «антропоцентристів», канадські соціологи Б. Веллман і Л. Рейні [204] та американські дослідники технологій А. де Соуза-і-Сільва і Е. Гордон [186], також розглядають цифрове середовище як середовище комунікативних процесів, але вважають, що сценарії використання цифрових технологій не закладені в цифровому середовищі з самого початку, а формуються за допомогою здатності людини адаптувати технології під власні потреби, а також завдяки впливу культурних і соціальних аспектів.

На думку В. Александрової [13], підходи до «цифровізації» менеджменту підприємства можна умовно поділити на 4 типи:

цифровізація менеджменту як специфічний напрям цифрової

трансформації підприємства предметно не розглядається, але розглядається як необхідна умова ефективного цифрового перетворення бізнес-процесів [16; 96; 132];

окремі аспекти цифровізації менеджменту підприємства розглядаються без їх взаємозв'язку з іншими, не менш важливими аспектами (створення цифрових проектних офісів, застосування цифрових технологій у процесі управління підприємством) цифровізації окремих функцій менеджменту [87; 104; 143];

розглядається досвід цифровізації діяльності конкретного підприємства з визначенням проблем, в тому числі й управлінських, які були повністю або частково розв'язані в процесі цифрової трансформації бізнес-процесів [38; 50; 103]. У цих працях не ставиться мета, пов'язана з розвитком наукової теорії цифрового менеджменту;

наукові праці переважно зарубіжних авторів, у яких вивчаються цифрові технології менеджменту в процесі функціонування кіберфізичних систем [180; 186; 191; 196].

Проведений аналіз підходів до сутності цифрового менеджменту підприємства дозволив визначити трансформацію основних функцій менеджменту, які в умовах цифровізації управління та переходу до Індустрії 4.0 набувають іншого змісту (табл. 1.1).

Таблиця 1.1

Вплив цифровізації на трансформацію основних функцій менеджменту в умовах переходу до Індустрії 4.0 [узагальнено на основі 13; 126; 128; 156; 163; 164; 223]

Функція менеджменту	Класичне трактування функції менеджменту	Цифровий формат функції менеджменту в умовах переходу до Індустрії 4.0	Пріоритет у пошуку резервів підвищення ефективності	Вплив на показники діяльності підприємства
1	2	3	4	5
Планування	Визначення системи цілей функціонування і розвитку організації, а також способів і засобів їх досягнення; ключовий процес, який допомагає перетворити цілі на реальні результати	Моделювання сценаріїв розвитку підприємства; інтегроване планування показників діяльності	Пошук найбільш ефективного варіанта плану з урахуванням досягнення комплексу цілей	Збільшення обсягу випуску, рентабельності та якості продукції

1	2	3	4	5
Організація	Формування керуючої і керованої підсистем, встановлення конкретних параметрів, режимів роботи підрозділів підприємства, відносин між ними	Симуляція бізнес-процесів у режимі реального часу; обмін даними, знаннями та досвідом у реальному режимі часу між географічно розосередженими учасниками виробничого процесу	Запобігання непродуктивним витратам, конфлікту інтересів, виробничим інцидентам, наднормативним витратам, підвищенню ризиків	Зниження операційних витрат, обсягу наднормативних платежів, витрат на відшкодування збитків від ризику
Координація	Діяльність менеджера, спрямована на узгодження активності елементів системи управління; узгодженість дій органів управління і посадових осіб у часі та просторі, а також загалом між системою і зовнішнім середовищем	Платформні методи координації діяльності учасників усього ланцюжка створення цінності; методи координації роботизованої і живої праці	Встановлення єдиних вимог до учасників усього ланцюжка створення цінності; гармонізація всіх видів праці	Зростання якості продукції і праці, зменшення виробничого циклу, зниження витрат
Мотивація	Спонування себе та інших до діяльності для досягнення особистісних цілей і цілей організації	Стимулювання персоналу за результатами звітів KPI, в яких враховується виконання заходів із цифровізації діяльності підприємства	Орієнтація персоналу на прискорення процесу цифровізації діяльності підприємства	Зростання якості праці, скорочення термінів цифровізації виробництва
Аналіз і контроль	Спостереження за об'єктом із метою оцінки його відповідності реальному стану по відношенню до бажаного стану	Превентивна діагностика стану обладнання; моніторинг втрат продуктивності обладнання і персоналу; аналіз інформації про показники виробничої діяльності в режимі реального часу	Раннє виявлення і усунення відхилень від плану; розробка запобіжних заходів щодо їх запобігання в майбутніх періодах	Зменшення (виняток) випадків невиконання планових завдань, зниження витрат на розробку заходів із коригування планів

Практичне значення цифрового менеджменту в умовах цифрової

трансформації є важливим і актуальним, про що свідчать дослідження, проведені Gargemini Consulting and MIT Sloan School of Management (рис. 1.3).



Рис. 1.3. Цифрова зрілість за галузями [222; 223]

Лідерами цифрового виробництва є сфера цифрових і нанотехнологій, банківська сфера та сфера роздрібної торгівлі, саме вони зараз отримують найбільшу користь від цифрової трансформації. Для телекомунікацій і готельного бізнесу потрібно змінити бізнес-модель і залучити нові методів управління.

Консерваторами виявилися страхові компанії, які перш за все турбуються про скорочення ризиків, що перешкоджає впровадженню цифрових інновацій. У сферах енергетики та комунальних послуг заважає успадкована інфраструктура. Початківцями у рейтингу цифрової зрілості виявилися: фармацевтика, промислове виробництво та виробництво товарів народного споживання, а також агропродовольча сфера – їм ще належить

вибудувати модель цифрової трансформації.

Зазначене зумовлює необхідність цілеспрямованого та активного розвитку і впровадження в практику спеціальних управлінських рішень, основою яких є орієнтація на застосування архітектури цифрового середовища, головна мета якої полягає у формуванні цілісної й ефективної системи цифрового менеджменту. На основі узагальнення досліджуваних аспектів цифрового менеджменту [15; 26; 28; 86; 113; 126; 153; 180; 222; 223] запропоновано дев'ять основних напрямів, які визначають його архітектуру:

1. «Відцифровані» об'єкти й моделі.

По-перше, цифрові дані, особливо економічного й управлінського характеру, потрібно перекладати в семантично правильні та цілісні інформаційні структури задля здійснення ефективного процесу розробки управлінських рішень.

По-друге, відображення об'єктів реального світу у віртуальному просторі дозволяє широко застосовувати цифрові технології, тому відцифровані об'єкти управління розглядаються не тільки як структуровані дані, що підлягають автоматизованій обробці та аналітиці, але і як цілісні керовані об'єкти, які дозволяють значно розширити можливості щодо їх трансформації. Цифрові об'єкти «оживляють» дані предметної області через розширюваний функціонал та інтерфейси. Цільові моделі, які конструюються на основі пов'язаних і взаємодіючих цифрових об'єктів, надають економічним суб'єктам варіанти їх активного застосування для виконання безлічі практичних завдань.

У межах концепції розвитку цифрового менеджменту постає завдання глобального переходу до мережі взаємодіючих цифрових об'єктів у середовищі інтегруючих цифрових платформ. Подібне рішення здатне реорганізувати та підвищити якість використовуваних цифрових даних, підвищити рівень інформаційної взаємодії, мінімізувати технічні та семантичні помилки й поліпшити керованість, у тому числі інформаційної безпеки.

2. Мережа компетенцій.

Мережа компетенцій – це управлінське розв'язання проблеми взаємодії завдань, знань і досвіду, тобто своєрідний маркетплейс, де зустрічаються проекти, які визначають цілі та завдання замовника, й індивідуальні працівники або сформовані команди, які надають власні компетенції для реалізації проектів. Очевидно, що базисом цього елементу архітектури цифрового менеджменту є не організація «зустрічей», а формування високого рівня цифрової довіри, зокрема облік і контроль компетенцій фахівця або

команди, оцінка компетенцій і проектів, проведення сертифікації та рецензування, аналітика за компетенціями та проектами, професійне спілкування тощо.

3. Спільне споживання.

Цифровий менеджмент передбачає так зване спільне споживання – спільне використання ресурсів, сервісів, можливостей учасниками ринку, галузі, економіки тощо. Проте справедливе, якісне та конкурентне спільне споживання потребує відповідного правового й управлінського рішення, захисту постачальників і клієнтів, підтримки базових юридично значимих транзакцій, надання гарантій, зниження можливих ризиків, контролю безпеки споживання та забезпечення високого рівня цифрової довіри.

4. Цифрова довіра.

У глобальній інформаційній мережі, де сторони взаємодіють дистанційно, особливого значення набуває довіра. Тому необхідно шукати найбільш ефективний спосіб розв’язання проблеми формування довіри в цифровому середовищі, що наразі можливо завдяки забезпеченню базових функцій, таких як ідентифікація, надійна аутентифікація та коректна авторизація користувача. А для того, щоб цифрова довіра була дійсно ефективною і повноцінною, необхідно реалізувати спеціальні розширені функції, серед яких: накопичення, зберігання та подання інформації про репутацію економічного суб’єкта (цифрового об’єкта); створення, виконання і контроль алгоритмізованих контрактів; формування та актуалізація мотиваційних чинників впливу при прийнятті рішень. Крім того, розширюючи цифрову довіру, необхідно забезпечити правомірність і легітимність транзакцій. Без кардинального вирішення питань довіри подальший розвиток цифрової економіки пов’язаний із постійним зростанням кількості та різноманітності ризиків і ймовірності їх виникнення.

5. Цифровий ризик-менеджмент.

Цифровий менеджмент повинен кваліфіковано забезпечувати цифровий ризик-менеджмент, який створюватиме і застосовуватиме спеціальні знання (актуальну інформацію та професійний досвід), володітиме відповідними інструментами (методиками та технологіями запобігання, ліквідації, компенсації ризиків і відновлення після настання несприятливих подій), пропонуватиме програми навчання, розвиватиме та «захищатиме» інструменти управління та цифрові платформи менеджменту цифрових об’єктів.

6. Програмоване право і алгоритмічне регулювання.

Цифровий менеджмент передбачає нову якість регулювання відносин між традиційними економічними суб’єктами – споживачами, бізнес-

структурами, державними та соціальними організаціями тощо. Проте у зв'язку з появою нових цифрових об'єктів регулювання, таких як «розумні» речі, «Інтернет речей», спеціальні алгоритми, хмарні технології, віртуальні платформи, а також у зв'язку з появою нової категорії цифрових активів, потрібен додатковий розділ права. Ефективним було б введення цифрового кодексу, який був би реалізований як юридична модель цифрових об'єктів, що дозволяє в автоматичному режимі реалізовувати право суб'єктами або видавати суб'єктам вказівки на виконання зобов'язань.

7. Розподілені проекти.

З розвитком цифрової економіки моделі споживання стають настільки складними і комплексними, а бізнес-проекти інтегрують таку кількість учасників, що власне управління окремим цільовим проектом перетворюється на трудомістке і складне завдання. Необхідно пов'язати та поєднати інвестиційну стратегію, дефіцитні матеріальні та розподілені інформаційні ресурси, підібрати компетентну команду, скоординувати і структурувати паралельні та пересічні потоки робіт, забезпечити стійкий темп виконання з урахуванням високих швидкостей, які формує цифровізація. Розподілені проекти як новий рівень менеджменту інформації припускають віртуалізацію та цифровізацію операцій розробки і реалізації проекту з відповідним набором даних, з цифровими моделями та з повноцінною автоматизацією на основі цифрових технологій.

8. Персоналізовані ринки.

Кількість споживчих характеристик збільшується, і все частіше їх можна коригувати відповідно до потреби конкретного клієнта. Одночасно постачальники персоналізованих продуктів і сервісів намагаються володіти цінною інформацією про своїх фактичних і потенційних споживачів, щоб найбільш точно ідентифікувати й управляти цільовими сегментами ринку.

9. Трансфер публічних даних.

В умовах цифрової економіки бізнес і держава мають проблему зі збором і накопиченням зайвих даних. Особливого значення набуває політика відкритих цифрових даних з боку державних структур і механізм спільного використання даних різними організаціями та приватними особами.

Трансфер публічних даних – це системне та платформне рішення, яке повинно забезпечити взаємний обмін відкритими державними, розподіленими комерційними й делегованими особистими даними. Взаємний обмін слід розуміти як не тільки статичне завантаження наборів даних, але і як динамічний доступ до сховищ за уніфікованими запитами на основі API, а також як надання доступу до попередньо оброблених масивів даних [153].

Результати аналізу свідчать про те, що перехід від традиційної концепції

управління до концепції цифрового менеджменту як сучасного наукового напрямку сфери управління потребує значних зусиль теоретиків менеджменту для формування новітньої – цифрової парадигми управління, яка інтегруватиме інформаційну, віртуальну, цифрову сфери, штучний інтелект та людські знання. Концептуалізація цифрового менеджменту має відповідати цифровому способу виробництва та системі цифрового управління, що потребує видозміни основних традиційних інструментів менеджменту з урахуванням основних положень середовища функціонування – цифрової економіки (табл. 1.2).

Таблиця 1.2

Порівняльна характеристика традиційного і цифрового менеджменту підприємства [узагальнено на основі 13; 24; 113]

Ознака порівняння	Традиційний менеджмент	Цифровий менеджмент
Використання технологій Індустрії 4.0	Не використовується	Є основою прийняття управлінських рішень
Основна роль менеджера	Організатор, координатор	Комунікатор, координатор
Тип комунікацій	Переважає особисте спілкування	Переважають онлайн-комунікації, дистанційне спілкування
Формування управлінських команд	Обмежене територіально	Обмеження відсутні
Етика спілкування з персоналом	Етика особистого спілкування	Етика віртуального спілкування
Критерії відбору на посаду менеджера	Професійні компетенції	Професійні та цифрові компетенції
Глобальні цілі менеджменту	Цілі розвитку тисячоліття	Цілі сталого розвитку
Інфраструктура менеджменту	Відділи та служби апарату управління підприємством	Цифрові офіси, цифрові та віртуальні платформи
Оперативні рішення	Приймаються протягом декількох годин, днів	Приймаються в режимі реального часу
Стратегічні рішення	Рішення, орієнтовані на досягнення ключових цілей розвитку підприємства	Інтегровані рішення з урахуванням досягнення ключових цілей розвитку підприємства і цілей його структурних одиниць
Тип автоматизації праці менеджерів	Автоматизація окремих робіт	Автоматизація функцій менеджменту
Об'єкт менеджменту	Жива праця	Комбінації роботизованої і живої праці
Особа, яка приймає рішення	Людина, яка самостійно генерує рішення	Людина, що генерує рішення за допомогою штучного інтелекту
Стандарти	Стандартизація менеджменту за окремими функціональними сферами менеджменту	Цифрові стандарти

Отже, необхідно і доцільно використовувати новий засіб сучасної парадигми управління – цифровий менеджмент, який у межах цього дослідження пропонується розглядати як сукупність функцій, методів, інструментів управління цифровими технологіями на засадах інтеграції бізнес-процесів, архітектури цифрового управління, людського фактора, комунікативних медіа та цифрових технологій із метою формування цифрової або віртуальної моделі управління соціально-економічним об'єктом.

На зміну індустріальному етапу суспільного розвитку приходить еволюційна фаза – інформаційна, за якої всі соціально-економічні структури суспільства перетворюються таким чином, щоб забезпечити найбільш ефективний і динамічний розвиток на основі максимально повного використання наявних інформаційних ресурсів. Традиційні матеріальні ресурси поступово втрачають своє первісне значення, а на зміну приходять інформаційні ресурси. Для їх ефективної участі в інформаційних процесах створюється потужна інфраструктура засобів комп'ютерної та телекомунікаційної техніки, цифрових технологій, що змінюють не тільки процес і характер трудової діяльності, а й сам спосіб життя, систему цінностей людини. Інформаційні технології набувають глобального характеру, охоплюючи всі сфери життєдіяльності, формуючи інформаційну єдність всієї людської цивілізації. Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, являє собою сукупність інформації, інформаційної інфраструктури суб'єктів, які здійснюють збір, формування, поширення та використання інформації. Будучи системоутворюючим фактором життя суспільства, інформаційна сфера активно впливає на стан політичної, економічної, оборонної та інших складових безпеки країни. Національна безпека є залежною від забезпечення інформаційної безпеки, а в процесі цифровізації економіки та інформатизації суспільних відносин ця залежність набуває особливого значення.

Поняття інформаційної безпеки в повному обсязі включає забезпечення захисту та безпеки інформації, інформаційного ресурсу. В прямому розумінні захист інформації – це недопущення будь-якого впливу на інформацію, яку необхідно зберегти в певному стані. Захист інформаційного ресурсу – тільки частина проблем інформаційної безпеки. Забезпечення інформаційної безпеки – це комплексне завдання, метою якого є створення балансу між потребою в інформації у великій кількості різноманітних суб'єктів і необхідністю ефективно використовувати наявний інформаційний ресурс.

Тому наступним етапом дослідження буде визначення концептуальної сутності інформаційної безпеки підприємства.

1.2. Сутність інформаційної безпеки підприємства

У сучасних умовах до побудови глобального та європейського інформаційного суспільства залучено значну частину інтелектуальної політичної й економічної еліти провідних світових держав. Інформаційні технології та інформаційно-комунікативні системи за нинішніх умов глобального цивілізаційного розвитку є ключовими ресурсами суспільства та держави й необхідною передумовою їх конкурентоспроможності на глобальних ринках. Саме інформаційна сфера здатна виступати провідним фактором реалізації найважливіших суспільних проєктів динамічного розвитку, становлення громадянського суспільства, а також входження до світової спільноти.

Через посилення ролі інформації сформувався інформаційний простір, який необхідно захищати від несанкціонованого або ненавмисного впливу на рівні держави, регіону і навіть на рівні окремих підприємств. Політика у сфері інформаційної безпеки здійснюється з метою недопущення перешкоджання реалізації життєво важливих інтересів і потреб громадянина, суспільства і держави зовнішніми і внутрішніми загрозами національній безпеці в інформаційній сфері, що є запорукою сталого розвитку національного інформаційного простору. В економічній діяльності захист інформації дає можливість отримувати високі доходи, укласти вигідні контракти з контрагентами, істотно підвищує рівень конкурентоспроможності підприємства, а також дозволяє значно підвищити ефективність діяльності організації загалом. У зв'язку з цим інформаційна безпека є невід'ємним елементом системи безпеки на різних рівнях управління.

Наукові основи інформаційної безпеки, її стану і перспектив розвитку, методологічне та теоретичне підґрунтя досліджуваної проблеми висвітлювалися в наукових працях вітчизняних і зарубіжних учених, а саме: М. Алієвої [14], О. Горбатюк [43], О. Данільяна [46], Я. Жаркова [75], Р. Калюжного [81], С. Ковтуна [88], Б. Кормича [92], О. Литвиненко [101], В. Ліпкана [102], Н. Мороза [115], С. Мочерного [117], І. Панаріна [121], О. Сороківської [142], А. Тер-Акопова [149], В. Ярочкіна [178] та інших.

У працях, присвячених захисту інформації вищезазначених та інших фахівців, найчастіше виявляється, що погляди і термінологія в цій сфері суттєво різняться, іноді вони майже протилежні. Перш ніж перейти до розгляду сутності поняття «інформаційна безпека», пропонується розглянути основні терміни, які характеризують це поняття і можуть бути об'єднані в чотири групи: ті, що визначають наукову основу інформаційної безпеки; ті,

що визначають предметну область інформаційної безпеки; ті, що визначають основи діяльності щодо забезпечення інформаційної безпеки; ті, що визначають основу ризику інформаційної безпеки [23] (рис. 1.4).

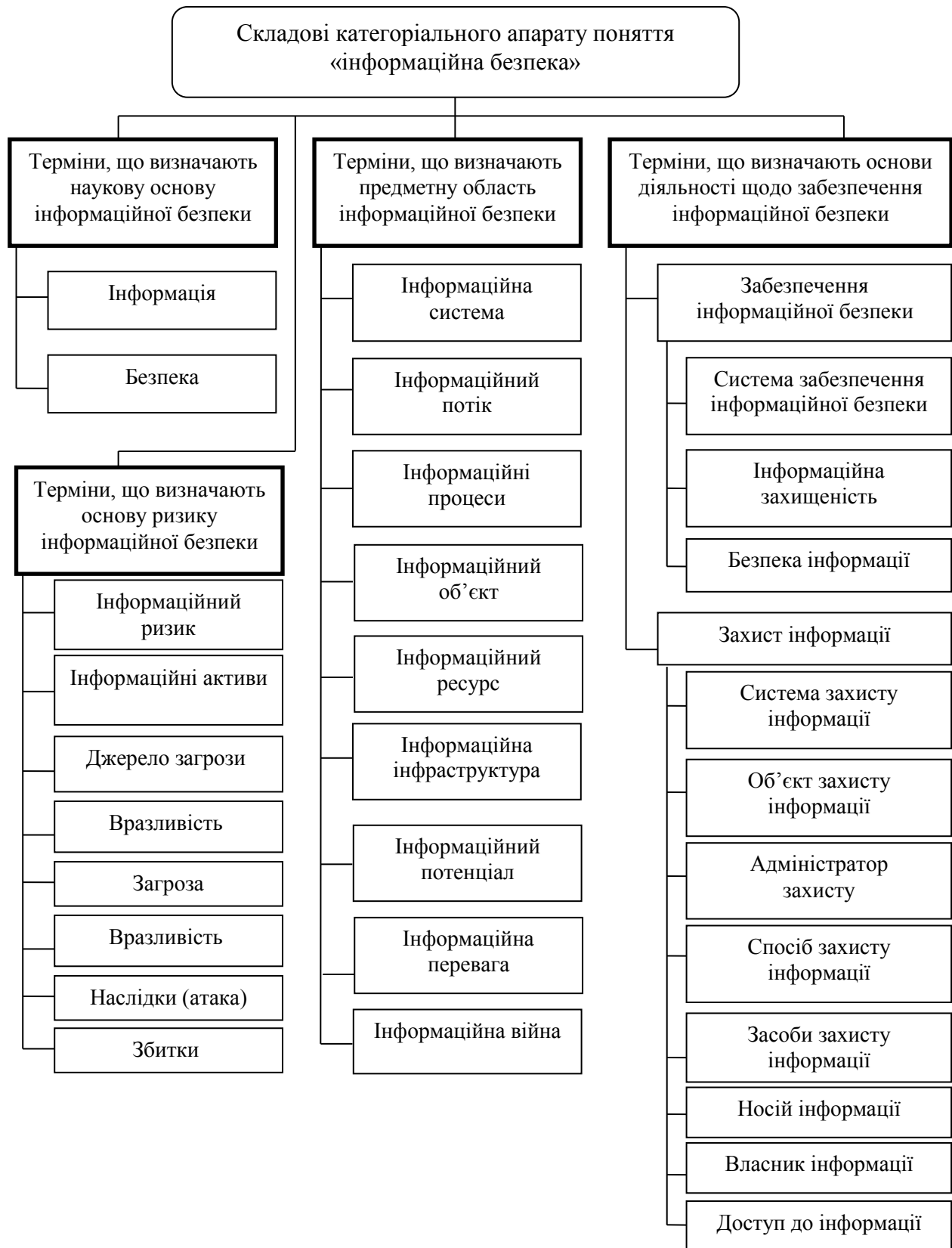


Рис. 1.4. Логіко-понятійна структура категоріального апарату поняття інформаційної безпеки [доопрацьовано на основі 23]

До першої групи зараховані терміни, які використовуються в декількох галузях знань, є однозначними, семантично уніфікованими та стилістично нейтральними. Терміни цієї групи відповідають вимогам однозначності та стійкості, тобто вони однозначно вживаються в одній галузі знань і зберігають свій основний зміст в інших галузях знань, а також є загальновизнаними. До цієї групи належать терміни «інформація» та «безпека».

Інформація (від латинського «information» – роз’яснення, виклад) – в найзагальнішому розумінні визначає міру розподілу матерії та енергії в просторі й часі та міру змін, якими супроводжуються всі процеси. Враховуючи визначення й тлумачення терміна «інформація» та узагальнюючи погляд різних авторів [3; 14; 23; 27; 30; 122; 125; 172; 176], пропонується визначати інформацію як результат взаємодії об’єктів (предметів, засобів) і процесів матеріального світу, які сприймаються соціальним об’єктом (людиною) або технічним пристроєм у вигляді відомостей (повідомлень, даних) у різній формі їх подання з метою прийняття рішень та адаптації до змін навколишнього середовища.

Поняття «безпека» – багатоаспектне, його слід трактувати, по-перше, як наявність і взаємодію зовнішніх факторів, умов, мінімально необхідних для благополучного існування та прогресивного розвитку об’єкта безпеки, збереження його цілісності, відновлення життєдіяльності й працездатності у разі виникнення небезпек і загроз; по-друге, як сукупність окремих властивостей самого об’єкта, що відображають його здатність активно функціонувати в зазначених вище умовах, а також зберігати власну цілісність і відновлювати працездатність при реалізації небезпек і загроз [17; 23; 42; 74; 95; 155; 173].

Другу групу становлять терміни, які утворюють предметне поле, в якому формується поняття «інформаційна безпека»:

- інформаційна система – це природна (біологічна) або цільова (організаційно-технічна) сукупність взаємопов’язаних закономірно розташованих об’єктів, сукупність відомостей про об’єкт (предмет, засіб, явище, процес) і його діяльність, а також використовувані інформаційні технології [12; 23; 31; 123; 130; 138];

- інформаційний потік – це сукупність відомостей (повідомлень, даних) незалежно від форми їх подання, що циркулюють у системі, а також між системою і зовнішнім середовищем, призначених для реалізації сигнальних і керуючих функцій [23; 40; 80; 162]. Інформаційні процеси – це процеси створення, збору, обробки, накопичення, зберігання, пошуку, розповсюдження та споживання інформації, діяльність суб’єкта і

функціонування природних і технічних засобів в інформаційній сфері. Діяльність при цьому слід розуміти як генерування, добування, зберігання, переробку, передачу, використання і захист інформації. До інформаційних об'єктів належать об'єкти матеріального світу, які реалізують функції генерації (виробництва, відтворення), збору та накопичення, зберігання, переробки і передачі інформації [12; 23; 74; 80; 162];

- інформаційні ресурси – це інформаційна інфраструктура та її потоки. Поняття «інформаційний ресурс» включає в себе як власне відомості, так і відомості в базах даних інформаційних систем. База даних – об'єктивна форма представлення та організації сукупності даних, систематизованих таким чином, щоб ці дані могли бути знайдені й оброблені за допомогою ЕОМ [23; 112; 127; 175; 203]. Складна організація взаємодії інформаційної інфраструктури та користувачів (споживачів: людини, окремих груп людей і суспільства загалом) може бути умовно представлена у вигляді ієрархії окремих рівнів:

рівень користувача – рівень генераторів і споживачів інформаційного ресурсу відповідно до правил їх взаємодії з інформаційною структурою;

функціональний рівень із сукупністю послуг, що надаються користувачам (споживачам) різними постачальниками інформації;

інформаційний рівень, у якому безпосередньо міститься інформаційний ресурс;

комунікаційний рівень, що розглядається як єдина інформаційна магістраль – інформаційна мережа [23; 36; 52];

- інформаційний потенціал: в процесі боротьби в інформаційній сфері будь-які інформаційні впливи як наступального, так і оборонного характеру в кінцевому підсумку впливають (позитивно чи негативно) на інформаційні потенціали. При цьому інформаційним потенціалом вважалася сукупність технічної, технологічної та економічної інформації, інформаційних ресурсів, інформаційних систем і технологій, засобів комунікацій і здатність кваліфікованого персоналу їх використовувати, спрямованих на результативне управління підприємством і подальший його розвиток [146];

- інформаційна перевага – це здатність ефективніше отримувати, переробляти та розподіляти безперервний потік інформації про обставини, які складаються в реальному часі, перешкоджаючи протиборчій силі здійснювати аналогічні дії [23];

- інформаційна війна – це дії, вжиті для досягнення інформаційної переваги шляхом заподіяння збитку через процеси, засновані на інформації, інформаційних системах і діях працівників організації при одночасному захисті власної інформації. Складовими частинами інформаційної війни є

психологічні операції, електронна війна, дезінформація, фізичне руйнування, заходи безпеки, прямі інформаційні атаки [198].

До третьої групи термінів належать терміни, характерні для діяльності у сфері забезпечення інформаційної безпеки. Така діяльність є багатоплановою. Терміни цієї групи окреслюють широке коло понять різного рівня – від сигнального до системного.

Перший термін – забезпечення інформаційної безпеки – розглядається на макрорівні і розуміється як проведення єдиної державної політики у сфері безпеки у вигляді системи заходів організаційно-технічного, правового, соціального та іншого характеру, відповідних загрозам життєво важливим інтересам людини, суспільства та держави в інформаційній сфері [23; 120; 183].

Зазначений термін має три складові:

- система забезпечення інформаційної безпеки – здебільшого визначається як цілеспрямована сукупність взаємопов'язаних організаційно-технічних, правових і соціальних норм, механізмів, спрямованих на протидію загрозам інформаційній безпеці з метою зведення до мінімуму можливих збитків в інформаційній сфері [23; 92, 115, 117, 150];

- інформаційна захищеність – являє собою сукупність засобів, що забезпечують протидію зовнішньому інформаційному впливу, а також інформаційні засоби, призначені для протидії психологічним впливам, реалізованим по каналах поширення інформації [22; 23; 129];

- безпека інформації – стан захищеності інформації, в тому числі тієї, що обробляється засобами обчислювальної техніки, від загроз деструктивного впливу. Це стан, при якому забезпечується необхідний ступінь захищеності інформації від витоку, розкрадання, втрати, несанкціонованого знищення, руйнування, спотворення, модифікації, копіювання та блокування [20; 23; 37; 161].

Другий термін – захист інформації – передбачає здійснення процесу забезпечення цілісності, надійності, конфіденційності інформації завдяки використанню комплексу організаційно-технічних, правових і соціальних заходів, спрямованих на забезпечення захисту інформації від незаконного втручання, знищення, модифікування, блокування, копіювання, надання, поширення, а також від інших неправомірних дій стосовно інформації; на дотримання конфіденційності інформації обмеженого доступу; на реалізацію права на доступ до інформації.

Зазначений термін має вісім складових:

- система захисту інформації – являє собою цілеспрямовану сукупність об'єктів захисту, органів управління інформаційною системою та виконавців,

а також систему технічних і програмних засобів захисту інформації та механізмів захисту. Система захисту інформації є організованою і функціонує за правилами, встановленими правовими, розпорядчими та нормативними документами в галузі захисту інформації [23; 97; 174];

- об'єкт захисту інформації – власне інформація, носій інформації, інформаційний ресурс, інформаційний процес або інформаційний актив, для яких необхідно забезпечити захист відповідно до поставленої мети захисту [1; 23; 148; 151];

- адміністратор захисту – суб'єкт доступу, відповідальний за захист автоматизованої системи від несанкціонованого доступу до інформації [23; 157];

- спосіб захисту інформації – обрана дія або система дій (комплекс певних заходів, прийомів), які застосовуються під час виконання будь-якої роботи або здійснення чого-небудь, а також закономірний порядок і послідовність (впорядкована послідовність) їх застосування, кінцевою метою яких є захист інформації [23; 121; 179];

- засоби захисту інформації – технічні, криптографічні, програмні, організаційні та інші засоби, а також системи управління комплексами засобів, призначені для захисту і контролю ефективності захисту інформації [23; 179];

- носій інформації – будь-який матеріальний об'єкт, у тому числі фізичне поле, в якому інформація відображається у вигляді символів, образів, явищ або, наприклад, технічних рішень і процесів. З появою ЕОМ виник такий вид інформації, як комп'ютерна інформація. Наразі широко використовуються електронні носії інформації [23; 214];

- власник інформації – фізична або юридична особа, громадська організація або держава, які самостійно створили інформацію або отримали на підставі закону чи договору право дозволяти чи обмежувати доступ до інформації [23; 26; 214];

- доступ до інформації – можливість отримання інформації, в тому числі і з метою її подальшого використання. Доступ передбачає спеціальний тип взаємодії між суб'єктом і об'єктом інформаційного обміну, внаслідок якого створюється потік інформації від одного до іншого. Доступ до інформації передбачає отримання суб'єктом можливості ознайомитись із інформацією, включаючи можливості її обробки, зокрема копіювання, модифікації або знищення, в тому числі за допомогою технічних засобів. Надання суб'єкту деяких прав доступу до інформаційного обміну називається авторизацією [2; 3; 23; 29; 110]. У сфері захисту державних

секретів поняття «доступ до секретної інформації» трактується як санкціонований процес ознайомлення із секретною інформацією фізичної особи, що має допуск до такої секретної інформації [2].

Вищезазначене поняття має декілька складових:

об'єкт доступу – одиниця інформаційного ресурсу, доступ до якого регламентується правилами розмежування доступу;

несанкціонований доступ до інформації – процес, що порушує прийняті або встановлені власником інформації правила розмежування доступу до неї, наслідком якого можуть бути витік, спотворення, руйнування, знищення, блокування інформації, а також втрата, знищення або збій функціонування носія інформації;

вплив на інформацію – система заходів, що впливають на кількісне або якісне (сміслові) утримання інформації, яка циркулює в інформаційних системах, і проводяться з метою навмисного спотворення, затримки поширення, руйнування або знищення в процесі створення інформації, її переробки або передачі [23].

Терміни четвертої групи є загальними. Застосування їх до предметної області дослідження дозволяє визначити основні етапи настання інформаційного ризику: від виникнення джерела загрози до наслідків від її настання. Ця група містить такі терміни:

інформаційний ризик – події, які безпосередньо впливають на інформацію – її видалення, спотворення, порушення її конфіденційності, доступності або цілісності [85; 118]; небезпека виникнення збитків або шкоди внаслідок застосування інформаційних технологій [85; 114];

інформаційні активи – ключові компоненти інфраструктури і важлива для власника інформація, що обробляється в інформаційній системі та має певну цінність [39; 118; 131];

джерело загрози інформаційній безпеці – суб'єкт доступу, матеріальний об'єкт або фізичне явище, що є причиною виникнення загрози безпеці інформації [39];

вразливість – будь-яка характеристика або властивість інформаційної системи, використання якої зловмисником може призвести до реалізації загрози [32]; властивості об'єкта, які потенційно можуть призвести до порушення безпеки інформації на цьому об'єкті, зумовлені особливостями його функціонування, властивостями архітектури інформаційної системи, протоколами обміну, програмним забезпеченням, апаратною платформою та умовами їх експлуатації суб'єктами [118];

загроза – ймовірна подія або процес, який завдяки впливу на компоненти інформаційної системи може призвести до заподіяння шкоди інформаційним

активам підприємства, зокрема до порушення конфіденційності інформації обмеженого доступу [32]; загроза (дія) – реально існуюча або потенційна небезпека вчинення будь-якого діяння (дії або бездіяльності), спрямованого проти об'єкта інформаційного захисту, що завдає шкоди власнику або користувачеві інформації та виявляється в небезпеці спотворення, втрати та витоку інформації [23; 29; 39];

наслідки (атака) – можливі наслідки реалізації загрози (можливі дії) при взаємодії з джерелом загрози через наявну уразливість [39; 85; 118; 131];

збитки – витрати для відновлення системи до робочого стану після можливого інциденту інформаційної безпеки, а також на відновлення спотвореної, втраченої інформації або ж нейтралізацію наслідків витоку конфіденційної інформації [39].

Важливо підкреслити, що розташування термінів у кожній групі визначається не алфавітним порядком, а таким принципом: визначення попереднього терміна має сприяти розумінню кожного наступного. Такий підхід повинен дозволити в подальшому розширювати і доповнювати категоріальний апарат термінів предметної області «інформаційна безпека».

Найбільш узагальненим і широкоживаним трактуванням поняття «інформаційна безпека» вважається її визначення як стану захищеності інформаційного середовища суспільства, яке забезпечує формування, використання і розвиток останнього для задоволення потреб і дотримання гармонії інтересів громадян, організацій і держави. Інформаційне середовище, в свою чергу, включає сферу діяльності суб'єктів щодо створення, перетворення і споживання інформації та розподіляється на три основні предметні та дві забезпечувальні предметні частини [92] (рис. 1.5).

На макрорівні інформація, інформаційна система та новітні інформаційні технології є одним із основних факторів забезпечення національної безпеки та умовою її соціально-економічного розвитку. Відповідно, макрорівень передбачає ефективність дій управлінського персоналу суб'єкта господарювання щодо виконання процесів роботи з інформаційними ресурсами, інформаційними системами та інформаційними технологіями підприємства, які не тільки дозволяють автоматизувати та інформаційно забезпечити основні види діяльності, а й створити інформаційні продукти та надати інформаційні послуги.

Інформаційна безпека залежно від контексту її представлення відображає різноманітну етимологію цього поняття. Наприклад, у Доктрині інформаційної безпеки України інформаційна безпека трактується у широкому значенні цієї дефініції та розглядається як стан захищеності національних інтересів в інформаційній сфері, що визначаються сукупністю

збалансованих інтересів у системі «особистість – суспільство – держава» [8].

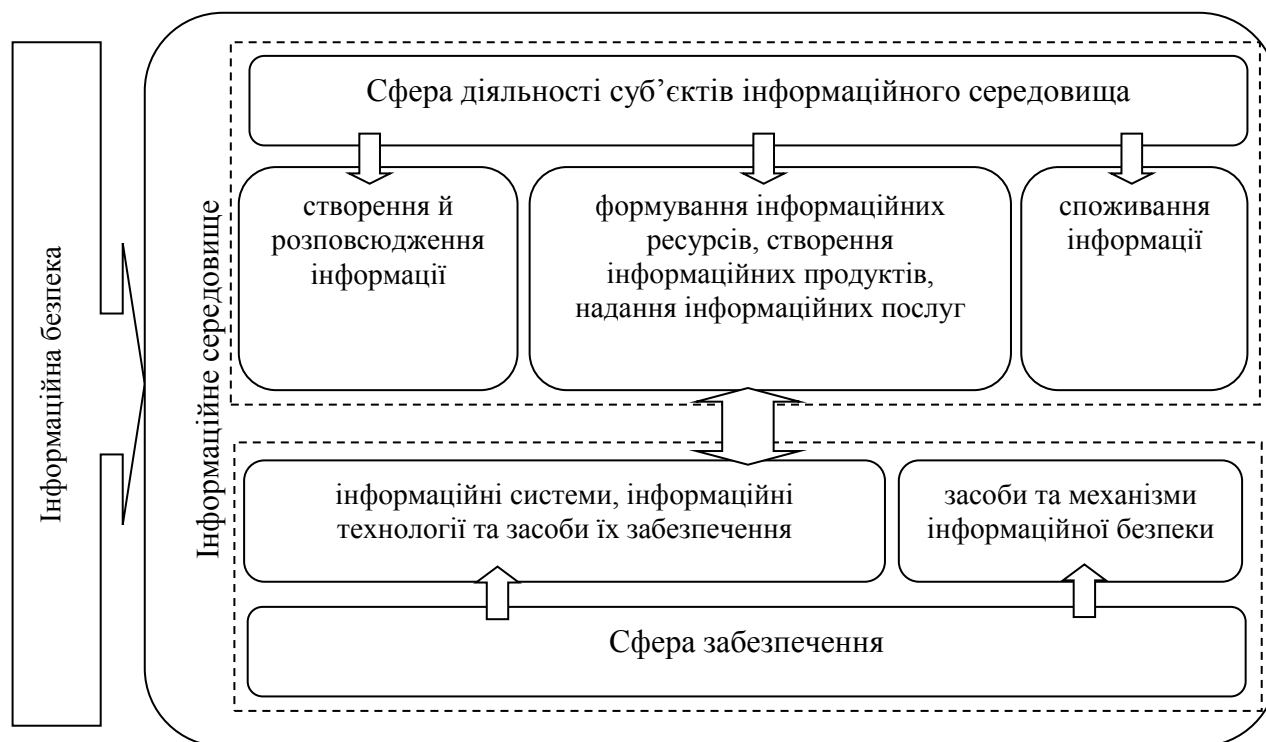


Рис. 1.5. Формалізація поняття «інформаційна безпека» [розроблено на основі 92; 115; 117, 150]

Натомість поняття «комп'ютерна безпека», яке інколи є аналогом поняття «інформаційна безпека» і використовується переважно в технічній сфері, є вузьким, оскільки апаратна частина є лише однією зі складових інформаційної системи. Хоча при визначенні поняття «інформаційна безпека» увага зосереджується на інформації як основному об'єкті захисту, яка підлягає процесам обробки, передачі та зберігання за допомогою використання комп'ютерної техніки, її безпека визначається всіма елементами інформаційної системи, а також людиною, яка здійснює процеси обробки інформації [224]. Зазначений підхід підтримують І. Панарін [121], Ю. Шемшученко [171], фахівці Лабораторії сітьової безпеки [224], які стверджують, що інформаційна безпека формується не за допомогою апаратної частини, зокрема комп'ютерної техніки, а переважно завдяки підтримуючій інфраструктурі, яка включає, окрім вищезазначеного інформаційні системи, засоби комунікацій і, звичайно, обслуговуючий персонал.

Одна зі світових енциклопедій визначає термін «інформаційна безпека» як захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення доступності, модифікації або знищення з метою забезпечення:

цілісності, що означає захист інформації від модифікації несанкціонованого доступу або знищення і включає гарантування справжності;

конфіденційності – запобігання розкриттю і обмеженню доступності, передбачаючи засоби захисту приватної та конфіденційної інформації;

доступності – своєчасний і надійний доступ до використання інформації [202].

Відповідно до тлумачень, поданих у словниках, інформаційна безпека є системою захисту в інформаційній сфері від навмисних і ненавмисних загроз і впливів [211].

Правові аспекти визначення сутності інформаційної безпеки на макрота і мікрорівні відображають Закони України «Про основи національної безпеки України» [4], «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [6], проект Закону України «Про засади інформаційної безпеки України» [7] та інші нормативно-правові акти [2; 5; 8; 9; 10; 217]. Наприклад, у Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» цей термін трактується так: «Стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [6].

Попри низку законодавчих актів і концепцій в Україні не існує окремого правового документа з регулювання питань інформаційної безпеки. Відповідно, досі не розроблено єдиного плану стратегічних дій, політики інформаційної безпеки, інших стратегічних регуляторів питань правової безпеки інформаційної та суміжних сфер. Доцільно відмітити, що було чотири спроби ухвалити концепцію державної інформаційної політики – 2002, 2009, 2010 і 2018 рр. Деякі автори інформаційну безпеку визначають як стан захищеності національних інтересів країни, суспільства, підприємства, особистості в інформаційній сфері, який передбачає інтеграцію збалансованих інтересів у системі «особистість – підприємство – суспільство – держава» [7; 8; 9; 92].

У цій системі інтереси особистості в інформаційній безпеці перш за все передбачають реалізацію конституційних прав людини і громадянина, права доступу до інформації, права використання інформації в інтересах фізичного духовного та інтелектуального розвитку з метою здійснення не забороненої

законом діяльності, а також для захисту інформації, що забезпечує особисту безпеку.

Інтереси суспільства в забезпеченні інформаційної сфери в системі «особистість – підприємство – суспільство – держава» полягають у зміцненні демократії, створенні правової соціальної держави, досягненні та підтримці суспільної злагоди.

Інтереси держави у сфері інформаційної безпеки включають: конституційні права та свободи людини і громадянина; отримання людиною інформації для дотримання непорушності конституційного ладу, суверенітету і територіальної цілісності країни, політичної, економічної та соціальної стабільності для гармонійного розвитку інформаційної інфраструктури через забезпечення законності та правопорядку, для розвитку міжнародної співпраці.

Загалом доцільно вказати на три основні аспекти поняття «інформаційна безпека»: нормативно-правовий – ґрунтується на аналізі нормативно-правових актів; доктринальний – базується на аналізі трактувань праць теоретиків-дослідників, фахівців у галузі захисту та безпеки; енциклопедичний – передбачає аналіз визначень, наведених у енциклопедіях і словниках.

Недостатній ступінь обґрунтованості підходів до визначення сутності інформаційної безпеки, в яких науковці намагаються інтегрувати існуючі положення, найбільш повно відобразити сутність досліджуваної дефініції, зосереджуючи увагу на окремих властивостях, призводить до необґрунтованого розширення меж предметної області дослідження.

Узагальнення трактувань і етимологія сутності поняття «інформаційна безпека» відповідно до поглядів різних авторів наведено в табл. 1.3.

Таблиця 1.3

Сутність поняття «інформаційна безпека» [узагальнено на основі 6; 8; 11; 14; 25; 43; 46; 48; 53; 75; 81; 88; 92; 94; 98; 101; 102; 111; 117; 121; 135; 142; 144; 147; 149; 154; 158; 159; 166; 167; 168; 171; 177; 178; 187; 210; 212; 219; 224]

Зміст поняття	Автор
1	2
Інформаційна безпека – це захищеність життєво важливих інтересів суспільства, держави та особи, за якої виключається заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення інформації, забороненої чи обмеженої для поширення законами України.	ЗУ «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [6]

1	2
Інформаційна безпека – це невід’ємна складова кожної зі сфер національної безпеки. Інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.	Указ президента «Про Доктрину інформаційної безпеки України» [8]
Інформаційна безпека – стан захищеності інформаційних відносин і пов’язаних із ними інформаційних процесів, за якого досягається стабільний інформаційний розвиток, унеможливується негативний інформаційний вплив і негативні наслідки незаконного застосування інформаційних технологій в усіх сферах суспільного життя, унаслідок чого можна досягти створення та ефективного функціонування інформаційного суспільства.	В. Абакумов [11]
Інформаційна безпека – це захищеність інтересів окремих суб’єктів.	М. Алієва [14]
Інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.	В. Богуш, О. Юдін [25]
Інформаційна безпека являє собою стан захищеності потреб в інформації особистості, суспільства та держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.	О. Горбатюк [43]
Інформаційна безпека – стан, що характеризується відсутністю небезпеки, тобто тих чинників і умов, які загрожують безпосередньо індивіду, державі, спільноті з боку інформаційно-комунікаційного середовища.	О. Данільян [46, с. 12]
Інформаційна безпека – властивість інформації, яка передається, накопичується, обробляється і зберігається та характеризує її ступінь захищеності від дестабілізуючого впливу зовнішнього середовища та внутрішніх загроз, тобто її конфіденційність, цілісність і стійкість до руйнівних впливів і перешкод.	Є. Джумалієва [48]
Інформаційна безпека – захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, що можуть призвести до нанесення шкоди власникам або користувачам інформації і підтримуючій інфраструктурі.	В. Домарев [53]
Інформаційна безпека – безпека об’єкта від інформаційних загроз або негативних впливів, пов’язаних із інформацією та нерозголошення даних про той чи інший об’єкт, що є державною таємницею.	Я. Жарков [75]

1	2
Інформаційна безпека – це вид суспільних інформаційних правовідносин стосовно створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності, спеціальних правовідносин, які пов’язані зі створенням, зберіганням, поширенням і використанням інформації.	Р. Калюжний, В. Говловський, В. Цимбалюк, М. Гузальок [81, с. 18]
Інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування та розвитку людини, всього суспільства і держави.	С. Ковтун [88]
Інформаційна безпека – інформаційний компонент національної безпеки по співвідношенню «частина – ціле». Тобто, будучи складовою частиною національної безпеки, інформаційна безпека повинна сприйматися як стан захищеності держави від зовнішніх і внутрішніх загроз у сфері обігу інформації.	Б. Кормич [92, с. 132]
Визначається шляхом використання неповної, неточної і суперечливої інформації у процесі прийняття управлінських рішень. Протидією повинна займатись інформаційно-аналітична служба спільно зі службою охорони.	Т. Косянчук, В. Лук’янова, Н. Майорова, В. Швид [94, с. 311]
Інформаційна безпека – стан захищеності основних інтересів особистості, суспільства і держави у сфері інформації, включаючи інформаційну та телекомунікаційну інфраструктуру, власне інформацію та її параметри: повноту, об’єктивність, доступність і конфіденційність.	С. Легомінова [98, с. 88]
Під інформаційною безпекою слід розуміти одну зі сторін розгляду інформаційних відносин у межах інформаційного законодавства.	О. Литвиненко [101, с. 48]
Інформаційна безпека – сфера інформаційних технологій, для успішного освоєння якої важливо з самого початку засвоїти сучасний базис, узгоджений з іншими гілками інформаційних технологій.	В. Ліпкан, Ю. Максименко, В. Желіховський [102, с. 26]
Інформаційна безпека підприємства – це цілеспрямована діяльність його органів і посадових осіб із використанням дозволених сил і засобів з досягнення стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.	А. Марущак [111, с. 94]
Інформаційна безпека підприємства – отримання за доступними цінами основних видів економічної інформації, необхідної для ефективного використання ресурсів, проведення комплексної аналітичної діяльності на підприємстві з метою систематизації та класифікації інформації, вміння прогнозувати на цій основі тенденції розвитку підприємства на коротко- середньо- та довготерміновий період тощо.	С. Мочерний, О. Устенко, С. Чоботар [117, с. 272]

1	2
Інформаційна безпека – це стан інформаційного середовища суспільства та політичної еліти, що забезпечує її формування і розвиток в інтересах керівництва країни, громадян і суспільства.	І. Панарін [121, с. 128]
Інформаційна безпека – захищеність інформації, якою володіє підприємство (виробляє, передає або отримує) від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні. Інформаційна безпека включає в себе заходи щодо захисту процесів створення даних, їх введення, обробки та виведення.	А. Садердинов, А. Трайнев, В. Федулов [135]
Під інформаційною безпекою підприємства слід розуміти суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності.	О. Сороківська [142, с. 33]
Інформаційна безпека – неможливість нанесення шкоди властивостям об'єкта безпеки зумовленим інформацією та інформаційною інфраструктурою.	А. Стрільцов [144]
Інформаційна безпека підприємства – це відношення рівня інформаційного захисту до рівня інформаційних загроз; сукупність засобів і дій уповноважених осіб, спрямованих на захист інформаційних ресурсів та інформаційної інфраструктури цього підприємства в процесі обміну, обробки і зберігання інформації на всіх рівнях інформаційної системи підприємства.	М. Танцюра [147, с. 5]
Інформаційна безпека – стан захищеності основних сфер життєдіяльності по відношенню до небезпечних інформаційних впливів.	А. Урсул [154, с. 7]
Інформаційна безпека – це отримання максимальної інформації про наміри та потенційні дії своїх опонентів, мінімальний витік інформації про свої плани. Вона містить комплекс заходів і сукупність дій, спрямованих на захист власних джерел інформації, каналів її передачі та створення систем дезінформації.	Г. Феоктистов [158, с. 211–212]
Інформаційна безпека як стан захищеності інформаційного середовища, який відповідає інтересам держави, що забезпечує формування, використання і можливості розвитку незалежно від впливу внутрішніх і зовнішніх інформаційних загроз.	Ю. Фісун [159, с. 101]
Інформаційна безпека – стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації.	Л. Хоффман [166]
Інформаційна безпека підприємства – ефективне інформаційно-аналітичне забезпечення господарської діяльності підприємства (організації).	І. Цигилик, Я. Бирик, М. Ємбрик, В. Паращич [167, с. 153]
Інформаційна безпека підприємства – це суспільні відносини щодо створення та підтримання на належному рівні життєдіяльності відповідної інформаційної системи.	В. Цимбалюк [168]

1	2
Інформаційна безпека означає: законодавче формування державної інформаційної політики; гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України; створення і впровадження безпечних інформаційних технологій; охорону державної таємниці, а також інформації з обмеженим доступом; захист національного інформаційного простору України від розповсюдження спотвореної або забороненої для поширення інформаційної продукції.	Юридична енциклопедія [171, с. 714]
Інформаційна безпека підприємства – рівень якісної, точної, своєчасної інформації про умови зовнішнього середовища, контрагентів (конкурентів, клієнтів, постачальників і т. ін.), захисту наукового забезпечення наукової, виробничо-комерційної і маркетингової діяльності підприємства.	О. Яременко [177, с. 150]
Інформаційна безпека – стан захищеності особи, суспільства та держави від зовнішніх і внутрішніх небезпек та загроз, який базується на діяльності людей, суспільства, держави та світового співтовариства з виявлення (вивчення), попередження, ліквідації та відбиття небезпек і загроз, здатних знищити їх, позбавити фундаментальних матеріальних і духовних цінностей, завдати шкоди, ускладнити шлях до прогресивного розвитку.	В. Ярочкін [178, с. 28]
Інформаційна безпека – захист особистої інформації про відправників та одержувачів; захист інформації від несанкціонованого доступу; створення надійного джерела постачання інформації, інформаційних послуг і необхідного обладнання; захист інформації, що безпосередньо стосується національної безпеки.	Report of the Secretary General [187]
Інформаційна безпека – збереження конфіденційності, цілісності та доступності інформації.	ISO/IEC 27000:2009 [210]
Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання і розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення (у цьому значенні частіше використовують термін «захист інформації»).	Вікіпедія – вільна енциклопедія [212]
Інформаційна безпека – захист інформації та інформаційних систем від несанкціонованого доступу або модифікації інформації, яка зберігається, обробляється або передається, а також від відмови в обслуговуванні авторизованих користувачів.	Міністерство оборони США [219]
Інформаційна безпека – захист комп'ютерних систем, який досягається завдяки забезпеченню конфіденційності, цілісності та достовірності даних, що обробляються, а також доступності та цілісності інформаційних компонентів і ресурсів системи.	The main concepts of information protection and information security [224]

1	2
Інформаційна безпека – стан захищеності інформаційного середовища, який забезпечується діями компетентних осіб завдяки використанню сучасних інформаційних і цифрових технологій від випадкових або навмисних впливів природного чи штучного характеру, які можуть завдати неприйняттого збитку суб'єктам інформаційних відносин і суперечити їхнім інтересам.	Авторське визначення

Велике розмаїття визначень поняття «інформаційна безпека» свідчить про його багатоаспектність і широту сфер його застосування на різних рівнях, у різних галузях, у різних напрямках.

Тому пропонується здійснити етимологічний аналіз цього поняття на основі ключових слів і змісту залежно від контексту застосування та предметної області, враховуючи об'єкт і предмет спрямування (табл. 1.4).

Таблиця 1.4

Етимологічний аналіз поняття «інформаційна безпека» [авторська розробка]

Ключові слова визначення поняття «інформаційна безпека»	Об'єкт спрямування	Предмет спрямування
1	2	3
1. Захищеність	життєво важливі інтереси	суспільство, держава й особа
	інформація і підтримуюча інфраструктура	власники або користувачі інформації та підтримуючої інфраструктури
	встановлені законом правила	інформаційні процеси в державі
	комп'ютерні системи	інформаційна система
2. Стан	захищеність	інформаційні відносини та пов'язані із ними інформаційні процеси
		інформаційне середовище суспільства
		потреби в інформації
		інтереси особистості, суспільства і держави
	відсутність небезпеки	індивід, держава, спільнота
	інформація	підприємство
	особа, суспільство та держава	зовнішні та внутрішні небезпеки й загрози

1	2	3
3. Рівень	захищеність інформаційного середовища суспільства	суспільство
	захист від інформаційних загроз; сукупність засобів і дій уповноважених осіб	підприємство
	інформаційно-аналітичне забезпечення	підприємство
	інформація	підприємство
4. Властивість	інформація	конфіденційність, цілісність і стійкість до руйнуючих впливів та перешкод
		неповність, неточність і суперечливість інформації
5. Неможливість	отримання інформації	підприємство
	заподіяння шкоди	властивості інформаційного об'єкта
6. Складова частина	невід'ємна складова	національна безпека держави
	інформаційний компонент національної безпеки по співвідношенню «частина-ціле»	
7. Збереження	інформація	інформаційні ресурси, інформаційні активи
	конфіденційність, цілісність і доступність	інформація
8. Вид відносин	вид суспільних інформаційних правовідносин	безпечні умови життєдіяльності людини, суспільства і держави
		життєдіяльність інформаційної системи
	вид відносин у межах інформаційного законодавства	суб'єкти господарювання, держава
	законодавче формування державної інформаційної політики	система «громадянин – підприємство – суспільство – держава»
9. Вид діяльності	цілеспрямована діяльність органів управління підприємства	підприємство

Відповідно до етимологічного аналізу більшість теоретиків у сфері інформаційної безпеки визначають її, по-перше, як захищеність інтересів на рівні держави й особи; по-друге, – як встановлені у державі правила захисту інформації та інформаційних процесів на міжнародному рівні; по-третє, – як захист інформації та інформаційної інфраструктури як на рівні держави, суспільства, так і на рівні підприємства, що передбачає захищеність інтересів власників або користувачів інформації; по-четверте, – як захист технічної сторони інформаційної системи. Доцільно відмітити, що переважна більшість

авторів розглядає інформаційну безпеку як стан захищеності, стан інформації, стан «безпеки» тощо.

Через категорію «рівень» інформаційну безпеку розглядають як рівень захищеності інформаційного середовища суспільства, яке забезпечує формування, використання та розвиток цього середовища в інтересах громадян, організацій, держави та нейтралізації негативних наслідків цифровізації суспільства; як рівень захисту від інформаційних загроз через сукупність засобів і дій уповноважених осіб на рівні суб'єкта господарювання; як рівень інформаційно-аналітичного забезпечення, що надає захист інформаційному середовищу підприємства; і нарешті, як рівень якісної, точної, своєчасної інформації, яка використовуватиметься задля захисту різних напрямів діяльності підприємства.

Існує також підхід, відповідно до якого інформаційну безпеку розглядають як складову національної та економічної безпеки, виключаючи самостійність існування досліджуваної категорії. Такий підхід можливий в разі здійснення комплексного аналізу рівня безпеки об'єкта та водночас неприпустимий при визначенні рівня його інформаційного захисту.

Досить розповсюдженим є визначення інформаційної безпеки на макро- та макрорівні через призму взаємовідносин із приводу її забезпечення. Відтак її розглядають як вид суспільних інформаційних правовідносин і вид відносин у межах інформаційного законодавства, що, на нашу думку, є суміжними поняттями для визначення управлінської та економічної суті цього поняття. Поняття «інформаційна безпека» в системі «громадянин – підприємство – суспільство – держава» розглядається на дещо вищому рівні, а саме як законодавче формування державної інформаційної політики, гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України [171].

Недостатньо розповсюдженим, проте важливим для цього дослідження, є визначення інформаційної безпеки як виду цілеспрямованої діяльності органів управління підприємством, в якому ставиться акцент власне на участі управлінського персоналу в процесі створення системи захисту інформаційних ресурсів на підприємстві.

Досить оригінальним є підхід, у якому інформаційна безпека визначається як «властивості інформації», які потрібно зберегти та захистити, зокрема такі, як конфіденційність, цілісність і доступність, а також властивості інформаційних ресурсів та інформаційні активи підприємства. Цей підхід розкриває ресурсну частину інформаційної безпеки, що, по суті, є основою діяльності не тільки інформаційної системи, але й управлінської і виробничої системи загалом. З огляду на вищезазначене

доступність даних – це їх властивість, що визначає можливість їх отримання і подальшого використання на вимогу уповноважених осіб, конфіденційність – властивість, пов’язана з тим, що ці дані не стануть доступними для третіх осіб без згоди уповноважених осіб, а цілісність – це незмінність інформації в процесі її зберігання або передачі. Тобто для захисту інформації вона повинна бути досить захищена від проникнення ззовні; недоступна для неуповноважених осіб; процеси з інформацією повинна здійснювати компетентна особа. Отже, захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки.

Схожим на попередній є підхід до аналізу поняття «інформаційна безпека» через категорію «збереження», де основним об’єктом переважно є також інформація та її властивості, рідше – інформаційна система. Проте в останньому випадку сутність інформаційної безпеки набуває технічного характеру, а не інформаційного та управлінського.

Діаметрально протилежним є підхід до визначення сутності інформаційної безпеки через категорію «неможливість», а саме через неможливість настання шкоди від втрати інформації або недопущення, неможливість втрати інформацією її основних властивостей, а також неможливість допущення ситуації неотримання інформації з будь-яких причин.

У ході проведення етимологічного аналізу поняття залежно від предмета захисту інформаційної безпеки доцільно виокремити:

інформаційну безпеку особи, що передбачає захист людини від навмисно або не навмисно завданої істотної шкоди шляхом здійснення впливу на навколишній інформаційний простір. У процесі формування цифрового середовища людина стала «інформаційно прозорою»;

інформаційну безпеку суспільства – стан суспільства, в якому йому не може бути завдано істотної шкоди шляхом впливу на його інформаційну сферу. В її основі лежить безпека індивідуальної, групової та масової свідомості громадян при наявності інформаційних загроз, до яких перш за все слід зарахувати інформаційно-психологічний вплив. Дія цих загроз може спричиняти психоемоційну та соціально-психологічну напруженість, спотворення моральних критеріїв і норм, морально-політичну дезорієнтацію і внаслідок цього – неадекватну поведінку окремих осіб, груп і мас людей. Унаслідок таких дій можливі глибокі трансформації індивідуальної, групової та масової свідомості, негативні зміни морально-політичного та соціально-психологічного клімату в суспільстві;

інформаційну безпеку держави – стан держави, в якому їй не може бути завдано істотної шкоди шляхом впливу на її інформаційну сферу.

Забезпечення інформаційної безпеки держави нерозривно пов'язане із забезпеченням національної безпеки [82];

інформаційну безпеку підприємства, організації, яка полягає у здійсненні цілеспрямованої діяльності органів управління та посадових осіб підприємства з використанням дозволених сил і засобів для досягнення стану захищеності інформаційного середовища, що забезпечує нормальне функціонування і динамічний розвиток.

На основі даних, наведених у табл. 1.3 та 1.4, та враховуючи особливості інформаційної безпеки, можна визначити її основні характерні ознаки:

по-перше, положення доктринального підходу визначають одну з головних характерних ознак інформаційної безпеки – стан захищеності наявних інформаційних ресурсів (або відсутності небезпеки для них), інформаційних систем, інформаційного середовища загалом як на рівні особистості, підприємств, так і на рівні держави [11; 46; 98; 121];

по-друге, дослідження науковців, що розглядають не тільки стан, а і здатнісну частину інформаційної безпеки, вказують на її залежність не стільки від стану інформаційних ресурсів, скільки від захищеності методів їх обробки, захисту процесів використання та управління інформаційними ресурсами [6, 14, 88, 224];

по-третє, існує нормативно-правовий підхід, який ґрунтується на аналізі нормативно-правових актів і передбачає, що інформаційна безпека – це вид правовідносин [8; 81; 88; 101; 171];

по-четверте, окрема група науково-прикладних надбань у сфері дослідження розкриває суб'єктну складову функціонування інформаційної безпеки, яка визначає, що вона може бути реалізована лише за наявності та причетності кваліфікованого людського фактора [81; 94; 111];

по-п'яте, інформаційну безпеку розглядають як складову загальної або національної безпеки [8; 92; 223].

Тому поняття «інформаційна безпека» в межах проведеного дослідження пропонується розуміти як стан захищеності інформаційного середовища, який забезпечується діями компетентних осіб завдяки використанню сучасних інформаційних і цифрових технологій проти випадкових або навмисних природних чи штучних впливів, які можуть завдати неприйняттого збитку суб'єктам інформаційних відносин і суперечити їхнім інтересам. Отже, з методологічного погляду такий підхід до проблем інформаційної безпеки починається з визначення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних із використанням інформаційних систем.

Із поширенням цифровізації соціально-економічних відносин, розвитком

інформаційно-комунікаційних технологій держава, підприємства та громадяни стають усе більш залежними від інформаційних продуктів і послуг, а отже, і більш уразливими по відношенню до загроз їх безпеці, зокрема інформаційній. Сучасні трансформації інформаційної сфери породжують безліч загроз інформаційній безпеці, спричинених втратою контролю над даними і використанням мережі Інтернет для їх передачі, розвитком мобільних систем і додатків, поширенням шкідливого програмного забезпечення та здійсненням атак на основі соціальної інженерії, складністю хмарних систем, великою кількістю їх компонентів, що зумовлено недостатньо високим рівнем управління інформаційним захистом.

Тому головною метою будь-якої системи інформаційної безпеки, як і системи безпеки загалом, є забезпечення сталого функціонування об'єкта, запобігання загрозам його безпеці, недопущення розкрадання матеріально-технічних, фінансових та інших ресурсів, витоку, модифікації та знищення інформації.

Моделі процесів управління інформаційною безпекою є одними із основних елементів науково-методологічного базису інформаційного захисту, тому однією з нагальних проблем, яка виникає в ході виконання завдання з побудови системи інформаційного захисту, є формування дієвої моделі інформаційної безпеки, яка матиме набір ефективних структурно-функціональних параметрів.

1.3. Сучасні моделі управління інформаційною безпекою підприємства

У рамках комплексного підходу інформаційна безпека має бути забезпечена на організаційно-управлінському, процедурному та програмно-технічному рівнях. При цьому незалежно від рівня розгляду основними інструментами опису предметної області є архітектура опису, а також моделі процесів інформаційної безпеки, які визначають ключові особливості захисту інформації на підприємстві.

Отже, важливим аспектом забезпечення інформаційної безпеки є характеристика організаційних і функціональних моделей управління інформаційною безпекою підприємства. Проведені дослідження дають змогу констатувати, що більшість дослідників організаційну модель інформаційної безпеки розуміють як формально описану політику безпеки – сукупність норм і правил, що забезпечують ефективний захист системи обробки інформації від заданої множини загроз безпеці [9; 77; 78; 79; 92; 128; 140; 169; 170; 181].

Проте в більшості описаних моделей інформаційної безпеки фрагментарно визначаються структурні складові з позиції функціональних елементів.

Загалом, поняття «безпека» визначається як стан, при якому не загрожує небезпека. З огляду на це, поняття «забезпечення безпеки» може бути визначено, по-перше, як виявлення потенційних загроз; по-друге, – як засіб запобігання нанесенню шкоди реалізацією загроз; по-третє, – як діяльність із запобігання заподіяння цієї шкоди.

Враховуючи термінологію поняття «інформаційна безпека» та основні його властивості й ознаки у загальному вигляді, переважна більшість науковців пропонує розглядати модель інформаційної безпеки в системі інтеграції суб'єктів «особа – суспільство – держава» на основі характеристики інформаційних загроз об'єктам зазначеної системи та переліку дій і завдань щодо забезпечення інформаційної безпеки (рис. 1.6).

До узагальненої моделі забезпечення інформаційної безпеки включені такі об'єкти захисту, як особа, суспільство й держава, а не безпосередньо інформація, оскільки саме завдяки останній здійснюється вплив на зазначені об'єкти.

Особливістю цієї моделі є те, що власне суб'єктами управління інформаційною безпекою є її об'єкти. Проте слід відмітити, якщо об'єктами є особа, суспільство, держава, то суб'єктами – особа та суспільство (групи людей, громадські об'єднання, організації тощо), а також державні органи законодавчої і виконавчої влади та спеціалізовані державні органи (Міністерство цифрової трансформації України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації в Україні, Національний координаційний центр кібербезпеки, Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України, поліція тощо).

Суб'єкти є виконавцями відповідних функцій, спрямованих на формування стану захищеності за допомогою реалізації превентивних заходів, заходів захисту та заходів нейтралізації основних видів загроз інформаційній безпеці.

В умовах стрімкої цифровізації та інформатизації соціально-економічних відносин розглянуту модель потрібно оптимізувати та адаптувати до сучасних умов господарювання.

На основі узагальнення [79; 169; 170; 215] пропонується доповнити основні компоненти та розширити модель забезпечення інформаційної безпеки і, крім об'єктів та суб'єктів інформаційної безпеки, основних видів загроз інформаційній безпеці, додати нові компоненти – напрями та цілі

захисту інформації (рис. 1.7).

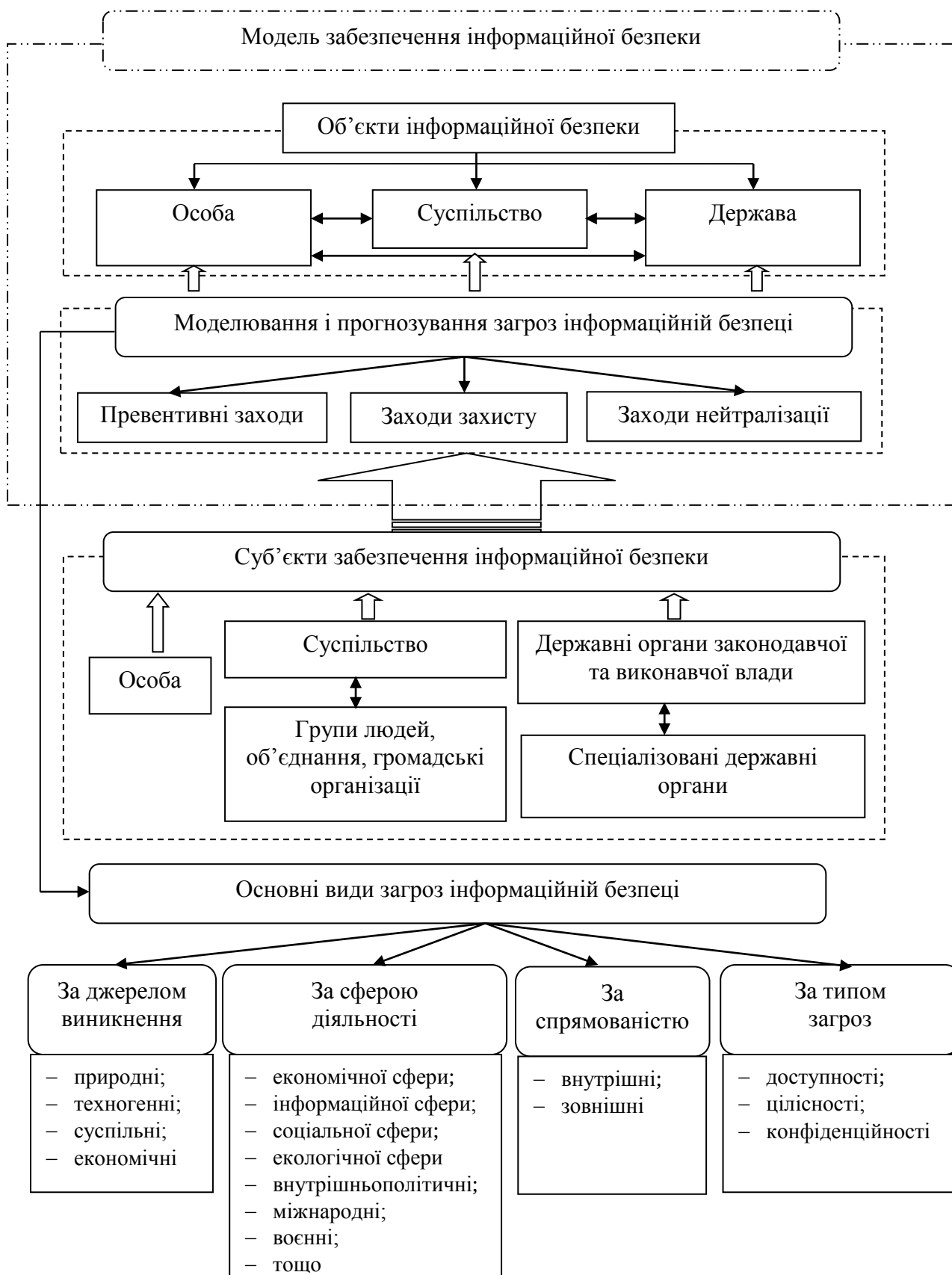


Рис. 1.6. Узагальнена модель забезпечення інформаційної безпеки [розроблено на основі 79; 169; 170; 215]

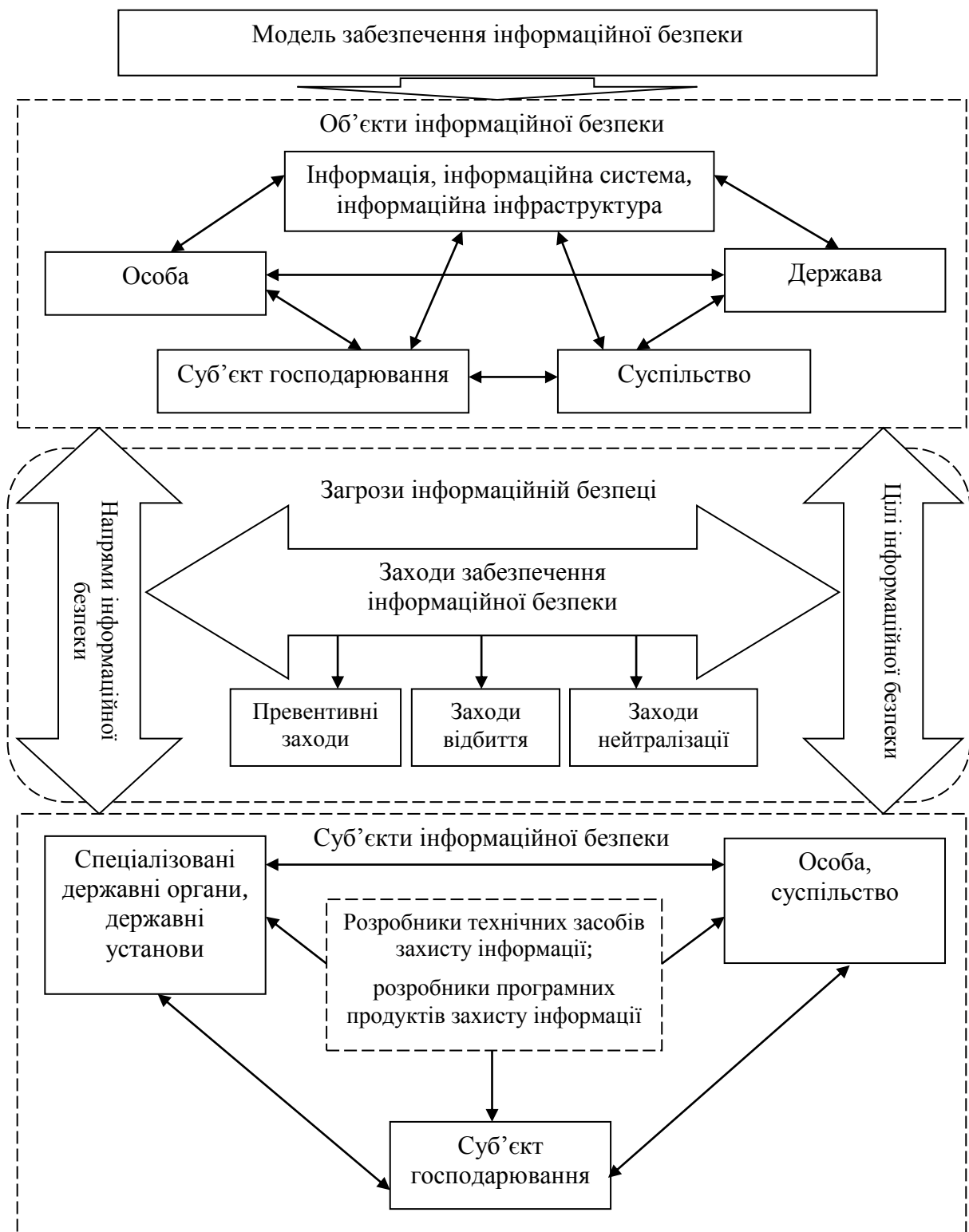


Рис. 1.7. Модель забезпечення інформаційної безпеки [авторська розробка]

Базові компоненти моделі теж пропонується адаптувати до сучасних умов. Отже, об'єктами інформаційної безпеки, на відміну від розглянутої узагальненої моделі (див. рис. 1.6), є не тільки особа, суспільство та держава,

але й суб'єкт господарювання (підприємство) – як ключовий елемент соціально-економічних відносин, а також інформація, інформаційна система та інформаційна інфраструктура. Саме останні забезпечують інформаційне середовище функціонування зазначених об'єктів.

Слід зазначити, що на рівні держави інформаційну безпеку доцільно визначати як складову національної безпеки. Також інформаційна безпека зазвичай є сполучною ланкою між політикою національної безпеки та інформаційною політикою країни. Небезпека, яка може виникати в інформаційній сфері, – це незбалансованість інтересів суб'єктів суспільних відносин. Також у процесі функціонування держави породжується інформація, розкриття якої може знизити ефективність проведеної політики, тому подібна інформація приховується. У цьому разі об'єктом безпеки є режим доступу до інформації, а інформаційна безпека полягає в неможливості порушення цього режиму [105].

Важливим елементом моделі забезпечення інформаційної безпеки є законодавча і нормативно-правова база забезпечення інформаційної безпеки, що виражає державну політику в цій сфері. Держава керується тим, що інформаційні ресурси є об'єктами власності, які беруть участь у процесі господарювання. Закони та правові акти забезпечення інформаційної безпеки наділяють певні органи державної влади повноваженнями здійснювати державне регулювання, контроль (моніторинг) та управління у сфері інформаційного захисту, а також визначають взаємовідносини суб'єктів інформаційної діяльності. Технічні нормативні акти являють собою стандарти і технічні регламенти, які можуть (або зобов'язані) використовувати суб'єкти інформаційної діяльності [210].

Об'єктом інформаційного захисту також є захищеність інформації, інформаційного середовища та інфраструктури від навмисних або випадкових природних і штучних впливів, що можуть призвести до заподіяння шкоди власникам або користувачам інформації.

Заподіяння шкоди інформаційній інфраструктурі може призвести до порушення цілісності суспільства, діяльності його інститутів та організацій тощо. Тому інформаційна безпека суспільства полягає в неможливості заподіяння шкоди перш за все культурним цінностям, духовній сфері, соціальним регуляторам поведінки людей, інформаційній інфраструктурі та організаціям, об'єднанням, інститутам.

Наступним об'єктом інформаційного захисту є особа. Заподіяння шкоди здатності особи сприймати та осмислювати інформацію істотно знижує можливість безпечного існування. З огляду на це інформаційна безпека особи полягає в неможливості заподіяння шкоди їй як особистості, соціальна

діяльність якої значною мірою базується на осмисленні одержуваної інформації та інформаційних взаємодіях з іншими індивідами і має інформацію як предмет діяльності.

Важливим об'єктом інформаційної безпеки є суб'єкт господарювання (підприємство). Зміст інформаційної безпеки такого об'єкта в найбільш загальному вигляді буде полягати в захисті від несанкціонованого доступу до тих відомостей, які власник вважає важливими. У разі, якщо власник підприємства не вбачає необхідності в захисті своєї інформації, то зміст інформаційної безпеки може бути звужений до захисту конкретної інформації, розкриття якої може завдати помітний збиток.

Відповідно до пропонованої моделі суб'єкти у сфері інформаційної безпеки можна умовно поділити на три групи: перша група – державні установи, що здійснюють державне регулювання у цій сфері, та спеціалізовані державні органи; друга група – користувачі, до яких належать особа, суспільство та суб'єкти господарювання; третя група – розробники технічних засобів і програмних продуктів захисту інформації. Очевидно, що всі ці групи взаємопов'язані.

Повноваження і діяльність суб'єктів першої групи визначені законом або спеціальними положеннями. Ця група координує діяльність із захисту інформації, розробляє нормативні правові акти або бере участь в їх підготовці, здійснює експертизу (сертифікацію) технічних засобів програмних продуктів інформаційної безпеки. Крім того, суб'єкти цієї групи управляють державними інформаційними системами, пов'язаними з інформаційною безпекою.

Друга група – користувачі (особа, суспільство, суб'єкт господарювання), що є найчисленнішою групою суб'єктів у сфері інформаційної безпеки. Суб'єкти цієї групи застосовують засоби технічного захисту інформації для захисту власних інформаційних ресурсів і взаємодіють із системами захисту інших суб'єктів. У своїй діяльності вони можуть використовувати державні інформаційні системи, інфраструктуру та інформаційні ресурси.

Основною діяльністю суб'єктів третьої групи є розробка технічних засобів і програмних продуктів захисту інформації. Свою діяльність вони здійснюють на основі процесів ліцензування, а створені ними засоби захисту повинні пройти сертифікацію, перш ніж їх будуть застосовувати користувачі.

Основою моделі забезпечення інформаційної безпеки є власне загрози інформаційній безпеці, а одним із найбільш важливих аспектів інформаційної безпеки є визначення та класифікація можливих загроз безпеки. Загалом загроза інформаційній безпеці – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства та держави [140].

Прийнятна для практичного застосування вітчизняна класифікація загроз інформаційній безпеці не закріплена ні на теоретичному, ні на практичному рівнях. У Законі України «Про основи національної безпеки» загрозу інформаційній безпеці визначено як намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації. З-поміж інших загроз – прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність і комп'ютерний тероризм; розголошення інформації, яка становить державну таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб і національних інтересів суспільства та держави [4].

У Доктрині інформаційної безпеки визначені такі загрози інформаційній безпеці країни:

- поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;

- зовнішні деструктивні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет;

- деструктивні інформаційні впливи, які спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності України;

- прояви сепаратизму в ЗМІ та Інтернеті за етнічною, мовною, релігійною та іншими ознаками [8].

Закон України «Про основні засади забезпечення кібербезпеки України» визначає, що суб'єкт господарювання будь-якого рівня може піддатися новому виду інформаційної небезпеки – кіберзагрозі, яка визначається як наявне та потенційно можливе явище або чинник, що створює небезпеку життєво важливим національним інтересам України у кіберпросторі, негативно впливає на стан кібербезпеки держави та кіберзахист її об'єктів [5]. Отже, на законодавчому рівні питання визначення сутності загроз, їх класифікації та визначення напрямів їх уникнення розглянуто фрагментарно і лише на рівні держави. Що стосується суб'єктів мікрорівня, то проблематика визначення загроз інформаційній безпеці або розглядається на рівні теоретичних узагальнень окремих дослідників, або на емпіричному рівні суб'єктів господарювання.

Огляд різних поглядів сутності загроз інформаційній безпеці [5; 7; 9; 19; 25; 36; 41; 44; 77; 78; 79; 90; 92; 128; 140; 169; 170; 181; 220; 225] показав, що наразі немає обґрунтованого визначення сутності загроз інформаційній

безпеці та їх уніфікованої класифікації. Доцільно відмітити, що загрози інформаційній безпеці можуть бути як реальними, тобто ті, які проявляються в своєму негативному, руйнівному впливі на об'єкт безпеки, так і потенційними, тобто їх негативний вплив може проявитися в найближчому або віддаленому майбутньому.

Найбільш розповсюдженою класифікацією джерел загроз інформаційній безпеці є джерела, спричинені людським фактором, проникненням і шкідливим програмним забезпеченням та неантропогенними природними факторами.

«Людським фактором» (антропогенними джерелами загроз безпеці інформації) є суб'єкти, дії яких кваліфікуються як умисне або ненавмисне порушення чи здійснення злочину. Ця група факторів є найбільш чисельною, а отже, становить найбільший інтерес з погляду організації захисту та управління ним, оскільки дії конкретного суб'єкта завжди можна спрогнозувати й оцінити та вжити відповідних превентивних заходів. Методи інформаційного захисту залежать від організаторів захисту інформації та є керованими. Проте, крім навмисних порушень, до цієї групи слід зарахувати ще й «ненавмисні» порушення інформаційної безпеки. За статистикою, наданою організацією LETA [220], кожен четвертий користувач залишає зловмисникам можливість проникнути в корпоративну мережу; кожен другий користувач не знайомий з правилами інформаційної безпеки; двоє з трьох користувачів відвідують потенційно небезпечні сайти з робочого ПК; третина користувачів зберігає паролі в легкодоступному місці; 15 % працівників готові передати третім особам конфіденційну інформацію; понад 60 % мобільних телефонів не захищені паролем; кожен третій працівник постійно використовує той самий пароль під час реєстрації на різних видах ресурсів; вісім із десяти користувачів не знищують носії, що містять корпоративну інформацію.

Друга група – «проникнення, шкідливе програмне забезпечення» – передбачає такі джерела загроз, які спричиняються технократичною діяльністю людини та розвитком цивілізації. Наслідки, спричинені такою діяльністю, можуть бути непередбачуваними і неконтрольованими. Такі джерела загроз є менш прогнозованими та безпосередньо залежать від властивостей техніки, тому їм необхідно приділяти особливу увагу. Третю групу джерел загроз становлять фактори неантропогенного походження. Вони об'єднують обставини, які мають об'єктивний і абсолютний характер. До них зараховують стихійні лиха або інші обставини, які неможливо передбачити та яким неможливо запобігти або ж можливо передбачити, але неможливо запобігти. Заслугове на увагу класифікація загроз інформаційній

безпеці, запропонована компанією VPS.house [225], яка базується на основних характеристиках і властивостях інформації [44] (рис. 1.8).

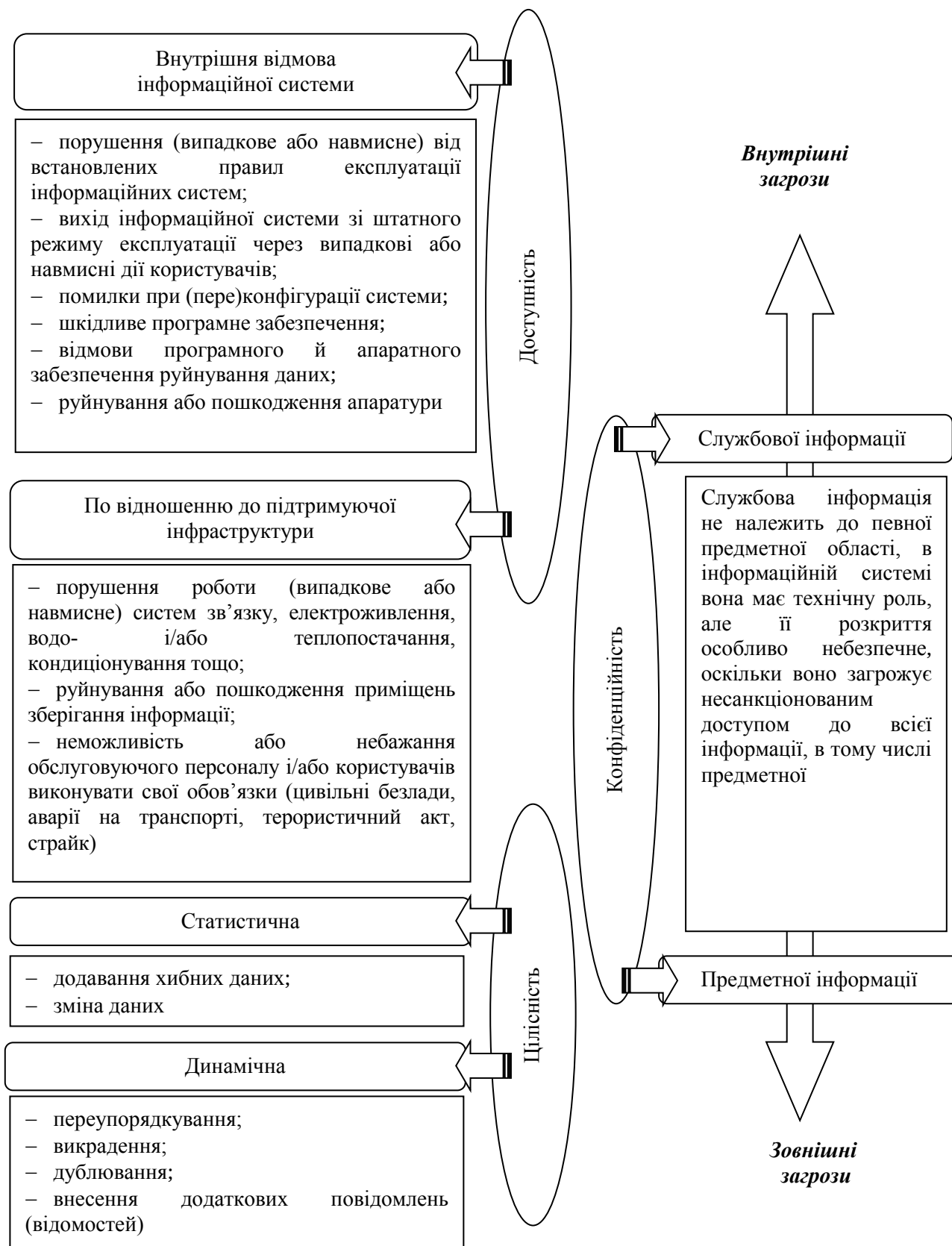


Рис. 1.8. Класифікація видів загроз інформаційній безпеці [згруповано на основі 44; 181; 225].

Натомість А. Артемов визначає такі основні загрози, які породжують інформаційні втрати та призводять до різних видів пошкоджень і зростання збитків від неправомірних дій: нещасні випадки, що спричиняють вихід з ладу обладнання та втрату інформаційних ресурсів; поломки технічних засобів обробки інформації; наслідки природних явищ; крадіжки, навмисне псування матеріальних засобів; помилки у функціонуванні або поломки програмного забезпечення, баз даних, моделей захисту; помилки накопичення, зберігання, передачі, використання інформації; помилки сприйняття, читання, інтерпретації змісту інформації; помилки як результат невміння здійснювати операції з інформацією; наявність перешкод, збоїв і спотворень окремих елементів інформаційної системи; помилки експлуатації – порушення захисту, переповнення файлів, помилки мови управління даними, помилки при підготовці та введенні інформації, помилки операційної системи, програмування, апаратні помилки, зловмисні дії в матеріальній сфері; розголошення; збитки соціального характеру [19].

Представники провідної компанії-розробника засобів інформаційної безпеки та боротьби з інформаційними загрозами «Searchinform» з практичного погляду визначають три групи вразливостей по відношенню до загроз інформаційній безпеці (табл. 1.5).

Таблиця 1.5

**Групи вразливостей по відношенню до загроз інформаційній безпеці
[згруповано на основі 19; 152; 221]**

Група вразливостей	Загрози	Характеристика факторів
1	2	3
Випадкові види вразливостей Фактори, які залежать від непередбачуваних обставин і особливостей інформаційного середовища, які практично неможливо прогнозувати, але можна розробити заходи щодо їх попередження шляхом проведення інженерно-технічного огляду	1. Збої і відмови роботи інформаційної системи	– несправності технічної частини інформаційної системи на різних рівнях обробки та зберігання інформації; – збої програмного забезпечення, що забезпечують отримання, зберігання, надання та інші процеси обробки інформації; – збої в роботі допоміжного обладнання інформаційних систем, пошкодження інформаційної інфраструктури
	2. Загрози, що послаблюють інформаційну безпеку	– пошкодження забезпечуючих підсистем для ефективної роботи інформаційної системи (підсистема електропостачання, підсистема кондиціювання тощо); – недосконалість фізичного захисту інформаційної системи (охорона, паркани, приміщення, обладнання, де зберігається інформація тощо)

1	2	3
Об'єктивні різновиди вразливостей Фактори, які залежать від технічної структури обладнання на об'єкті, що вимагає захисту, і його характеристик	1. Загрози, що пов'язані з технічними засобами випромінювання	– електромагнітні методики; – звукові методики; – електричні методики
	2. Загрози, які активізуються	– шкідливе програмне забезпечення, нелегальні програми, технологічні виходи з програм, що об'єднується терміном «програмні закладки»; – закладки апаратури
	3. Загрози, які створюються особливостями об'єкта, що знаходяться під захистом	– розташування об'єкта (відсутність зони контролю об'єкта зберігання інформації, можливість віддаленого доступу до елементів об'єкта); – формування каналів передачі інформації
	4. Загрози, що залежать від особливостей елементів-носіїв	– засоби, які підпадають впливу електромагнітного поля (носії, мікросхеми та інші елементи).
Суб'єктивні різновиди вразливостей Група факторів здебільшого є результатом неправильних дій співробітників на рівні розробки систем зберігання і захисту інформації.	1. Загрози, спричинені неточностями і грубими помилками, що порушують інформаційну безпеку	– на етапі завантаження готового програмного забезпечення або попередньої розробки алгоритмів, а також у момент його використання; – на етапі управління програмами і інформаційними системами; – під час користування технічною апаратурою (на етапі увімкнення або вимкнення, експлуатації пристроїв для передачі або отримання інформації).
	2. Загрози, спричинені порушенням роботи систем в інформаційному просторі	– порушення режиму захисту особистих даних (проблеми створюють звільнені працівники або працюючі співробітники в неробочий час, які отримують несанкціонований доступ до системи); – порушення режиму збереження і захищеності (під час отримання доступу до об'єкта або до технічних пристроїв); – порушення під час роботи з технічними пристроями (можливі порушення в енергозбереженні або забезпеченні техніки); – під час роботи з даними (перетворення інформації, її збереження, пошук і знищення даних, усунення браку та неточностей).

На основі узагальнення поглядів науковців і практиків на проблему визначення загроз інформаційній безпеці, в цьому дослідженні загрозу об'єкту інформаційної безпеки пропонується розуміти як сукупність факторів і умов, що виникають у процесі взаємодії різних об'єктів між собою і об'єктів із суб'єктами та здатні здійснювати негативний вплив на конкретний об'єкт інформаційної безпеки. Особлива увага в цьому аспекті акцентована саме на суб'єктивізмі, оскільки як об'єктивні, так і випадкові загрози інформаційній безпеці виникають через невміння, небажання, неухважність, відсутність компетенції або досвіду конкретної особи – суб'єкта.

Розглянуті розподіли груп загроз інформаційній безпеці є досить умовними і потребують взаємоінтеграції з іншими класифікаціями загроз. Це пояснює необхідність поєднання реальних і потенційних загроз, загроз, що виникають на різних рівнях господарювання (міжнародному, національному, регіональному та локальному), загроз інформаційній безпеці, спричинених антропогенними та неантропогенними чинниками (не виключаючи суб'єктивізму). Вищезазначене доцільно здійснити шляхом побудови функціональної моделі загроз безпеці інформаційній системі, схематичне зображення якої відображено на рис. 1.9.

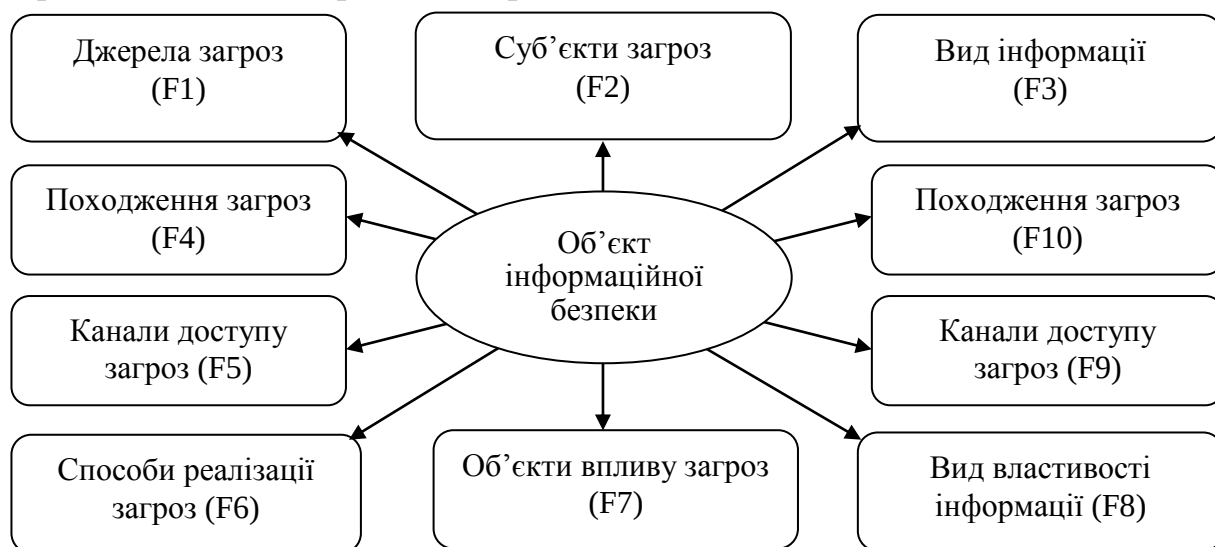


Рис. 1.9. Структура функціональної моделі загроз інформаційній безпеці [розроблено на основі 54; 78; 79; 105; 136; 152]

На основі зазначеної структури функціональної моделі загроз інформаційній безпеці доцільно визначити функціональну залежність її складових через формулу (1.1):

$$F_{is}(t) = f \{((F1(t), F2(t), F3(t), F4(t), F5(t), F6(t), F7(t), F8(t), F9(t), F10(t))), (1.1)$$

де $F1(t), F2(t), F3(t), F4(t), F5(t), F6(t), F7(t), F8(t), F9(t), F10(t)$ – функції

загроз об'єкту інформаційної безпеки. Відповідно:

- функція за джерелом загроз, $F1(t) = f(a_1, a_2, a_3, a_4)$,
де a_1 – загрози, що створює порушник (суб'єкт);
 a_2 – загрози, що створюють апаратні засоби;
 a_3 – загрози, що створюють програмні засоби;
 a_4 – загрози, що створюють неантропогенні чинники;
- функція загроз за суб'єктом загроз, $F2(t) = f(b_1, b_2, b_3, b_4)$, де
 b_1 – загрози, що створює держава (державні органи);
 b_2 – загрози, що створює суб'єкт господарювання;
 b_3 – загрози, що створюють приватні особи, суспільство;
 b_4 – загрози, що створюють розробники технічних засобів захисту;
- функція загроз за видом інформації, $F3(t) = f(c_1, c_2, c_3, c_4, c_5)$, де
 c_1 – загрози від мовної інформації;
 c_2 – загрози від візуальної інформації;
 c_3 – загрози від цифрової інформації;
 c_4 – загрози в технічних засобах обробки інформації;
 c_5 – загрози від інформації, що обробляється в автоматизованих системах;
- функція загроз за походженням (місцем виникнення) загроз,
 $F4(t) = f(d_1, d_2)$, де
 d_1 – зовнішні загрози інформаційній безпеці;
 d_2 – внутрішні загрози інформаційній безпеці;
- функція загроз за каналом доступу, $F5(t) = f(e_1, e_2, e_3, e_4, e_5, e_6)$, де
 e_1 – наявність в автоматизованих системах шкідливої програми;
 e_2 – наявність в автоматизованих системах апаратних закладок;
 e_3 – дія в ході реалізації протоколів мережевої взаємодії і каналів передачі даних;
 e_4 – недостатність технічного захисту інформації;
 e_5 – вразливість засобів захисту інформації;
 e_6 – вразливість системи в разі виникнення позаштатних ситуацій;
- функція загроз за способом реалізації загроз, $F6(t) = f(g_1, g_2)$, де
 g_1 – загрози від спеціальних впливів;
 g_2 – загрози від технічних каналів;
- функція загроз за об'єктами впливу, $F7(t) = f(h_1, h_2, h_3, h_4, h_5)$, де
 h_1 – загрози, що впливають на рівні держави;
 h_2 – загрози, що впливають на рівні суспільства;
 h_3 – загрози, що впливають на рівні особи;
 h_4 – загрози, що впливають на рівні суб'єкта господарювання;
 h_5 – загрози інформаційній системі, інформаційній інфраструктурі,

інформаційному середовищу;

– функція загроз властивості інформації, яку порушують, $F8(t) = f(i_1, i_2, i_3)$, де

i_1 – загрози конфіденційності;

i_2 – загрози цілісності системного програмного забезпечення;

i_3 – загрози доступності програмних засобів захисту інформації;

– функція загроз за ступенем реалізації, $F9(t) = f(j_1, j_2)$, де

j_1 – реалізовані загрози;

j_2 – нереалізовані загрози;

– функція загроз за розміром збитку, $F10(t) = f(k_1, k_2, k_3)$, де

k_1 – загрози, які не завдають збитку;

k_2 – загрози, які завдають незначний збиток;

k_3 – загрози, які завдають значний збиток;

k_4 – загрози, які завдають критичний збиток.

Остаточно функціональну модель безпеки конфіденційної інформації в інформаційній системі можна відобразити у вигляді формули (1.2):

$$FIS(t) = f \{ (Fuc; Fis(t)) \}, \quad (1.2)$$

де $FIS(t)$ – загальний стан інформаційної системи, спричинений інформаційними загрозами.

Розробка функціональної моделі загроз інформаційній безпеці в інформаційній системі дозволить змодельовати передбачувані загрози в системі захисту для забезпечення їх нейтралізації.

Заходи із забезпечення інформаційної безпеки в пропонованій моделі також передбачають формування стану захищеності через реалізацію превентивних заходів, заходів відбиття загроз і заходів нейтралізації загроз інформаційній безпеці. Але на відміну від існуючої моделі (див. рис. 1.6) у пропонованій моделі зазначений елемент залежить від цілей захисту та напрямів захисту інформації. На рис. 1.10. представлені напрями й цілі захисту інформації та їх взаємозв'язок у межах запропонованої моделі забезпечення інформаційної безпеки [44; 181].

Запропонована модель забезпечення інформаційної безпеки, складові цієї моделі та функціональна модель загроз інформаційній безпеці дозволяють збільшити ефективність процесів і результатів управління інформаційною діяльністю на рівні держави, суспільства та особи.

Побудова моделі управління інформаційною безпекою на рівні суб'єкта господарювання (підприємства) має свої особливості.

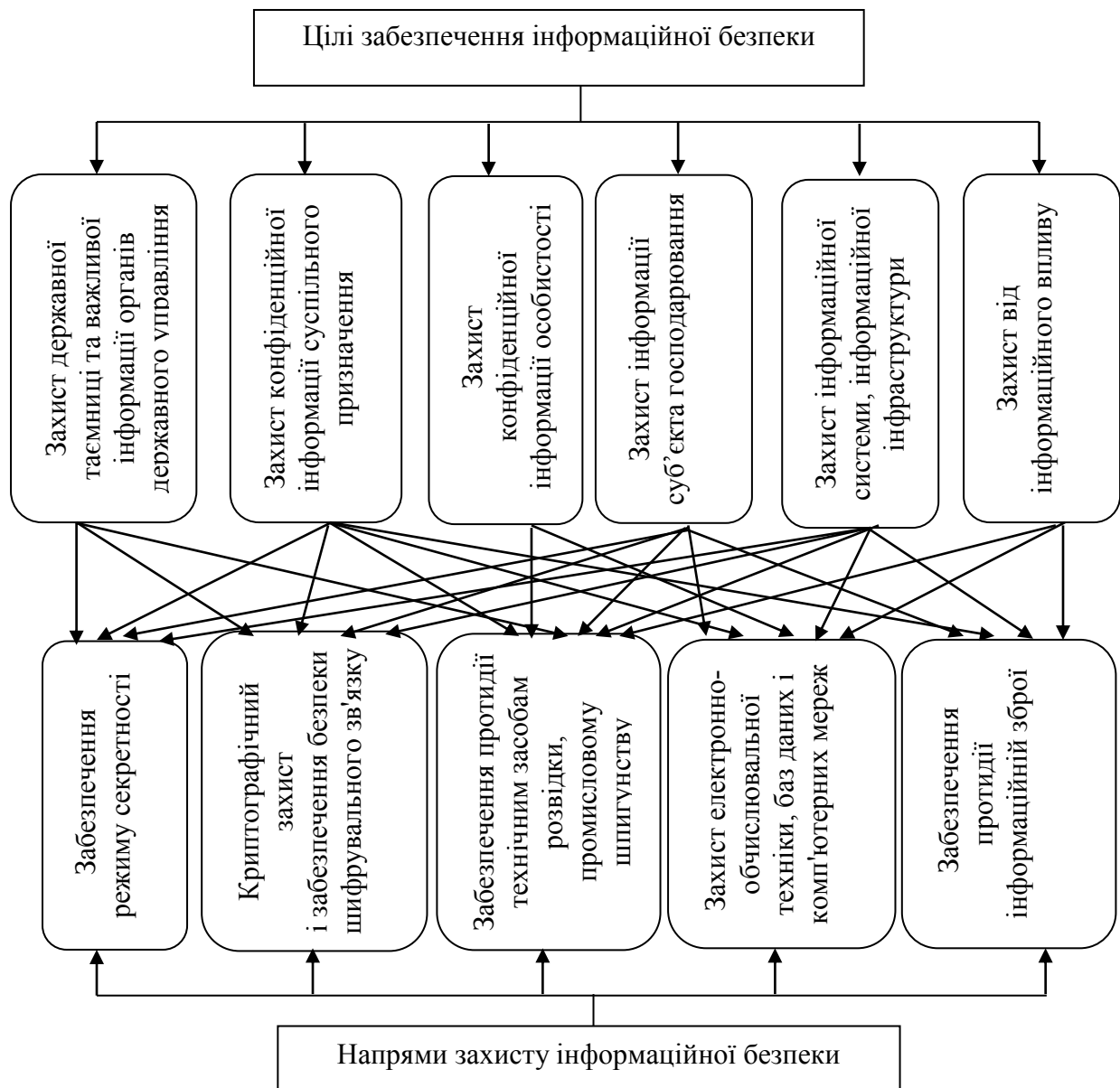


Рис. 1.10. Взаємозв'язок цілей і напрямів інформаційної безпеки [доопрацьовано на основі 54; 155; 169; 170; 175]

Зважаючи на фрагментарність досліджень із зазначеної проблематики, пропонується власне бачення структури моделі управління інформаційною безпекою на підприємстві, базисом для створення якої стала модель забезпечення інформаційної безпеки та функціональна модель загроз інформаційній безпеці (рис. 1.11).

У структурі моделі наявні суб'єкти управління інформаційною безпекою підприємства, які можна умовно поділити на три основні групи.

Група I – вище керівництво підприємства, яке здійснює загальне управління системою управління інформаційною безпекою і виконує загальні функції управління нею, зокрема:

планування – визначення варіанта створення системи управління інформаційною безпекою підприємства та ресурсного забезпечення

функціонування цієї системи;

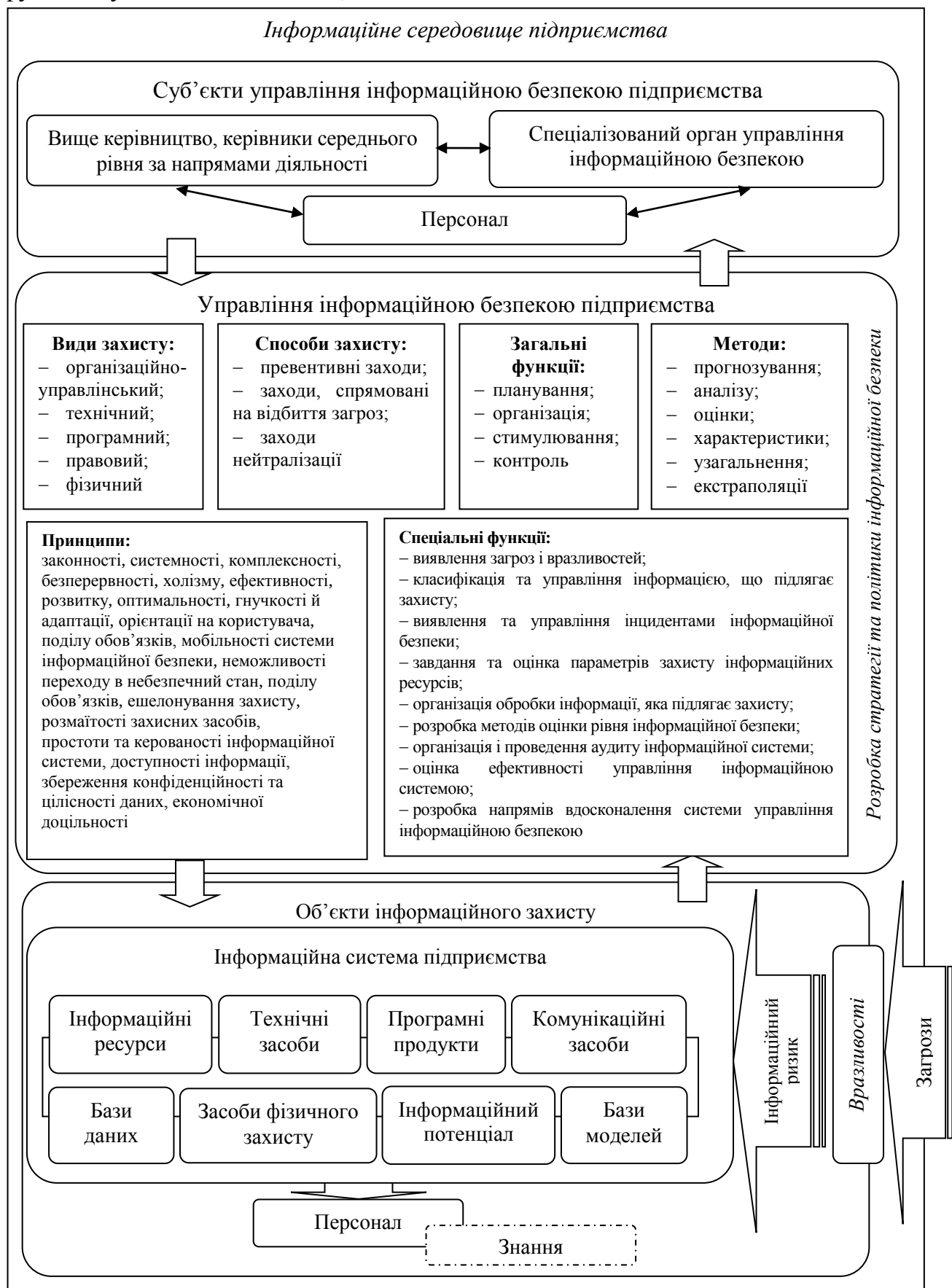


Рис. 1.11. Організаційно-функціональна модель управління інформаційною безпекою підприємства [авторська розробка]

організація – визначення повноважень і здійснення специфічних функцій системою управління інформаційною безпекою;

стимулювання – затвердження політики безпеки та стратегії інформаційної безпеки, методів проведення роз'яснювальних заходів для персоналу з питань інформаційного захисту, мотивація працівників системи управління інформаційною безпекою підприємства;

контроль за станом, порядком і правилами формування, розвитку та використання інформаційних ресурсів; регулювання сфери інформатизації щодо забезпечення науково-технічних і організаційно-економічних умов створення та застосування інформаційних технологій на підприємстві.

До цієї групи доцільно включити також провідних спеціалістів підприємства (головний бухгалтер, економіст, начальник виробництва, маркетолог), які б здійснювали захист інформації відповідно до напрямів діяльності (комерційної таємниці, статистичної, економічної, технологічної та маркетингової інформації).

Групу II утворюють спеціалізовані органи управління інформаційною безпекою підприємства.

Є декілька варіантів організації діяльності спеціалізованих органів управління інформаційною безпекою підприємства (рис. 1.12).

Найбільш простою із організаційного погляду є наявність одного або декількох фахівців, що спеціалізуються на забезпеченні інформаційної безпеки всередині ІТ-відділу підприємств. Це найбільш поширений спосіб організації з огляду на сформовані стереотипи про те, що інформаційна безпека – це частина процесу забезпечення функціонування інформаційного середовища підприємства. Надалі підприємство в разі розширення масштабів діяльності або інформатизації виробничих і управлінських процесів переходить до наступного етапу – виділення служби інформаційної безпеки як окремої структури всередині ІТ-відділу. Цей варіант кращий тільки тому, що діяльність із забезпечення інформаційної безпеки виділяється вже як окрема вагома складова серед іншої діяльності ІТ-відділу, а також надається більше як людських, так і фінансових ресурсів.

Отже, за «спрощеним» варіантом організації діяльності спеціалізованих органів управління інформаційною безпекою підприємства всередині ІТ-служби має переваги легка організація та можливості роботи безпосередньо у внутрішніх або зовнішніх ІТ-проектах, що сприяє впровадженню вимог з безпеки на етапі реалізації, інтеграції з інформаційним середовищем. Недоліки спрощеного підходу полягають у тому, що спеціалісти або служба працюють у «консультаційному режимі» та мають підлегле становище по відношенню до ІТ-відділу, а як наслідок – залишковий принцип

фінансування. В такому разі інформаційна безпека розглядається як частина інформаційної системи, що не передбачає комплексного підходу.



Рис. 1.12. Альтернативи організації спеціалізованих органів управління інформаційною безпекою підприємства [доопрацьовано на основі 141]

Наступний підхід відображає варіант створення служби інформаційної безпеки всередині служби загальної безпеки. Цей підхід поширений у державних організаціях або на великих підприємствах, де особлива увага приділяється питанням економічної та фізичної безпеки. Перевагами такого підходу у тому, що він легко реалізується та не потребує значних ресурсів для забезпечення спеціалістів з інформаційної безпеки або створення служби всередині зазначеного відділу; є можливість створення ряду організаційних заходів, що сприяють підвищенню загального рівня захищеності. Недоліками є «консультаційний» режим роботи, нерозуміння важливості інформаційної безпеки безпосереднім керівництвом, ускладнення роботи з IT-службою, залишковий принцип фінансування.

Оптимальним варіантом є «комплексний» підхід, який передбачає наявність незалежних фахівців з інформаційної безпеки, що безпосередньо

підпорядковуюються вищому керівництву підприємства. Зазначений підхід доцільно застосовувати підприємствам малого та середнього бізнесу, які поки що не мають змоги створити в організації повноцінну службу інформаційної безпеки. Основною умовою є наявність підготовленого менеджера з інформаційної безпеки, здатного виконувати як аналітичні завдання, так і завдання спектра питань, пов'язаних із інформаційною безпекою. Для створення процесу управління інформаційною безпекою в цьому варіанті повинні використовуватися ресурси інших підрозділів і служб, у тому числі IT-відділу. Перевагами комплексного підходу є можливість контакту з топ-менеджментом, паритетне становище з IT-відділом. Недоліками є відсутність структури, залежність від людських ресурсів, відсутність власної бюджетної статті, а також те, що цей підхід не прийнятний для великих підприємств. Найкращим є комплексний підхід до організації, коли служба інформаційної безпеки організована у вигляді повноцінної незалежної структури, яка підпорядкована вищому керівництву підприємства. Навіть при такому варіанті залишається проблема взаємодії з іншими службами, і перш за все – з IT-відділом [141].

Група III – персонал підприємства, який опосередковано бере участь у створенні належних умов забезпечення інформаційної безпеки, збереження комерційної таємниці.

Наступним елементом моделі є власне процес управління інформаційною безпекою підприємства, тобто її забезпечення, що передбачає наявність таких складових, як види захисту, способи захисту, загальні функції, спеціальні функції, методи, принципи.

Варто відмітити, що спеціальні функції передбачають їх реалізацію саме групою II суб'єктів управління інформаційною безпекою підприємства.

Об'єктами захисту є інформаційні ресурси, інформаційний потенціал, технічні засоби, програмні продукти, засоби комунікації, засоби фізичного захисту, бази даних, бази моделей. До окремої групи об'єктів захисту зараховано персонал, оскільки він як причетний до управління іншими об'єктами, що підлягають захисту, так і є власне основною загрозою порушення інформаційної безпеки. А знання визначено як особливий об'єкт – результат симбіозу інформаційних ресурсів і персоналу.

Ураховуючи структуру пропонованої моделі, управління інформаційною безпекою підприємства пропонується розуміти як можливість і здатність суб'єктів управління інформаційною безпекою підприємства створити та підтримувати такий оптимальний стан інформаційного середовища підприємства, за якого забезпечуються умови ефективного функціонування об'єктів захисту (інформаційних ресурсів, інформаційного потенціалу,

технічних засобів, програмних продуктів, засобів комунікації, засобів фізичного захисту, баз даних і банків моделей, персоналу та знань) і мінімізація випадкових або навмисних природних чи штучних впливів, які можуть завдати збитків суб'єктам інформаційних відносин.

Проте динамічні умови функціонування суб'єктів господарювання обумовлюють необхідність формування комплексної методології діагностики рівня інформаційної безпеки підприємства, що враховуватиме не тільки оцінку технічних аспектів і рівня інформаційного ризику, але й передбачатиме аналіз економічної та управлінської складової системи інформаційної безпеки підприємств агропродовольчої сфери України.

Список використаних джерел до розділу 1

1. Про державну таємницю : Закон України. *Відомості Верховної Ради України*. 1994. № 16. URL: <https://zakon.rada.gov.ua/laws/show/3855-12>.
2. Про доступ до публічної інформації: Закон України. *Відомості Верховної Ради України*. 2011. № 32. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T112939.html.
3. Про інформацію : Закон України. *Відомості Верховної Ради України*. 1992. № 48. ст.650. URL: <https://zakon.rada.gov.ua/laws/show/2657-12>.
4. Про національну безпеку України : Закон України. *Відомості Верховної Ради*. 2018. № 31. URL: <https://zakon.rada.gov.ua/laws/show/2469-19>
5. Про основні засади забезпечення кібербезпеки України : Закон України. *Відомості Верховної Ради України*. 2017. № 45. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>.
6. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України. *Відомості Верховної Ради України*. 2007. № 12. URL: <https://zakon.rada.gov.ua/laws/show/537-16>.
7. Про засади інформаційної безпеки України : проект Закону України. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JG3TH00A.htm.
8. Про Доктрину інформаційної безпеки України : Указ Президента України. URL: <http://www.president.gov.ua/documents/472017-21374>.
9. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації : Розпорядження Кабінету міністрів України від 17 січня 2018 р. № 67-р. URL: <http://zakon.rada.gov.ua/laws/show/67-2018-%D1%8>.
10. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : Розпорядження Кабінету міністрів України від 15 травня 2013 р.

№ 386-р. URL: <https://zakon.rada.gov.ua/laws/show/386-2013-р>.

11. Абакумов В. М. Інформаційна безпека підприємництва як об'єкт адміністративно-правової охорони. *Форум права*. 2012. № 4. С. 10-16. URL: <http://arhive.nbu.gov.ua/e-journals/FP/2012-4/12avmapo.pdf>

12. Абрамов В. І., Арутюнов В. Х. Методологія системного підходу та наукових досліджень (дослідницькі та інноваційні процеси в державній службі): навч.-метод. посіб. для самост. вивч. дисц. К. : КНЕУ, 2005. 178 с.

13. Александрова Т. В. Цифровизация как современный тренд развития менеджмента производственных организаций. *Вестник Южно-Уральского государственного университета. Серия : Экономика и менеджмент*. 2019. Вып. 13. № 3. С. 137–144.

14. Алиева М. Ф. Информационная безопасность как элемент информационной культуры. *Вестник Адыгейского государственного университета. Серия 1: Регионоведение : философия, история, социология, юриспруденция, политология, культурология*. 2012. № 4. С. 97–102.

15. Апалькова В. В. Концепція розвитку цифрової економіки в Євросоюзі та перспективи України. *Вісник Дніпропетровського університету. Серія : Менеджмент інновацій*. 2015. Вип. 4. С. 9–18.

16. Аренков И. А., Смирнов С. А. Шарафутдинов Д. Р., Ябурова Д. В. Трансформация системы управления предприятием при переходе к цифровой экономике. *Предпринимательство*. 2018. Т. 19. № 5. С. 1710–1723.

17. Арєф'єва О. В., Кузенко Т. Б. Планування економічної безпеки підприємств. К. : Вид-во Європ. ун-ту, 2004. 170 с.

18. Арістова І. В. Державна інформаційна політика та її реалізація в діяльності ОВС України : організаційно-правові засади : дис. ... д-ра юрид. наук : 12.00.07 / Нац. ін-т внутр. справ. Х., 2002. 408 с.

19. Артемов А. В. Информационная безопасность. Курс лекций. М. : Академия безопасности и выживания, 2014. 161 с.

20. Афанасьев В. Г. Социальная информация и управление обществом. М. : Наука, 1975. 316 с.

21. Бажал Ю. Інформаційна економіка. URL: http://www.ekmair.ukma.kiev.ua/bitstream/123456789/2430/1/Bazhal_Informatsiy_na_ekonomika.pdf.

22. Балабіна В. В. Нарис теорії і практики інформаційно-психологічних операцій. К. : ВІТІ НТУУ«КПІ», 2006. 178 с.

23. Баранов Н. Понятийный аппарат информационной безопасности. 2018. URL: <https://www.nicbar.ru/politology/study/56-kurs-informatsionnaya-bezopasnost-v-mezhdunarodnykh-otnosheniyakh/582-tema-2-ponyatijnyj-apparat-informatsionnoj-bezopasnosti>.

24. Бех В. П., Бех Ю. В. На порозі сингулярності : планетарна спільнота

у вирі Всесвіту. К. : Леся, 2014. 220 с.

25. Богуш В., Юдін О. Інформаційна безпека держави / гол. ред. Ю. Шпак. К. : «МК-Прес», 2005. 432 с.

26. Борецька Н., Петренко Л. Парадигма розвитку цифрової економіки в Україні. *Проблеми інтеграції освіти, науки та бізнесу в умовах глобалізації*: матеріали Міжнародної науково-практичної конференції, 4 жовтня 2019 р. К. : КНУТД, 2019. С. 93–94.

27. Борисов М. А., Роман О. А. Основы организационно-правовой защиты информации : учеб. пособ. М. : Книжный дом «ЛИБРОКОМ», 2012. 208 с.

28. Бразевич Д. С., Герасимова А. Ю., Заварицкая О. В. Трансформация менеджмента как результат воздействия новых информационных технологий на современное общество и экономику. *Научный журнал НИУ ИТМО. Серия «Экономика и экологический менеджмент»*. 2015. № 2. С. 278–289.

29. Брижко В. М., Гавловський В. Д., Калюжний Р. А., Попович В. М., Цимбалюк В. С. Вступ до інформаційної культури та інформаційного права. Науково-дослідний центр правової інформатики Академії правових наук України. Ужгород : ІВА, 2003. 240 с.

30. Буряк В. В. Механізм управління інформаційними ресурсами промислових підприємств : автореф. дис. на здобуття наук. ступеня канд. екон. наук : 08.06.01 / Хмельницький, 2006. 22 с.

31. Бутинець Ф. Ф., Давидюк Т. В., Євдокимов В. В., Легенчук С. В. Інформаційні системи і технології в обліку : підруч. 3-є вид., перероб. і доп. Житомир : ПП «Рута», 2007. 467 с.

32. Варлатая С. К., Файзенгер А. А., Тимофеева А. И. Определение уязвимостей информационных систем как способ снижения угрозы. *Актуальные вопросы технических наук в современных условиях* : сб. науч. труд. по итогам Международной научно-практической конференции. № 2. Санкт-Петербург, 2015. 231 с.

33. Веретюк С. М., Пілінський В. В. Визначення пріоритетних напрямків розвитку цифрової економіки в Україні. *Наукові записки Українського науково-дослідного інституту зв'язку*. 2016. № 2. С. 51–58.

34. Войнаренко М. П., Скоробогата Л. В. Мережеві інструменти капіталізації інформаційно-інтелектуального потенціалу та інновацій. *Вісник Хмельницького національного університету. Економічні науки*. 2015. № 3. Т. 3. С. 18–24.

35. Войнаренко М. П., Рзаєв Г. І., Рзаєва Т. Г. Інформаційна безпека підприємства у динамічному ринковому середовищі. *Вісник Хмельницького національного університету*. 2014. № 1. С. 59–63.

36. Волох О. К. Поняття і складові інформаційно-комунікаційної

інфраструктури. *Науковий вісник Ужгородського національного університету*. 2014. Вип. 29. Ч. 2, т. 4 / 2. С. 29–32.

37. Волошина Н. М. Поняття «безпека інформації» та «інформаційна безпека» в сучасному науковому просторі. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2010. № 2 (8). С. 53–56.

38. Воробьев А., Тчаро Н. Цифровизация нефтяной отрасли Казахстана. *Проблемы недропользования*. 2018. № 1. С. 66–75.

39. Галатенко В. А. Основы информационной безопасности. М., 2004. 264 с.

40. Гафіяк А. М., Фінагіна О. В. Методологічні основи розвитку інформаційних систем та технологій на підприємстві. *Економіка і регіон*. 2010. № 3. С. 111–114.

41. Геець В. М., Мазаракі А. А. Пріоритети національного економічного розвитку в контексті глобалізаційних викликів : монографія у 2 ч. К. : Київ. нац. торг.-екон. ун-т, 2008. Ч.1. 389 с.

42. Голіков І. В. Сутність та еволюція поняття економічна безпека. *Проблеми економіки*. 2014. № 1. С. 309–314.

43. Горбатюк О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть. *Вісник Київського університету імені Т. Шевченка : Міжнародні відносини*. 1999. Вип. 14. С. 46–48.

44. Горбулін В. П., Додоно О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. К. : Інтертехнологія, 2009. 164 с.

45. Гусева И. Б. Экономические стимулы повышения эффективности продукции с использованием инструментов цифровой экономики. *Экономика и жизнь*. 2018. № 11 (9727). URL: <https://www.eg-online.ru/article/369172/>

46. Данільян О. Г., Дзьобань О. П., Панов М. І. Національна безпека України: сутність, структура та напрямки реалізації. Х. : «ФОЛІО», 2002. 296 с.

47. Дєєва Н. Е., Делейчук В. В. Механізми залучення інвестицій емітентами в умовах розвитку цифрової економіки. Київ: Молодий вчений. 2018, 670 с.

48. Джумалиева Е. Р. Информационная компетентность как составляющая профессионализма будущих специалистов в области информационной безопасности и защиты информации МНКО. 2013. № 5. С. 7–9.

49. Діброва О. В. Інформаційна безпека наукоємного сектору як фактор розвитку національної економіки. *Формування ринкових відносин в Україні*. 2017. № 12. С. 19–23.

50. Дмитриевский А. Н. Цифровое нефтегазовое производство. *Нефть. Газ. Инновации*. 2017. № 5. С. 58–61.

51. Добрынин А. П., Черных К. Ю., Куприяновский В. П., Куприяновский П. В., Синягов С. А. Цифровая экономика – различные пути к эффективному применению технологий. *International Journal of Open Information Technologies*. 2016. № 4. С.4–11.

52. Довгань О. Д. Сучасна інформаційна інфраструктура України і основні завдання щодо її захисту. *Юридична наука*. 2015. № 7. С. 64–73.

53. Домарев В. В. Безопасность информационных технологий. Системный подход. К. : ООО ТИД Диа Софт, 2004. 992 с.

54. Дорофеев А. В., Марков А. С. Менеджмент информационной безопасности: основные концепции. *Вопросы кибербезопасности*. 2014. № 1 (2). С. 67–73.

55. Дятлов С. А. Принципы информационного общества. 2013. URL: <http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/34a0170934d95e29c32569e5004d6643>

56. Дячков Д. В. Інформаційні технології в сфері соціального обслуговування. *Сучасні інформаційно-телекомунікаційні технології* : матер. Междун. науч.-технич. конф., 17–20 листопада 2015 р. К. С. 183–184.

57. Дячков Д. В. Перспективи інформатизації соціо-еколого-економічних програм концепції сталого розвитку. *Устойчивое развитие экономики: состояние, проблемы, перспективы* : сб. труд. X Междун. научно-практ. конф., 04 апреля 2016 г. Пинск : ПолесГУ, 2016. С. 34–36.

58. Дячков Д. В. Принципи формування освітнього віртуального простору ВНЗ на основі освітніх нанотехнологій. *Управління соціально-економічним розвитком держави, регіону, підприємства* : матер. II Міжнар. наук.-практ. інтернет-конф., 01 листопада – 01 грудня 2014 р. Полтава : ПолтНТУ, 2014. С. 556–558.

59. Дячков Д. В. Теоретичні основи дослідження сутності інформаційної безпеки. *Наукові праці Полтавської державної аграрної академії*. Полтава : ПДАА, 2016. Вип. 2 (13). С. 110–116.

60. Дячков Д. В. Формування моделі інформаційної безпеки. *Причорноморські економічні студії*: науковий журнал. О. : ПУ «Причорноморський науково-дослідний інститут економіки та інновацій», 2017. С. 263–267.

61. Дячков Д. В., Борщ К. О. Дуальність процесного підходу в адміністративному менеджменті. *Управління соціально-економічним розвитком держави, регіону, підприємства* : матер. II Міжнар. наук.-практ. інтернет-конф., 01 листопада – 01 грудня 2014 р. Полтава : ПолтНТУ, 2014. С. 53–55.

62. Дячков Д. В., Кіт В. В. Сутність та роль інформаційної безпеки підприємства в умовах ринку. *Розвиток агропродовольчого ринку в умовах*

глобалізації економіки : матер. III Всеукр. наук.-практ. конфер., 30 листопада 2017 р. Полтава : ПДАА, 2017. С. 123–124.

63. Дячков Д. В., Малоосвітня Т. С., Потапенко М. М. Плата за знання як новітня форма оплати праці людського капіталу. *Управління соціально-економічним розвитком держави, регіону, підприємства* : матер. II Міжнар. наук.-практ. інтернет-конф., 01 листопада – 01 грудня 2014 р. Полтава : ПолтНТУ, 2014. С. 464–466.

64. Дячков Д. В., Навагіна А. М., Рогова В. В. Озеленення інформаційних систем і технологій управління. *Управління соціально-економічним розвитком держави, регіону, підприємства* : матер. II Міжнар. наук.-практ. інтернет-конф., 01 листопада – 01 грудня 2014 р. Полтава : ПолтНТУ, 2014. С. 466–468.

65. Дячков Д. В., Очнев А. О. Інформаційні війни – як засіб управління суспільною свідомістю. *Управління соціально-економічним розвитком держави, регіону, підприємства*: матер. II Міжнар. наук.-практ. Інтернет-конф., 01 листопада – 01 грудня 2014 р. Полтава : ПолтНТУ, 2014. С. 462–464.

66. Дячков Д. В., Сутуга У. В., Якимчук Н. О. Хмарні технології в управлінні. *Управління соціально-економічним розвитком держави, регіону, підприємства* : матер. II Міжнар. наук.-практ. інтернет-конф., 01 листопада – 01 грудня 2014 р. Полтава : ПолтНТУ, 2014. С. 468–470.

67. Дячков Д. В., Фастівець Д. С. Проблеми цифрової нерівності суспільства. *Управління соціально-економічним розвитком держави, регіону, підприємства* : матер. II Міжнар. наук.-практ. інтернет-конф., 01 листопада – 01 грудня 2014 р. Полтава : ПолтНТУ, 2014. С. 470–472.

68. Дячков Д. В., Хомович В. В. Реформування податкової системи України на шляху до євроінтеграції в умовах глобальних викликів. *Проблеми інформаційно-аналітичного забезпечення управління економічною безпекою підприємства, регіону, країни* : матер. Міжнар. наук.-практ. інтернет-конф., 19 травня 2016 р. Ч. 1. Полтава : ПолтНТУ, 2016. С. 41–42.

69. Дячков Д. В., Черниш І. В., Потапук І. П. Особливості забезпечення економічної безпеки в контексті інформатизації соціально-економічних відносин. *Менеджмент у XXI сторіччі: методологія і практика* : монографія / колектив авторів за ред. д-ра екон. наук І. А. Маркіної. Полтава : В-во «Сімон», 2015. С. 160–174.

70. Дячков Д. В. Особливості впровадження стандартів інформаційної безпеки на вітчизняних підприємствах. *Економічний розвиток : теорія, методологія, управління* : матер. IV Міжнарод. наук.-практич. конференції. Будапешт-Прага-Київ, 2016. С. 104–112.

71. Дячков Д. В. Структурно-функціональні параметри інформаційної

безпеки. *Менеджмент XXI століття : глобалізаційні виклики* : колективна монографія / за ред. І. А. Маркіної. Полтава : В-во «Сімон», 2017. С. 585–595.

72. Евтянова Д. В., Тиранова М. В. Цифровая экономика как механизм эффективной экологической и экономической политики. *Наукоедение*. 2017. Т. 9. № 6. URL: <https://naukovedenie.ru/PDF/79EVN617.pdf>

73. Ефимушкин В. А., Ледовских Т. В., Щербакова Е. Н. Инфокоммуникационное технологическое пространство цифровой экономики. *T-Com – Телекоммуникации и Транспорт*. 2017. № 11 (5), С. 15–20.

74. Жаліло Я. А. До формування категоріального апарату науки про економічну безпеку. *Стратегічна панорама*. 2004. № 3. С. 12–16.

75. Жарков Я. М., Беседіна Л. М. Напрямки зовнішнього інформаційно-психологічного впливу на Україну. *Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка*. 2009. № 19. URL: <http://www.nbuv.gov.ua/portal/natural/znpviknu/2009-19/vip19-21.pdf>.

76. Запорожец О. Н., Лапина-Кратасюк Е. Г. Антропология цифрового города : К вопросу о выборе метода. *Этнографическое обозрение*. 2015. № 4. С. 41-55.

77. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. М. : Горячая линия Телеком, 2000. 452 с.

78. Игнашова Л. В. Анализ угроз информационной безопасности и методы их предотвращения. URL: http://e-lib.kazntu.kz/sites/default/files/articles/21_ignashova_2009_6.pdf.

79. Ищейнов В. Я., Чудинов С. М. Модель безопасности конфиденциальной информации в информационной системе. *Научные ведомости Белгородского государственного университета. Серия : Экономика. Информатика*. 2012. № 13-1 (132). URL: <http://cyberleninka.ru/article/n/model-bezopasnosti-konfidentsialnoy-informatsii-v-informatsionnoy-sisteme-1>

80. Иванова О. М. Інформаційні потоки у системі управління персоналом підприємства. *Економіка, організація і управління підприємством. Науковий вісник Полтавського університету економіки і торгівлі*. 2011. № 4 (49). С. 188–191.

81. Калюжний Р., Говловський В., Цимбалюк В., Гузалюк М. Питання концепції реформування інформаційного законодавства України. *Збірник Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. К. : НТУУ «КПІ». 2000. С. 17–21.

82. Карманова Е. В. Технический аспект организации информационной безопасности в системе дистанционного обучения. *Информационная*

безопасность и вопросы профилактики киберэкстремизма среди молодежи : Материалы внутривузовской конференции. 2015. С. 233–238.

83. Карчева Г. Т., Огородня Д. В., Опенька В. А. Цифрова економіка та її вплив на розвиток національної та міжнародної економіки. *Фінансовий простір*. 2017. № 3 (27). С. 13–21.

84. Кешелава А. В., Буданов В. Г., Румянцев В. Ю. Введение в «цифровую» экономику / под общ. ред. А. В. Кешелава; гл. «цифр.» конс. И. А. Зимненко. ВНИИГеосистем, 2017. 28 с.

85. Киселева И. А., Исканджан С. О. Информационные риски: методы оценки и анализа. *ИТ-портал*. 2017. № 2 (14). URL: <http://itportal.ru/science/economy/informatsionnye-riski-metody-otsenk/>

86. Кіт Л. З. Еволюція мережевої економіки. *Вісник Хмельницького національного університету. Економічні науки*. 2014. № 3. Т. 2. С. 187–194.

87. Коваленко Б. Б., Гусейнова И. В., Гусарова Т. И. Влияние цифровизации экономики на методологию управления проектами. *Научный журнал НИУ ИТМО. Серия Экономика и экологический менеджмент*. 2019. № 2. С. 135–144.

88. Ковтун С. В. Інформаційна безпека : підруч. Харків : Вид. ХНЕУ, 2009. 368 с.

89. Коженювскі Л. Управління безпекою. *Актуальні проблеми економіки*. 2004. №1 (31). С. 147-154.

90. Колодюк А. В. Інформаційне суспільство. Шлях України. Бібліотека інформаційного суспільства. К. : Фонд «Інформаційне Суспільство України», 2004. 309 с.

91. Коляденко С. В. Цифрова економіка: передумови та етапи становлення в Україні і у світі. *Економіка. Фінанси. Менеджмент*. 2016. № 6. С. 105–112.

92. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України : монографія. Одеса : Юридична література, 2003. 472 с.

93. Косогов О. М. Підхід до побудови державної системи протидії інформаційним загрозам в особливий період. *Збірник наукових праць Харківського університету Повітряних Сил*. 2015. Вип. 4. С. 40–43.

94. Косянчук Т. Ф., Лук'янова В. В., Майорова Н. І., Швид В. В. Економічна діагностика : навч. посіб. Львів : В-во «Новий світ-2000», 2007. 452 с.

95. Крихтіна Є. І. Соціальна політика та економічна безпека. Донецьк : Каштан, 2004. 335 с.

96. Кунцман А. А. Специфика адаптации современных компаний к условиям цифровой экономики. *Инновации*. 2017. № 9. С. 14–21.

97. Курмаев П. Ю. Направления формирования модели электронного

управления социально-экономическим развитием. *Сборник научных трудов SWorld*. 2013. Вып. 3. Том 38. Иваново : МАРКОВА АД. С. 3–5.

98. Легомінова С. В. Теоретичні засади інформаційної безпеки підприємства. *Економіка. Менеджмент. Бізнес*. 2015. № 3 (13). С. 87–92.

99. Левченко Є. Г., Демчишин М. В., Рабчун А. О. Математичні моделі економічного менеджменту інформаційної безпеки. *Системні дослідження та інформаційні технології*. 2011. № 4. С. 88–96.

100. Лемещенко П., Шумских Е. Информационная экономика: мировые тенденции и специфика развития в Республике Беларусь. *Сборник : Научные труды Донецкого национального технического университета. Серия экономика*. Донецк, 2014. № 31. С. 154–163.

101. Литвиненко О. Інформація і безпека. Нова політика. 1998. № 1. С. 47–49.

102. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. К. : КНТ, 2006. 280 с.

103. Ляшенко В. І., Вишневський О. С. Цифрова модернізація економіки України як можливість проривного розвитку : монографія. Київ, 2018. 252 с.

104. Макаrenchенко М. А., Павлова О. Н. Особенности трансформации классического командообразования в виртуальное в условиях цифровизации. *Научно-технические ведомости СПбГПУ. Экономические науки*. 2018. Т. 11. № 1. С. 39–53.

105. Мамедова К. А. Основные принципы обеспечения информационной безопасности страны. *Информационная безопасность регионов*. 2016. №1 (22). С.16–20.

106. Маркіна І. А., Дячков Д. В. Управління безпекою в бізнес-середовищі : навч. посіб. Полтава : Вид-во «Сімон», 2017. 205 с.

107. Маркіна І. А., Дячков Д. В., Сьомич М. І. Організаційно-економічний механізм управління інформаційним потенціалом підприємства. *Економічний форум*. Луцьк : РВВ Луцького НТУ, 2016. № 2. С. 175–181.

108. Маркіна І. А., Зось-Кіор М. В., Дячков Д. В. Сутність глобальної деформації в контексті управління національними ресурсами. *Теорія та практика менеджменту* : матер. Міжнар. наук.-практ. конф., 19 травня 2016 р. Т. 33. Луцьк, 2016. С. 142–144.

109. Маруховський О. Формування концепції суспільства знань в працях Ф. Махлупа, Ф. Бекона та В. І. Вернадського. *Історико-політичні проблеми сучасного світу*. 2011. Т. 23-24. С. 60–64.

110. Марущак А. Визначення поняття «доступ до інформації». *Правова інформатика*. 2006. № 3 (11). С. 69–74.

111. Марущак А. І. Інформаційно-правові напрями дослідження проблем

інформаційної безпеки. *Державна безпека України*. 2011. № 21. С. 92–95.

112. Маслянюк П. П., Лісов П. М. Інформаційно-комунікаційні системи та технології обробки інформаційних ресурсів. *Науковий вісник Кременчуцького університету економіки, інформаційних технологій і управління*. 2007. № 1-2. С. 164–168.

113. Мельник В. Концептуалізація цифрового менеджменту як реалізація і вираження креативності освіти та особистості. *Нова парадигма. Філософія. Соціологія : журнал наукових праць*. Київ: Вид-во НПУ ім. М. П. Драгоманова, 2018. Вип. 134. С. 108–122.

114. Мишель М. Управление информационными рисками. *Финансовый директор*. 2007. № 9. С. 64–68.

115. Мороз Н. С. Сущность информации в контексте общих принципов информационной безопасности. *Вісник Національного університету «Львівська політехніка»*. Серія: Юридичні науки. 2016. № 845 (10). С. 137–142.

116. Мочерний С. В. Економічна енциклопедія : у трьох томах. Т. 1. К. : Вид. центр «Академія», 2000. 864 с.

117. Мочерний С. В. Устинко О. А., Чоботар С. І. Основи підприємницької діяльності : посіб. К. : Вид. центр «Академія», 2001. 280 с.

118. Муханова А. А., Ревнивых А. В., Федотов А. М. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах. *Вестн. Новосиб. гос. ун-та. Серия : Информационные технологии*. 2013. Т. 11. Вып. 2. С. 55–72.

119. Олизарович Е. В., Бражук А. И. Концептуальные основы анализа моделей информационной безопасности облачных систем класса «Инфраструктура как услуга». *Доклады Белорусского государственного университета информатики и радиоэлектроники*. 2019. № 6 (124). С. 12–19.

120. Олійник О. В. Суб'єкти забезпечення інформаційної безпеки невідомого характеру. *Наукові записки інституту законодавства Верховної Ради України*. 2013. № 1 (16). URL: [http://www.nbuv.gov.ua/old_jrn/Soc_Gum /Nzizvru /2013_1/p16_21.html](http://www.nbuv.gov.ua/old_jrn/Soc_Gum/Nzizvru /2013_1/p16_21.html).

121. Панарин И. Технология информационной войны. М. : КСП+, 2003. 320 с.

122. Партико З. В. Теорія масової інформації та комунікації. Л. : Афіша, 2008. 290 с.

123. Плєскач В. Л. Затонацька Т. Г. Електронна комерція. К. : Знання, 2007. 535 с.

124. Пономаренко В. С., Бутова Р. К., Журавльова І. В., Назарова Г. Н., Павленко Л. А., Пушкар О. І. Інформаційні системи і технології в економіці. К. : ВЦ «Академія», 2002. 544 с.

125. Пономаренко В. С., Журавльова І. В., Туманов В. В. Основи захисту інформації : навч. посіб. Харків : Вид. ХДЕУ, 2003. 176 с.

126. Попрозман О. І. Формування взаємозв'язків та взаємодія функцій менеджменту з метою удосконалення роботи підприємств. *Формування ринкових відносин в Україні*. 2018. № 1. С. 93–100.

127. Приймак Ю. Ю. Національні інформаційні ресурси – джерело державних інформаційних продуктів та послуг. Державне управління: теорія та практика. 2009. № 2. URL: http://www.academy.gov.ua/ej/ej10/doc_pdf/Priymak.pdf

128. Пунченко Н. О. Информационные технологии, их место в структуре конвергентных технологий и информатизации. *Гуманітарний вісник Запорізької державної інженерної академії*. 2016. № 64. С. 168–177.

129. Пучков О. О. Інформаційна безпека у контексті сьогоденних реалій : філософський аспект. *Гуманітарний вісник ЗДІА*. 2015. № 60. С. 239–245.

130. Пушкар М. С. Розробка систем обліку : навч. посіб. Тернопіль : Карт-бланш, 2003. 198 с.

131. Радько Н. М., Скобелев И. О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. М. : Радио Софт, 2010. 254 с.

132. Роджерс Д. Л. Цифровая трансформация М. : Издательская группа «Точка», 2017. 344 с.

133. Рященко В. П., Дячков Д. В. Підходи до визначення економічної безпеки суб'єктів господарювання в умовах інтеграційних процесів. *Проблеми інформаційно-аналітичного забезпечення управління економічною безпекою підприємства, регіону, країни* : матер. Міжнар. наук.-практ. інтернет-конф., 19 травня 2016 р. Ч. 1. Полтава : ПолтНТУ, 2016. С. 17–20.

134. Сагынбекова А. С. Цифровая экономика : понятие, перспективы, тенденции развития в России. *Международный научно-технический журнал «Теория. Практика. Инновации»*. 2018. URL: <http://www.tpinauka.ru/2018/04/Sagynbekova.pdf>

135. Садердинов А. А., Трайнев А. А., Федулов В. А. Информационная безопасность предприятия : уч. пособ. М. : Дашков и К, 2004. 336 с.

136. Семёнов М. С. Методика оценки эффективности комплексной защиты информации на основе стандарта «критерии оценки безопасности информационных технологий». *Студенческий: электрон. научн. журн*. 2019. № 14 (58). URL: <https://sibac.info/journal/student/58/137554>.

137. Семячков К. А. Цифровая экономика и ее роль в управлении современными социально-экономическими отношениями. *Современные технологии управления*. 2017. № 8 (80). URL: <http://sovman.ru/article/8001/>

138. Ситник В. Ф., Писаревська Т. А., Єрьоміна Н. В., Краєва О. С.

Основи інформаційних систем : навч. посіб. К. : КНЕУ, 2001. 420 с.

139. Смачило Т. В., Кахній М. І. Теоретичні засади управління системою інформаційної безпеки підприємства. *Молодий вчений*. 2016. № 12.1 (40). С. 969–972.

140. Смелов В. В. Методологические основы информационной безопасности автоматизированных систем. *Труды БГТУ. Серия: Физико-математические науки и информатика*. 2009. № 6. URL: <http://cyberleninka.ru/article/n/metodologicheskie-osnovy-informatsionnoy-bezopasnostiavtomatizirovannyh-sistem>

141. Смородникова Е. Модели построения отношений между службами информационной безопасности и ИТ. *Securitylab*. 2007. URL: <https://www.securitylab.ru/analytics/293391.php>

142. Сороківська О. А., Гевко В. Л. Інформаційна безпека підприємства: нові загрози та перспективи. *Вісник Хмельницького національного університету : економічні науки*. 2010. № 2. Т. 2. С. 32–35.

143. Стеців Л. П. Теоретико-методичні основи побудови ефективної системи фінансового менеджменту підприємства. *Наукові записки*. 2013. № 4 (45). С. 39–45.

144. Стрельцов А. А. Обеспечение информационной безопасности России. Теоретические и методологические основы. М. : МЦНМО, 2002. 336 с.

145. Сюттюренко О. В. Цифровая среда : тренды и риски развития. *НТИ*. 2015. № 2. С. 1–7.

146. Талалаєв В. О., Дячков Д. В. Онтологічні основи формування логіко-понятійної моделі предметної області «управління інформаційним потенціалом соціально-економічної системи». *Інноваційна економіка*. 2011. № 7 (26) С. 14–19.

147. Танцюра М. Ю. Забезпечення ефективності системи інформаційного забезпечення підприємства (на прикладі туристичних підприємств АР Крим) : автореф. дис. на здобуття наук. ступеня канд. екон. наук : 08.00.04. Сімферополь, 2012. 21 с.

148. Тардаскін М. Ф., Захарченко М. В., Кононович В. Г. Технічний захист комерційної таємниці підприємства зв'язку : навч. посіб. Одеса : ОНАЗ, 2002. 76 с.

149. Тер-Акопов А. А. Безопасность человека. М. : Изд-во МНЭПУ. 1998. 256 с.

150. Теренин А. А. Проектирование экономически эффективной системы информационной безопасности. *Защита информации. Инсайд*. 2005. № 1. С. 23-25.

151. Ткач Ю. М. Окремі аспекти інформаційно-аналітичної діяльності у

процесі навчання математики фахівців з інформаційної безпеки. *Дидактика математики : проблеми і дослідження : міжнародний збірник робіт*. 2013. Вип. 40. С. 151-158.

152. Тусков М. В., Семёнов В. В. Проблемы обеспечения информационной безопасности. *Электронный научный журнал «Международный студенческий научный вестник»*. URL: <https://science forum. ru/2018/article/201800067>

153. Тюрин В. Матрица управленческих решений, или Как пробежать по лезвию бритвы к цифровой экономике. URL: <https://www.itweek.ru/idea/article/detail.php?ID=196744>

154. Урсул А. Д. Информационная стратегия и безопасность в концепции устойчивого развития. *Научно-техническая информация. Серия : Организация и методика информационной работы*. 1996. № 1. С. 1-9.

155. Уткин А. И. Мировой порядок XXI века. М. : Алгоритм, 2001. 478 с.

156. Файоль А., Эмерсон Г., Тэйлор Ф., Форд Г. Управление – это наука и искусство. Москва : Республика, 1992. 351 с.

157. Фенюк М. В. Аналіз недоліків систем автоматизованого захисту інформації та методів біометричної автентифікації, які в них використовуються. *Математические машины и системы*. 2012. № 1 (3). С. 116–123.

158. Феоктистов Г. Г. Информационная безопасность общества. *Социальнополитический журнал*. 1996. № 5. С. 211–212.

159. Фисун Ю. А. Проблемы внутренней безопасности России в XXI веке. М., 2001. 234 с.

160. Фіщук В. Цифрова економіка – це реально. НВ Бізнес. 2017. URL: <https://biz.nv.ua/ukr/experts/fichuk/tsifrova-ekonomika-tse-realno-1001102.html>.

161. Фурашев В. М. Сутність та визначення понять «інформаційна безпека» і «безпека інформації». *Правова інформатика*. 2012. № 2 (34). URL: <http://ippi.org.ua/sites/default/files/12fvmbbi.pdf>

162. Харченко В. Ф. Вплив інформаційних потоків на витрати логістичної системи. *Вісник Донецької академії автомобільного транспорту*. 2011. № 1. С. 23–26.

163. Хміль Ф. І. Функції менеджменту «реалізація» та «контроль»: Лекція для студентів вищих та середніх спеціальних навчальних закладів. Київ : Укоопспілка, 1992. 29 с.

164. Хміль Ф. І. Функції менеджменту «цілевстановлення» та «планування»: лекція. Київ : Укоопспілка, 1992. 22 с.

165. Хомяков В. І. Функції менеджменту: планування, організація, мотивація, контроль. Менеджмент підприємства : навч. посібник. 2-ге вид., перероб. і доп. Київ : Кондор, 2005. С. 91–153.

166. Хоффман Л. Дж. Современные методы защиты информации; пер. с

англ. М. : Советское радио, 1980. 57 с.

167. Цигилик І. І., Бибик Я. Р., Ємбрик М. Я., Паращич В. Ф. Економіка підприємства (в питаннях та відповідях). Івано-Франківськ : Вид-во «Полум'я», 2003. 212 с.

168. Цимбалюк В. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації). *Підприємництво, господарство і право*. 2004. № 3. С. 88–91.

169. Цымбалова А. А., Губенко Н. Е. Анализ модели использования ресурсов с точки зрения информационной безопасности. *Информационные управляющие системы и компьютерный мониторинг* : матер. II Всеукр. науч.-технич. конфер. студ., аспид. и молодых ученых. 2011. Донецк, ДонНТУ. С. 292–295.

170. Шелупанов А. А. Основы защиты информации : учеб. пособ. изд. 5-е, перераб. и доп. Томск : В-Спектр, 2011. 244 с.

171. Шемшученко Ю. С. Юридична енциклопедія : в 6 т. К. : Укр. енцикл., 1998. 1999. Т. 2. С. 714.

172. Шеннон К. Работы по теории информации и кибернетики. М. : Иностранная литература, 1963. 830 с.

173. Шкарлет С. М. Еволюція категорії «безпека» в науковому та економічному середовищі. *Формування ринкових відносин*. 2007. № 6. С. 7–12.

174. Шорошев В. В. Нова архітектура системи захисту інформації в комп'ютерних системах від несанкціонованого доступу. *Інформаційна безпека*. 2009. № 2 (2). С. 53.

175. Юдін О. К., Бучик С. С. Концептуальний аналіз уразливості державних інформаційних ресурсів. *Наукоємні технології*. 2013. № 3 (19). С. 299–304.

176. Яковець Е. Н. Основы правового захисту інформації та інтелектуальної власності : навч. посіб. 2-ге вид., доп. і перероб. М. : Юрлитинформ, 2013. 440 с.

177. Яременко О. Ф. Середовище підприємства як чинник небезпеки діяльності суб'єкта господарювання. *Вісник Хмельницького національного університету. Економічні науки*. 2006. № 5. Т. 2. С. 144–150.

178. Ярочкин В. И. Секьюритология – наука о безопасности жизнедеятельности. М. : «Ось-89», 2000. 288 с.

179. Яшина А. М. Современные способы защиты информации и информационная безопасность. *Надежность и качество: труды Международного симпозиума*. 2018. № 2. С. 104–106.

180. Berman S. J. Digital transformation: opportunities to create new business

models. *Strategy and Leadership*. 2012. Vol. 40 (2). P. 16–24.

181. Bishop M. What Is Computer Security? *IEEE Security & Privacy*. 2013. Vol. 1.1. P. 67–69.

182. Brockman J. *Digerati: encounters with the cyber elite*. Publisher: Hardwired; 1st ed edition, 1996. 354 p.

183. Carey-Smith M., May L. Information security and civil society organizations. *OAI (Recent advances in security technology)*. 2007. P. 314–327.

184. Connors M. *The Race to the Intelligent State: Towards the Global Information Economy of 2005*. Oxford, UK, Cambridge, Mass. : Blackwell Business. 2005. 252 p.

185. Croteau D., Hoynes W. *Media society : industries, images and audiences*. Pine Forge Press. 2003. 322 p.

186. De Silva S., Gordon A. From cyber to hybrid: mobile technologies as interfaces of hybrid spaces. *Space & Culture*. 2006. Vol. 9 (3). P. 261–278.

187. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary General. Fifty-six session. 3 July, 2001. United Nations. A/56/164.

188. Diachkov D. Information war as an instrument of management by public consciousness. *Information technologies and management : the 13th International scientific conference*, 16-17 april 2015. Riga, Latvia, 2015. P. 186.

189. Diachkov D. Peculiarities of classification of information security threats for different subjects of information relations : collective monograph. *Management of the 21st century: globalization challenges*. Nemoros s.r.o., Prague, 2018. P. 289–296.

190. Diachkov D. Threats to information security: monitoring aspect. *Management of the 21st century : globalization challenges*. Issue 2 : collective monograph. Prague: Nemoros s.p.o., 2019. P. 60–65.

191. Kane G., Palmer D., Philips N., Kiron D., Buckley N. *Strategy, not technology, drives digital transformation. Becoming a digitally mature enterprise*. Cambridge, MA : MIT Sloan Management School; Deloitte. 2015. 630 p.

192. Lepeyko T., Shcherbak A. Determining factors to ensure the effective formation of the information process in the industrial enterprise management. *Development Management*. 2018. №4(4). P. 88–97.

193. Machlup F., Princeton N. *The production and distribution of knowledge in the United States*. Princeton University Press. 1962. 416 p.

194. Manovich L. Media visualization: Visual techniques for exploring large media collections. *Media studies futures*. 2011. URL: <http://manovich.net/content/old/03-articles/66-article-2011/66-article-2011.pdf>

195. Manovich L. *Trending: the promises and the challenges of big social*

data. *Debates in digital humanities*. 2011. URL: <http://manovich.net/content/04-projects/067-trending-the-promises-and-the-challenges-of-big-social-data/64-article-2011.pdf>

196. Manovich L. What is visualization? Visual studies, an overview of content analysis. *Practical assessment*. 2011. Vol. 26. no.1. P. 36–49.

197. Markina I., Diachkov D., Digital management as a tool of the world's most advanced technologies management. *Modern Science – Moderni veda*. Praha. Ceska republika, Nemoros. 2017. № 4. P. 47–56.

198. Markina I., Diachkov D. The main features of information warfare in the modern business sector. *Scientific letters of academic society of Michal Baludansky*. 2016. № 4 (2). P. 82–84.

199. Markina I., Diachkov D. Trends of the development of the digital economy in Ukraine. *Вісник Сумського національного аграрного університету*. 2018. 6 (76). С. 3–7.

200. Mesenbourg T. L. Measuring the Digital Economy. US Bureau of the Census, Suitland, MD. 2001. URL: <https://www.census.gov/content/dam/Census/library/workingpapers/2001/econ/umdigital.pdf>.

201. Negroponte N. Being digital. Printed and bound in Great Britain by Mackays of Chatham PLC, Chatham, Kent. 1995. 252 p.

202. Paulsen C., Byers R. Glossary of key information security terms. 2019. *NISTIR 7298*. Rev. 3. URL: <https://csrc.nist.gov/glossary?index=I>

203. Porat M. U. Porat global implications of information society. *Journal of communication*. 1978. Vol. 28 (1). P. 70–80.

204. Rainie L. Wellman B. Networked : the new social operating system. Cambridge, MA : MIT Press. 2012. 358 p.

205. Safire W. On Language; ruling the jet set. *The New York Times*. 2008. URL: <http://www.nytimes.com/2008/01/24/magazine/on-language-ruling-the-jet-set.html>.

206. Tapscott D. The digital economy: promise and peril in the age of networked intelligence. McGraw-Hill. 1995. 342 p.

207. Tugui A. Calm technologies as the future goal of information technologies. *Encyclopedia of multimedia technology and networking*. 2009, P. 7.

208. Tugui A. Meta-digital accounting in the context of cloud computing. *Encyclopedia of information science and technology, third edition*, 2015. URL: <https://www.igi-global.com/book/encyclopedia-information-science-technology-third/76156>

209. ГОСТ Р 52292-2004. Информационная технология : Термины и определения. URL: http://gostisnip.ru/dokumenty/gosty/prochie/gost_r_52292-2004/

210. Information technology – Security techniques – Information security

management systems. Overview and vocabulary : ISO / IEC 27000:2009. URL: <https://www.iso.org/standard/41933.html>

211. Большая российская энциклопедия. Информационная безопасность / В. Ф. Прокофьев URL: https://bigenc.ru/military_science/text /2015869

212. Вікіпедія: Інформаційна безпека. URL: https://uk.wikipedia.org/wiki/Інформаційна_безпека

213. Закон Мерфі для програмістів. URL: <http://poklykannja.com.ua /merfi>

214. Конкурент: інформаційне агентство. Як змінювалися носії інформації – від перфокарт до хмарних сховищ. 2019. URL: <https:// konkurent.in.ua/publication/36866/yak-zminuvalisya-nosii-informatsii-vid-perfokart-do-hmarnih-shovisch/>

215. Структура и модель обеспечения информационной безопасности. URL: <https://cyberpedia.su/11x2dd3.html>

216. Технопедия словарь. URL: <https://www.techopedia.com/definition /604/digitaldefinition>

217. Цифрова адженда України – 2020 («Цифровий порядок денний» – 2020) Концептуальні засади (версія 1.0) Першочергові сфери, ініціативи, проекти «цифровізації» України до 2020 року. К. : ГС «Хай-тек офіс Україна», 2016. 90 с.

218. Digital economy: as specialists understand this term. RIA News-2017. URL: <https://ria.ru/science/20170616/1496663946.html>

219. Information security. DOD. Dictionary of Military Terms. URL: http://www.dtic.mil/doctrine/dod_dictionary/data/i/10211.html.

220. LETA : блог компании. URL: <https://letablog.livejournal.com>.

221. Searchinform information security. 2018. Information security Solutions of «SorchInform». URL: <https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti>

222. Special reports «Digital in 2016». We are social. URL: <http://wearesocial.com/uk/specialreports/digital-in-2016>.

223. The Digital Advantage: How digital leaders outperform their peers in every industry. *Gapgemini consulting*. URL: https://www.capgemini.com/resource-fileaccess/resource/pdf/The_Digital_Advantage_How_Digital_Leaders_Outperform_their_Peers_in_Every_Industry.pdf

224. The main concepts of information protection and information security. URL: <http://ypn.ru/102/introduction-to-information-protection-and-information-security>

225. VPS.house. Основы информационной безопасности. Часть 1: Виды угроз. URL: https://habr.com/company/vps_house/blog/343110/.

РОЗДІЛ 2

ДІАГНОСТИКА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ АГРОПРОДОВОЛЬЧОЇ СФЕРИ УКРАЇНИ

2.1. Характеристика стану і визначення тенденцій розвитку агропродовольчої сфери України

Шляхи розвитку агропромислового сектору України передбачають збалансовані та взаємозв'язані структурні перебудови усіх його галузей, максимальне впровадження у виробництво найважливіших досягнень науково-технічного прогресу, світового досвіду, найбільш прогресивних форм економіки і організації виробництва на основі першочергового розв'язання актуальних проблем: перерозподіл землі та майна, включаючи поглиблення відносин власності на землю та запровадження механізмів реалізації права на власність; приватизація переробних підприємств; реструктуризація підприємств та форм господарювання; розвиток кооперації; впровадження ринкових методів господарювання – менеджменту та маркетингу; державне регулювання аграрної економіки шляхом ефективнішого використання цінових важелів, фінансово-кредитної і податкової систем; розвиток ринків сільськогосподарської продукції, матеріально-технічних ресурсів та послуг; інтенсифікація і диверсифікація зовнішньоекономічної діяльності тощо. Пріоритетність розвитку агропромислового сектору України і його провідних галузей дає можливість забезпечити населення продовольчими товарами, промисловість – сировиною, а зовнішню торгівлю – експортними товарами.

Зміни в бізнес-моделях під впливом широкого застосування цифрових пристроїв призвели до появи нових технологій, які є основою сучасної економіки, що переважно базуються на горизонтальних взаємодіях (самоорганізації і сингулярності), інноваційному підприємстві (саморозвитку), інформаційному інжинірингу (самовдосконаленні) й автоформалізації економічних процесів. За вказаних умов зазнають трансформації всі галузі економіки України. Не стала винятком і агропродовольча сфера України. Чинником виникнення і постійного посилення уваги до питань аналізу стану агропродовольчої сфери України в умовах цифровізації економіки є трансформаційна криза вітчизняної економіки, яка охопила всі сфери і стала суттєвою перешкодою для забезпечення населення вітчизняною якісною продовольчою продукцією і, відповідно, стабільного розвитку економіки. Тому в сучасних умовах

питання моніторингу та оцінки стану агропродовольчого ринку з метою забезпечення прогнозованого розвитку і регулювання агропромислового сектора економіки розглядаються як один із найважливіших національних пріоритетів, якому необхідна посилена увага вчених. Крім того, дослідження проблем розвитку вітчизняної агропродовольчої сфери у контексті інформатизації та цифровізації соціально-економічних процесів на різних рівнях господарювання не можна визнати вичерпаними [31; 52; 185].

Для моніторингу та аналізу були обрані найважливіші ринкові тенденції розвитку агропродовольчої сфери України.

Перш за все доцільно відмітити негативні тенденції зменшення кількості сільських населених пунктів (табл. 2.1), що протягом 1991–2019 рр. зменшилася на 469 од., а за період 2009–2019 рр. – на 114 од., що є ознакою деградації сільських територій і не сприяє розвитку сільського господарства загалом.

Таблиця 2.1

Кількість адміністративно-територіальних одиниць в Україні (станом на 1 січня) за 1991–2019 рр.* [сформовано на основі 106]

Роки	Райони, од.	Міста, од.		Райони в містах, од.	Селища міського типу, од.	Сільські населені пункти, од.
		всього	у тому числі спеціального статусу, республіканського та обласного значення			
1991	481	436	149	120	925	28845
2009	490	459	179	118	886	28490
2010	490	459	179	118	885	28471
2011	490	459	180	118	885	28457
2012	490	459	180	114	885	28450
2013	490	460	180	111	885	28441
2014	490	460	182	111	885	28397
2015	490	460	184	111	885	28388
2016	490	460	187	111	885	28385
2017	490	460	189	111	885	28377
2018	490	461	189	108	883	28378
2019	490	461	189	108	883	28376

* За даними офіційного вебпорталу Верховної Ради України

Доцільно відзначити, що і чисельність населення України з 1991 р. по 2019 р. зменшилася на 3962695 осіб (або на 23,5 %), а з 2009 р. по 2019 р. – на 1660006 осіб (або на 11,4 %), що підвищило пропорційно рівень урбанізації (табл. 2.2). Зазначені тенденції загрожують розвитку сільського господарства, збільшуючи навантаження на зайнятих у сільському господарстві та демонструючи відсутність трудового резерву на селі. Цей факт обумовлений від’ємним природним приростом населення України в сільській місцевості (Додаток Б), що тільки 2019 р. становив 108 161 осіб, і від’ємним міграційним

приростом у 2018 р. на 10 742 осіб (Додаток В). Водночас у сільському господарстві України задіяна значна кількість фізичних осіб-підприємців (табл. 2.3), тенденція зміни чисельності яких має хвилеподібну динаміку та залежить здебільшого від зовнішніх факторів – переважно кон’юнктурних і податкових. Наприклад, 2018 р. у сільському господарстві України кількість фізичних осіб-підприємців становила 20 943, тобто 30,1 % від усіх суб’єктів господарювання (загалом в економіці – 1 483 716 осіб, або 80,7 %).

Таблиця 2.2

Чисельність наявного населення (станом на 1 січня) України у 1991, 2009–2019 рр. [сформовано на основі 106]

Роки	Осіб			Загальна чисельність населення у відсотках до попереднього року	Питома вага міського населення у загальній чисельності, %
	усе населення	міське	сільське		
1991	51944400	35085200	16859200	100,20	67,54
2009	46143714	31587203	14556511	99,50	68,45
2010	45962947	31524795	14438152	99,60	68,59
2011	45778534	31441649	14336885	99,60	68,68
2012	45633637	31380874	14252763	99,70	68,77
2013	45553047	31378639	14174408	99,80	68,88
2014*	45426249	31336623	14089626	99,70	68,98
2015*	42929298	29673113	13256185	99,70	69,12
2016*	42760516	29584952	13175564	99,60	69,19
2017*	42584542	29482313	13102229	99,60	69,23
2018*	42386403	29370995	13015408	99,50	69,29
2019*	42153201	29256696	12896505	99,40	69,41

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій і Луганській областях

Чисельність зайнятих і найманих працівників суб’єктів господарювання та підприємств за видами економічної діяльності в Україні (Додаток Г) постійно зменшується, зокрема й у сфері сільського господарства, в якому працює 7,0 % усіх найманих працівників суб’єктів господарювання та 8,2 % загальної чисельності найманих працівників. Слід також відмітити тенденцію до збільшення чисельності фізичних осіб-підприємців у сільському господарстві (загалом в економіці 2018 р. їх питома вага становила 15,4 % від загальної кількості суб’єктів господарювання, а в сільському господарстві – 2,5 %).

Окрім зменшення загальної чисельності найманих працівників, зменшилася чисельність працівників в одному господарстві (11,6 осіб 2018 р. порівняно з 14,1 осіб 2010 р.) та на 1 га сільгоспугідь у користуванні як підприємств, так і всіх суб’єктів господарювання (працевзабезпеченість), що пов’язано не стільки із заміною живої праці автоматизацією виробничих процесів, скільки із депопуляцією сільських територій.

Таблиця 2.3

Кількість суб'єктів господарювання, чисельність зайнятих і найманих працівників у суб'єктів господарювання за видами економічної діяльності в Україні протягом 2010–2018 рр., осіб [сформовано на основі 112]

Галузь	Роки	Кількість суб'єктів господарювання з урахуванням банків, од.		Чисельність найманих працівників у суб'єктів господарювання з урахуванням банків, од.		Чисельність зайнятих працівників у суб'єктів господарювання з урахуванням банків, осіб	
		усього	з них фізичні особи-підприємці	усього	з них у фізичних осіб-підприємців	усього	з них у фізичних осіб-підприємців
Усього*	2010	2184105	1805118	9073663	1009420	11000590	2814538
	2011	1701797	1325925	8986914	1045485	10393516	2371410
	2012	1600304	1235192	8861469	1042674	10198733	2277866
	2013	1722251	1328743	8515401	993839	9965076	2322582
	2014 ¹	1932325	1591160	7311607	907020	9008271	2498180
	2015 ¹	1974439	1630878	6589472	659452	8331931	2290330
	2016 ¹	1865631	1559161	6597595	748024	8244025	2307185
	2017 ¹	1805144	1466803	6706198	861313	8271338	2328116
	2018 ¹	1839672	1483716	7088709	1089240	8661298	2572956
Сільське господарство	2010	72697	23637	656527	9250	723390	32887
	2011	56197	16246	645012	11276	664502	27522
	2012	62878	16955	636096	12229	666761	29184
	2013	65238	17412	593341	11104	645224	28516
	2014*	67967	23787	598602	67654	654722	91441
	2015*	70721	25824	510330	7634	563859	33458
	2016*	66837	23478	523898	8929	577807	32407
	2017*	69536	21225	501033	10107	556527	31332
	2018*	69596	20943	493607	12209	549254	33152

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій і Луганській областях

Обсяг реалізованої продукції (товарів, послуг) суб'єктів господарювання за видами економічної діяльності в Україні за 2010–2018 рр. значно збільшився (табл. 2.4). Загалом по економіці України таке зростання становило 174,8 %, зокрема сільського господарства – 428,2 %. При цьому питома вага обсягу реалізованої продукції (товарів, послуг) фізичними особами-підприємцями становила 7,5 % від загального обсягу загалом по економіці, а в сільському господарстві – 2,3 %.

За цей період питома вага обсягу реалізованої продукції (товарів, послуг) сільського господарства збільшилася з 2,6 % 2010 р. до 5,1 % 2018 р. На підставі цього можна відзначити не стільки зростання обсягу реалізації в сільському господарстві, скільки незначні темпи приросту обсягу реалізованої продукції серед інших галузей економіки.

Таблиця 2.4

Обсяг реалізованої продукції (товарів, послуг) суб'єктів господарювання за видами економічної діяльності в Україні за 2010–2018 рр. [сформовано на основі 106; 112]

Галузь	Роки	Обсяг реалізованої продукції (товарів, послуг) суб'єктів господарювання з урахуванням банків, млрд грн	
		усього	з них у фізичних осіб-підприємців
Усього	2010	3692,55	230,42
	2011	4302,63	211,22
	2012	4563,79	256,65
	2013	4437,33	284,24
	2014*	4608,98	289,04
	2015*	5716,43	397,47
	2016*	6877,08	489,20
	2017*	8467,03	604,34
	2018*	10148,85	760,76
Сільське господарство	2010	97,73	2,88
	2011	122,10	3,00
	2012	159,57	3,87
	2013	158,16	4,17
	2014*	210,15	4,88
	2015*	357,38	7,64
	2016*	397,28	8,62
	2017*	447,46	10,02
	2018*	516,25	11,67

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій і Луганській областях

Зростання обсягів виробництва продукції в деякій мірі залежить від ефективності розподілу структури необоротних і оборотних активів суб'єктів аграрного ринку України (табл. 2.5).

Таблиця 2.5

Показники балансу підприємств за видами економічної діяльності в Україні за 2013–2018 рр.* [сформовано на основі 112]

Галузі	Роки	Необоротні активи, млрд грн	Оборотні активи, млрд грн	Власний капітал, млрд грн
Всього по економіці	2013	2639,81	3069,04	1950,37
	2014*	2717,62	3271,95	1480,66
	2015*	3960,15	4108,60	2288,74
	2016*	4212,81	5772,82	2445,80
	2017*	4303,28	5650,82	2458,53
	2018*	4584,32	6285,07	2708,58
Сільське господарство	2013	115,47	193,24	154,80
	2014*	120,61	265,50	162,12
	2015*	168,27	511,53	272,37
	2016*	215,26	1315,00	366,01
	2017*	268,80	634,78	432,84
	2018*	324,82	648,94	479,11

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій і Луганській областях

Загалом по економіці країни необоротні активи становлять 7,1 % від їх вартості на підприємствах, натомість оборотні – 10,3 %.

Простежується закономірність щодо прискореного збільшення оборотних активів підприємств сільського господарства, оскільки вони зберігають частину врожаю для подальшого продажу, а також мають достатньо значні обсяги кормів, ПММ, насіння, ЗЗР, ЗЗТ, враховуючи також те, що частина поголів'я та багаторічні насадження теж є оборотними засобами. В першу чергу, темп їх зростання характеризує вищі врожаї порівняно з попередніми роками.

На сільськогосподарських підприємствах України спостерігаються доволі значні зміни продуктивності праці (табл. 2.6).

Таблиця 2.6

Продуктивність праці на сільськогосподарських підприємствах України протягом 1990–1991, 2009–2018 рр. [сформовано на основі 112]

Роки	На одного зайнятого в сільськогосподарському виробництві, у постійних цінах 2010 р., грн			У відсотках до попереднього року		
	сільськогосподарське виробництво	рослинництво	тваринництво	сільськогосподарське виробництво	рослинництво	тваринництво
1990	50388,5	59554,9	41184,4	...	...	...
1991	42826,6	49187,9	36506,7	85,0	82,6	88,6
2009	131332,0	138741,7	113976,7	103,1	97,4	122,9
2010	132680,4	133603,0	130473,7	101,0	96,3	114,5
2011	165229,0	171142,8	148840,3	124,5	128,1	114,1
2012	159679,0	155543,8	171798,3	96,6	90,9	115,4
2013	201216,9	202220,5	198185,6	126,0	130,0	115,4
2014*	227753,4	228884,7	224105,1	109,1	108,2	111,6
2015*	223309,9	218768,0	237990,0	98,0	95,6	106,2
2016*	275317,8	270863,2	292511,2	123,3	123,8	122,9
2017*	271491,4	260793,7	315503,8	98,6	96,3	107,9
2018*	313627,3	305314,5	348901,4	115,5	117,1	110,6

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій і Луганській областях

Загальний показник продуктивності праці сільськогосподарського виробництва зріс із 2009 р. до 2018 р. на 138,8 %, зокрема в рослинництві – на 120,0 %, в тваринництві – на 206,1 % (щорічний приріст протягом 2009–2018 рр. становив від 3,4 до 26,0 %). В іноземній валюті зазначений показник значно зменшився загалом у сільськогосподарському виробництві на 31,6 %, зокрема в рослинництві – на 37,0 %, в тваринництві – на 12,3 %.

За один місяць 2018 р. один сільгосппрацівник у середньому виробляв продукції на 26 136 грн (у постійних цінах 2010 р.), що пояснюється сировинною спрямованістю сільського господарства та невисоким рівнем

фондоозброєності праці аграрних підприємств, і в підсумку зумовлює невисокий рівень її оплати, що може призвести до загрози втрати персоналу.

Капітальні інвестиції підприємств за видами економічної діяльності в Україні (Додаток Д) мають тенденцію до збільшення. Як загалом в економіці, так і в сільському господарстві найбільша сума інвестицій вкладається в машини та обладнання (2018 р. – 68,4 %), у будівництво та перебудову будівель (2018 р. – 18,5 %) в існуючі будівлі та споруди (2018 р. – 3,3 %). Через невизначені відносини на ринку землі спостерігається надзвичайно малий обсяг інвестування у земельні ресурси, здебільшого для їх покращення, пов'язаного зі зрошенням (2018 р. – 0,3 %). Оскільки земля є основним активом у сільському господарстві, а її стан упродовж 1991–2018 рр. значно погіршився (зменшення вмісту гумусу, знищення лісосмуг, ерозія ґрунтів, несформованість під'їзних шляхів, незаконна зміна цільового призначення, парцеляція, необґрунтовані конфігурації полів тощо), то основні інвестиції мали б бути спрямовані саме в поліпшення її якості.

Загалом простежується значна залежність між обсягом виробництва продукції сільського господарства, реалізованої підприємствами (табл. 2.7), і середніми цінами продукції сільського господарства, реалізованої підприємствами в Україні протягом 2009–2019 рр. Ця закономірність відповідає законам ринкової економіки й умовам ринку покупця: чим більший врожай, тим нижча ціна.

Таблиця 2.7

Індекси фізичного обсягу продукції сільського господарства, реалізованої підприємствами (у відсотках до попереднього року) України, за 2009–2019 рр. [сформовано на основі 117]

Роки	Продукція сільського господарства – всього	У тому числі	
		продукція рослинництва	продукція тваринництва
2009	120,0	128,4	108,3
2010	95,8	90,1	107,8
2011	112,0	114,5	106,9
2012	117,5	122,9	105,3
2013	110,6	111,4	108,6
2014*	107,7	108,7	105,3
2015*	106,9	111,1	95,4
2016*	87,9	83,4	105,1
2017*	107,5	108,3	103,1
2018*	105,7	107,2	98,8
2019*	114,1	116,9	101,2

*Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій і Луганській областях

Мінімізація ризиків для аграрних підприємств вбачається у розвитку переробної промисловості та логістичної невиробничої інфраструктури, що

дозволить як збільшити додану вартість, так і посилити конкуренцію на внутрішньому ринку, зберігати продукцію сільського господарства до настання цінових піків. Водночас необхідно на сучасних підприємствах запровадити технології відповідно до концепції Zero Waste, що передбачає використання не тільки основної, але і побічної продукції з метою отримання додаткової доданої вартості як сировини для фармацевтичної, хімічної, косметологічної, харчової галузей тощо. Це дозволить підвищити інноваційно-інвестиційний потенціал підприємств агропродовольчої сфери.

Характеризуючи господарства населення (Додаток Е), доцільно відзначити значну зміну індексів фізичного обсягу продукції сільського господарства (зокрема продукції тваринництва, обсяги якої систематично зменшуються). Це пов'язано зі зменшенням чисельності сільського населення, а відповідно, і домашніх господарств (особистих селянських), що здатні виробляти товарну продукцію. За відсутності кооперативних утворень виробничого та невиробничого характеру ціни закупівлі надлишків продукції у господарств населення формують перекупники, що збирають продукцію для переробних підприємств (здебільшого молоко) або ринків.

Слід відмітити значні зміни обсягу посівних площ сільськогосподарських культур і площ багаторічних насаджень в Україні в усіх категоріях господарств (табл. 2.8).

Таблиця 2.8

Посівна площа сільськогосподарських культур і площа багаторічних насаджень в Україні в усіх категоріях господарств за 1991, 2009–2019 рр., [сформовано на основі 116]

Роки	Посівна площа, тис. га					Загальна ¹ площа насаджень культур плодових і ягідних, тис. га
	культури зернові та зернобобові	буряк цукровий фабричний	соняшник	картопля	культури овочеві	
1991	14671	1558	1601	1533	477 ²	842
2009	15837	322	4232	1409	453	260
2010	15090	501	4572	1408	465	255
2011	15724	532	4739	1439	501	255
2012	15449	458	5194	1440	498	255
2013	16210	280	5051	1388	488	253
2014 ³	14801	331	5257	1348	467	239
2015 ³	14739	237	5105	1291	446	235
2016 ³	14401	292	6073	1312	447	224
2017 ³	14624	316	6034	1323	445	226
2018 ³	14839	276	6117	1319	439	228
2019 ³	15318	222	5928	1309	452	225

¹ Без урахування площі ягідників у міжряддях садів.

² Овочі відкритого ґрунту.

³ Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій і Луганській областях.

При фактично незмінній площі сільгоспугідь спостерігається значне скорочення площ під вирощування цукрових буряків і багаторічних насаджень. Насичення внутрішнього ринку завдяки цим культурам можна пояснити збільшенням їх урожайності, що є позитивним фактором. Зменшення посівних площ відбулося одночасно зі зменшенням площ під посіви кормових культур та збільшенням площ посіву соняшнику, ріпаку, сої та інших культур, баланс вмісту гумусу після вирощування яких від'ємний, що несе значну загрозу як українським землям, так і сільському господарству загалом. Нехтування тваринництвом (яке, крім іншого, є продуцентом органічних добрив), а відповідно, і вирощуванням кормових культур, більшість з яких має позитивний баланс гумусу, знижує продуктивні можливості українського сільського господарства, додану вартість галузі, вартість українських земель сільгосппризначення, що є особливо негативним у період формування ринку землі.

Доцільно відзначити, що обсяг виробництва сільськогосподарських культур в Україні у всіх категоріях господарств (Додаток Ж) за всіма основними культурами (крім цукрових буряків) 2019 р. значно збільшився порівняно з 1991 р. Порівняно з 2009 р. спостерігалось збільшення обсягу зернових і зернобобових на 63,3 %, цукрового буряку – на 1,4 %, соняшнику – на 139,7 %, картоплі – на 3,1 %, овочевих культур – на 16,1 %; плодових і ягід – на 31,0 %. Водночас слід відмітити доволі значні темпи приросту потужностей для зберігання зернових культур і соняшнику, картопле- та овочесховищ, підприємств із переробки зерна та виробництва олії, палет, крохмалю, овочів і фруктів глибокої заморозки, сублімованих овочів і фруктів тощо. Зараз в Україні зареєстровано близько 966 зерносховищ (за даними платформ Zernovoz.ua і Zernotorg.ua). Фактично існує приблизно 46–47 млн т сучасних елеваторних потужностей (одночасного зберігання) при потребі близько 70 млн т, і при цьому ще заплановано збільшення валового збору та експорту. За найбільш оптимістичними прогнозами потужність буде зростати на 7–10 % щороку (реально – на 5–6 %). Найбільше бракує сучасних сховищ у Вінницькій, Дніпропетровській і Чернігівській областях [122].

Невирішеними залишаються питання нерозвиненої логістичної інфраструктури, здебільшого пов'язаної з автошляхами невідповідної якості, з роботою ПАТ «Укрзалізниця», необхідністю відволікання обігових коштів зернових трейдерів на рухомий склад, виробництво й обслуговування власного річкового флоту, розчищення річок тощо, що взагалі то є завданнями держави. Робочий парк «Укрзалізниці» має 10800 вагонів, 5200 зерновозів, які належать приватним компаніям. Вартість доставки зернових

від сільгоспвиробника до порту в Україні вища, ніж у США і більшості країн Європи.

Близько 18 % логістичних витрат в Україні пов'язані з доставкою пшениці безпосередньо з поля в порт, тоді як у Франції та Німеччині цей показник становить лише 8 %, у США – близько 6 %. Близько 20 % припадає на доставку зерна з елеватора в порт, тоді як у Франції та Німеччині витрати становлять 13–14 %, а в США – до 22 % усіх логістичних витрат. Загальний рівень витрат на зернову логістику в Україні становить у середньому \$40 за тону [123].

Річкові перевезення могли б відчутно здешевити логістику в Україні. Зараз обсяг річкових перевезень Дніпром становить лише 10 % від початкового обсягу в 90-х рр. через замуленість фарватеру Дніпра та Прип'яті. В проект відновлення водного шляху Е–40 планується вкласти \$30 млн. Здешевлення доставки, наприклад, зерна з елеваторів до морських портів, призведе до зростання експорту (обсяг перевалки товарів через Україну, за прогнозними оцінками, зросте до \$300 млрд). Річковий маршрут Е–40 входить в інфраструктурний проект «Транс'європейські транспортні мережі» і є одним із пріоритетів «Національної транспортної стратегії України до 2030 року» [84]. У зв'язку з цим Туреччина розробила проект створення в Україні логістичного хабу для збільшення флоту і нарощування морського сполучення між країнами в Чорному морі. Планується розвиток мережі: Карс – Тбілісі – Баку, оскільки весь транзит з України до Ірану і на Близький Схід здійснюється через цей регіон [115].

Агрохолдинг «НІБУЛОН» за десять років інвестував у будівництво власного флоту \$600 млн і на сьогодні є найбільшим суднобудівником і судновласником в Україні. Власний флот компанії складається з 75 барж, катерів, плавкранів. У 2018–2019 маркетинговому році агрохолдинг відвантажив на зовнішні ринки 5,2 млн т зернових і олійних культур, із них 3,3 млн т «НІБУЛОН» перевіз внутрішніми водними шляхами України – Дніпром і Південним Бугом. Для реалізації такого логістичного сполучення, «НІБУЛОН» побудував 12 портових терміналів на Дніпрі та Південному Бугу, а також придбав суднобудівний завод «Лиман». На сьогодні у структурі вантажоперевезень компанії річковий транспорт становить 60 %, залізниця – третину, решту – автотранспорт [103].

Досягненням діджиталізації слід вважати значне підвищення врожайності сільгоспкультур 2019 р. як порівняно із 1991 р., так і з 2009 р. (зернові та зернобобові культури – 64,8 %; буряк цукровий фабричний – 46,3 %; соняшник – 68,4 %; картопля – 11,5 %; культури овочеві – 16,9 %; культури плодові та ягідні – 52,9 %), що пов'язано із системою точного

землеробства, біоінноваційними технологіями у насінництві, успішною боротьбою за чесне оприбуткування продукції. Тобто сільське господарство України поступово переходить на індустріальні рейки, що дозволяє нівелювати такі ризики як природні впливи, проте не рятує від цінової волатильності (табл. 2.9).

Таблиця 2.9

Урожайність сільськогосподарських культур в Україні в усіх категоріях господарств за 1991, 2009–2019 рр., центнерів з 1 га зібраної площі [сформовано на основі 116]

Роки	Культури зернові та зернобобові ¹	Буряк цукровий фабричний	Соняшник ¹	Картопля	Культури овочеві	Культури плодові та ягідні ²
1991	26,5	234	14,6	95	128	23,0
2009	29,8	315	15,2	139	183	70,7
2010	26,9	279	15,0	132	174	78,2
2011	37,0	363	18,4	168	195	84,9
2012	31,2	411	16,5	161	199	89,9
2013	39,9	399	21,7	160	200	103,5
2014 ³	43,7	477	19,4	176	208	95,2
2015 ³	41,1	436	21,6	161	206	104,5
2016 ³	46,1	482	22,4	166	211	101,9
2017 ³	42,5	475	20,2	168	208	103,1
2018 ³	47,4	509	23,0	171	214	128,4
2019 ³	49,1	461	25,6	155	214	108,1

¹ У масі після доробки.

² З площі насаджень у плодоносному віці.

³ Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій і Луганській областях.

Щодо використання мінеральних добрив зауважимо (Додаток И), що хоча їх внесення і зменшилося 2018 р. проти 1990 р. фактично вдвічі, проте збільшилось у 2,5 раза порівняно з 2009 р. Позитивним аспектом є їх значно більша дієвість і ефективність завдяки точковому дозованому внесенню на основі більш об'єктивного аналізу стану ґрунтів. Водночас менші обсяги внесення мінеральних добрив дають більш якісну продукцію. Зазначена тенденція простежується і порівняно з іншими країнами.

Наприклад, якщо оцінювати вирощування кукурудзи на зерно у найбільшого конкурента України – США, то при урожайності в США, більшій на 11,9 % (дані 2019 р. по штату Огайо), витрати на мінеральні добрива на 1 га більші на 19,9 %, на ЗЗР – на 90 %, на насіння – на 183 %, на оплату оренди землі – на 276,7 %, на управління, робочу силу й адміністративні витрати – на 19,4 % (при цьому стаття витрат «механізація і паливо» в Україні дорожча на 8,7 %) [55]. Слід відмітити незначну питому

вагу обробітку сільгоспугідь мінеральними (38,8 %) та органічними (1,9 %) добривами. Через значне зменшення поголів'я сільгосптварин у сільському господарстві спостерігається гострий дефіцит гною, що унеможливорює підтримування балансу гумусу, оскільки за нинішніх умов внесення 280,7 кг/га, однозначно, є недостатнім.

Основні досягнення НТП в агропродовольчій сфері формують додаткові можливості у виробничих процесах переважно для середніх і великих господарств (Додаток К). Це простежується через показники урожайності основних сільгоспкультур, які у великих господарствах (понад 3000 га) набагато вищі, ніж у малих підприємствах (до 100 га): 2018 р. зернових і зернобобових культур – на 97,6 %, соняшнику – на 25,8 %, сої – на 29,7 %. Доцільно відмітити високий рівень концентрації виробництва: так 1,4 % великих господарств вирощують 27,9 % зернових і зернобобових культур, 0,5 % великих господарств – 9,8 % соняшнику, 0,8 % – 20,5 % сої. Аналогічна ситуація і в тваринництві (Додаток Л), де спостерігається надпотужний розвиток інформаційних технологій: збалансована дозована система годівлі, чіпування тварин, упровадження безвідходних технологій під час забою, роботи з побічною продукцією та відходами, подачі води, збирання гною, ветеринарних обробок, закупівлі, формування мікроклімату (освітлення, системи вентиляції, термо- і вологорежим) тощо. Концентрація виробництва в тваринництві теж на високому рівні: 7,6 % великих господарств утримують 40,1 % поголів'я ВРХ, 3,2 % – 23,3 % корів, 4,3 % – 62,0 % свиней, 8,2 % – 78,5 % свійської птиці тощо. Щодо групування підприємств за кількістю сільськогосподарських тварин в Україні слід звернути увагу на абсолютно незначну кількість підприємств, які утримували сільськогосподарських тварин: ВРХ – 4,7 % господарств, корів – 4,4 %, свиней – 3,6 %, птицю – 0,9 %. При цьому на одне господарство, що утримувало ВРХ, припадало до 496 гол., корів – 220 гол., свиней – 1964 гол., птиці – 264617 гол. Тобто концентрація худоби та птиці доволі значна.

Ситуацію у тваринництві (крім виробництва м'яса птиці та яєць) можна назвати критичною (Додаток М). Основною проблемою залишається збитковість виробництва, що значно відобразилося на поголів'ї тварин. Якщо змодельовати ситуацію, що 1 413,5 тис. гол. ВРХ дасть по 1 кг середньодобового приросту, то на одного українця припадатиме по 7,32 кг яловичини (без урахування експортно-імпортних операцій та з урахуванням 60 % виходу м'яса ВРХ, 77 % – м'яса свиней, 60 % – м'яса птиці), якщо 6 025,3 тис. свиней дасть по 1 кг середньодобового приросту, то на одного українця припадатиме по 40,2 кг свинини, забій усієї птиці (при середній забійній вазі 2 кг) дасть по 6 кг м'яса птиці. Тобто за найбільш високотехнологічних умов

виробництва максимально можна отримати 53,52 кг на душу населення при нормативі 83 кг. У разі відсутності ялових корів і надоїв навіть по 10 тис. л молока від корови на рік можна отримати 45,5 л молока на одного українця, що менше від нормативу (365 л на рік) у 8 разів. Тобто склалася абсолютно неприпустима ситуація – занепад галузі тваринництва, що загрожує продовольчій безпеці країни. Виробництво основних видів продукції тваринництва в Україні у всіх категоріях господарств 2018 р. порівняно з 1990 р. значно скоротилося (м'яса – на 46,0 %, молока – на 58,9 %, яєць – на 0,9 %, вовни – на 93,6 %), що відображено в додатку Н. При цьому 2018 р. порівняно з 2009 р. зменшення виробництва основних видів продукції тваринництва не було значним, враховуючи критично низький обсяг виробництва. Обсяг виробництва м'яса збільшився на 22,8 %, молока – зменшився на 13,3 %, яєць – збільшився на 1,4 %, вовни – зменшився на 53,6 %. Слід відмітити, що незначне збільшення обсягу виробництва м'яса та яєць відбулося включно за рахунок м'яса птиці, що є сферою інтересів великих експортоорієнтованих агрохолдингів (м'ясо птиці – МХП, ТОВ «Комплекс «Агромарс», Птахокомплекс «Дніпровський», АПГ «Пан Курчак», Компанія «Агро-Овен», ПрАТ «Володимир-Волинська птахофабрика», УЛАР тощо; яйця – Агрохолдинг «Авангард» (найбільший виробник яєць у Євразії), ТОВ «Ясенсвіт», група компаній «Інтер-Запоріжжя», ТОВ «Березанська птахофабрика», ТОВ «Птихофабрика „Поділля”» тощо). Через значний попит та високу якість продукції ці компанії щорічно збільшують обсяг виробництва та географію експорту, формуючи власні логістичні системи. Недооціненою галуззю залишається вівчарство (виробництво м'яса овець і вовни) через закриття основних заводів з переробки цієї сировини (зокрема з виробництва валянків та шинелей), що потребує державної підтримки.

Слід акцентувати увагу на значних змінах продуктивності сільгосптварин. Середній річний удій молока від однієї корови в Україні зріс з 1990 р. по 2018 р. на 71,9 % (на підприємствах – на 110,5 %, в господарствах населення – на 72,9 %), що відображено в додатку П. Це пов'язано не тільки зі зміною породного складу чи більшою збалансованістю раціону (Додаток Р), іншими технологічними особливостями, скільки із значним скороченням поголів'я (див. додаток М). Характеризуючи кризу в тваринництві, не можна оминати одну з його головних галузей – бджільництво (Додаток С). Її розвиток є загальносвітовою проблемою, оскільки в світі через негативні антропогенні фактори значно скорочується кількість бджіл, а отже, – і можливість ведення сільського господарства загалом через його біологічні особливості. В Україні кількість бджолосімей невинно зменшується: з 1991 р. по 2019 р. – на 26,0 %, хоча водночас значно

збільшилися обсяги виробництва рослинницької продукції.

Розглядаючи витрати на виробництво продукції (товарів, послуг) підприємств за видами економічної діяльності в Україні (табл. 2.10), доцільно відзначити збільшення питомої ваги матеріальних витрат і витрат на оплату послуг у виробництві, амортизацію і одночасне зменшення питомої ваги витрат на оплату праці.

Таблиця 2.10

Витрати на виробництво продукції (товарів, послуг) підприємств за видами економічної діяльності в Україні за 2012–2018 рр. [сформовано на основі 112]

Вид економічної діяльності	Роки	Витрати на виробництво продукції (товарів, послуг), млрд грн	З них за складовими витрат					
			матеріальні витрати та витрати на оплату послуг, використані у виробництві		амортизація		витрати на оплату праці	
			млрд грн	у відсотках до загальних витрат	млрд грн	у відсотках до загальних витрат	млрд грн	у відсотках до загальних витрат
Усього	2012	2077,9	1544,8	74,3	128,3	6,2	274,9	13,2
	2013	1984,1	1434,7	72,3	139,6	7,0	278,1	14,0
	2014*	1952,6	1419,8	72,7	138,1	7,1	261,5	13,4
	2015*	2446,1	1805,6	73,8	171,4	7,0	295,8	12,1
	2016*	2759,9	2048,0	74,2	224,6	8,1	360,8	13,1
	2017*	3525,2	2644,5	75,0	247,1	7,0	472,8	13,4
	2018*	4263,0	3165,3	74,3	287,1	6,7	601,7	14,1
В тому числі сільське господарство	2012	127,5	98,7	77,4	7,3	5,7	14,5	11,3
	2013	150,4	119,2	79,3	9,5	6,3	14,8	9,8
	2014*	181,4	148,6	81,9	10,2	5,6	14,9	8,2
	2015*	263,3	220,0	83,5	14,0	5,3	17,8	6,8
	2016*	312,3	260,6	83,4	16,8	5,4	22,4	7,1
	2017*	372,6	304,0	81,6	22,8	6,1	30,0	8,1
	2018*	461,5	375,4	81,3	30,5	6,6	37,9	8,2
З нього: рослинництво	2012	93,1	72,6	77,9	5,1	5,5	10,3	11,1
	2013	109,9	87,2	79,4	6,9	6,3	10,7	9,7
	2014*	137,1	112,7	82,2	7,5	5,5	11,0	8,0
	2015*	204,0	170,2	83,4	10,7	5,3	13,6	6,6
	2016*	249,5	208,5	83,6	12,9	5,2	17,3	6,9
	2017*	309,8	254,6	82,2	17,7	5,7	24,0	7,7
	2018*	383,4	314,2	82,0	24,2	6,3	30,0	7,8
тваринництво	2012	28,1	22,0	78,2	1,6	5,8	3,0	10,7
	2013	31,1	24,9	80,0	1,9	6,0	3,1	9,8
	2014*	35,7	29,5	82,6	1,9	5,2	3,0	8,5
	2015*	50,2	43,1	85,8	2,4	4,8	3,3	6,5
	2016*	54,0	45,8	84,8	3,1	5,7	3,7	6,9
	2017*	47,5	38,1	80,2	3,8	7,9	4,1	8,7
	2018*	61,0	48,9	80,3	4,6	7,6	5,4	8,9

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій і Луганській областях

Це пов'язано зі збільшенням вартості основних засобів, їх продуктивності, агрегованості, застосування сучасних методів амортизації при одночасному

зменшенні трудомісткості та працевзабезпеченості на підприємствах агропродовольчої сфери.

Слід звернути увагу на волатильність середніх цін продукції сільського господарства, реалізованої підприємствами України (Додаток Т). Ціни, за якими продають свою продукцію господарства населення, мають ще більшу амплітуду коливань, що створює значний ризик для виробників, факторами посилення якого є нерозвиненість кооперативного руху в Україні, недосконалість інфраструктури та відсутність державної підтримки у період, максимально сприятливий для виробництва сільгоспкультур і продукції тваринництва.

Для об'єктивності висновків пропонується розглянути цю амплітуду, враховуючи коливання курсу національної валюти. Попри зростання цін протягом 2009–2019 рр. у гривневому еквіваленті на зернові й зернобобові культури – на 384,0 %, насіння олійних культур – на 298,9 %, цукровий фабричний буряк – на 83,9 %, картоплю – на 321,6 %, овочеві культури – на 151,2 %, плодові та ягідні культури – на 243,2 %, сільськогосподарських тварин – на 215,4 %, молоко – на 334,0 %, яйця – на 198,6 % в доларах США все виглядає зовсім інакше – зростання на зернові та зернобобові культури на 38,6 %, насіння олійних культур – на 14,3 %, картоплю – на 20,8 %, молоко – на 24,3 %, і навіть зниження цін: на цукровий фабричний буряк – на 47,3 %, овочеві культури – на 28,0 %, плодові та ягідні культури – на 1,7 %, сільськогосподарських тварин – на 9,7 %, яйця – на 14,5 %. Тобто насправді на більшість видів сільгосппродукції відбулося падіння цін при значному зростанні цін на промислову та імпортовану продукцію, що знизило ефективність агробізнесу загалом, та не сприяло підготовці підприємств до запровадження повноцінного ринку землі через від'ємну курсову різницю для внутрішнього ринку та позитивну – для експортерів. Незадовільна динаміка цін не сприяє й розвитку тваринництва, крім того, що значну питому вагу земельного банку (до 50 %) необхідно відводити під кормові культури для апріорі збиткового тваринництва.

Питома вага підприємств України, що отримали чистий прибуток в сільському господарстві 2018 р. набагато більша, ніж в середньому по економіці – 86,5 % проти 73,9 % (табл. 2.11). В останні роки їх частка мала тенденцію до збільшення. Питома вага чистого прибутку, який отримали сільгосппідприємства, становила 24,4 % від загального чистого прибутку по економіці загалом. Водночас у сільському господарстві 2018 р. працювало 8,7 % зайнятих, питома вага сільгосппідприємств у загальній кількості підприємств в економіці становила 13,7 %, питома вага валової продукції – 5,1 %.

Таблиця 2.11

Чистий прибуток (збиток) підприємств України за видами економічної діяльності за 2010–2018 рр.* [сформовано на основі 112]

Галузь	Роки	Усього				
		чистий прибуток (збиток), млрд грн	підприємства, які одержали прибуток		підприємства, які одержали збиток	
			у відсотках до загальної кількості підприємств	фінансовий результат, млрд грн	у відсотках до загальної кількості підприємств	фінансовий результат, млрд грн
Всього по економіці	2010	13,91	57,30	155,20	42,70	141,29
	2011	67,80	63,50	208,90	36,5	141,10
	2012	35,07	63,00	210,61	37,0	175,54
	2013	-22,84	65,00	179,26	35,0	202,10
	2014*	-590,07	65,50	202,70	34,5	792,77
	2015*	-373,52	73,30	352,98	26,7	726,50
	2016*	29,71	73,00	396,75	27,0	367,04
	2017*	168,75	72,40	515,46	27,6	346,71
	2018*	288,31	73,90	584,36	26,1	296,05
Сільське господарство	2010	17,24	69,10	22,10	30,9	4,86
	2011	25,25	83,30	30,18	16,7	4,93
	2012	26,72	78,40	33,57	21,6	6,86
	2013	14,91	80,00	26,19	20,0	11,28
	2014*	21,39	84,40	51,67	15,6	30,28
	2015*	101,89	88,70	127,53	11,3	25,64
	2016*	89,79	88,10	102,50	11,9	12,71
	2017*	68,24	86,50	88,69	13,5	20,45
	2018*	70,42	86,50	93,26	13,5	22,84
Рослинництво	2010	13,30	72,70	16,44	27,3	3,14
	2011	20,56	86,20	23,20	13,8	2,64
	2012	18,48	80,00	23,80	20,0	5,32
	2013	7,55	81,80	16,42	18,2	8,87
	2014*	16,10	86,50	39,75	13,5	23,65
	2015*	88,29	90,70	108,19	9,3	19,90
	2016*	81,76	90,30	91,38	9,7	9,62
	2017*	58,71	88,30	76,39	11,7	17,67
	2018*	62,79	88,50	81,42	11,5	18,63
Тваринництво	2010	4,03	63,00	5,00	37,0	0,97
	2011	4,29	68,80	6,14	31,2	1,85
	2012	6,82	71,10	7,77	28,9	0,94
	2013	6,27	70,60	7,42	29,4	1,15
	2014*	6,93	74,40	8,92	25,6	1,99
	2015*	13,74	77,90	16,23	22,1	2,49
	2016*	7,07	72,50	8,99	27,5	1,91
	2017*	8,26	75,80	9,80	24,2	1,54
	2018*	7,38	76,30	9,58	23,7	2,20

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій і Луганській областях

На одне підприємство в економіці 2018 р. припадало 810,23 тис. грн чистого прибутку, а в сільському господарстві – 1447,39 тис. грн, на одного працівника – 48,38 тис. грн і 136,45 тис. грн відповідно. Тобто відносні показники у сільському господарстві останнім часом набагато ефективніші,

ніж середні показники по економіці, що не є позитивним явищем, бо сировинна галузь не може апріорі бути ефективнішою за більш технологічні галузі, та свідчить про переважно аграрний напрям розвитку України та деіндустріалізацію.

Слід зазначити, що рослинництво наразі є набагато ефективнішим, ніж тваринництво, його питома вага у чистому прибутку сільгосппідприємств становить 89,2 %, а тваринництва – 10,8 %.

Ідентичні тенденції спостерігаються і стосовно фінансових результатів до оподаткування підприємств України за видами економічної діяльності (Додаток У). Слід зазначити, що значний по відношенню до всієї економіки, але не значний порівняно із сільським господарством розвинених країн рівень оподаткування у вітчизняному сільському господарстві зумовлений, крім іншого, недостатнім розвитком харчової промисловості, про що свідчать фінансові результати діяльності аграрних підприємств [18; 59; 60].

Фінансові результати сільського господарства і харчової промисловості різняться майже в 6 разів, що свідчить не про неефективну діяльність останньої, а про експорт більшої частини валової продукції, що призводить до скорочення робочих місць і до недоотримання податків, зокрема доданої вартості загалом.

Фінансовий результат до оподаткування за розмірами підприємств в Україні за період 2010–2018 рр. (Додаток Ф) визначає тенденцію до зростання кількості середніх і малих підприємств, зокрема мікропідприємств, які отримують прибутки (питома вага великих підприємств – 15,8 %, середніх – 53,9 %, малих – 30,3 %, з них мікропідприємств – 23,3 %). Складається парадоксальна ситуація, коли агрохолдинги, володіючи більшою часткою основних засобів, земельними банками, основним контингентом працівників, інвестують у значні проекти з горизонтальної та вертикальної інтеграції, проте де-юре не мають достатнього прибутку. При цьому загалом по економіці найбільший прибуток мають саме великі та середні підприємства.

Рівень рентабельності виробництва продукції сільського господарства на сільськогосподарських підприємствах України (табл. 2.12) нестабільний і має негативну тенденцію до більшої частини видів продукції.

Якщо порівнювати рівень рентабельності 1990 і 2018 рр., то відбулося зменшення рівня рентабельності виробництва зерна на 250,4 %, насіння соняшнику – на 204 %, цукрового буряку – на 40,9 %, картоплі – на 20,4 %, овочів відкритого ґрунту – на 10,9 %, м'яса ВРХ – на 38,3 %, м'яса свиней – на 13,8 %, м'яса овець і кіз – на 18,9 %, м'яса птиці – на 11,3 %, молока – на 16,1 %, яєць – на 21,9 %.

Таблиця 2.12

Рівень рентабельності виробництва продукції сільського господарства на сільськогосподарських підприємствах України за 1990–1991, 2009–2018 рр., % [сформовано на основі 112]

Роки	Зерно	Насіння соняшнику	Цукрові буряки (фабричні)	Картопля	Овочі відкритого грунту	М'ясо великої рогатої худоби ¹	М'ясо свиней ¹	М'ясо овець і кіз ¹	М'ясо птиці ¹	Молоко	Яйця
1990	275,1	236,5	29,5	27,2	27,6	20,6	20,7	2,3	17,0	32,2	27,3
1991	166,2	307,6	59,9	150,4	60,3	43,9	36,0	29,3	2,6	21,7	47,1
2009	7,3	41,4	37,0	12,9	19,1	-32,9	12,1	-31,8	-22,5	1,4	13,1
2010	13,9	64,7	16,7	62,1	23,5	-35,9	-7,8	-29,5	-4,4	17,9	18,6
2011	26,1	57,0	36,5	17,7	9,9	-24,8	-3,7	-39,6	-16,8	18,5	38,8
2012	15,2	45,8	15,7	-21,5	-6,8	-29,5	2,0	-40,0	-7,2	2,3	52,6
2013	1,5	28,5	2,7	23,0	7,0	-43,3	0,2	-42,8	-10,0	13,6	47,6
2014 ²	25,8	36,5	17,9	9,2	16,7	-35,9	5,6	-52,2	-15,4	11,0	58,8
2015 ²	43,1	80,5	28,2	24,2	47,5	-17,9	12,7	-29,6	-6,1	12,6	60,9
2016 ²	37,8	63,0	24,3	-3,2	19,7	-24,8	-4,5	-35,2	5,0	18,2	0,5
2017 ²	25,0	41,3	12,4	10,0	15,6	3,4	3,5	-39,6	7,0	26,9	-9,0
2018 ²	24,7	32,5	-11,4	6,8	16,7	-17,7	6,9	-16,6	5,7	16,1	5,4

¹У забійній вазі.

²Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій і Луганській областях.

Якщо порівнювати рівень рентабельності 2009 р. і 2018 р., то відбулося зменшення рівня рентабельності виробництва насіння соняшнику на 8,9 %, цукрового буряку – на 48,4 %, картоплі – на 6,1 %, овочів відкритого ґрунту – на 2,4 %, м'яса свиней – на 5,2 %, яєць – на 7,7 %, а збільшення: зерна – на 17,4 %, м'яса ВРХ – на 15,2 %, м'яса овець і кіз – на 15,2 %, м'яса птиці – на 28,2 %, молока – на 14,7 %. При цьому амплітуда коливань упродовж 2009–2018 рр. становила по зерну – 41,6 %, насінню соняшнику – 52 %, цукровому буряку – 48,4 %, картоплі – 83,6 %, овочам відкритого ґрунту – 54,3 %, м'ясу ВРХ – 46,7 %, м'ясу свиней – 20,5 %, м'ясу овець і кіз – 35,6 %, м'ясу птиці – 29,5 %, молока – 25,5 %, яйцях – 69,9 %. Нестабільність рівня рентабельності як узагальнюючого показника ефективності функціонування агро підприємств свідчить про непередбачуваність у формуванні довгострокових планів щодо інвестування коштів у виробничі проекти.

Розподіл великих, середніх, малих і мікропідприємств за рівнем рентабельності операційної та всієї діяльності підприємств України за видами економічної діяльності (Додаток Х) підтверджує попередні висновки про набагато меншу ефективність менших за розміром сільгосппідприємств. Доходність великих господарств визначається не тільки ефектом масштабу, але й упровадженням у них системи горизонтальної та вертикальної

інтеграції, що актуалізує після запровадження ринку землі популяризацію кооперативного досвіду роботи в сільському господарстві.

На основі проведеного аналізу доцільно відмітити як позитивні, так і негативні тенденції розвитку підприємств агропродовольчої сфери України.

Серед негативних тенденцій трансформації агропродовольчої сфери України слід відзначити такі: зменшення кількості сільських населених пунктів; зменшення індексів фізичного обсягу продукції сільського господарства, зростання навантаження на зайнятих в сільському господарстві та відсутність трудового резерву на селі, зменшення питомої ваги витрат на оплату праці, зменшення питомої ваги тваринництва в загальній структурі виробництва сільськогосподарської продукції через збитковість виробництва, волатильність середніх цін на продукцію сільського господарства.

До позитивних зрушень у розвитку агропродовольчої сфери України слід зарахувати: зростання обсягів реалізованої продукції (товарів, послуг) суб'єктів господарювання; значне зростання продуктивності праці в сільськогосподарських підприємствах, особливо у сфері тваринництва; зростання обсягів капітальних інвестицій підприємств; значне зростання врожайності сільгоспкультур і продуктивності сільгосптварин; надпотужний розвиток інформаційних технологій; тенденції до збільшення ролі середніх і малих підприємств, зокрема мікропідприємств.

Управління підприємствами агропродовольчої сфери ґрунтується на актуальній інформації, статистичних збірниках, аналізі економічної ситуації галузі тощо. Для їх ефективного функціонування необхідно своєчасно впроваджувати інноваційні розробки та якісне інформаційне обслуговування. Інформатизація агропродовольчої сфери є стратегічним завданням розвитку аграрного виробництва та його інноваційного розвитку. Засоби автоматизації створюють необхідну матеріально-технічну базу, яка здатна впливати на поширення знань завдяки електронній фіксації і загальній автоматизації інформаційних процесів. Основними сучасними напрямками розвитку інформаційних технологій у сільському господарстві є точне землеробство, геоінформаційні та інтелектуальні системи агромоніторингу, системи підтримки прийняття рішень. Водночас ці фактори впливають на результативні показники діяльності аграрних підприємств як позитивно, автоматизуючи окремі процеси та збільшуючи прибуток, так і негативно – шляхом впливу на їх інформаційну, а отже, й на економічну безпеку.

Тому наступними етапами аналізу будуть характеристика факторів впливу на інформаційну безпеку та власне оцінка рівня інформаційної безпеки підприємств агропродовольчої сфери.

2.2. Оцінка зовнішніх та внутрішніх факторів впливу на систему управління інформаційною безпекою аграрних підприємств України

У сучасних умовах досягнення необхідного рівня національної безпеки вимагає передбачати одночасно й у комплексі всі загрози, реальні й потенційні, життєво важливим інтересам особистості, суспільства й держави. Це викликає необхідність безупинного одержання достовірної і повної інформації не тільки про загрози і ступінь їхньої небезпеки, але й про можливості впливу на них з метою усунення, нейтралізації чи зниження їхньої небезпеки. Інформаційна безпека посідає одне з ключових місць у системі забезпечення життєво важливих інтересів усіх без винятку країн. Це в першу чергу обумовлено нагальною потребою створення розвиненого інформаційного середовища суспільства. Але саме через інформаційне середовище найчастіше здійснюються загрози національній безпеці в різних сферах діяльності особистості, суспільства й держави. У сучасних умовах виникла потреба в переосмисленні та уточненні проблеми інформатизації України крізь призму її інформаційної безпеки з урахуванням сучасних інформаційних впливів

Прогрес у галузі інформаційно-комунікаційних технологій є джерелом переваги, що підвищує рівень продуктивності та надає конкурентну прерогативу підприємствам і організаціям, пов'язаним із виробництвом, переробкою та реалізацією сільськогосподарської продукції. Проте використання інформаційних і комунікаційних технологій пов'язане з ризиками інформаційної безпеки, що загрожують ефективному веденню аграрного бізнесу та цілісності інформаційних активів [124; 125; 126; 127]. Отже, інформаційно-комунікаційні технології на підприємствах агропродовольчої сфери є джерелом ряду переваг, а також ризиків, пов'язаних із порушенням інформаційної безпеки та водночас виникненням інцидентів з порушенням безпеки.

Проблемам аналізу загроз інформаційній безпеці підприємств, факторів впливу на їх виникнення присвячено багато праць зарубіжних і вітчизняних науковців, зокрема М. Ананьєва [11], В. Андріанова [12], І. Арістової [14], В. Болека [89], Є. Гарифулліної [53], І. Глотіної [29], В. Голованова [12], М. Голдуєва [12], М. Гупта [101], Ю. Данька [31; 32; 52; 88], В. Жмайлової [52], С. Зефірова [12], З. Ісламова [53], О. Качана [54], А. Козлова [29], Д. Кранца [101], А. Латечкової [89; 93], І. Макатури [94], Б. Маумбе [99], Є. Міщука [68], Є. Муратової [71], Д. Новака [100], С. Норзкат [100],

А. Ойха [101], Д. Окелло [99], А. Піко [101], М. Пугача [79], Л. Сабо [93], О. Сазонця [54], А. Сінгха [101], Г. Телеги [68], Ю. Ухтинської [11], О. Шумкова [52] та інших.

Динамічний процес інформатизації, цифровізації та автоматизації виробничих й управлінських процесів підприємств агропродовольчої сфери зумовлює необхідність подальших досліджень у цій предметній області.

Разом з іншими галузями промисловості сучасне сільське господарство перебуває в епіцентрі цифрової революції, яка базується на автоматизації, інформатизації, цифровізації та використанні Big data. Цифрові технології перетворюють сільське господарство. Комп'ютери, роботи, сенсори та аналітика Big data сприяють прийняттю рішень для отримання більш високих і стійких врожаїв, ефективнішого ведення тваринництва, підвищення якості, конкурентоспроможності продукції, зменшення її собівартості тощо. Сільськогосподарські підприємства орієнтуються на впровадження концепції точного землеробства на основі використання ГІС, методології оптимізації виробництва рослинництва, автоматизовані та комп'ютеризовані технологічні процеси відбору проб ґрунту, цифровий моніторинг карт урожайності, GPS-системи, супутникові знімки та автоматизацію процесів управління. Зазначені новітні інформаційно-комунікаційні технології та цифровізація виробничих і управлінських процесів дозволяють збільшити врожайність на існуючих сільськогосподарських землях на 70 %, допомагаючи фермерам досягти більш сталого виробництва [68].

Відповідно до досліджень А. Пугача та І. Арістової, розвиток аграрного сектора України залежить від ефективності побудови та функціонування інформаційного простору цього сектора економіки, оскільки інформатизація в напрямі розвитку аграрного потенціалу сприяє:

- освоєнню та впровадженню інноваційних технологій з обов'язковим використанням потенціалу обчислювальної техніки;

- створенню єдиного інформаційного простору, який буде доступний для всіх аграрних товаровиробників і їх партнерів;

- переходу до впровадження новітніх інформаційних технологій у сфері управління аграрним виробництвом на всіх рівнях на основі впровадження електронних систем зв'язку, мереж обчислювальної техніки;

- оптимізації управління аграрними виробничими процесами;

- впровадженню автоматизованих робочих місць для аграрних фахівців, а також диспетчеризації виробництва;

- інтенсифікації аграрної науки на основі застосування методів системного аналізу математичного моделювання, інформатики та широкого використання сучасних засобів обчислювальної техніки в дослідних,

наукових і проектних розробках;

застосуванню інноваційних досягнень фундаментальної науки у сфері теорії прийняття рішень і автоматизованих систем, застосуванню концепцій цифрового управління [14; 76; 79; 86].

Водночас агропродовольчий сектор, зокрема його суб'єкти, стають об'єктом навмисних і ненавмисних дій, пов'язаних із заподіянням шкоди економічній діяльності через вплив на інформаційно-комунікаційну складову, що зумовлює визначення основних видів загроз системі управління інформаційної безпеки аграрних підприємств. Результати узагальнення досліджень [25; 29; 54; 68] дозволяють зробити висновки про основні загрози інформаційній безпеці підприємств агропродовольчої сфери, серед яких слід виокремити:

основними каналами витоку інформації є власні співробітники та бізнес-партнери;

укладення договорів не завжди зумовлюються заходами щодо інформаційної безпеки, відповідальністю за розголошення інформації;

на підприємствах відсутній контроль за зберіганням, знищенням і копіюванням документів;

дані, які містять комерційну таємницю, часто не мають відповідного грифу;

в корпоративних комп'ютерних системах аграрних підприємств і засобах зв'язку не приділяється достатньої уваги способам захисту інформації;

підприємства не встановлюють співвідношення витрат на забезпечення інформаційної безпеки та втрат інформаційної безпеки у разі виникнення інцидентів її порушення.

Аналіз сфери інформаційної діяльності аграрних підприємств, проведений З. Ісламовою та Є. Гарифулліною, дозволив виявити ряд управлінських проблем, пов'язаних зі створенням належних умов для забезпечення інформаційної безпеки, а саме:

нерозуміння важливості використання сучасних інформаційних технологій у діяльності органів управління підприємствами агропродовольчої сфери;

нерозвиненість інфраструктури інформаційного забезпечення органів управління підприємствами агропродовольчої сфери;

нерівномірний розподіл інформаційних послуг, ресурсів і програмних продуктів по сільськогосподарських територіях і агропідприємствах;

відсутність системного підходу до управління інформаційною безпекою на підприємствах агропродовольчої сфери [53].

Стримується розв'язання проблем формування ефективної системи управління інформаційною безпекою суб'єктів аграрного бізнесу ще й такими факторами, як:

обмеженість ресурсів сільськогосподарських підприємств (переважно фінансових);

недостатня кваліфікація кадрового складу;

відсутність у багатьох господарств підключення до глобальної мережі;

відсутність інформаційно-консультаційних служб на підприємствах;

тривалі терміни розробки та впровадження системи інформаційної безпеки, відсутність у керівників необхідного досвіду роботи в умовах прозорості ринкової економіки та розуміння нагальності цього [11; 21; 54].

Доволі неординарним є підхід В. Андріанова, М. Голдуєва, С. Зефірова, В. Голованова [12], які зазначають, що окремі аспекти бізнесу, пов'язані з інформацією і даними, дозволяють зробити висновок, що інформаційна сфера є одним із головних джерел ризиків бізнесу. Вони вирізняють чотири основні групи проблем забезпечення інформаційної безпеки підприємств:

зростаюча складність інформаційної сфери зумовлює значне посилення взаємозв'язків між об'єктами господарських відносин інформаційного середовища, що потребує врахування більшої кількості факторів, а для цього, в свою чергу, необхідно створити інформаційну інфраструктуру з відповідними технічними та програмними засобами. Складність інформаційної сфери багаторазово підсилює дію інших факторів ризику та водночас породжує уразливості, спричинені дефіцитом часу на обробку й усвідомлення варіантів можливих рішень, неможливістю перевірки достовірності всіх використовуваних даних. Додаткові ризики пов'язані з використанням і підтриманням інформаційної інфраструктури, технічних і програмних засобів обробки даних, комп'ютерних мереж і телекомунікацій;

неточність відображення матеріального світу в інформаційних образах (моделях), що визначає наявність іншої проблеми, пов'язаної із забезпеченням адекватності інформаційних моделей, які беруть участь в обробці даних і прогнозах, реальним об'єктам. Неточність відображення матеріального світу в інформаційному середовищі та інформаційних об'єктів у часі породжує згодом неадекватність інформаційного образу реальному об'єкту. Оскільки дії над матеріальними об'єктами у більшій мірі заміщаються діями над їх описами (інформаційними образами), то неадекватність цих описів призводить до колізій, із яких найбільш значущими є два крайніх випадки: відсутність інформаційного образу для реально існуючого об'єкта, який міг би бути використаний в бізнесі; наявність інформаційного образу для об'єкта, який реально не існує.

Зазначена теоретична можливість колізій породжує ризик їх штучного створення (знищення даних про об'єкт, вилучення об'єкта), що призводить до збитку і втрат. Отже, і без злочинних дій неадекватність інформаційних образів (моделей) об'єктів самим матеріальним об'єктам створює значні інформаційні ризики;

конфлікт інтересів. Складність цієї проблеми посилюється через зростання кількості взаємодій між суб'єктами різних рівнів і різних соціально-економічних відносин. Автори виокремлюють два взаємопов'язаних між собою рівня конфлікту інтересів: усередині підприємства (внутрішній конфлікт інтересів) і між організаціями. Внутрішній конфлікт інтересів – одне з головних джерел ризику і головна загроза бізнесу, оскільки в цьому разі персонал підприємства, особливо суб'єкти відповідальності, та вищий менеджмент використовують у своїх інтересах активи аграрного підприємства, включаючи інформацію, матеріальні та фінансові активи й інші ресурси. Зі збільшенням розмірів суб'єкта аграрного ринку конфлікт інтересів теж посилюється. Це не тільки об'єктивна властивість будь-якого бізнесу, а й основа механізму його самознищення. Накопичення надмірного ресурсу в підрозділах підприємства призводить до різкого зниження ефективності бізнесу. Використання інформаційних та інших надлишкових активів для своїх цілей не відповідає цілям розвитку підприємства та створення за допомогою інформаційних впливів, таких як спотворення звітності, ослаблення контролю, маскуванню причин невдач під випадковість, ілюзії, що бізнес реалізується нормально й ефективно, призводить врешті решт до втрати управління, збитків і ліквідації бізнесу. Штучно створити умови, сприятливі для внутрішнього конфлікту інтересів, і погіршити бізнес може й інформаційна атака ззовні. Конфлікт інтересів між організаціями – це, як правило, конкуренція і боротьба за загальний ресурс;

проблема довіри. В середині організації – це проблема довіри власників персоналу підприємства, в першу чергу керівництву та менеджменту вищого рівня. Ззовні – це неможливість контролю за виконанням бізнес-партнерами та конкурентами законодавчо встановлених правил. Проблема інформаційної безпеки полягає в тому, чи може організація використовувати інформаційну сферу на всіх етапах свого життєвого циклу в реалізованих нею видах бізнесу, в умовах загроз, пов'язаних із перерахованими вище проблемами та особливостями. По суті, це технології, що дозволяють ефективно використовувати інформаційну сферу відповідно до особливостей вищезазначених груп проблем [4; 12; 69; 81; 86].

Група зарубіжних науковців виокремлює зовнішні та внутрішні фактори впливу на стан системи інформаційної безпеки аграрних підприємств та

процеси управління нею [89; 93; 94; 99; 100; 101; 102]. Серед внутрішніх факторів інформаційної небезпеки автори виокремлюють ті, що найбільше впливають на управління соціально-економічної складової діяльності аграрних підприємств, а саме:

неосвіченість працівників – відсутність знань у працівників щодо захисту інформаційного середовища підприємства, що може призвести до значних економічних збитків і актуалізує необхідність орієнтованості сільськогосподарських підприємств на навчання працівників, що передбачає уточнення процедур захисту конфіденційних даних від небажаних витоків і роз'яснення положень інформаційної політики та політики інформаційної безпеки. Взагалі крадіжки, зловживання та несанкціонована зміна інформації або маніпулювання даними часто відбуваються безпосередньо чи опосередковано через незнання працівниками основних принципів інформаційної безпеки [75; 93];

поведінка працівника – людський фактор – особливо слабкий елемент системи управління інформаційною безпекою. Співробітники загрожують зараженими електронними листами та флешками, підключаються до корпоративних серверів через загальнодоступні мережі Wi-Fi, використовують ті самі паролі, що й в акаунтах соціальних мереж тощо. Слід відзначити, що дії співробітників щодо порушення інформаційної безпеки можуть бути навмисними та мати різні мотиви [89];

відсутність відділу управління інформаційною системою або відділу інформаційної безпеки. Значення такого відділу у різних галузях бізнесу є діаметральним. Очевидно, що зусилля управління бізнесом в аграрному секторі повинні бути зосереджені на узгодженні загальної стратегії та стратегії управління захистом інформаційних активів аграрного підприємства [74; 89; 93; 94];

відсутність підтримки вищого керівництва. Управління ризиком інформаційної безпеки є основою інформаційної стратегії аграрного підприємства, безпосередньо пов'язаної зі стратегічним планом і бізнес-стратегією. Недооцінка важливості інформаційної безпеки вищим керівництвом є причиною значних порушень в економічній, технологічній, виробничій та інших сферах діяльності агропідприємства, що спричинено проблемами в інформаційному середовищі [89; 94; 101];

недостатнє технічне оснащення. Науково-технічний прогрес постійно підвищує вимоги до рівня технічного оснащення. Тому в сільському господарстві широко застосовуються технології «Інтернет речей», інтелектуальний моніторинг клімату, хмарні технології обміну даними, технології GPS для відстеження руху транспортних засобів і худоби тощо.

Використання застарілої технології негативно впливає на економічні показники підприємств і їх результативність. Використання застарілого обладнання робить бізнес-інформатику вразливою до нових загроз. Тому недостатньо використовувати сучасне програмне забезпечення без відповідного апаратного обладнання [89; 93; 102];

помилки технологій роботи з інформаційними ресурсами (апаратне, програмне забезпечення). Навіть незначна помилка технології обробки інформації може призвести до виникнення серйозних проблем, які спричиняють ланцюгову реакцію від виробництва сільськогосподарської продукції, зберігання, обробки або переробки до реалізації та споживання. Будь-яка помилка в інформаційній технології, що забезпечує виробничі та управлінські процеси аграрного суб'єкта господарювання може призвести до перерв (простоїв) у господарській діяльності підприємства, відділу, працівника, що є критичним, враховуючи специфіку діяльності та відповідно специфіку продукції сільського господарства [89; 109];

невідповідне програмне забезпечення. Програмне забезпечення повинно відповідати виробничим та управлінським запитам підприємства. Недостатньо володіти лише базовими комп'ютерними програмами та регулярно оновлювати програмне забезпечення. Окрім того, надмірне перенасичення програмним забезпеченням може збільшити ризик зниження інформаційної безпеки та кількість інцидентів її порушення [89; 93; 94; 101; 102];

відсутність внутрішніх стандартів, положень з інформаційної безпеки. Крім профілактичного контролю, важливим елементом управління інформаційною безпекою є здатність розпізнавати та оцінювати інциденти небезпеки та здійснювати відповідні коригувальні дії. Комплексне впровадження і дотримання стандартів і вказівок дозволяє зміцнити захист інформаційних активів і ефективно реагувати на інциденти порушень інформаційної безпеки [89; 101; 102];

відсутність або низький рівень фінансового забезпечення інформаційних систем і систем захисту інформації. Недофінансування безпосередньо впливає на рівень безпеки та спричиняє виникнення вразливостей захисту інформації [71; 89; 93; 109].

З-поміж зовнішніх факторів впливу на систему управління інформаційною безпекою аграрного підприємства слід виокремити:

сертифікацію. Стандарти серії ISO/IEC 27000, ISO 15408, ISO 17799 стосуються системи управління інформаційною безпекою (ISMS) та забезпечують загальну безпеку діяльності суб'єктів господарювання, в тому числі й аграрних [4; 6; 7]. На основі класифікації Макатура визначено основні причини необхідності впровадження стандартів захисту інформації –

забезпечення ринку, дотримання законодавчих вимог і вимог регулятора ринку. ISMS забезпечує можливість сільськогосподарського підприємства захищати інформаційні активи, таким чином гарантуючи збереження конфіденційності, цілісності та доступності інформації. ISMS є визнаною проактивною системою управління інформаційною безпекою всередині організації [7; 75; 94];

законодавство. В контексті інформаційної безпеки законодавство є предметом багатьох дискусій на вітчизняному та міжнародному рівні. Законодавство повинно враховувати проблеми власників інформаційних систем, потреби та права їх користувачів – як фізичних, так і юридичних осіб. Законодавчі вимоги до забезпечення інформаційної безпеки є найважливішим аспектом діяльності аграрних утворень. Наразі в Україні немає достатнього нормативно-правового забезпечення для ефективного регулювання усіх аспектів інформаційної діяльності та цифровізації соціально-економічних відносин, а особливо аспектів інформаційної безпеки;

державна підтримка інформаційної безпеки. Потреба в інформаційній безпеці реалізована національними урядами та міжурядовими організаціями, такими як ОЕСР, НАТО, ООН та багатьма іншими. Проте захист вітчизняного бізнесу державою, особливо з позиції інформаційної безпеки, є першочерговим завданням, яке потрібно нагально виконувати [71];

технологічний прогрес. Вплив новітніх інформаційно-комунікаційних технологій на бізнес-структури та суспільство загалом є значним, а в деяких аспектах – вирішальним. Проте ця позитивна тенденція зростає разом із ризиком інформаційної безпеки та кількістю інструментів, методів, способів, механізмів, спрямованих на порушення інформаційної безпеки;

ризик стихійного лиха або аварії. Цей фактор є постійною загрозою через непередбачуваність і масштабні наслідки. Катастрофи можуть призвести до фізичного пошкодження технічного обладнання і відповідно до всіх інших технологічних, економічних, соціальних і навіть екологічних наслідків;

неспроможність надання сторонніх послуг. Надання послуг і якість послуг, узгоджені договорами, повинні забезпечуватися, застосовуватися та дотримуватися третьою стороною. Найкращим способом контролю за забезпеченням інформаційної безпеки є регулярні звіти, ревізії, інспекції та система багаторівневих засобів управління на всіх рівнях управління. Водночас інформаційний аутсорсинг – це нове і не розповсюджене явище для вітчизняних суб'єктів аграрного ринку [24; 89].

Інша група авторів відзначає складність ідентифікації та оцінки факторів порушення інформаційної безпеки суб'єктів аграрного бізнесу. Тому вони

згруповують ряд найбільш значущих чинників, що зумовлюють виникнення подій інформаційної безпеки, серед яких:

- неповна, недостовірна й несвоєчасна внутрішня звітність на підприємстві та пов'язаний із нею конфлікт інтересів;

- наявність стохастичної складової (сфер неформалізованої діяльності), що виключає будь-які форми контролю за діяльністю;

- недосконалість ролей, організаційної політики, брак відповідальності та пов'язана з цим інсайдерська діяльність;

- зловмисна активність персоналу;

- конкуренція організації за ресурси із зовнішніми суб'єктами;

- організаційна, функціональна та інформаційна недосконалість інформаційної сфери підприємства;

- недосконалість менеджменту в контексті накопичення, узагальнення, застосування досвіду захисту інформації для досягнення цілей підприємства;

- неможливість прогнозованості змін факторів, які призводять до збільшення кількості базових інформаційних ризиків, пов'язаних зі зміною, пошкодженням, модифікацією та втратою інформації.

Як зазначалося в розділі 1 цього дослідження, загрози інформаційній безпеці від персоналу становлять вагому групу ризиків інформаційної безпеки підприємств агропродовольчої сфери, оскільки спектр причин та умов їх реалізації дуже широкий. Узагальнюючи положення [12; 14; 20; 54; 83; 86; 89; 93], доцільно вирізняти такі види загроз цієї групи для підприємств агропродовольчої сфери:

- загрози, пов'язані з навмисними діями осіб, що мають доступ до інформаційних систем аграрних підприємств, включаючи активних користувачів інформаційної системи та співробітників, які реалізують загрози безпосередньо всередині підприємства (внутрішні порушники);

- загрози, пов'язані із навмисними діями осіб, що не мають доступу до інформаційних систем підприємства та реалізують загрози із зовнішніх мереж зв'язку загального користування або мереж міжнародного інформаційного обміну;

- загрози, пов'язані з навмисними діями осіб, що не мають доступу до інформаційних систем і реалізують загрози технічними каналами витоку інформації [85].

У межах вищезазначеної групи також доцільно вирізнити випадкові та навмисні джерела спричинення загроз інформаційній безпеці. Випадкові (ненавмисні) джерела передбачають такі вразливості, як помилки, вчинені під час проектування інформаційної системи підприємства та її елементів, помилки в процесі розробки або адаптації програмного забезпечення, різної

збої та відмови апаратних засобів, пошкодження, притаманні інформаційній системі. До таких джерел можна зарахувати персонал власне аграрного підприємства, персонал підприємств-контрагентів, персонал постачальників різноманітних послуг. Дії (загрози) цих джерел відбуваються через незнання, неуважність або недбалість, з цікавості, але без злого наміру.

Навмисні джерела проявляються в корисливих діях зловмисників. Основна мета таких джерел – умисна дезорганізація роботи, припинення функціонування інформаційної системи підприємства, спотворення, модифікація або знищення інформації через проникнення в інформаційні ресурси підприємства шляхом несанкціонованого доступу.

Внутрішні суб'єкти (джерела) – це, як правило, висококваліфіковані фахівці у сфері розробки та експлуатації програмного забезпечення й технічних засобів, які мають знання відносно специфіки виконуваних завдань, структури та основних функцій, принципів роботи програмно-апаратних засобів захисту інформації, мають можливість використовувати штатне обладнання й технічні засоби мережі. До них належать управлінський персонал, провідні фахівці, персонал, який забезпечує функціонування інформаційної системи підприємства або здійснює управління інформаційною безпекою, основний виробничий персонал, допоміжний персонал, технічний персонал. Серед внутрішніх джерел загроз особливе місце посідають загрози у вигляді помилкових дій та/або порушень вимог експлуатаційної та іншої документації співробітниками підприємства агропродовольчої сфери [100].

Враховуючи те, що значна частина внутрішніх загроз реалізується за участі або сприяння персоналу, можна вважати, що основним джерелом таких загроз є працівники цього підприємства. Тому М. Будник і Д. Тимофеев вважають, що внутрішні загрози інформаційній безпеці можуть утворюватися внаслідок непрофесійних дій працівників, низького стану виховної та профілактичної роботи на підприємствах агропродовольчої сфери, недосконалої системи заробітної плати та стимулювання праці персоналу, порушень правил кадрової роботи, невідповідності кадрової політики умовам роботи в організації, психологічних і комунікаційних особливостей працівників, відсутності нормативної бази, яка б визначала режими діяльності та правила поведінки персоналу, низького стану трудової та виробничої дисципліни, слабкої вимогливості керівного складу [20].

Розглянуті положення дозволили визначити сім основних типів порушників інформаційної безпеки: зовнішній зловмисник (індивідуальний, кримінальні структури), контрагент підприємства, конкурент підприємства, вище керівництво підприємства, адміністратор інформаційної системи або

системи інформаційної безпеки, працівник підприємства, персонал постачальників різних послуг (аутсорсинг) [20; 54; 89; 104]. На основі зазначеного проранжовано основні типи порушників (включаючи зовнішніх порушників) залежно від масштабу передбачуваного збитку від їх дій. Виведено середній бал (рівень небезпеки) для кожного типу порушника (рис. 2.1).

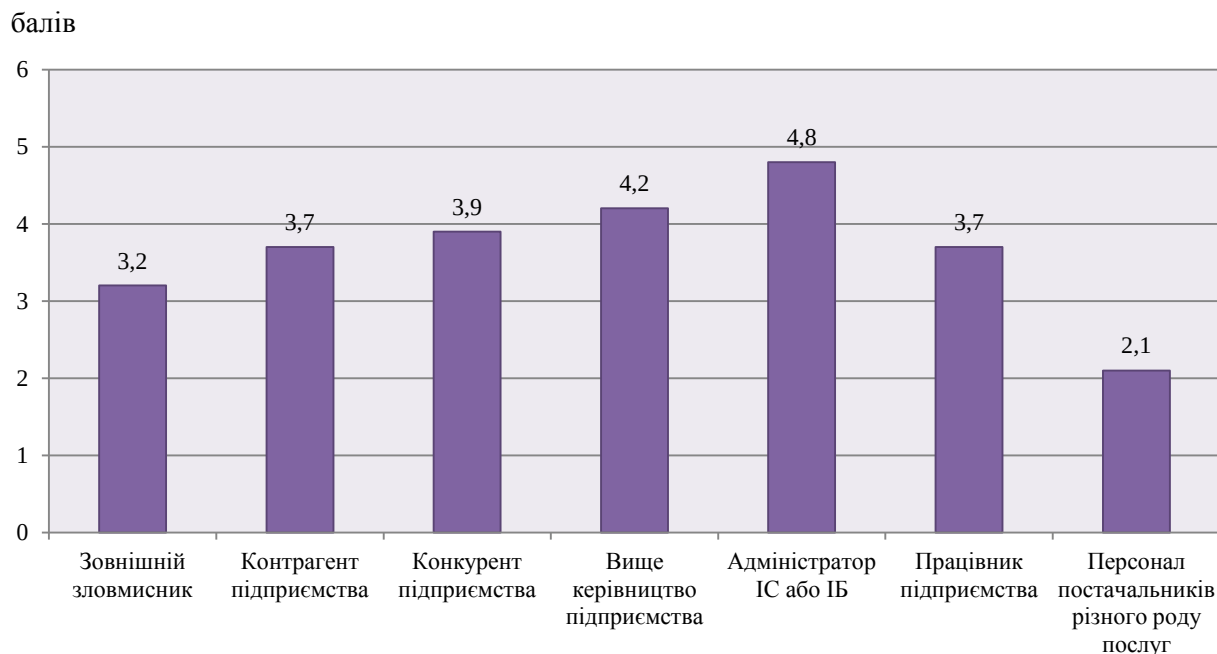


Рис. 2.1. Карта порушників з типами порушників за тяжкістю передбачуваних втрат для бізнесу (за п'ятибальною шкалою) [сформовано на основі 69; 87; 104; 121]

Результати аналізу показали, що найбільшою загрозою є співробітники з розширеними правами доступу до інформації та інформаційної інфраструктури – адміністратори мережі, баз даних, системи захисту інформації тощо. Проте сам розподіл є майже однорідним – розбіжність результатів в межах 1,6 бала (в діапазоні 3,2–4,8), не враховуючи персонал постачальників різних послуг (аутсорсинг), оскільки цей вид порушників, як і вид послуг у вітчизняних суб'єктів господарювання агропродовольчої сфери, є доволі рідкісним явищем з результатом 2,1 бала.

На основі узагальнення класифікації загроз інформаційній безпеці підприємства від персоналу та сформованої карти порушників з їх типами за тяжкістю передбачуваних втрат для бізнесу сформовано структурно-логічну схему суб'єктно-об'єктних відносин (рис. 2.2).

З огляду на вищезазначену структурно-логічну схему суб'єктно-об'єктних відносин захисту інформації від внутрішніх і зовнішніх суб'єктів доцільно зазначити, що зовнішні суб'єкти можуть як діяти самостійно, так і

впливати на внутрішніх суб'єктів і спричиняти загрози інформаційній безпеці через дії або бездіяльність останніх.

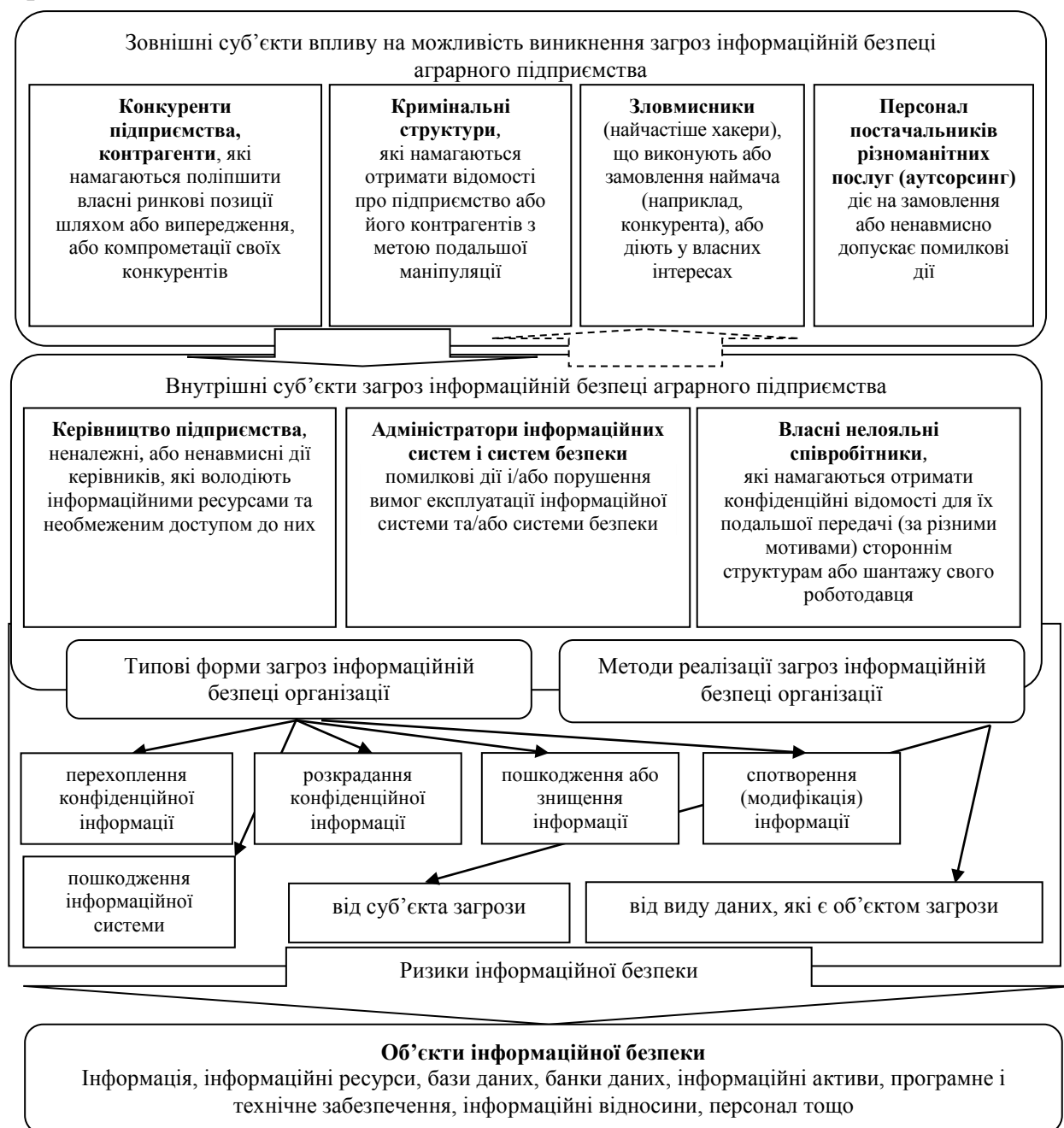


Рис. 2.2. Структурно-логічна схема суб'єктно-об'єктних відносин захисту інформації від внутрішніх і зовнішніх суб'єктів на підприємствах агропродовольчої сфери [авторська розробка]

У свою чергу, внутрішні суб'єкти можуть впливати на систему інформаційної безпеки через залучення зовнішніх суб'єктів, особливо індивідуальних зловмисників і кримінальних структур. У будь-якому із перелічених випадків результатом такої діяльності є виникнення ризику загрози інформаційній безпеці.

З цією метою пропонується описати ризики інформаційної безпеки від

зовнішніх і внутрішніх суб'єктів у вигляді факторної моделі – системи причин та умов, що сприяють реалізації таких ризиків. Загальна структура факторної моделі ризиків інформаційної безпеки від зовнішніх і внутрішніх суб'єктів представлена на рис. 2.3.

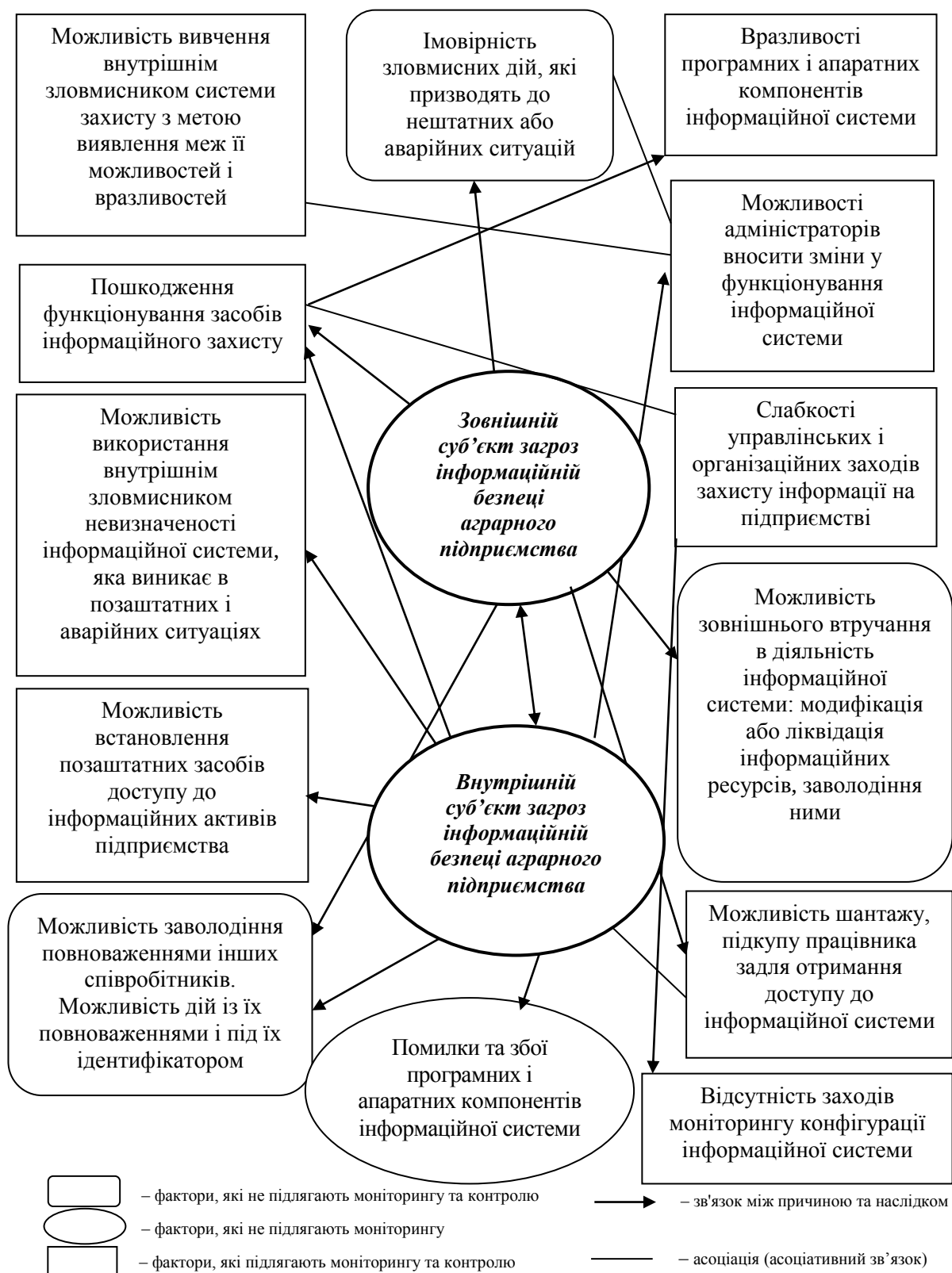


Рис. 2.3 Структура факторної моделі ризиків порушень інформаційної безпеки від зовнішніх і внутрішніх суб'єктів [доопрацьовано на основі 12]

Фактори ризику в межах пропонованої моделі поєднані в єдину мережу причинно-наслідковими зв'язками.

Усі фактори системи пов'язані в межах величезної причинно-наслідкової мережі, в якій частина підлягає моніторингу та контролю і частина прихована від менеджменту підприємства.

Пропонована система моделі факторів може бути використана для:
визначення сукупності факторів, які підлягають моніторингу і контролю,
та розробка способів їх вимірювання;

визначення сукупності контрольованих факторів і встановлення механізму їх контролю;

організації за допомогою створених механізмів системи контролю ризиків інформаційної безпеки, пов'язаних із зовнішніми та внутрішніми суб'єктами;

здійснення за допомогою створеної системи контролю послідовних заходів щодо приведення ризиків інформаційної безпеки у відповідність до очікуваного рівня.

Крім того, модель ризиків порушення інформаційної безпеки від зовнішніх і внутрішніх суб'єктів може бути використана для виконання таких завдань:

зіставлення значимості для підприємств агропродовольчої сфери різних загроз інформаційній безпеці залежно від суб'єктів;

оцінка можливих змін значущості загроз інформаційній безпеці залежно від суб'єктів унаслідок змін, що проводяться в інформаційному середовищі підприємства;

підтримка діяльності з розробки на підприємстві внутрішніх нормативних і організаційно-розпорядчих документів інформаційного захисту;

аналітичне забезпечення діяльності з виявлення сфер підвищеного ризику порушень інформаційної безпеки від зовнішніх і внутрішніх суб'єктів;

інші завдання, пов'язані як із прийняттям рішень про захисні заходи, так і з застосуванням захисних заходів.

Отже, пропонована структурно-логічна схема суб'єктно-об'єктних відносин захисту інформації від персоналу підприємства та мережна модель ризиків загроз інформаційній безпеці від персоналу в їх інтеграції забезпечать формування ефективної системи інформаційної безпеки підприємства, постійну підтримку атмосфери відповідального ставлення до питань безпеки, зменшення негативного впливу людського чинника на захищеність інформаційних систем і стан інформаційної безпеки, а отже, дозволить обрати відповідні ситуаційні

заходи для протидії виникненню і реалізації інформаційних загроз від зовнішніх і внутрішніх суб'єктів.

З метою визначення основних загроз інформаційній безпеці підприємств аграрної сфери України було взято за основу класифікацію, запропоновану зарубіжними дослідниками [89; 93], яку було доповнено та адаптовано до умов функціонування вітчизняних суб'єктів господарювання агропродовольчої сфери. На основі проведеного анкетування фахівців різних за розміром, організаційно-правовою формою, спеціалізацією, та територіальним розміщенням підприємств агропродовольчої сфери (Додаток Ц) визначено основні групи факторів, які впливають на формування загроз їх інформаційній безпеці та управління нею (за баловою системою) (табл. 2.13).

Таблиця 2.13

Внутрішні та зовнішні фактори впливу на виникнення загроз інформаційній безпеці та управління нею на аналізованих аграрних підприємствах (2014–2018 рр.), в балах [сформовано на основі 89; 93; 99; 100; 101; 102; 127]

Групи факторів	Фактори	ПрАТ «ЛОЕЗ Кернел-груп»	ФГ «Батківщина»	СК «Іскра»	СТОВ «Мусіївське»	ПрАТ «Агрогон»	ТОВ «РОСТ АГРО»	ПСП «Солоничке»	СТОВ «Агрофірма «Оржипка»	ТОВ «Агрофірма ім. Довженка»	СТОВ «Агрофірма «Дружба»	ПП «Альгаір»	ФГ «Товсте»	ПП «Надь»	СФГ «Зеніт»	ТОВ «АПК Докучаєвські чорноземи»	Середнє значення	Ранг фактора
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Внутрішні	Неосвіченість працівників	4	4	5	4	5	4	3	4	4	3	4	5	4	5	5	4,20	1
	Поведінка працівника	3	4	3	4	3	5	4	3	4	4	4	4	3	4	4	3,73	2
	Дії зловмисників	3	2	2	2	2	2	3	1	2	2	1	2	2	1	2	1,93	12
	Відсутність відділу управління інформаційною системою	4	1	1	2	2	1	1	1	2	2	1	1	1	1	2	1,53	16
	Відсутність підтримки вищого керівництва	3	2	2	3	4	2	2	2	3	3	2	4	4	2	4	2,80	6
	Застаріле технічне обладнання	4	2	2	2	2	3	2	3	2	2	2	2	2	3	2	2,33	8

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	Помилки технологій роботи інформаційними ресурсами з	3	2	3	2	2	2	2	2	2	2	2	2	2	1	2	2,07	10
	Недостатній рівень програмного забезпечення	5	3	3	3	4	3	3	3	4	3	2	2	1	3	3	3,00	5
	Відсутність внутрішніх інструкцій і стандартів	4	3	2	2	3	3	2	3	4	2	1	2	1	3	2	2,47	7
	Відсутність або низький рівень фінансування ресурсів інформаційних систем і систем захисту інформації	3	2	2	2	3	2	1	2	1	1	1	1	1	1	2	1,67	15
	Відсутність стратегії інформаційної безпеки та політики інформаційної безпеки	5	5	3	3	3	3	3	3	3	3	2	2	2	2	4	3,07	4
Зовнішні	Сертифікація	4	2	3	2	3	2	3	2	2	3	1	1	1	1	3	2,20	9
	Законодавство	3	2	2	2	3	2	1	2	2	2	1	1	1	1	2	1,80	13
	Державна підтримка інформаційної безпеки	3	1	2	1	2	1	2	1	1	1	1	2	2	1	1	1,47	17
	Технологічний прогрес	5	4	3	3	3	2	3	4	4	4	2	3	3	3	4	3,33	3
	Ризик стихійного лиха	3	4	2	2	2	2	3	2	2	2	2	1	1	1	1	2,00	11
	Помилка надання послуг сторонніми організаціями (аутсорсинг)	3	2	1	1	2	3	2	1	1	2	2	2	1	1	2	1,73	14

Оцінка від 1 до 5 по висхідній: 1 – найменший ступінь впливу фактора на формування загрози інформаційній безпеці підприємства; 2 – нижче середнього ступінь впливу фактора на формування загрози інформаційній безпеці підприємства; 3 – середній ступінь впливу фактора на формування загрози інформаційній безпеці підприємства; 4 – вище середнього ступінь впливу фактора на формування загрози інформаційній безпеці підприємства; 5 – найбільший ступінь впливу фактора на формування загрози інформаційній безпеці підприємства.

* Складено за матеріалами анкетування.

Відповідно до проведеного аналізу загроз системі управління інформаційною безпекою аграрних підприємств особливого значення набувають неосвіченість і поведінка працівника, технологічний прогрес, відсутність стратегії інформаційної безпеки та політики інформаційної безпеки, недостатній рівень програмного забезпечення.

Технологічний прогрес у цій сфері розглядається як найбільш значущий

зовнішній фактор. Технологічний прогрес галузі інформаційно-комунікаційних технологій сприяє позитивним змінам структури агропродовольчої сфери. Водночас існує безліч ризиків, які сприяють виникненню інцидентів інформаційної небезпеки.

Як найбільш значущий внутрішній фактор, який впливає на рівень інформаційної безпеки та на ефективність управління нею, було виокремлено неосвіченість працівників і, отже, поведінку працівників, яку розуміють як сукупність навмисних і ненавмисних дій, які призводять до виникнення загроз інформаційній безпеці.

Наступними за значеннями факторами є внутрішні фактори впливу: відсутність стратегії інформаційної безпеки, політики інформаційної безпеки та недостатній рівень програмного забезпечення.

Як найменш значущі фактори, які впливають на систему управління інформаційною безпекою підприємств агропродовольчої сфери, фахівці відзначили переважно зовнішні фактори, серед яких: відсутність законодавства щодо забезпечення інформаційної безпеки вітчизняних суб'єктів господарювання, помилка надання послуг сторонніми організаціями (аутсорсинг) через низький рівень використання аутсорсингу підприємствами агропродовольчої сфери та незначний рівень державної підтримки інформаційної безпеки.

Серед внутрішніх факторів була відмічена відсутність або низький рівень фінансування ресурсів інформаційних систем і систем захисту інформації, що спричинено тим, що керівництво та фахівці переконані, що при незначному рівні витрат на забезпечення інформаційної безпеки можливо створити ефективні системи захисту та немає потреби у відділі управління інформаційною системою, оскільки утворення організаційної одиниці не завжди є фінансово та організаційно доцільним і можна обмежитися делегуванням функцій інформаційного захисту окремим фахівцям інформаційного відділу або найняти окремого фахівця – менеджера або адміністратора системи інформаційної безпеки.

Разом з тим анкета містила питання про основні наслідки загроз інцидентів порушення інформаційної безпеки на досліджуваних підприємствах за п'ятирічний період (2014–2018 рр.), результати якої дозволили узагальнити та визначити найбільш розповсюджені загрози інформаційній безпеці аграрних підприємств (табл. 2.14).

Отже, відповідно до аналізованих даних найбільш розповсюдженими наслідками порушення інформаційної безпеки підприємств агропродовольчої сфери є перерва в господарській діяльності підприємства або працівника, спричинена неможливістю виконання певних управлінських або виробничих

процесів, знищення / пошкодження програмного забезпечення та апаратних засобів, пошкодження елементів інформаційної системи підприємства, недоступність ІКТ-послуг через зовнішні атаки (електронна пошта, Інтернет, віддалений доступ, хмарна технологія, вебсайт тощо).

Таблиця 2.14

Наслідки настання загроз інформаційній безпеці для аналізованих аграрних підприємств, в балах (2014–2018 рр.) [сформовано на основі 89; 93; 127]

Фактори	ПрАТ «ПОЕЗ Кернел-груп»	ФГ «Батківщина»	СК «Іскра»	СТОВ «Мушківське»	ПрАТ «Агротон»	ТОВ «РОСТ АГРО»	ПСП «Солоницьке»	СТОВ «Агрофірма «Оржицька»	ТОВ «Агрофірма ім. Довженка»	СТОВ «Агрофірма «Дружба»	ПП «Альгаір»	ФГ «Говсте»	ПП «Надь»	СФГ «Зеніт»	ТОВ «АПК Докучаєвські чорноземи»	Середнє значення	Ранг фактора
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Знищення / пошкодження апаратних засобів	2	1	2	2	2	1	2	2	3	2	0	1	1	1	1	1,53	4
Знищення / пошкодження програмного забезпечення	4	2	2	2	3	3	2	2	1	1	2	1	1	2	1	1,93	2
Проникнення в інформаційну систему підприємства	3	2	2	1	2	3	2	1	1	0	0	0	0	0	2	1,27	6
Пошкодження елементів інформаційної системи підприємства	3	2	2	2	4	3	2	2	2	1	0	1	0	1	2	1,80	3
Несанкціонований доступ до інформаційних активів та інформаційних ресурсів	3	1	1	1	2	2	0	1	1	0	0	0	0	0	2	0,93	7
Знищення даних	1	1	1	1	2	1	1	1	2	0	0	0	0	0	1	0,80	8
Втрата конфіденційних даних	0	0	0	0	3	0	2	0	0	1	0	0	1	0	1	0,53	9
Несанкціонована модифікація інформації	2	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0,33	10

Продовж. табл. 2.14

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Розкриття / викрадення фінансової інформації	0	0	0	1	1	0	0	0	1	0	0	0	0	0	1	0,27	11
Недоступність ІКТ-послуг через зовнішні атаки (електронна пошта, Інтернет, віддалений доступ, хмарна технологія, веб-сайт тощо)	1	1	1	1	2	1	2	1	2	0	1	2	2	2	2	1,40	5
Перерва в господарській діяльності підприємства / працівника	1	2	2	2	3	2	2	3	3	2	3	3	2	2	3	2,33	1
Заподіяння шкоди діловій репутації / бренду підприємства	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	12

Оцінка від 0 до 5 по висхідній: 0 – подія внаслідок настання загроз інформаційній безпеці не настала; 1 – подія внаслідок настання загроз інформаційній безпеці наставала рідше, ніж 1 раз на рік; 2 – подія внаслідок настання загроз інформаційній безпеці наставала не рідше, ніж 1 раз на рік; 3 – подія внаслідок настання загроз інформаційній безпеці наставала не рідше, ніж 1 раз на квартал; 4 – подія внаслідок настання загроз інформаційній безпеці наставала не рідше, ніж 1 раз на місяць; 5 – подія внаслідок настання загроз інформаційній безпеці має певну періодичність (не рідше, ніж 1 раз на тиждень).

* Складено за матеріалами анкетування.

Найменш розповсюдженими наслідками порушення інформаційної безпеки підприємств є несанкціонована модифікація інформації, розкриття або викрадення фінансової інформації, заподіяння шкоди діловій репутації / бренду підприємства.

Проведений аналіз дозволив визначити основні фактори впливу на стан управління інформаційним захистом підприємств агропродовольчої сфери та наслідки настання загроз інформаційній безпеці, до яких призводить їх реалізація. На основі узагальнення сформовано карту впливу зовнішніх і внутрішніх факторів на виникнення загроз інформаційній безпеці аграрних підприємств (рис. 2.4).

Це дало змогу визначити неосвіченість і поведінку працівників, дії зловмисника, відсутність відділу управління інформаційною системою і недостатній рівень програмного обладнання як основні внутрішні фактори, які спричиняють порушення інформаційної безпеки суб'єктів аграрного бізнесу та заважають здійсненню ефективних процесів управління нею.

До зовнішніх факторів впливу на цілісність інформаційних активів аграрного товариства слід зарахувати: технологічний прогрес і помилку надання послуг сторонніми службами, а також стихійні лиха.

Проведене дослідження дозволило охарактеризувати сучасні загрози системі управління інформаційною безпекою підприємств агропродовольчої сфери України та визначити ключові зовнішні та внутрішні фактори впливу на їх формування та виникнення. Це, в свою чергу, дозволило сформувати карту ризиків порушення інформаційної безпеки суб'єктів аграрного бізнесу, що в подальшому сприятиме оцінці цих ризиків і формуванню напрямів зниження рівня їх інформаційної небезпеки, ефективності управління нею. Проте карта ризиків не дозволяє визначити рівень наслідків реалізації кожного окремого фактора та їх впливу при одночасній взаємодії декількох із них. Тому наступним етапом дослідження стане безпосередня кількісна оцінка рівня інформаційної безпеки підприємств агропродовольчої сфери.

2.3. Аналіз рівня інформаційної безпеки підприємств агропродовольчої сфери України

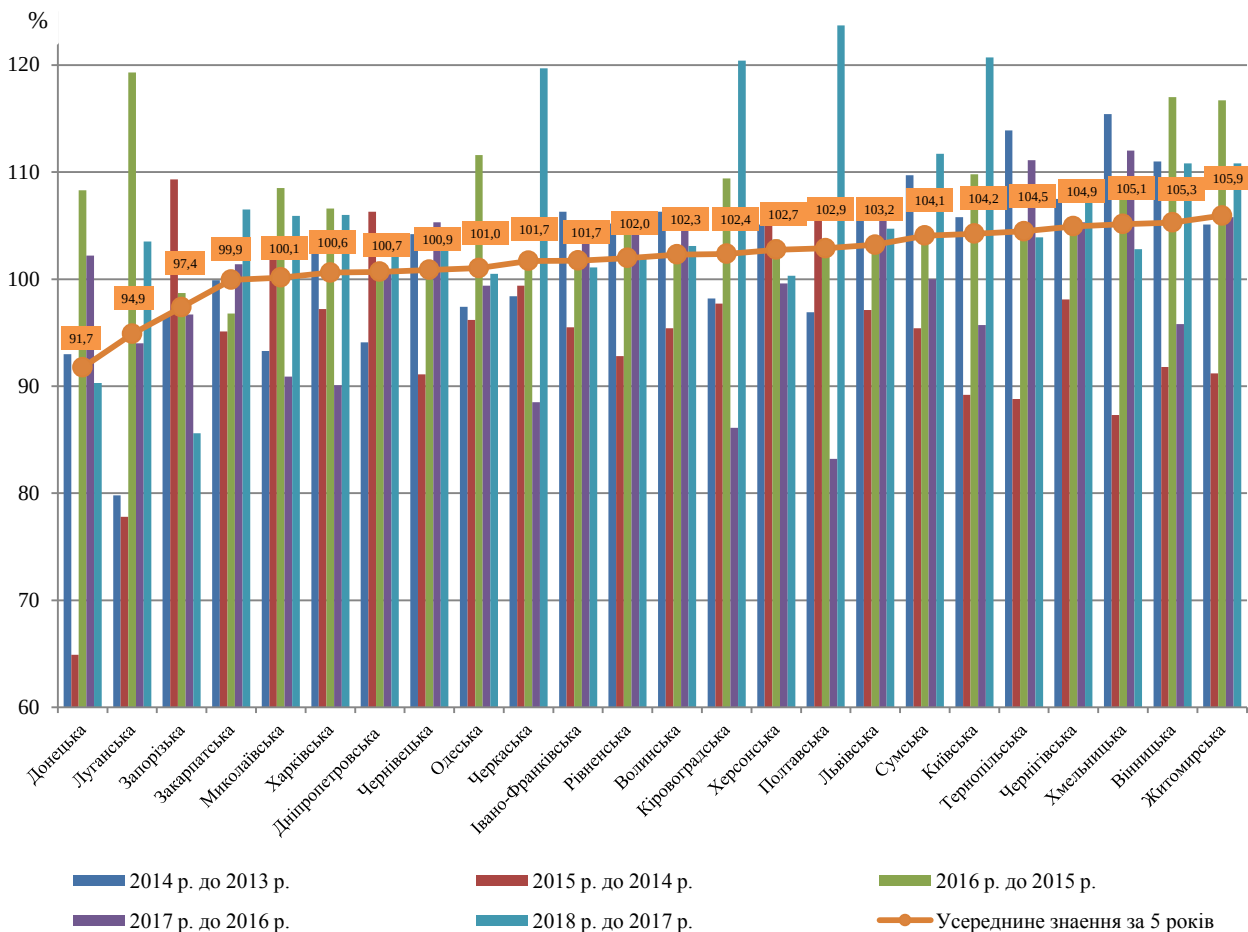
В нинішній час для забезпечення належного стану інформаційної безпеки потрібна не просто розробка окремих механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів тощо). Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування підприємства, запобігання загроз його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення в рамках виробничої діяльності всіх підрозділів підприємства.

А. Велігура зазначає, що процес забезпечення інформаційної безпеки підприємства можна представити як взаємодію трьох підсистем: підсистема інформаційного забезпечення процесу управління на підприємстві; підсистема захисту інформаційного середовища підприємства; підсистема діагностики рівня інформаційної безпеки. Ключовими задачами підсистеми інформаційного забезпечення процесу управління на підприємстві є: збирання необхідної інформації; обробка і систематизація інформації; оцінка й аналіз інформації; прогнозування всіх аспектів діяльності підприємства; надання необхідної інформації особам, що приймають рішення. Безперервне виконання всіх цих задач необхідне для ефективного функціонування зазначеної підсистеми. Захист інформаційного середовища підприємства включає захист від зловмисних дій як конкурентів, так і

власних співробітників, а також захист від незловмисних внутрішніх негативних впливів [22].

З метою проведення об'єктивної оцінки рівня інформаційної безпеки підприємств агропродовольчої сфери було здійснено анкетування управлінського персоналу, провідних фахівців сільськогосподарських підприємств різних напрямів діяльності та спеціалістів у сфері забезпечення інформаційної підтримки, інформаційної безпеки суб'єктів господарювання аграрного сектора Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей.

Такий вибір областей зумовлений рівнем приросту виробництва продукції сільськогосподарського призначення підприємств за 2013–2018 рр. (Додаток III), (рис. 2.5), оскільки зазначений показник характеризує одночасно економічний стан підприємств окремої області та їх продовольчий потенціал, що є основними показниками результативності їх діяльності.



Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій і Луганській областях.

Рис. 2.5. Рейтинг областей України за усередненим показником приросту виробництва сільськогосподарської продукції за 2013–2018 рр. [згруповано на основі 107; 108; 113; 118]

З метою проведення об'єктивного аналізу, встановлення взаємозв'язків між показниками інформаційної безпеки підприємств агропродовольчої сфери та економічної діяльності та для надання більш точних прогнозів враховано й кластеризацію областей України за індексом сільськогосподарської продукції за 2018 р. (Додаток Щ).

З-поміж областей із підприємствами-лідерами за приростом агровиробництва обрано Полтавську область (усереднений показник – 102,7 %, 2018 р. – 123,7 %), Сумську (усереднений показник – 104,1 %, 2018 р. – 111,7 %) та Кіровоградську (усереднений показник – 102,4 %, 2018 р. – 120,4 %). З-поміж областей, що мають підприємства із середнім рівнем приросту сільськогосподарської продукції обрано Харківську область (усереднений показник – 100,6 %, 2018 р. – 106,0 %).

Підприємства Луганської області обрано як підприємства з від'ємним значенням приросту виробництва продукції сільськогосподарського призначення (усереднений показник – 94,9 %, 2018 р. – 103,5 %).

Вибірка підприємств здійснювалась таким чином, щоб аналіз міг охопити як підприємства областей-лідерів (Полтавська, Сумська, Кіровоградська), підприємства областей середнього рівня за рейтингом приросту виробництва продукції (Харківська) та підприємства Луганської області, які мають від'ємний відсоток приросту.

Для аналізу використано дані 74 підприємств агропродовольчої сфери та опитано 238 працівників на основі анкетування (Додаток Ю). Зазначена кількість об'єктів дослідження дозволяє стверджувати про об'єктивність отриманих результатів аналізу, оскільки найважливіші тенденції найкращим чином відображаються на великій кількості об'єктів дослідження, тому що діє закон великих чисел. Відповідно до запропонованої системи показників діагностики, яка включає п'ять груп показників оцінки рівня інформаційної безпеки підприємств агропродовольчої сфери, що характеризують різні її аспекти (програмно-технічної захищеності інформаційної системи, фінансування забезпечення інформаційної безпеки підприємства, інформаційної надійності персоналу, інформації, що надається ОПР, системі інформаційного забезпечення / системі інформаційного захисту, системі інформаційної безпеки підприємства) (Додаток Я) [39], та результатів анкетування здійснено групування первинних показників інформаційної безпеки підприємств аграрного комплексу кожної із зазначених областей і визначено їх середні значення за період 2009–2018 рр. (Додаток АА).

Для проведення аналізу та можливості зіставлення та порівняння показників інформаційної безпеки підприємств агропродовольчої сфери було розраховано їх усереднені значення.

Відповідно до розрахунків усереднених значень групи показників оцінки програмно-технічної захищеності інформаційної системи підприємств агропродовольчої сфери (рис. 2.6) з найвищим значенням коефіцієнта технічного захисту інформаційної системи – 0,777 лідируючі позиції посідають підприємства Полтавської та Сумської областей, що свідчить про потужну технічну частину системи інформаційної безпеки підприємств, яка забезпечує відбиття інформаційних і кібератак. Питома вага відбиття атак підприємствами Кіровоградської області становила близько 70,6 % за період 2009–2018 рр. Дещо меншими є показники аграрних підприємств Харківської та Луганської областей – 0,619 та 0,622 відповідно.

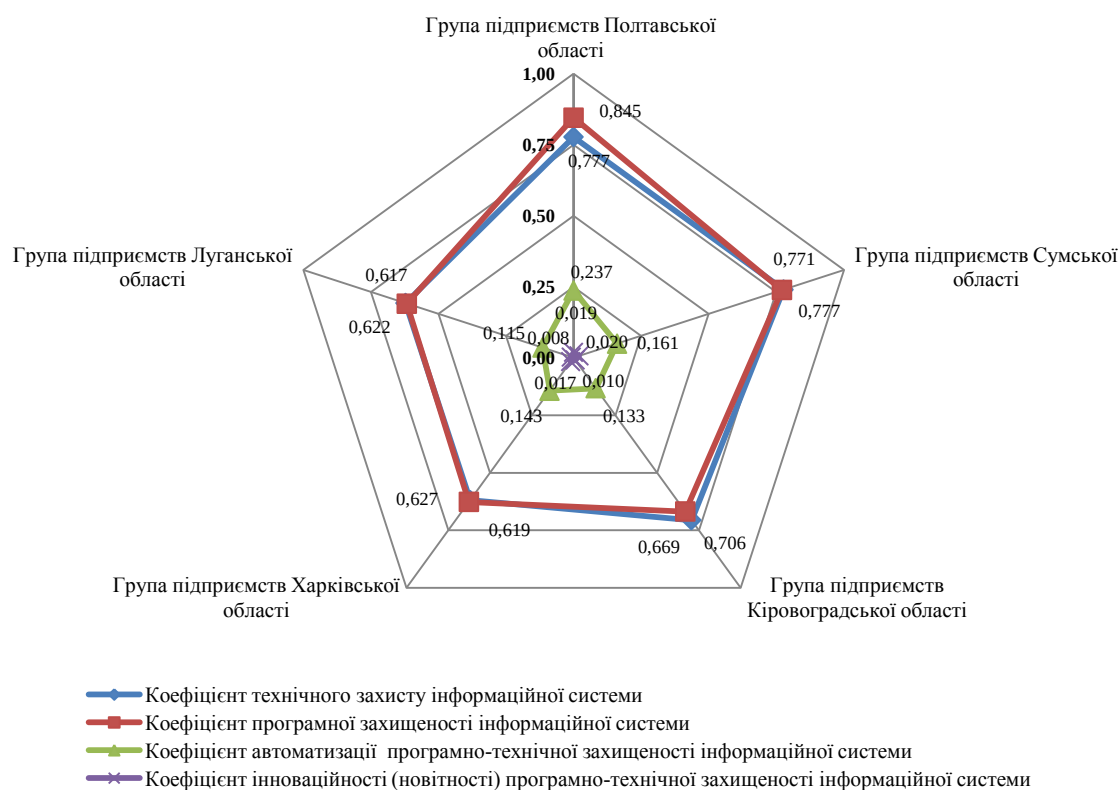


Рис. 2.6. Усереднені показники оцінки програмно-технічної захищеності інформаційної системи підприємств агропродовольчої сфери Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей [побудовано автором]

Наступний показник зазначеної групи, а саме коефіцієнт програмної захищеності інформаційної системи – 0,845, свідчить про ефективність безперебійного функціонування інформаційної системи Полтавської області. Найгірші значення показника спостерігаються в сільськогосподарських підприємствах Харківської та Луганської областей.

Невисоким є значення коефіцієнта автоматизації програмно-технічної захищеності інформаційної системи з-поміж досліджуваних підприємств

агропродовольчої сфери, що дозволяє стверджувати про необхідність автоматизації процесів інформаційного захисту та автоматизації процесів управління системою безпеки загалом. Найбільше значення показника мають підприємства Полтавської області – 23,7 % автоматизації процесів інформаційної безпеки. Найменше значення цього коефіцієнта серед аграрних підприємств Луганської області – лише 11,5 % автоматизації.

Незначним є і значення коефіцієнта інноваційності програмно-технічної захищеності інформаційної системи, що передбачає збільшення чисельності вразливостей інформаційної системи з позицій технічного захисту, оскільки програмні додатки й апаратні засоби, що забезпечують дотримання інформаційної безпеки є морально застарілими та не в змозі протистояти новітнім видам інформаційних і кібератак. Найвищим цей показник є на сільськогосподарських підприємствах Сумської області – і становить лише 2 % від загальної кількості технічного й програмного забезпечення.

Загалом показники цієї групи свідчать про рівень «нижче середнього» забезпечення технічними та програмними засобами інформаційної системи досліджуваних підприємств і вказують на необхідність фінансування зазначених складових інформаційної безпеки. Особливо це стосується агропродовольчих підприємств Кіровоградської, Харківської та Луганської областей.

Тому наступна група показників оцінки інформаційної безпеки – це показники оцінки фінансових витрат на її забезпечення (рис. 2.7).

Аналіз показників витрат на забезпечення інформаційної безпеки досліджуваних підприємств агропродовольчої сфери дозволив дійти висновку, що їх фінансування на досить низькому рівні, зокрема найбільше усереднене значення коефіцієнта фінансування інформаційної безпеки на підприємствах Полтавської області – лише 0,042, що вказує на недостатній рівень фінансового забезпечення інформаційного захисту, оскільки нормативне значення цього показника повинно бути не нижче 0,070. Дещо меншим є значення цього показника на підприємствах Сумської області – 0,038, та взагалі незначним на підприємствах Кіровоградської, Харківської та Луганської областей – від 0,017 до 0,024.

У розрізі цього коефіцієнта виокремлено його складові:

коефіцієнт фінансування інформаційних служб підприємства, значення якого до 2013 р. було нульовим через те, що майже на всіх досліджуваних підприємствах не існувала окрема структурна одиниця управління інформаційним забезпеченням. Фінансові ресурси спрямовувалися лише на оплату праці окремих фахівців, які перебували у складі інших підрозділів, проте виконували функції адміністраторів інформаційних систем аграрних

підприємств. Значення коефіцієнта є найбільшим у підприємств Полтавської області коливалося близько 0,030 за період 2013–2018 рр. Найменше значення цього показника спостерігалось у сільськогосподарських підприємств Луганщини, Кіровоградщини та Харківщини, усереднені значення яких за 2009–2018 рр. становили 0,005, 0,006 та 0,008 відповідно при нормативному значенні 0,030–0,040;

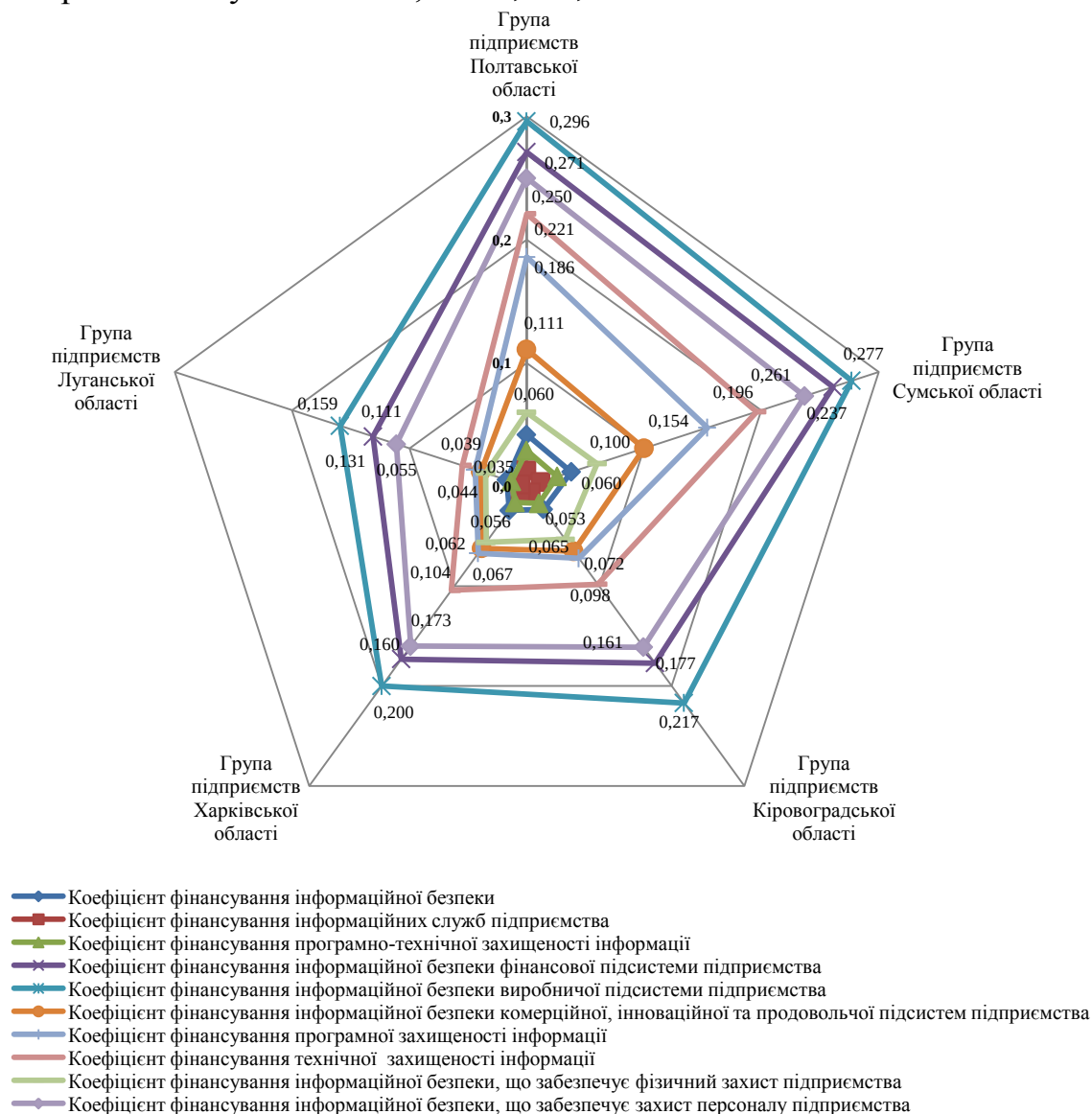


Рис. 2.7. Усереднені показники оцінки фінансування (витрат) забезпечення інформаційної безпеки підприємств агропродовольчої сфери Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей [побудовано автором]

коефіцієнт фінансування програмно-технічної захищеності інформації, усереднене значення якого майже сягає нормативного у підприємств Полтавської області – 0,029 та є дещо меншим за норматив у підприємств Сумщини – 0,026. Значення коефіцієнта свідчить про орієнтованість

підприємств агропродовольчої сфери цих областей на розробку та придбання перш за все програмних і технічних засобів захисту фінансової, виробничої, інноваційної, продовольчої та інших сфер діяльності. Вищезазначене підтверджується і вищим за норматив значенням коефіцієнта за 2014–2018 рр. аграрних підприємств Полтавської області (5 % на програмно-технічний захист від загальних витрат) і аграрних підприємств Сумської області за 2014 р. і 2016–2018 рр. (4 % на програмно-технічний захист від загальних витрат підприємств). Керівництву досліджуваних підприємств доцільно звернути увагу на управлінський аспект інформаційного захисту, оскільки від суб'єкта управління на 80 % залежить ефективність цього процесу [30; 58].

Розглядаючи співвідношення витрат на забезпечення інформаційної безпеки, спрямованої на захист фінансової підсистеми аграрного підприємства, до загальних витрат на інформаційну безпеку, доцільно відзначити низький рівень фінансування. При нормативах 40–45 % від загальних витрат на фінансування інформаційної безпеки підприємства агропродовольчої сфери Полтавщини витрачали в середньому 27,1 % протягом 2009–2018 рр., підприємства Сумщини – 26,1 %, аграрні підприємства Кіровоградщини – 17,7 %, Харківщини – 17,3 %. Аутсайдерами в цьому переліку були сільськогосподарські підприємства Луганщини, витрат на забезпечення інформаційного захисту фінансової сфери яких становили 13,1 %.

В умовах інформатизації та цифровізації соціально-економічних відносин, автоматизації виробничих процесів аграрних підприємств важливою особливістю сільськогосподарського виробництва є необхідність його захисту не тільки від негативного впливу природно-кліматичних і екологічних факторів. Інформаційна безпека виробничого процесу на підприємствах агропродовольчої сфери набуває особливого та важливого значення, оскільки втрата новітніх технологій виробництва сільськогосподарської продукції, землекористування при сучасних тенденціях автоматизації та віртуалізації, витік інформації про контрагентів, про фінансові показники діяльності підприємства та його персонал критично впливають на ефективність діяльності та ставлять під загрозу подальше перебування конкретного суб'єкта господарювання на аграрному ринку.

Проведені розрахунки та результати анкетного опитування керівників і фахівців досліджуваних сільськогосподарських підприємств дозволили констатувати низький рівень фінансування інформаційного захисту виробничої сфери. Зокрема підприємства Полтавської області витратили від 21 до 35 % у різні періоди протягом 2009–2018 рр. (усереднене значення –

29,6 %) від загальних витрат на забезпечення інформаційної безпеки. Підприємства Сумської області – від 19 до 37 % (усереднене значення – 27,7 %), Кіровоградщини – від 16 до 31 % (усереднене значення – 21,7 %), аграрні підприємства Харківщини – від 15 до 25 % (усереднене значення – 20,0 %), Луганщини – від 14 до 19 % (усереднене значення – 15,9 %). Такий рівень витрат не забезпечує необхідні умови для ефективного захисту виробничої сфери, що потребує збільшення фінансування заходів інформаційної безпеки, з одного боку, та розробки більш ефективного механізму управління інформаційною безпекою, який би базувався на новітніх технологіях захисту інформації – з іншого. Цей симбіоз дозволить створити ефективну систему управління інформаційною безпекою підприємств агропродовольчої сфери, зменшити витрати на її створення та функціонування, та забезпечить зростання економічних і соціальних показників результативності діяльності досліджуваних суб'єктів аграрного ринку України.

Ще нижчим порівняно з попередніми коефіцієнтами є рівень витрат на забезпечення інформаційного захисту продовольчої, інноваційної, комерційної та інших сфер діяльності підприємств агропродовольчої сфери. Значення коефіцієнта є найбільшим у підприємств Полтавської області – 0,111 та підприємств Сумської області – 0,100 при нормативному значенні 0,200–0,300. Найменше значення коефіцієнта спостерігалось на підприємствах Луганської області – від 0,030 до 0,050 з усередненим значенням 0,039 за аналізований період. Такий рівень фінансування є недостатнім і може бути передумовою:

недостатньої або спотвореної інформації про стан продовольчого забезпечення та продовольчої безпеки загалом, рівень доступності продукції сільськогосподарського призначення [80];

неналежного рівня інформування посередників і споживачів продукції про її асортимент і ціни, інноваційні технології, новітні технічні та програмні засоби підвищення ефективності виробництва, обробітку, зберігання та продажу продукції сільськогосподарського призначення;

втрати аграрним підприємством комерційної таємниці щодо здійснення інноваційної, продовольчої та комерційної діяльності тощо.

Інформаційний супровід і захист зазначених вище напрямів діяльності здійснюється завдяки забезпеченню технічного, програмного, фізичного захисту та формуванню безпечних умов діяльності персоналу [56].

Для створення ефективних умов інформаційного захисту на агропродовольчому підприємстві коефіцієнт фінансування програмної захищеності інформації має бути в межах 0,200–0,250, але на підприємствах

аналізованих областей він не сягав нормативного значення. Найвищим його значення було у підприємств Полтавської області – 0,186 і Сумської – 0,154, а найнижчим – у підприємств Кіровоградської області – 0,072, Харківської – 0,067 та Луганської – 0,044.

Забезпечення безпеки інформації на програмному рівні сприяє захисту відомостей від несанкціонованого доступу та знижує ризики розкрадання і подальшого неправомірного використання отриманих інформаційних ресурсів аграрного підприємства.

Показники фінансування як програмної частини, так і технічної (апаратної) дають змогу стверджувати про високу ймовірність виникнення загроз інформаційній безпеці та зростання кількості вразливостей інформаційної системи сільськогосподарського підприємства, оскільки коефіцієнт фінансування технічної захищеності інформації на досліджуваних підприємствах має низькі значення: у Полтавській області – 0,221, Сумській – 0,196, Кіровоградській – 0,098, Харківській – 0,104 та Луганській – 0,055 при мінімальному нормативному значенні 0,300–0,350.

Важливо враховувати, що на вибір технологій (рис. 2.8) інформаційної безпеки значно впливає рівень її зрілості та масштаб об'єднання комп'ютерів та інших апаратних засобів.

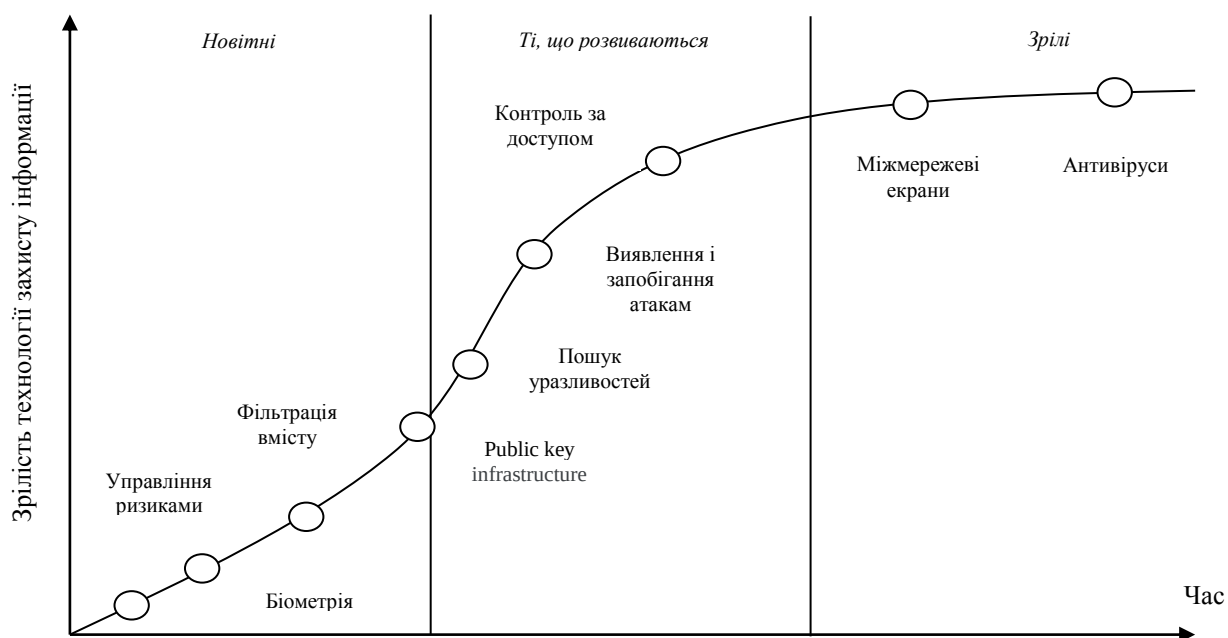


Рис. 2.8. Розподіл технологій захисту інформації за рівнем зрілості [побудовано на основі 15; 69; 77]

Якщо рівень зрілості характеризується часом (давністю) застосування технологій інформаційного захисту, то масштаб визначається як через обмеження фінансових ресурсів на придбання потрібних засобів захисту

інформації, так і через відсутність потреби в цих засобах. У невеликих мережах не настільки гостро стоїть проблема централізованого управління інформаційною безпекою, а в мережах великих підприємств агропродовольчої сфери без таких засобів взагалі не обійтися.

Тому у великих мережах (переважно на великих підприємствах, наприклад ПРАТ «ПОЕЗ - Кернел Груп», Білоцерківська агропромислова група) застосовується система кореляції Public-Key Infrastructure – інфраструктура відкритих ключів, а традиційні засоби захисту змінюються під впливом масштабу мережі та доповнюються новими функціями – інтеграцією із системами мережного управління, ефективною візуалізацією подій, розширеною генерацією звітів, ієрархічним і рольовим управлінням тощо (рис. 2.9).

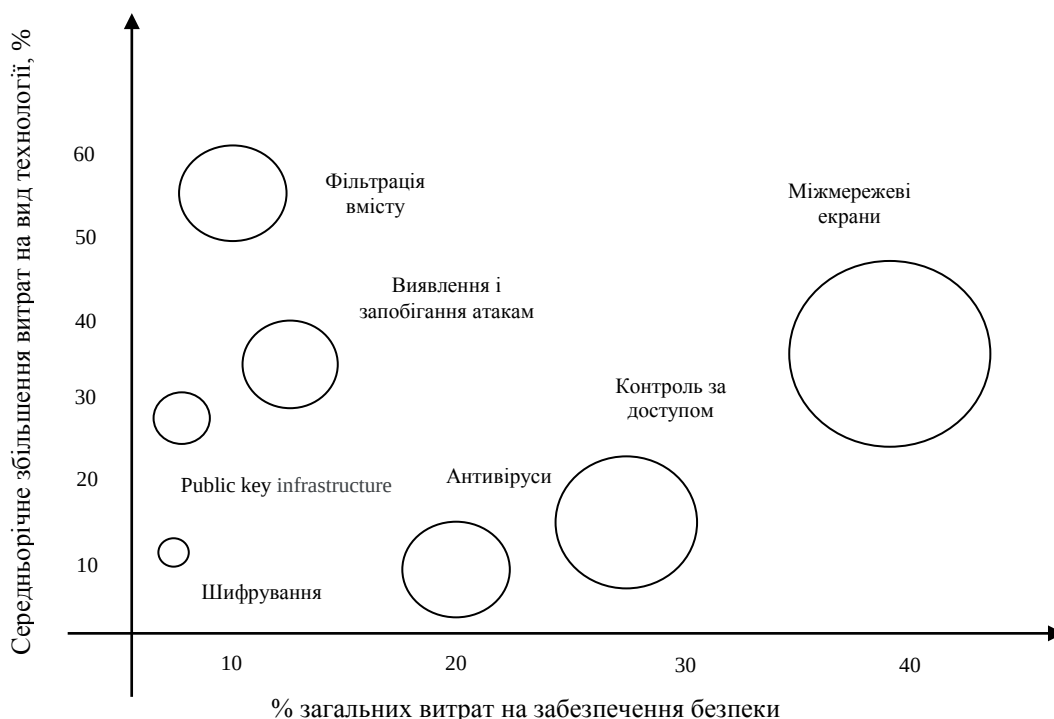


Рис. 2.9. Найбільш розповсюджені технології інформаційного захисту та рівень витрат на їх забезпечення (загальносвітові тенденції) [побудовано на основі 15; 32; 56; 69; 70]

Фізичний захист є першим бар'єром для зловмисника, а тому і одним із базисів комплексного забезпечення безпеки підприємства. Завдання, що покладаються на фізичні засоби захисту: забезпечення безпеки будівель, внутрішніх приміщень, територій; захист обладнання та документів від несанкціонованого доступу до них; забезпечення захисту від перехоплення інформаційного потоку методами промислового шпигунства; захист від пожеж та інших загроз, які можуть призвести до знищення інформації,

пошкодження інформаційної системи, руйнування інформаційного середовища підприємства, а отже, і до фінансових збитків.

Основними засобами фізичного захисту для підприємств агропродовольчої сфери є:

механічні перешкоди: загородження, решітки, ударостійкі екрани, пристрої зберігання, замки (механічні, електричні, електромеханічні, гідравлічні) та ніші засоби;

датчики: GPS, ультразвукові, інфрачервоні, томографічні, мікрохвильові, лазерні, фотоелектричні, акустичні, відкриття вікон і дверей, а також системи відеоспостереження тощо;

засоби ідентифікації особистості: за програмованими ключами та картками, сканери відбитків пальців, геометрії руки і сітківки ока, аналізатори голосу, зчитувачі геометрії особи, аналізатори механічного та клавіатурного почерку;

пристрої просторового зашумлення, мережні фільтри;

автоматизовані системи пожежогасіння, датчики наявності задимлення і займання тощо [9; 33; 88].

Значення фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства, применшується та залишається поза увагою переважної більшості підприємств, зокрема й аграрної сфери. Наприклад, коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємств агропродовольчої сфери Полтавської та Сумської областей, становить 0,060 при мінімальному нормативному значенні 0,100. Дещо меншими є значення цього показника у підприємств Харківської та Кіровоградської областей – 0,056 та 0,053 відповідно. Найменше значення спостерігається на підприємствах Луганщини – 0,035. Низький рівень фінансування інформаційного напрямку зумовлює низький рівень його захисту, що сприяє можливості як проникнення на фізичний об'єкт із метою заволодіння інформацією або іншими видами ресурсів підприємств, так і можливості безперешкодного витоку інформаційних ресурсів через персонал підприємства. Тому далі розглянемо значення показника, який характеризує захист персоналу підприємства з погляду забезпечення інформаційної безпеки.

Співробітнику підприємства недостатньо знати тільки свої трудові обов'язки, від також повинен знати основи інформаційної безпеки, що зумовлено не тільки нормативно-правовими актами й стандартами, а й простими вимогами безпеки для збереження конфіденційної інформації [25]. Порушення правил інформаційної безпеки, які призводять до витоку інформації, зараження вірусами або знищення даних переважно відбувається через працівників, які порушують вимоги до захисту інформації або зовсім не

ознайомлені з ними. Опитані фахівці у сфері інформаційної безпеки погоджуються зі статистикою, що понад 80 % випадків порушень інформаційної безпеки відбуваються з провини співробітників, причому значна частина – унаслідок ненавмисних дій: через недбалість, неуважність або незнання [78].

Експерти у сфері забезпечення інформаційної безпеки визначили нормативне порогове значення витрат на інформаційну безпеку, що забезпечує захист персоналу, – від 25 до 40 % від загальних витрат на забезпечення інформаційної безпеки аграрного підприємства. Відповідно до розрахованих усереднених коефіцієнтів лише підприємства агропродовольчої сфери Полтавської області досягають порогового значення коефіцієнта фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства, – 0,250 (25 % від загальних витрат на забезпечення інформаційної безпеки підприємства). Слід відмітити, що значення цього коефіцієнта перевищувало порогове значення упродовж 2015–2018 рр. і становило 0,280–0,320. Значення цього коефіцієнта у підприємств Сумської області становило 0,237 (найбільше значення спостерігалось 2013, 2014 та 2016 рр. – від 0,260 до 0,290), Кіровоградської – 0,161, Харківської – 0,160 та Луганської – 0,111, що свідчить про необхідність збільшення рівня фінансування інформаційної безпеки, що забезпечує захист персоналу, а отже, і цінних інформаційних ресурсів та інформаційних активів. Зазначене лише підтверджує дані світової статистики та підвищує коефіцієнт інформаційного ризику, спричиненого людським фактором.

Загалом щодо групи показників оцінки фінансування забезпечення інформаційної безпеки підприємств агропродовольчої сфери доцільно відзначити, що майже всі досліджувані підприємства Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей потребують, по-перше, збільшення витрат на захист їх інформаційного середовища, по-друге, оптимальний перерозподіл фінансових ресурсів на забезпечення інформаційного захисту напрямів діяльності, сфер діяльності, об'єктів захисту, елементів системи інформаційної безпеки.

Далі проаналізуємо групу показників оцінки інформаційної надійності персоналу досліджуваних підприємств (рис. 2.10).

Основою забезпечення дієвості системи інформаційної безпеки підприємства є дотримання політики інформаційної безпеки у формалізованому або неформалізованому вигляді. Поінформованість співробітника у сфері інформаційної безпеки означає наявність у нього знань про загальні питання забезпечення інформаційної безпеки та розуміння ним своїх ролей і обов'язків як посадових, так і щодо забезпечення інформаційної

безпеки, та засобів виконання цих обов'язків, а також усвідомлення ним важливості дотримання режиму інформаційної безпеки й персональної відповідальності за його недотримання [16].

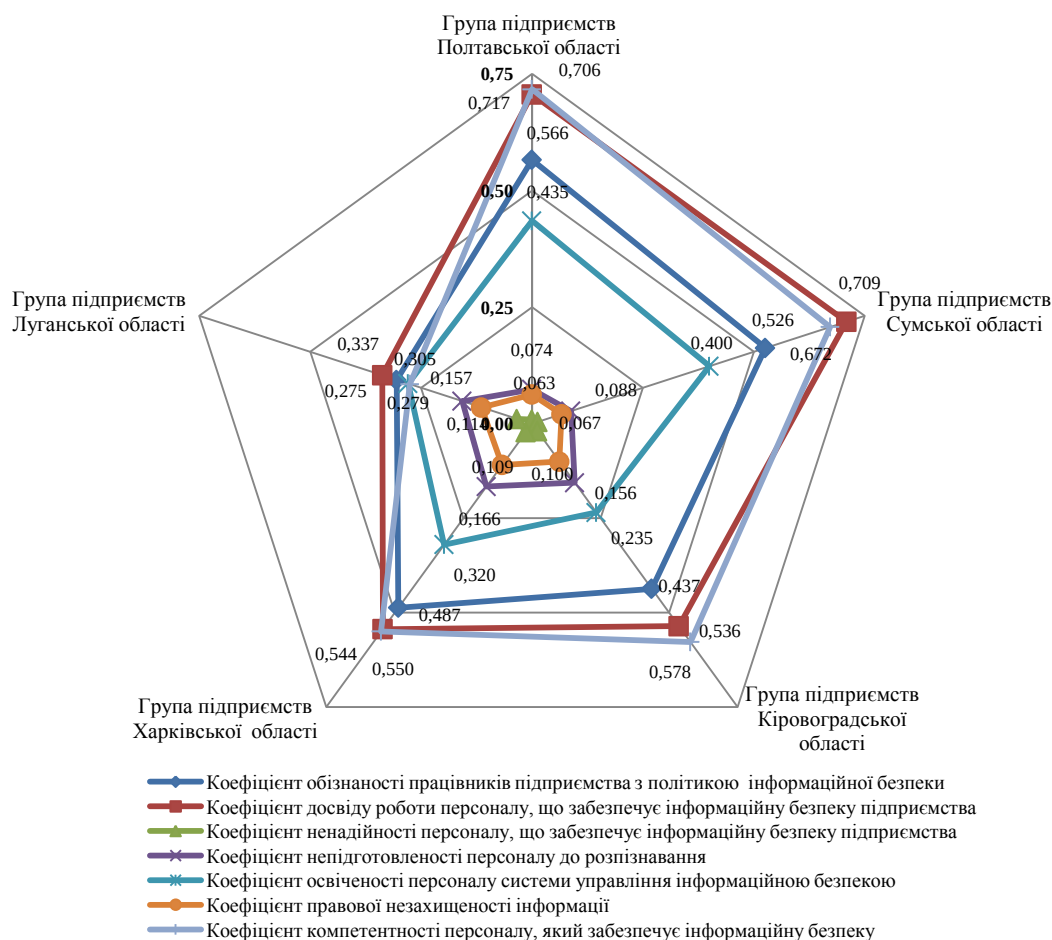


Рис. 2.10. Усереднені показники оцінки інформаційної надійності персоналу підприємств агропродовольчої сфери Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей [побудовано автором]

Отже, чим більша чисельність працівників ознайомих з політикою інформаційної безпеки підприємства, тим вищий рівень захисту його інформаційного середовища.

Важливим коефіцієнтом цієї групи є коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства, що дозволяє визначити персонал, який має досвід зберігання комерційної таємниці, захисту інформаційних ресурсів та інформаційних активів досліджуваних підприємств. Досить високим цей коефіцієнт є у підприємств Сумщини – 0,709 та Полтавщини – 0,706, що свідчить про низький показник плинності персоналу, що має доступ до цінних інформаційних ресурсів і даних комерційної таємниці. Протягом 2015–2018 рр. усереднене значення цього коефіцієнта у підприємств зазначених областей коливалося в межах

0,750–0,850, що дає змогу зробити висновок про достатній рівень досвіду персоналу для забезпечення інформаційного захисту. Натомість у підприємств Кіровоградщини та Харківщини усереднене значення за 2009–2018 рр. чисельності працівників, які мали доступ до цінних інформаційних ресурсів і комерційної таємниці понад рік, становило 53,6 і 54,4 % від загальної чільності персоналу, який мав доступ до захищених даних та інформації. Найменший досвід мали працівники підприємств Луганщини (усереднене значенням показника за досліджуваний період – 33,7 %).

Значення попереднього коефіцієнта доповнює характеристика коефіцієнта ненадійності персоналу, що забезпечує інформаційну безпеку підприємства, який визначає питому вагу працівників, звільнених через витік інформації, серед загальної чисельності звільнених працівників. Він був найменшим у підприємств Полтавської області, його усереднене значення становило 0,009, а інциденти звільнення із зазначених причин спостерігалися на них лише 2009 р. і 2012 р. Не набагато вищим цей показник був у підприємств Сумської області – 0,013, де ці порушення спостерігалися лише у період 2013–2015 рр. Приблизно однаковим значення цього коефіцієнта було в аграрних підприємств Кіровоградщини та Харківщини – 0,020 та 0,022, а найбільшим – у підприємств Луганської області – 0,034. Значення коефіцієнта було низьким перш за все через неможливість у більшості випадків довести, що втрата, модифікація, знищення або витік інформації відбулися внаслідок дій або бездіяльності працівників.

Найчастішими і найнебезпечнішими (з погляду розміру збитку) є ненавмисні помилки працівників – користувачів інформаційної системи підприємств агропродовольчої сфери через низький рівень компетентності персоналу та невміння розпізнавати загрози інформаційній безпеці. Цей показник зменшувався у всіх аналізованих підприємств усіх областей. Найменше його значення було у Полтавщини – 0,074, Сумщини – 0,088, а найбільше – в аграрних підприємств Харківщини – 0,166, Луганщини – 0,157 та Кіровоградщини – 0,156, що свідчить про те, що в середньому за 2009–2018 рр. підприємства агропродовольчої сфери цих трьох областей мали від 15,6 до 16,6 % працівників від загальної чисельності персоналу, який мав доступ до цінних інформаційних ресурсів і комерційної таємниці, ненавмисні дії яких призвели до витоку інформації через низький рівень компетентності персоналу та невміння ідентифікувати загрози.

Така статистика вимагає від керівництва підприємства щонайменше використання стандартів [1; 2; 3; 4; 6; 15; 28; 110] з інформаційної безпеки або принаймні їх окремих частин, введення на їх основі політики інформаційної безпеки та примусового ознайомлення з нею працівників

підприємства та щонайбільше – впровадження періодичних тренінгів, навчань із питань інформаційної безпеки та введення атестаційних норм.

Також ефективним способом боротьби з ненавмисними помилками є максимальна автоматизація та стандартизація інформаційних процесів, використання пристроїв «захист від дурня» (FoolProofDevice), регламентація та строгий контроль за діями користувачів. Необхідно також стежити за тим, щоб при звільненні працівника його права доступу (логічного та фізичного) до інформаційних ресурсів підприємства анулювалися [73].

Аналізуючи показники, які характеризують структуру персоналу з погляду інформаційної безпеки, доцільно відмітити низькі значення коефіцієнта освіченості персоналу системи управління інформаційною безпекою досліджуваних підприємств агропродовольчої сфери, зокрема у підприємств Полтавської області – 0,435, Сумської – 0,400, Харківської – 0,320, Луганської – 0,279 та Кіровоградської – 0,235. Тобто система управління інформаційною безпекою на підприємствах Полтавщини тільки на 43,5 %, а на підприємствах Кіровоградщини тільки на 23,5 % забезпечена фахівцями відповідної кваліфікації та відповідної компетентності, що негативно впливає на загальний стан захисту інформаційного середовища аналізованих підприємств і потребує перекваліфікації того відсотка працівників системи управління інформаційною безпекою, який не має відповідного фаху.

Інший бік освітньої структури персоналу досліджуваних підприємств характеризує коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку, значення якого є порівняно високим на підприємствах Полтавщини – 0,717 та Сумщини – 0,672, що вказує на відповідний відсоток відбитих атак на інформаційну систему через дії персоналу від загальної кількості цих атак. На агропродовольчих підприємствах Кіровоградської та Харківської областей значення цього коефіцієнта дещо нижче – 0,570 та 0,550 відповідно, що одночасно вказує як на нижчий рівень кваліфікованості та досвідченості персоналу щодо ідентифікації та відбиття загроз інформаційному середовищу, так і на вищий рівень автоматизованих програмно-технічних засобів, що забезпечують інформаційну безпеку без участі людини.

Заключним показником цієї групи є коефіцієнт правової незахищеності інформації, який дозволяє визначити питому вагу «критичної для розголошення» інформації. На досліджуваних підприємствах спостерігалось зменшення значення цього коефіцієнта, зокрема на підприємствах Полтавської та Сумської областей, з 0,090 2009 р. до 0,050 2018 р., з усередненими значеннями 0,063 та 0,067 відповідно. На сільськогосподарських

підприємствах Кіровоградщини у значення цього коефіцієнта не було стійкої тенденції до зміни, він коливався в межах 0,080–0,110, на підприємствах Харківщини – в межах 0,070–0,150, Луганської області – 0,080–0,150, з усередненими значеннями – 0,100, 0,109 та 0,114. Це дає змогу зробити висновок про значну питому вагу інформації, яка потребує захисту, адже рівень її захисту визначає подальше функціонування конкретних суб'єктів аграрного ринку України. За таких умов забезпечення захисту, в тому числі і правового, інформаційних ресурсів, інформаційних активів аграрного підприємства створює підґрунтя для захисту інтересів власників підприємств, інвесторів і виробників продукції від недобросовісної конкуренції в процесі господарської діяльності.

Щодо цієї групи показників слід відмітити середній рівень надійності персоналу досліджуваних підприємств агропродовольчої сфери відносно забезпечення та дотримання політики, стратегії та режимів інформаційної безпеки загалом. З метою підвищення надійності персоналу у сфері інформаційної безпеки для досліджуваних сільськогосподарських підприємств доцільно удосконалити систему найму, відбору оцінки ділових якостей працівників, активніше використовувати резерви механізму управління мотивацією співробітників, застосовувати грошові та негрошові інструменти, реалізовувати соціальні програми, удосконалювати організацію праці, відновлювати систему соціального, морального та творчого нематеріального стимулювання. А обов'язковою умовою є навчання працівників та обмін досвідом з питань інформаційного захисту [23].

Для якісної оцінки рівня інформаційної безпеки суб'єктів аграрного ринку доцільно проаналізувати показники оцінки інформації з позиції основного ресурсу захисту, прийняття рішень управлінського персоналу, оскільки саме від властивостей інформації, її наявності, форми подання, з одного боку, та компетентності, досвіду, здатності використовувати цю інформацію – з іншого залежить ефективність управлінського рішення в певній сфері діяльності досліджуваного підприємства агропродовольчої сфери (рис. 2.11).

Від повноти інформації, яку надає ОПР, загалом залежить можливість прийняття управлінського рішення. Аутсайдерами за цим коефіцієнтом були підприємства Сумської області зі значенням 0,365 та Полтавської – 0,360, що свідчить про те, що майже кожен третій управлінець на підприємствах цих областей не отримував належної інформації для прийняття релевантних управлінських рішень або про те, що лише майже третина інформації була корисною для менеджера в процесі виробітку варіантів ефективних рішень управління діяльністю підприємства. Вищими були значення коефіцієнта на

аграрних підприємствах Кіровоградської, Харківської областей – 0,415 та 0,430 відповідно.

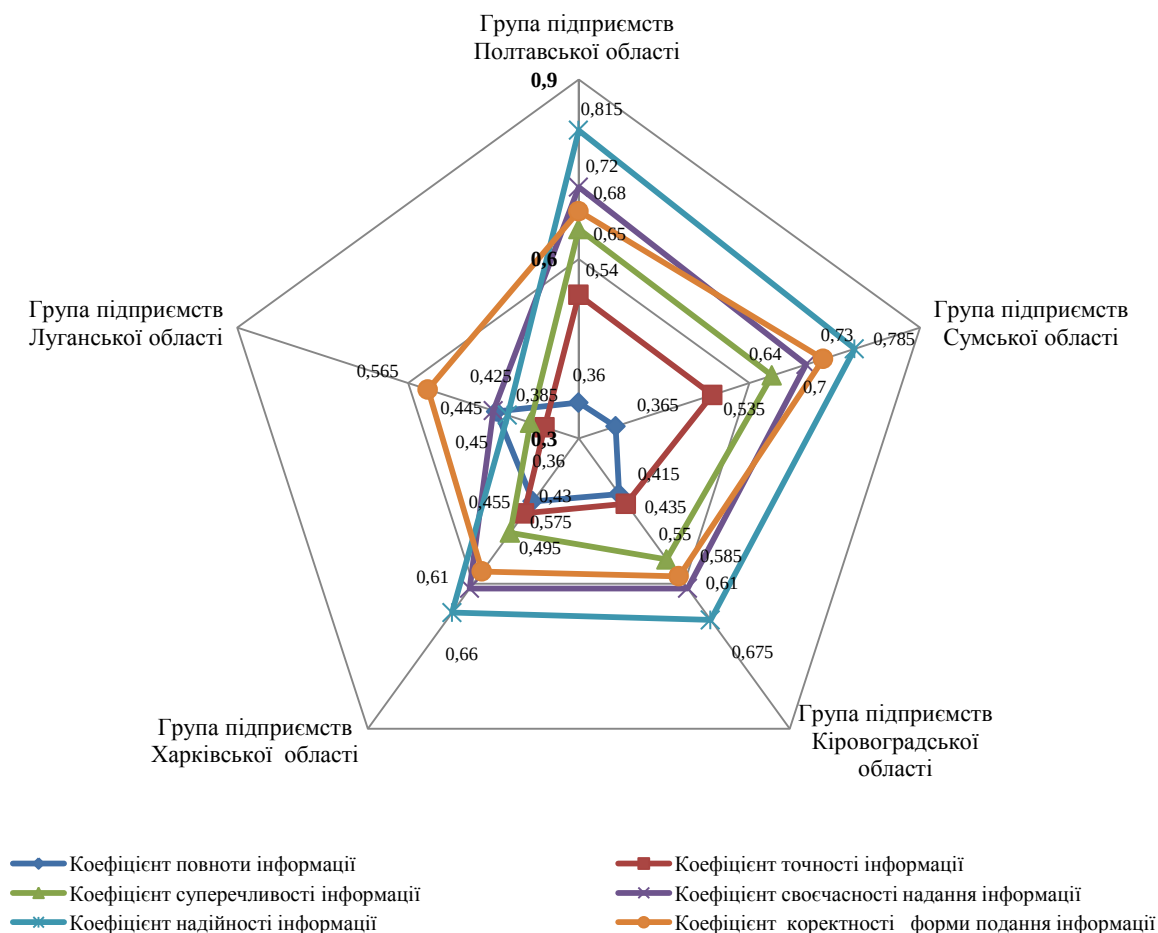


Рис. 2.11. Усереднені показники оцінки інформації, що надається особам, які приймають рішення, системою інформаційного забезпечення (системою інформаційного захисту) підприємств агропродовольчої сфери Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей [побудовано автором]

Мінімальний, але достатній для прийняття правильного рішення набір даних містить інформація, яку надавала ОПР на підприємствах агропродовольчої сфери Луганської області, про що свідчить усереднене значення показника – 0,445.

Пов'язаним із попереднім є коефіцієнт точності інформації, значення якого на сільськогосподарських підприємствах Полтавщини становило 0,540, що вказує на необхідність більш чіткого підбору даних для ОПР, оскільки 46 % інформації, що йому надавалась, не була потрібною для прийняття рішення і створювала інформаційний шум, і внаслідок цього виникав ризик прийняття неефективного управлінського рішення. Дещо меншим цей показник був у підприємств Сумщини – 0,535, а найменшим – у підприємств

Луганської області – лише 0,360.

Достатньо високим, порівняно з попередніми коефіцієнтами інформації для ОПР, є значення коефіцієнта суперечливості інформації: у підприємств агропродовольчої сфери Полтавської області – 0,650, Сумської – 0,640, Кіровоградської – 0,550, Харківської – 0,495 та Луганської – 0,385, що вказує на достатню кількість незалежних свідчень на користь ухвалення рішення в поданих даних.

Одним із важливих аспектів прийняття рішення є його швидкість, що безпосередньо залежить від швидкості отримання інформації ОПР. Цей показник був найбільш високим серед підприємств Полтавської та Сумської областей – 0,720 та 0,700 відповідно. Доцільно відзначити, що протягом 2016–2018 рр. значення цього коефіцієнта досягало 0,800–0,850. Усереднене значення для підприємств Харківської та Кіровоградської областей становило 0,610, хоча теж зростало протягом останніх років аналізованого періоду. Найменшим було значення на підприємствах Луганщини – 0,450. Загалом значення цього коефіцієнта підтверджують автоматизацію документообігу та його часткову цифровізацію, що, по-перше, сприяє швидкості передачі даних та інформації, по-друге, забезпечує її більш надійний захист під час здійснення процесів обміну.

Для обґрунтування вибору управлінського рішення підприємства застосовують доказовий підхід (evidence based policy), при якому рішення формулюються і приймаються на основі досліджень, що ґрунтуються на емпіричній, статистичній, експертній базі. Такий підхід мінімізує ризик невідповідності очікуваних ефектів управління його результатам.

Доцільно відмітити, що коефіцієнт надійності інформації, який власне відповідає за належне виконання доказового підходу під час надання інформації ОПР, свідчить про перевіреність даних та інформації, на основі яких приймаються управлінські рішення на підприємствах агропродовольчої сфери Полтавщини (усереднене значення 0,815) та Сумщини (усереднене значення 0,785). Не середньому рівні надійність інформації забезпечувалось аграрними підприємствами Кіровоградської області – 0,675 та Харківської – 0,660. Найнижчим був рівень перевіреності інформації, що надавалась менеджерам в аграрних підприємств Луганської області, – 0,425.

Рішення цієї проблеми вбачається, з одного боку, в модернізації методик проведення статистичних спостережень, з іншого – в пошуку альтернативних джерел інформації, які можуть бути використані в процесі прийняття рішень. Позитивний аспект такого підходу полягає в незалежності від статистики. Альтернативна інформація може виявитися більш доступною і своєчасною. Водночас таку інформацію здебільшого складно

формалізувати, або на її обробку потрібні великі витрати ресурсів (Big Data), або її складно отримати приватно (адміністративні дані) [70].

Репрезентативність інформації пов'язана з правильністю її відбору та формування для адекватного відображення властивостей об'єкта. Неодмінною умовою визначення властивості репрезентативності інформації є надходження схожої інформації з різних джерел. Зрозуміло, що повного збігу інформації з всіх джерел ніколи не буде.

Важливим аспектом є коректність форми подання інформації, що передбачає вибірку даних, та її передачі ОПР у найбільш зручній формі для швидкого прийняття найбільш обґрунтованого ефективного управлінського рішення. Оскільки більшість статистичних форм подачі економічної інформації, програмного забезпечення для роботи з останньою є уніфікованими, то виникає обґрунтована потреба у розробці «зручних» форм та програмних додатків для менеджерів усіх рівнів залежно від специфіки їх діяльності та спеціалізації конкретного підприємства агропродовольчого комплексу. Про зазначене свідчить і значення коефіцієнта коректності форми подання інформації, яке найбільше на аграрних підприємствах Сумської області – 0,730; Полтавської – 0,680, дещо меншим є цей показник у підприємств Кіровоградщини – 0,585, Харківщини – 0,575 та Луганщини – 0,565.

Окрім зручності, розробка форм і програмних додатків для подання інформації забезпечить вищий і надійніший рівень її захисту.

Щодо групи показників оцінки інформації, що надається ОПР системою інформаційного забезпечення (системою інформаційного захисту), доцільно відмітити позитивні тенденції її зміни, оскільки інформація, необхідна для ОПР у досліджуваних підприємств, має основні її властивості та забезпечена її цілісність, доступність і конфіденційність.

Спрямованою на управлінські аспекти та водночас узагальнюючою є група показників оцінки системи інформаційної безпеки підприємства агропродовольчої сфери (рис 2.12).

Першим і важливим показником цієї групи є коефіцієнт керованості системи інформаційної безпеки підприємства, значення якого відображає набір необхідних компетентностей управлінського персоналу, який власне і забезпечує управління системою захисту інформації. Значення цього коефіцієнта було приблизно однаковим у підприємств Полтавської, Сумської, Кіровоградської і Харківської областей, а його усереднене значення було в межах 0,620–0,685, що свідчить про достатній, але не повний набір компетентностей, необхідних для ефективного управління інформаційними середовищем підприємства та його захисту.

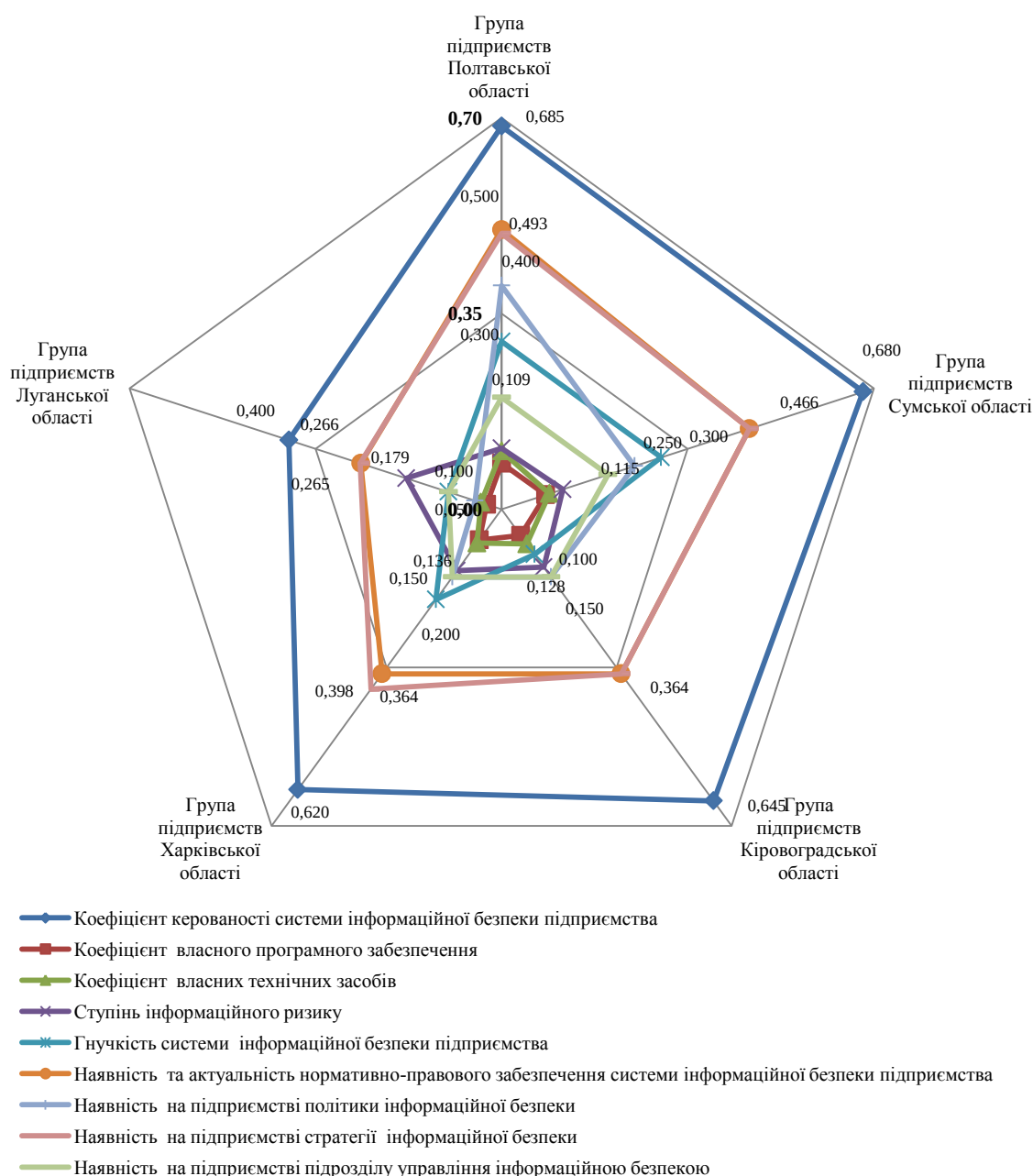


Рис. 2.12. Усереднені показники оцінки системи інформаційної безпеки підприємств агропродовольчої сфери Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей [побудовано автором]

Важливим доповненням до попереднього коефіцієнта є показник здатності системи управління інформаційною безпекою швидко адаптувати організаційну побудову до зовнішніх і внутрішніх потреб. Результати дослідження показали, що лише в останні роки (2016–2018 рр.) підприємства орієнтувалися на побудову або реорганізацію структури системи управління інформаційною безпекою таким чином, щоб вона могла швидко адаптуватися до вимог зовнішнього та внутрішнього інформаційного середовища, що дозволяло швидко реагувати на виникаючі загрози й оперативно приймати

рішення щодо захисту інформаційних ресурсів підприємства. Усереднене значення цього коефіцієнта у підприємств Полтавської та Сумської областей становило 0,300. Для підприємств Харківщини – 0,200; Кіровоградщини та Луганщини – 0,100.

Тобто найбільш адаптованими до реорганізації системи управління інформаційною безпекою є аграрні підприємства Полтавщини та Сумщини. Доцільно відмітити, що це переважно середні підприємства, оскільки системи управління великими підприємствами є більш механічними і менш гнучкими, на малих підприємствах ці системи відсутні, а управління інформаційною безпекою мінімальне і фрагментарне. Тому актуальним і важливим є значення наступного елемента показників цієї групи – наявність на підприємстві підрозділу управління інформаційною безпекою.

Аналіз дозволяє зробити висновок про небажання керівництва усвідомлювати необхідність окремого фахівця або формування окремого підрозділу, який би забезпечував процес захисту інформаційних ресурсів, здійснював його організацію, моніторинг, управління ним тощо. На більшості підприємств цей показник протягом 2009–2014 рр. дорівнював нулю, що означало відсутність підрозділу управління інформаційною безпекою на підприємстві. В останні роки спостерігалася наявність окремих фахівців, які забезпечують захист інформаційної безпеки підприємств агропродовольчого сектора, переважно в середніх і великих за розміром підприємствах Полтавської та Сумської областей з усередненим показником – 0,200, у підприємств Кіровоградської та Харківської областей усереднене значення цього показника становило 0,15. І лише на Луганщині найменша чисельність підприємств мала формалізовану систему управління інформаційною безпекою.

Відповідно до значення попереднього показника аналогічно змінюється значення показника наявності політики інформаційної безпеки. На більшості підприємств агропродовольчої сфери Полтавської області політика інформаційної безпеки була наявною, і лише в останні роки керівництво вирішило документально закріпити загальні положення управління інформаційним середовищем та інформаційною безпекою зокрема. Усереднене значення цього показника для цієї групи підприємств становило 0,400. Для аграрних підприємств Сумської області політика інформаційної безпеки залишається напівформалізованою, про що свідчить усереднене значення показника – 0,250. До 2014 р. більшість підприємств цієї групи не визнавали потреби в запровадженні політики інформаційної безпеки. Аналогічна ситуація спостерігалась на підприємствах агропродовольчої сфери Кіровоградщини та Харківщини, проте усвідомлення необхідності

реалізації політики інформаційної безпеки до керівництва прийшло, починаючи з 2016 р., тому усереднене значення показника становило 0,150. Найменшим цей показник був в аграрних підприємств Луганщини – лише 0,050, що свідчить про відсутність у майже всіх підприємств цієї області політики управління інформаційним захистом.

Водночас достатнім був показник наявності стратегії інформаційного захисту у формалізованому та неформалізованому вигляді.

Стратегія інформаційної безпеки підприємств агропродовольчої сфери визначена майже на всіх сільськогосподарських підприємствах Полтавської та Сумської областей, проте у більшості підприємств, переважно малих, – у неформалізованому вигляді. У формалізованому вигляді реалізували стратегію інформаційного захисту переважно середні та великі підприємства. Останні також мали взаємозв'язок цієї функціональної стратегії із загальною стратегією розвитку діяльності. Усереднене значення цього показника становило у підприємств Полтавської та Сумської областей 0,493 та 0,496 відповідно. Для сільськогосподарських підприємств Кіровоградської та Харківської областей цей показник був дещо нижчим і становив 0,364 та 0,398 відповідно, що означає наявність стратегії інформаційної безпеки у всіх підприємств, проте не у всіх у задокументованому вигляді. Найменше уваги цьому питанню присвячувало керівництво підприємств Луганщини, де усереднений показник становив 0,266.

Позитивним є зростання кількості підприємств агропродовольчої сфери із наявним нормативно-правовим забезпеченням системи інформаційної безпеки підприємства. Для підприємств Полтавщини цей показник становив 0,500, для підприємств Сумщини – 0,466, що свідчить про наявність формалізованого нормативно-правового забезпечення захисту інформаційного середовища, яке потребує його актуалізації та відповідності сучасним вимогам функціонування цифрового середовища. Для підприємств Кіровоградщини та Харківщини цей показник становив 0,364, для сільськогосподарських підприємств Луганської області – 0,265, що вказує на необхідність не тільки актуалізації, але й документального закріплення нормативного та правового регулювання сфери інформаційної безпеки.

Низьким було значення коефіцієнта власного програмного забезпечення, оскільки керівництво досліджуваних підприємств агропродовольчої сфери не збагнуло вигід від адаптації або створення власного програмного забезпечення, в тому числі і для забезпечення інформаційної безпеки, відповідно до типу спеціалізації бізнесу. Цей коефіцієнт вказує на найвищий рівень soft-development на підприємствах агропродовольчої сфери Сумської області зі значенням 0,083 та Полтавської – 0,082, що означає 8,3 та 8,2 %

власного програмного забезпечення від існуючого загалом на підприємстві. Для підприємств Харківської області цей показник становив 0,068, Кіровоградської області – 0,058, Луганської – 0,028. Варто враховувати, що якість програмного забезпечення залежить від восьми основних характеристик – функціональної придатності, ефективності, сумісності, зручності використання, надійності, безпеки, супроводжуваності, можливості перенесення. За умови досягнення максимального значення кожної з восьми характеристик якості можна досягти максимального значення якості програмного забезпечення [27].

Незначним є і значення показника розробки власних технічних засобів, що для аграрних підприємств Полтавської області становило 0,104, Сумської – 0,090, Харківської – 0,077, Кіровоградської – 0,075 та Луганської області – 0,039 при мінімальному нормативному значенні 0,250. На низьке значення цього показника в першу чергу вплинула відсутність спеціалістів для розробки спеціальних технічних і апаратних засобів для забезпечення інформаційної безпеки та відсутність бажання керівництва вирішувати це питання.

Відповідним до динаміки зміни розглянутих показників є показник ступеня інформаційного ризику, який був різним для підприємств агропродовольчої сфери досліджуваних областей (Полтавської – 0,109, Сумської – 0,115, Харківської – 0,128, Кіровоградської – 0,136, Луганської – 0,179), проте мав тенденцію до зниження упродовж 2009–2018 рр. Цей показник свідчить про зменшення відсотка втрат (у грошовому вираженні), спричинених пошкодженням інформаційної цілісності підприємства, до загальних втрат від порушення безпеки, що є позитивною тенденцією підвищення ефективності діяльності системи інформаційної безпеки опитаних підприємств агропродовольчої сфери України.

На основі проведеного аналізу групи показників оцінки системи інформаційної безпеки підприємств агропродовольчої сфери Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей доцільно відмітити значний потенціал інформаційного середовища. Майже всі досліджувані підприємства потребують кваліфікованих кадрів задля здійснення ефективного управління процесами захисту інформації, що зумовлює необхідність розробки рекомендацій щодо формування оптимальних моделей систем управління інформаційною безпекою, розробку дієвої та інтегрованої в загальну стратегії інформаційного захисту, формування та дотримання політики інформаційної безпеки та інших заходів.

Проте характеристика одиничних показників і коефіцієнтів не надає змоги зробити об'єктивні висновки та, відповідно, розробити найбільш актуальні та доречні рекомендації. З цією метою потрібно визначити

інтегральний показник за кожною із розглянутих груп і зробити висновки, що потребує формування методологічних аспектів оцінки інформаційної безпеки.

Доцільно відзначити, що питання, пов'язані із захистом інформації, для багатьох підприємств є складними через неточність методик, здатних виконувати завдання забезпечення інформаційної безпеки об'єкта з прийнятним рівнем адекватності. Завдання ускладнюється наявністю великої кількості факторів і їх взаємозв'язків, що впливають на саму систему [82].

Для того щоб наблизитися до розв'язання подібної проблеми, необхідно сформулювати новітню методологію діагностики та оцінки рівня інформаційної безпеки суб'єктів господарювання.

Список використаних джерел до розділу 2

1. Європейські стандарти безпеки ISO 15408 (Common Criteria for Information Technology Security Evaluation. URL: <https://www.sans.org/reading-room/whitepapers/standards/common-criteria-iso-iec-15408-insight-thoughts-questions-issues-545>).

2. Канадські критерії безпеки комп'ютерних систем (Canadian Trusted Computer Product Evaluation Criteria. URL: https://www.researchgate.net/publication/3506169_The_Canadian_Trusted_Computer_Product_Evaluation_Criteria_CTCPEC).

3. Критерії безпеки комп'ютерних систем (Trusted Computer System Evaluation Criteria). URL: <https://www.cs.clemson.edu/course/cpsc420/material/Evaluation/TCSEC.pdf>.

4. Критерії оцінки безпеки інформаційних технологій (Information Technology Security Evaluation Criteria). URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile.

5. Стандарты информационной безопасности : государственные и международные. URL: <http://tvoi.biz/biznes/informatsionnaya-bezopasnost/prakticheskaya-polza-standartov-info.html>.

6. ISO 17799: Code of Practice for Information Security Management. URL: http://www.iso.org/iso/catalogue_detail?csnumber=39612.

7. ISO/IEC 27000:2014. Information technology – Security techniques – Information security management systems – Overview and vocabulary. URL: <https://www.iso.org/standard/63411.html>.

8. NSA/NCSC Rainbow Series. URL: <http://fas.org/irp/nsa/rainbow.html>.

9. Абидарова А. А. Физические средства защиты информации. *Наука, образование и культура*. 2019. № 2 (36). С. 19–20.

10. Алавердов А. Р. Типовые причины, формы и методы реализации угроз информационной безопасности организации с участием ее персонала. Руководство по изучению дисциплины «Противодействие кадровым угрозам безопасности Организации». 2007. URL: <http://lectmania.ru/2x3084.html>.

11. Ананьев М. А., Ухтинская Ю. В. Применение информационных технологий в АПК. 2012. URL: http://sisupr.mrsu.ru/2012-4/PDF/Ananев_Ukhtinskaya.pdf.

12. Андрианов В. В., Зефилов С. Л., Голованов В. Б., Голдуев Н. А. Обеспечение информационной безопасности бизнеса : 2-е издание, переработанное и дополненное. URL: <https://pqm-online.com/assets/files/lib/books/andrianov.pdf>.

13. Аніловська Г. Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. *Науковий вісник НЛТУ України*. 2008. № 18 (9). С. 270–273.

14. Арістова І. В. Організаційно-правові засади інноваційного розвитку аграрного сектору в умовах розвитку інформаційного суспільства в Україні. *Вісник Сумського національного аграрного університету. Серія : Економіка і менеджмент*. 2012. Вип. 11. С. 161–164.

15. Артемов В. Міжнародний стандарт ISO 17799 як складова в галузі менеджменту інформаційної безпеки. *Юридичний журнал «ЮСТИНІ-АН»*. 2007. URL: <http://www.justinian.com.ua/article.php?id=2802>.

16. Астахова Л. В., Ульянов Н. Л. Модель политики управления осведомленностью сотрудников организации в области информационной безопасности. *Наука ЮУрГУ : материалы 67-й научной конференции*. С. 678–681.

17. Астахова Л. В. Проблема идентификации и оценки кадровых уязвимостей информационной безопасности организации. *Вестник Южно-Уральского государственного университета. Серия : Компьютерные технологии, управление, радиоэлектроника*. 2013. № 13 (1). С. 79–83.

18. Березіна Л. М. Тенденції та шляхи розвитку відносин підприємств АПК : монографія. Полтава: ТОВ НВП «Укрпромторгсервіс», 2012. 222 с.

19. Бойченко О. В., Торошанко Я. І. Модель корпоративного інформаційного захисту об'єкту інформатизації. 2011. *Наукові записки УНДІЗ*. № 4 (20). С. 15–19.

20. Будник М. М., Тимофеев Д. С. Внутрішні загрози інформаційної безпеки та заходи по їх мінімізації. URL: <http://ir.nmu.org.ua/bitstream/handle/123456789/1666/7.pdf?sequence=1&isAllowed=y>.

21. Валіулліна З. В. Фактори впливу на процес забезпечення інформаційної безпеки корпоративної економіки. *Бізнес-Інформ.* 2016. № 6 (461). С. 101–105.
22. Велігура А. В. Оцінювання стану інформаційної безпеки підприємства. *Управління проектами та розвиток виробництва.* 2014. № 4 (52). С. 28–39.
23. Верещагина Л. С. Развитие качества исполнителей на основе повышения надежности персонала. *Вестник Саратовского государственного социально-экономического университета.* 2007. № 18. С. 41–45.
24. Висоцький В. В. Аутсорсинг як технологія менеджменту інформаційної безпеки підприємства. *Вісник Хмельницького національного університету.* 2010. № 2, Т. 3. С. 62–64.
25. Гатиятуллин Т. Р., Сухова А. Р. К вопросу обучения основам информационной безопасности сотрудников предприятия. *Международный научный журнал «символ науки».* 2015. № 12. С. 128–130.
26. Герасименко О. В., Козак А. В. Інформаційна безпека підприємства: поняття та методи її забезпечення. URL: <http://intkonf.org/kengerasimenkoovk ozkavinformatsiynabezpekapidpriemstvaonyattyatametodiyiyizabezpechennya>.
27. Говорущенко Т. О. Аналіз галузі оцінювання якості програмного забезпечення. *Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі.* 2013. № 773. С. 41–48.
28. Гуз А. М. Еволюція світових стандартів інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави.* 2013. № 2 (12). С. 8–12.
29. Глотина И. М., Козлов А. Н. Обеспечение защиты коммерческой тайны как составляющая экономической безопасности. URL: <http://iii03.pfo-perm.ru/Data/glotina/glotina.htm>.
30. Гришина Н. В. Анализ проблем обеспечения информационной безопасности субъекта информационных отношений. *Вестник МФЮУ.* 2013. № 1. С. 68–73.
31. Данько Ю. І. Теоретико-методологічне обґрунтування підходів до моделювання рівня конкурентоспроможності аграрних підприємств. *Інноваційна економіка.* 2016. № 5–6. С. 76–80.
32. Данько Ю. І. Колодненко Н. В. Роль інформації у формуванні системи конкурентоспроможності підприємства. *Вісник Сумського національного аграрного університету.* 2019. № 3. С. 3–7.
33. Домбровская Л. А., Яковлева Н. А., Стахно Р. Е. Современные подходы к защите информации, методы, средства и инструменты защиты. *Наука, техника и образование.* 2016. № 7. С. 16–19.
34. Дячков Д. В. Educational and informational complexes as the basis of information-learning environment creation in a university. *Теорія та практика*

реформування економічних систем : матер. II Міжнар. наук.-практ. форуму «New economics». К. : В-во «Центр навчальної літератури», 01–10 листопада 2015 р. С. 47–50.

35. Дячков Д. В. Informatization of an economic system in the framework of sustainable development. *Економіка сталого розвитку: теоретичні підходи та практичні рекомендації* : матер. Міжнар. наук.-практ. конф. К. : В-во «Центр навчальної літератури», 2015. С. 44–46.

36. Дячков Д. В. Вовк В. О. Особливості проведення інноваційно-спрямованої реструктуризації підприємств агропродовольчої сфери. *Випереджаючий інноваційний розвиток: теорія, методика, практика* : монографія / за. ред. к.е.н., доцента Ілляшенко Н. С. Суми : Триторія, 2018. С. 328–338.

37. Дячков Д. В. Інформаційна безпека зовнішньоекономічної діяльності України. *Economics, science, education, integration and strategy* : materials of international scientific and practical conference, 18–21 January 2016. Slovak Republic. С. 58.

38. Дячков Д. В. Інформаційне забезпечення екологічної безпеки підприємств АПК. *Управління туристичною індустрією: методологія і практика* : матер. III Міжнар. наук.-практ. інтернет-конф., 06–07 жовтня 2016 р. Полтава : В-во «Копі-центр». С. 72–75.

39. Дячков Д. В. Методичні підходи до оцінки інформаційної безпеки підприємства. *Вісник Сумського національного аграрного університету : Серія «Економіка і менеджмент»*. 2017. № 12 (74). С. 87–92.

40. Дячков Д. В. Напрями розвитку інформаційного кластеру України. *Менеджмент XXI століття: глобалізаційні виклики* : матер. Міжн. наук.-практ. конф. : зб. наук. пр. Полтава : В-во «Сімон», 2017. С. 95–98.

41. Дячков Д. В. Особливості впровадження стандартів інформаційної безпеки на вітчизняних підприємствах. *Економічний розвиток: теорія, методологія, управління* : матер. IV Міжнарод. наук.-практ. конф. Будапешт-Прага-Київ, 2016. С. 104–112.

42. Дячков Д. В. Проблеми стандартизації та сертифікації формування системи інформаційної безпеки підприємства. *Сучасні технології менеджменту* : матер. Міжнар. наук.-практ. конф., 10 листопада 2016 р. Луцьк, 2016. С. 204–205.

43. Дячков Д. В. Характеристика сучасних загроз системі управління інформаційною безпекою аграрних підприємств. *Науково-виробничий журнал «Бізнес-навігатор»*. 2019. Вип. 6.1-1 (56). С. 172–178.

44. Дячков Д. В., Бурий Є. І., Вовковінський Ю. В. Оптимізаційне управління витратами на персонал в умовах економічної нестабільності.

Економічний форум. Луцьк : РВВ Луцького НТУ, 2018. № 1. С. 165–171.

45. Дячков Д. В., Дяченко А. В. Система менеджменту витрат на аграрному підприємстві. *Фінансові механізми сталого розвитку України* : матер. І Міжнар. наук.-практ. конф., 25–26 жовтня 2018 р. Х. : В-во Іванченка І. С., 2018. С. 199–201.

46. Дячков Д. В., Євченко В. І. Особливості формування комунікаційного механізму управління підприємством. *Науковий вісник Буковинського державного фінансово-економічного університету. Економічні науки* : зб. наук. пр. 2015. Вип. 28, Ч. 2. С. 68–71.

47. Дячков Д. В., Кисіль І. Г. Інновації в кадровому менеджменті. *Менеджмент ХХІ століття : глобалізаційні виклики* : матер. Міжн. наук.-практ. конф. : зб. наук. пр. Полтава : В-во «Сімон», 2017. С. 135–138.

48. Дячков Д. В., Кійко С. І. Управління конкурентоспроможністю підприємства в ринкових умовах. *Сучасний стан і перспективи вдосконалення практичної підготовки студентів економічного профілю* : матер. наук.-практ. конф. студ. за результатами проходження вироб. фах. практик за напрямками підготовки (спеціальностями). Вип. 10. Полтава : ПДАА, 2017. С. 40–41.

49. Дячков Д. В., Котенко Р. В. Особливості методичного інструментарію стратегічного аналізу зовнішньоекономічної діяльності підприємства. *Економіка. Управління. Інновації*. 2016. Вип. 1. URL: http://nbuv.gov.ua/UJRN/eui_2016_1_8.

50. Дячков Д. В., Тищенко А. О. Методи визначення стратегічних напрямів інноваційного розвитку підприємства. *Менеджмент ХХІ століття: глобалізаційні виклик* : матер. Міжн. наук.-практ. конф. : зб. наук. пр. Полтава : В-во «Сімон», 2017. С. 98–101.

51. Дячков Д. В., Потапюк І. П. Сучасні тенденції використання інформаційно-комунікативних технологій. *Економічний розвиток : теорія, методологія, управління* : зб. наук. пр. та тез наук. допов. за матер. VI Міжн. наук.-практ. конф. 2019. С. 115–122.

52. Жмайлова В. М., Данько Ю. І., Шумков О. В. Ринкова адаптація та економічна безпека сільськогосподарських підприємств : монографія. Суми : «Сумський національний аграрний університет», 2018. 396 с.

53. Исламова З. Р., Гарифуллина Э. Ф. Проблемы информационного обеспечения управления предприятиями АПК. *Никоновские чтения*. 2008. № 13. URL: <https://cyberleninka.ru/article/n/problemy-informatsionnogo-obespecheniya-upravleniya-predpriyatiyami-apk>.

54. Качан О. І., Сазонець О. М. Інформаційна безпека підприємства в умовах глобалізації. URL: <https://conf.ztu.edu.ua/wp-content/uploads/2017/09/>

234.pdf.

55. Коновальчук В. Украина и США : кто больше тратит на выращивание сельхозкультур. URL: <https://latifundist.com/blog/read/2604-ukraina-i-ssha-kto-bolshe-tratit-na-vyrashchivanie-selhozkultur>.

56. Лабутин Н. Г., Казаков В. В., Волков П. П. Применение инновационных программно-аппаратных средств защиты информации в целях обеспечения экономической безопасности. *Юридическая наука и практика: Вестник Нижегородской академии*. 2008. № 1 (8). С. 72–77.

57. Лукацкий А. Технологии информационной безопасности вчера и сегодня. *Компьютер-Пресс*. 2004. № 4. URL: <https://compress.ru/article.aspx?id=10465>.

58. Ляшенко О. М. Логіка керованості економічної безпеки підприємства. *Управління проектами та розвиток виробництва* : зб. наук. пр. Сєверодонецьк : вид-во СНУ ім. В. Даля, 2013. № 1 (45). С. 5–10.

59. Макаренко П. М. Моделі аграрної економіки : монографія. К. : ІАЕ УААН, 2006. 670 с.

60. Макаренко П. М. Топалов А. Д. Ринкова трансформація аграрного сектора : теорія та практика : монографія. З. : Запорізьк. національн. університет., 2006. 373 с.

61. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Горячая линия-Телеком, 2004. 280 с.

62. Маркина И. А., Зось-Киор Н. В., Дячков Д. В. Роль экономических и социальных индикаторов макроуровня на рейтинг стран в условиях глобализации. *Актуальные проблемы экономики, менеджмента и финансов в современных условиях* : заочная Междун. науч.-практ. конф., 10 марта 2015 г. Усть-Каменогорск, Казахстан : Восточно-Казахстанский государственный университет им. С. Аманжолова, 2015. С. 189–193.

63. Маркина И. А., Зось-Киор Н. В., Дячков Д. В. Управление земельными ресурсами как составляющая аграрного производства: теоретический аспект. *Новая индустриализация как драйвер экономического роста в Казахстане в условиях глобализации* : матер. Междун. науч. конф. молодых ученых, 25 мая 2016. Астана. С. 186–188.

64. Маркіна І. А., Дячков Д. В. Інформаційна безпека в системах електронних послуг. *Наукові розробки, передові технології, інновації* : зб. наук. праць та тез наук. доповідей за матер. III Міжнар. наук.-практ. конф. Прага-Будапешт-Київ : НДІСР. 2016. С. 214–218.

65. Маркіна І. А., Дячков Д. В. Правові засади регулювання інформаційного середовища. *Актуальні проблеми менеджменту: теоретичні*

і практичні аспекти: матер. Міжнар. наук.-практ. інтернет-конф. молодих науковців, аспірантів та студентів. Кам'янець-Подільський, 2015. С. 11–13.

66. Маркіна І. А., Дячков Д. В. Управління інформаційним потенціалом промислових підприємств : монографія. Полтава : В-во «Сімон», 2015. 238 с.

67. Махмудов Х. З., Устік Т. В. Напрямки імплементації стратегії сталого розвитку в аграрному секторі економіки України. Вісник ХНАУ ім. В. В. Докучаєва. Серія «Економічні науки». 2018. Вип. 4. С. 31–41.

68. Міщук Є. В., Телега Г. С. Прийняття управлінських рішень із забезпечення фінансової безпеки підприємства з урахуванням інформаційних загроз. *Агросвіт*. 2014. № 23. С. 56–60.

69. Молодецька-Гринчук К. Метод побудови профілів інформаційної безпеки акторів соціальних інтернет-сервісів. *Інформаційна безпека*. 2017. № 26. С. 104–110.

70. Морозов А. Н. Альтернативные источники статистической информации как основа принятия политических решений. *Вопросы государственного и муниципального управления*. 2018. № 2. С. 50–70.

71. Муратова Е. А. Применение информационных технологий в АПК. Московский экономический журнал. 2019. № 9. URL: <https://cyberleninka.ru/article/n/primenenie-informatsionnyh-tehnologii-v-apk>.

72. Нашинець-Наумова А. Ю. Питання забезпечення інформаційної безпеки підприємства. *Юридичний вісник: конституційне та адміністративне право*. 2012. № 3 (24). С. 58–62.

73. Никитин В. Е. Негативные последствия угроз информационной безопасности. *Эпоха науки*. 2015. № 4. С. 387–390.

74. Нікіфорова Л. О. Метод розрахунку рівня вмотивованості співробітників щодо збереження конфіденційності інформації в задачах інформаційної безпеки. *Інформаційна безпека*. 2014. № 4 (16). С. 175–182.

75. Ольшанська О. В. Основні положення інформаційної безпеки та її стан в сучасних умовах розвитку в Україні. *Вісник КНУТД : Серія «Економічні науки»*. 2015. № 2 (85). С. 62–68.

76. Парахонський Б. О., Яворська Г. М., Резнікова О. А. Міжнародне безпекове середовище: виклики і загрози національній безпеці України. Аналітична доповідь. К. : НІСД, 2013. 64 с.

77. Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. Компания АйТи; ДМК Пресс, 2004. 384 с.

78. Писаренко И. Повышение осведомленности пользователей по вопросам ИБ. URL: <http://www.itsec.ru/articles2/control/povyshenie-osvedomlenosti-polzovateley-po-voprosam-ib>.

79. Пугач А. М. Пріоритетні напрями забезпечення розповсюдження науково-технологічної інформації в аграрному секторі України. *Інвестиції : практика та досвід : Державне управління*. 2015. № 17. С. 95–98.

80. Решетникова Е. Г. Информационные аспекты обеспечения продовольственной безопасности. *Информационная безопасность регионов*. 2014. № 3 (16). С. 45–50.

81. Садовська Є. В. Міжнародний досвід у боротьбі із загрозами інформаційній безпеці – уроки для України. URL: http://www.dsaua.org/index.php?option=com_content&view=article&id=185%3A2013-05-12-18-06-49&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk.

82. Світлична В. Ю., Світлична Т. І. Інформаційна безпека: багатогранність сутності, види загроз та шляхи забезпечення. *Комунальне господарство міст : науково-технічний збірник*. 2013. № 109. С. 360–369.

83. Скиба В., Курбатов В. Керівництво по захисту від внутрішніх загроз інформаційної безпеки. В-во : Пітер, 2008. 320 с.

84. Ткачов В. Що очікує українську зернову логістику в майбутньому. URL: <https://landlord.ua/news/shcho-ochikuie-ukrainsku-zernovu-lohistyku-v-maibutnomu-valerii-tkachov/>.

85. Трещев И. А. Классификации угроз безопасности конфиденциальной информации предприятия. *Мир науки. Педагогика и психология*. 2014. № 3 (42). URL: <https://cyberleninka.ru/article/n/o-klassifikatsii-ugroz-bezopasnosti-konfidentsialnoy-informatsii-predpriyatiya>.

86. Харченко Л. С., Ліпкан В. А., Логінов О. В. Інформаційна безпека України: глосарій. К. : Текст, 2004. 136 с.

87. Чередниченко А. О. Управління персоналом в контексті забезпечення інформаційної безпеки будівельних підприємств аспірант. *Міжнародний науковий журнал «Науковий огляд»*. 2014. Том 8. № 7. URL: <https://naukajournal.org/index.php/naukajournal/article/view/305/498>.

88. Danko Y. I., Galinskaya A. V. Informational and communication component of providing the competitiveness of agrarian enterprises. *Економіка : реалії часу. Науковий журнал*. 2016. № 3 (25). С. 168–173. URL: <http://economics.opu.ua/files/archive/2016/n3.html>.

89. Bolek V., Látečková A, Romanová A., Korcek F. Factors affecting information security focused on SME and agricultural enterprises. *Agris On-line Papers in Economics and Informatics*. 2016. № 8 (4). P. 37–50.

90. Diachkov D. Information security threats on the part of the personnel: specifics of origin and realization. *Security of the XXI century: national and geopolitical aspects* : collective monograph / in edition I. Markina. Nemoros s.r.o., 2019. P. 438–444.

91. Diachkov D., Mandalina N. Modern innovative technologies in agricultural housing. *International problems of management and leadership* : International scientific and practical conference of students and young scientists, December 1st, 2017. Lutsk, 2018. P. 40–42.

92. Diachkov D., Potapiuk I. Economic security of an enterprise in the context of informatization of socio-economic relations. *Modern Transformation of Economics and Management in the Era of Globalization* : International scientific conference. Klaipeda University, Lithuania : Baltija Publishing. P. 98–101.

93. Látečková A., Bolek V., Szabo L. Information systems in agricultural enterprises: an empirical study in Slovak Republic. *Agris on-line papers in economics and informatics*. 2018. Vol. 10, № 2. P. 49–60.

94. Makatúra I. Čo je to bezpečnostný počítačový incident. *ITNews*. 2014. URL: <http://www.itnews.sk/2014-11-24/c166583-co-je-to-bezpecnostny-pocitacovy-incident>.

95. Markina I., Adedeji Oke, Diachkov D. Monitoring the level of sustainable development of the enterprise. *Problems and Perspectives in Management*. Vol. 15, Issue 1. 2017. P. 210–220.

96. Markina I., Diachkov D., Oke O. The influence of social responsibility on the quality of life improvement as a significant element of management of sustainable development of cooperatives: Ukrainian and foreign experience. *Journal of Research on Trade, Management and Economic Development*. 2018. Vol. 5, Issue 2 (10). URL: <http://jrtmed.uccm.md>.

97. Markina I., Diachkov D., S'omych M. The influence of the shadow economy on the socio-economic development of Ukraine. *Perspectives – journal on economic issues*. 28 jún 2017. Vol. 5. P. 37–50.

98. Markina I., Syomych M., Diachkov D. Cybercrime as a leading threat to information security in the countries with transitional economy. Proceedings of the 2nd International Conference on Social, Economic and Academic Leadership (ICSEAL 2018). URL: <https://www.atlantis-press.com/proceedings/icseal-18/25904333>.

99. Maumbe B. M., Okello J. Uses of information and communication technology (ICT) in agriculture and rural development in Sub-Saharan Africa: experiences from South Africa and Kenya. *International journal of ICT research and development in Africa (IJICTRDA)*. 2010. Vol. 1, No. 1. P. 1–22.

100. Northcutt S., Novak J. Networks intrusion detection: third edition. New riders, 2002. 512 p.

101. Singh A., Picot A., Kranz J., Gupta M., Ojha A. Information security management (ISM) practices : lessons from select cases from India and Germany. *Global Journal of flexible systems management*. 2013. Vol. 14, No. 4. P. 225–239.

102. Siponen M., Mahmood M., Pahlila S. Employees' adherence to

information security policies: an exploratory field study. *Information and Management*. 2014. Vol. 51, No. 2. P. 217–224.

103. Аграрний флот. Як Нібулон став найбільшим суднобудівником і судновласником в Україні. URL: <https://nv.ua/ukr/biz/markets/nibulon-yak-agrarna-kompaniya-stala-naybilshim-sudnobudivnikom-ukrajini-50036850.html>.

104. Аналитический центр InfoWatch. Безопасность информации в корпоративных информационных системах. Внутренние угрозы. URL: <https://www.infowatch.ru/resources/analytics>.

105. Структура керівних документів державної політики в інформаційній сфері : нагальні проблеми та шляхи впорядкування. URL: <http://www.niss.gov.ua/articles/572/>.

106. Населення України у 2018 р. Статистичний збірник / Відповідальний за випуск М. Б. Тімоніна. К. : Державна служба статистики України, 2019. 188 с.

107. Обсяг реалізованої промислової продукції за видами діяльності. *Державна служба статистики України*. URL: <http://www.ukrstat.gov.ua>.

108. ТОП-10 областей за рівнем приросту агровиробництва у 2018 році URL: <https://superagronom.com/news/6275-top-10-oblastey-za-rivnem-prirostu-agrovirobnitstva-u-2018-rotsi>.

109. Департамент фінансових розслідувань. Кіберзлочинність та відмивання коштів. URL: [http://minfin.kmu.gov.ua/file/link/396800/file/tipolog 2013.pdf](http://minfin.kmu.gov.ua/file/link/396800/file/tipolog%2013.pdf).

110. Державна служба спеціального зв'язку та захисту інформації України. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=92368&cat_id=48306.

111. Діяльність суб'єктів великого, середнього, малого та мікропідприємництва у 2018 р. Статистичний збірник / За ред. Кузнєцової М. С. К. : Державна служба статистики України, 2019. 373 с.

112. Діяльність суб'єктів господарювання у 2018 р. Статистичний збірник / за ред. Кузнєцової М. С. К. : Державна служба статистики України, 2019. 162 с.

113. Індекс сільськогосподарської продукції у 2018 р. Державна служба статистики України. URL: <http://www.ukrstat.gov.ua>.

114. Міністерство інформаційної політики України. URL: <https://mip.gov.ua/news/2402.html>.

115. НВ Бізнес. Туреччина хоче відкрити в Україні логістичний хаб. URL: <https://nv.ua/ukr/biz/economics/turechchina-hoche-vidkriti-v-ukrajini-logistichniy-hab-50013575.html>.

116. Рослинництво України у 2018 р. Статистичний збірник / Відповідальний за випуск О. М. Прокопенко. К. : Державна служба статистики України, 2019. 220 с.

117. Сільське господарство України у 2018 р. Статистичний збірник / Відповідальний за випуск О. М. Прокопенко. К. : Державна служба статистики України, 2019. 235 с.

118. Сільське, лісове та рибне господарство. Державна служба статистики України. URL: http://www.ukrstat.gov.ua/druk/publicat/kat_u/publ7_u.htm.

119. Тваринництво України у 2018 р. Статистичний збірник / Відповідальний за випуск О. М. Прокопенко. К. : Державна служба статистики України, 2019. 168 с.

120. Indbooks. Formalized presentation of information security threats from staff. URL: <http://indbooks.in/mirror4.ru/?p=225207>.

121. Falcongaze. The main tasks in the field of information security in 2018. URL: <https://falcongaze.ru/pressroom/publications/articles/information-security-2018.html>.

122. Landlord. Дефіцит хоперів у 2020 році складе 3 тис. вагонів. URL: <https://landlord.ua/news/dyfitsyt-khoperiv-u-2020-rotsi-sklade-3-tys-vahoniv/>.

123. Landlord. Зернова логістика в Україні дорожча, аніж у США і Європі. URL: <https://landlord.ua/news/zernova-logistika-v-ukrayini-dorozhcha-anizh-u-ssha-i-yevropi/>.

124. NCSI. National Cyber Security Index. URL: <https://ncsi.ega.ee/country/ua/?pdfReport=1>.

125. The Global Cybersecurity Index 2017. URL: <http://j-times.ru/rejting/globalnyj-indeks-kiberbezopasnosti-2017.html>.

126. The Global Cybersecurity Index and Cybersecurity Profile : Report. *ABI Research*. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-R.pdf.

127. The ITU Global Cybersecurity Index. URL: <https://digital.report/globalnyi-indeks-kiberbezopasnosti-ot-itu-gruziya-i-rossiya-voshli-v-top-10/#prettyPhoto>.

128. The Statistics Portal. URL: <http://www.statista.com/>.

РОЗДІЛ 3

МЕТОДОЛОГІЧНІ ПІДХОДИ ДО ОЦІНЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ АГРОПРОДОВОЛЬЧОЇ СФЕРИ УКРАЇНИ

3.1. Методичні підходи до оцінювання інформаційної безпеки підприємств агропродовольчої сфери

За сучасних умов значною проблемою організації функціонування підприємств є розробка та впровадження системи підтримки належного рівня інформаційної безпеки. У свою чергу, одним із ключових питань підтримки належного рівня інформаційної безпеки підприємства є здійснення оцінки цього рівня, і на цій основі формування проектів відповідних управлінських рішень. Діяльність суб'єктів господарювання, яка здійснюється в трансформаційному полі сучасної економіки України, характеризується багатовимірністю і потребує під час її аналізу врахування великої кількості показників. При цьому показники часто дублюють один одного і не завжди повно віддзеркалюють суттєві характеристики процесів функціонування підприємства. В такому випадку велику кількість вихідних ознак намагаються виразити через меншу кількість більш інформативно містких внутрішніх характеристик явищ. Відтак, проблема пошуку критеріїв та інструментів оцінювання рівня інформаційної безпеки підприємства, що функціонує у динамічному економічному середовищі, представляє значну теоретичну, науково-практичну і прикладну проблему.

Діяльність вітчизняних аграрних підприємств відбувається в умовах інформатизації управлінських процесів, автоматизації виробничих і технологічних процесів, а також цифровізації соціально-економічних взаємовідносин суб'єктів аграрного ринку. Це потребує встановлення не тільки прийнятного рівня інформатизації та автоматизації окремих бізнес-процесів підприємства, а й визначення рівня захисту інформаційної сфери функціонування підприємств агропродовольчої сфери. Оскільки сучасна інформаційна система аграрного підприємства являє собою складну систему, що містить велику кількість компонентів різного ступеня автономності, які пов'язані між собою та між якими здійснюються процеси обміну даними. Практично кожен компонент зазначеної інформаційної системи піддається впливам атак зловмисників або зовнішнього середовища. Найбільш уразливими до атак є програмні й технічні засоби та засоби захисту

інформації інформаційної системи. А найбільш розповсюдженими загрозами можуть бути атаки на операційну систему, на системи управління базами даних, на міжмережний екран, вебсервер, на комунікаційне обладнання тощо. При здійсненні зазначених атак для аграрних підприємств настають наслідки різних ступенів складності. Варто відмітити, що, крім втрати інформації, розголошення комерційної таємниці, втрати іміджу підприємства, у процесі здійснення інформаційної атаки значному ризику піддається економічна, зокрема фінансова складова, яка є результатом діяльності сільськогосподарського підприємства.

Власне тому особливої актуальності набуває обґрунтування методичних підходів до оцінювання та діагностики інформаційної безпеки підприємств агропродовольчої сфери.

Дослідження окремих теоретичних і практичних аспектів проблематики оцінки інформаційної безпеки аграрного підприємства, зокрема розробка методик її діагностики, відображені у працях вітчизняних і зарубіжних науковців, зокрема В. Алексєєва [30], В. Андріанова [6], В. Аранчій [72; 73], С. Бучика [9], А. Велігури [13], С. Грибкова [39], М. Журавель [29], С. Зефірова [30], С. Івка [53; 54], С. Ілляшенко [33], А. Козаченко [35; 36; 37; 38], В. Кононової [39], О. Кравчука [40], П. Кравчука [40], Н. Куканової [41], О. Лаврута [53; 54], В. Максименка [44], І. Маркіної [72], В. Морозової [47], В. Оксенюка [48], Т. Полозової [29], В. Пугіна [52], О. Пузиренко [53; 54], Н. Реверчука [56], Є. Родіна [57], С. Смірної [65], О. Стороженка [29], А. Сьомкіної [59], А. Ферінга [78], О. Харкянєна [39], Дж. Хоффмана [64], А. Цибуліна [59], О. Цуканової [65], В. Шалаєва [9], Е. Ясюка [44].

Водночас доцільно відзначити, що методичні підходи до оцінювання та діагностики інформаційної безпеки суб'єктів агропродовольчої сфери розроблені недостатньо. Якість та ефективність функціонування інформаційної системи визначається рівнем її захищеності від зовнішнього та внутрішнього впливів. Дані світової і вітчизняної статистики свідчать про тенденцію зростання масштабу комп'ютерних зловживань, що призводять до значних фінансових втрат суб'єктів господарювання різного рівня. Усунення та запобігання інформаційним загрозам різного характеру передбачає побудову чіткої системи діагностики, яка повинна базуватися на оцінці інформаційних ризиків і зміни економічних, соціальних, техніко-технологічних та інших показників, спричинених зміною стану інформаційної системи підприємства.

Тому з метою формування найбільш точної, об'єктивної та прийнятної з практичного погляду методології оцінювання рівня інформаційної безпеки доцільно проаналізувати існуючі методичні підходи, методики та метрики її оцінки й діагностики.

Відсутність уніфікованої та найбільш точної методики оцінки рівня безпеки суб'єктів підприємницької діяльності також можна пояснити складнощами математичної формалізації більшості показників інформаційної сфери діяльності аграрного підприємства, оскільки наявні методи оцінювання рівня інформаційної безпеки підприємств агропродовольчої сфери здебільшого не можуть забезпечити зіставність показників. Також сучасні методи характеризуються відсутністю фіксованих меж для інтегрального показника оцінки та діагностики інформаційної безпеки.

Залежно від основного критерію об'єкта оцінювання інформаційної безпеки доцільно визначити чотири основні напрями оцінки: оцінка якісних характеристик або кількісних показників захисту інформації / інформаційної системи / системи інформаційної безпеки / політики інформаційної безпеки; оцінка за еталоном; ризик-орієнтована оцінка; оцінка за економічними показниками.

Напрями оцінки якісних характеристик або кількісних показників захисту інформації / інформаційної системи / системи інформаційної безпеки / політики інформаційної безпеки є найбільш опрацьованими теоретично [1; 2; 3; 4; 6; 13; 29; 30; 33; 40; 41; 44; 47; 56; 64]. Зарубіжні вчені займаються проблемою оцінки інформаційної безпеки з початку появи інформаційних технологій. Найбільш актуальними та фундаментальними працями є нормативні документи, що зробили вагомий теоретичний і практичний внесок у виконання завдань забезпечення інформаційної безпеки, а саме: «Помаранчева книга» [1], у якій викладені та систематизовані критерії оцінки захисту комп'ютерних систем; Європейські критерії оцінки безпеки інформаційних технологій [3], що врахували усі недоліки та обмеження, наявні в «Помаранчевій книзі»; Канадські критерії оцінки безпеки надійності комп'ютерних систем [2]; Федеральні критерії США [4], розроблені на замовлення уряду США і спрямовані на усунення обмежень, тощо.

Концептуальні основи оцінки інформаційної безпеки виникли в 70-х рр. XX ст. у ході формування моделі фізичного захисту інформації з повним перекриттям (моделі Клементса – Хоффмана) [64]. У своєму первісному вигляді модель Клементса – Хоффмана була «ідеалізована», проте саме в процесі аналізу цієї моделі й виникла необхідність оцінки інформаційних загроз. Модель побудована згідно з постулатом, що система інформаційної безпеки повинна мати принаймні один засіб для забезпечення безпеки на кожному можливому шляху впливу порушника на інформаційну систему. Для опису системи захисту інформації з повним перекриттям розглядаються три підмножини [64]:

множина загроз: $U = \{U_i\}, i = 1, m;$

множина об'єктів захисту $O = \{O_j\}, j = 1, n;$

множина механізмів захисту $M = \{M_k\}, k = 1, r.$

Між елементами множин U і O існують відносини «загроза – об'єкт». Друга множина $\{U_i, O_j\}$ існує тоді, коли U_i – засіб отримання доступу до об'єкта O_j .

Погляди сучасників на проблеми оцінки інформаційної безпеки мають іншу спрямованість на відміну від основоположних концепцій. Зокрема Н. Реверчук пропонує використовувати показники інформаційної безпеки підприємства як продуктивність інформації, коефіцієнт інформаційної озброєності та коефіцієнт захищеності інформації [56]. Такий перелік коефіцієнтів є досить обмеженим. Варто зазначити, що всі три показники відображають лише фінансовий аспект інформаційної безпеки, оскільки як вихідні дані для розрахунку наведених показників виступають витрати на роботу з інформаційними ресурсами підприємства [29].

На противагу попередньому підходові вітчизняний науковець С. Ілляшенка рівень інформаційної безпеки визначає часткою неточної, суперечливої або неповної інформації, яка використовується в процесі прийняття управлінських рішень, тобто надає оцінку лише якісним властивостям інформації, яка надається ОПР [33].

З метою проведення комплексної оцінки рівня інформаційної безпеки О. Кравчук та П. Кравчук запропонували п'ять основних показників, які характеризують рівень інформаційно-аналітичного супроводу діяльності підприємства, рівень захищеності комерційної інформації і безпеки документообігу, рівень ділової репутації та рівень іміджу продукції [40].

На основі інтеграції вищезазначених підходів до оцінки рівня інформаційної безпеки вітчизняні вчені М. Журавель, Т. Полозова та О. Стороженко запропонували підхід, відповідно до якого діагностика рівня інформаційної безпеки підприємства проводиться на основі розрахунку трьох ключових напрямів: оцінки захищеності програмно-технічної частини безпеки інформації, оцінки «інформаційної надійності» персоналу, оцінки інформації, що надається ОПР, або оцінки інформації, що наявна в інформаційній службі підприємства [29].

А. Велігура визначає систему оцінки інформаційної безпеки на основі трьох показників, таких як:

- оцінка небезпек інформаційної спрямованості. Шляхом оцінювання небезпек визначаються загрози для інформації, імовірності їх виникнення, а також вразливості інформаційного середовища підприємства та можливий збиток від настання подій порушення інформаційної безпеки;
- рівень дотримання законодавчих, нормативних і договірних вимог,

яких повинні дотримуватися підприємство та його бізнес-партнери, підрядники та постачальники;

- рівень дотримання принципів, цілей і вимог до обробки інформації. Визначення вимог до безпеки проводиться шляхом методичної оцінки ризиків, на основі того принципу, що витрати на забезпечення інформаційної безпеки повинні бути зіставні із заподіяним збитком, який може виникнути в разі порушення інформаційної безпеки. Методи оцінки небезпек можна застосовувати до всього підприємства або лише до його окремих частин – інформаційної системи, системних компонентів і сервісів, залежно від того, що для конкретного підприємства є найбільш практичним, реалістичним і корисним.

Також А. Велігура звертає увагу на доцільність застосування методу критичних сценаріїв, який передбачає моделювання і аналіз ситуації заподіяння шкоди інформаційній системі підприємства та, відповідно, зниження здатності підтримувати управління в межах оптимальних параметрів [13].

В. Морозова та К. Врубльовський стверджують, що ефективність комплексної системи захисту інформації оцінюється як на етапі розробки, так і в процесі експлуатації. В процесі оцінки ефективності комплексної системи захисту інформації вони виокремлюють три підходи: класичний, офіційний, експериментальний [47].

Класичний підхід до оцінки ефективності передбачає використання критеріїв ефективності, значення яких отримуються шляхом моделювання або визначаються за характеристиками реальної інформаційної системи. Такий підхід використовується при розробці й модернізації комплексної системи захисту інформації.

Офіційний підхід передбачає, що політика інформаційної безпеки регулюється державою і повинна спиратися на нормативні акти. Такі документи повинні містити вимоги до захищеності інформації різних категорій конфіденційності та важливості. Вимоги можуть задаватися переліком механізмів захисту інформації, які необхідно мати в інформаційній системі, щоб вона відповідала певному класу захисту. Перевагою класифікаторів (стандартів) є простота їх використання. У багатьох розвинених країнах розроблені власні стандарти захищеності інформаційних систем. Так, у Міністерстві оборони США використовується стандарт TCSEC, який відомий як «Помаранчева книга», згідно з якою для оцінки інформаційних систем розглядається чотири групи безпеки: А, В, С, D [1; 41].

Експериментальний підхід передбачає організацію процесу визначення

ефективності комплексної системи захисту інформації шляхом спроб подолання захисних механізмів системи фахівцями, які виступають в ролі зловмисників. З цією метою складається план проведення експериментів, в якому визначаються їх черговість і матеріально-технічне забезпечення, для визначення недоліків системи захисту. Служба безпеки до моменту подолання захисту «зловмисниками» повинна ввести в комплексну систему захисту інформації нові механізми захисту або змінити існуючі, щоб уникнути проникнення в систему захисту. Одним із недоліків такого підходу є те, що більшість показників розраховується на основі експертного методу, що значно посилює вплив суб'єктивізму на кінцевий результат розрахунків.

В. Максименко та Е. Ясюк вирізняють два основні підходи до оцінки інформаційної безпеки підприємства [44].

Перший підхід орієнтується на стандарти у сфері інформаційної безпеки або на будь-який інший набір вимог. Відповідно, критерій досягнення мети у сфері інформаційної безпеки – це дотримання заданого набору вимог. Критерій ефективності – мінімальні сумарні витрати на виконання поставлених функціональних вимог. Водночас необхідний рівень захищеності в цих документах не завжди встановлений, тому визначити ефективний рівень захищеності інформаційної системи досить складно.

Другий підхід пов'язаний із оцінкою відповідно до принципу «розумної достатності», застосованого до сфери забезпечення інформаційної безпеки підприємства. Цей принцип ґрунтується на таких положеннях:

- абсолютно непорушної системи захисту досягти неможливо;
- необхідно дотримуватися балансу між витратами на захист і одержуваним ефектом;

- вартість засобів захисту не повинна перевищувати вартості інформації, що захищається;

- витрати порушника на несанкціонований доступ до інформації повинні перевищувати той ефект, який він отримає, здійснивши подібний доступ.

Поряд із основним призначенням оцінки інформаційної безпеки – створенням інформаційного захисту для вдосконалення інформаційної безпеки – можливі й інші цілі проведення оцінки інформаційної безпеки, зокрема:

- визначення ступеня відповідності встановленим критеріям окремих сфер забезпечення інформаційної безпеки, процесів забезпечення інформаційної безпеки, захисних заходів;

- виявлення впливу критичних елементів (факторів) і їх поєднання;

- порівняння зрілості різних процесів забезпечення інформаційної безпеки і їх ступеня відповідності різних захисних заходів установленим

вимогам [6; 29; 33; 47].

Отже, проведений аналіз дозволив визначити два основних підходи до методик оцінки інформаційної безпеки підприємства:

перший підхід – на основі оцінки характеристик захисних механізмів для об'єкта захисту та «достатності» системи захисту. Суть підходу полягає в тому, що висновок про рівень інформаційної безпеки здійснюється на основі значення показника ефективності системи захисту. В межах цього підходу увага приділяється лише одному з аспектів інформаційної безпеки – захисту інформації від несанкціонованого доступу;

другий підхід заснований на тісному зв'язку системи показників кількісних оцінок інформаційної безпеки з ефективністю функціонування інформаційної системи в умовах впливу всіх видів загроз інформаційної безпеки. Другий підхід є більш методологічно правильним з погляду системного аналізу, оскільки в цьому разі виконується один із основних принципів системного підходу, який полягає в тому, що кожен елемент системи, виконуючи певну функцію, сприяє досягненню мети (виконанню загальносистемної функції).

Напрямок оцінки інформаційної безпеки за еталоном передбачає порівняння діяльності та заходів щодо забезпечення інформаційної безпеки з вимогами, які виконує підприємство-еталон. Тобто здійснюється оцінка відповідності системи управління безпекою підприємства встановленим зразковим характеристикам та визначається ступінь відхилення від них. За допомогою зазначеного методу оцінки визначається відповідність системи захисту інформації, вимірюється ефективність реалізації процесів системи забезпечення інформаційної безпеки й ідентифікуються недоліки такої реалізації. В результаті оцінювання інформаційної безпеки повинна бути сформована оцінка ступеня відповідності системи інформаційної безпеки підприємства еталону, за який можуть бути прийняті (сукупно та окремо): вимоги законодавства, галузеві вимоги до забезпечення, вимоги нормативних, методичних та організаційно-розпорядчих документів щодо забезпечення інформаційної безпеки, вимоги національних і міжнародних стандартів у сфері інформаційної безпеки.

Алгоритм оцінки інформаційної безпеки за еталоном передбачає вибір еталона; формування критеріїв і показників оцінки інформаційної безпеки на його основі, визначення їх нормативних значень; оцінку системи інформаційної безпеки інших об'єктів і зіставлення отриманих значень із еталоном; визначення причин відхилень; розробку заходів з метою оптимізації рівня інформаційної безпеки об'єктів дослідження [6].

Ризик-орієнтований напрям до оцінки інформаційної безпеки аграрного

підприємства передбачає визначення ризиків інформаційної безпеки, що виникають в інформаційно-комунікаційній сфері цього підприємства, на основі яких розробляються заходи щодо недопущення ризиків, оптимізації та мінімізації їх впливів, усунення наслідків тощо [30].

Значна частина методик оцінки рівня інформаційної безпеки підприємства, аграрного підприємства зокрема, ґрунтується на визначенні інформаційних ризиків. У дослідженнях, проведених С. Бучиком [9], О. Губарєвою [52], С. Івком [53], Н. Кукановою [41], В. Оксенюком [48], В. Пугіним [52], Є. Родіним [57] та іншими науковцями, оцінку інформаційної безпеки пропонується визначати на основі американських і британських методик CRAMM, FRAP, OCTAVE, NIST, MSAT, COBRA та Digital Security Office 2006. Метод CRAMM реалізується у спеціалізованому програмному забезпеченні, яке налаштовується на різні сфери діяльності за допомогою «профілів», а його базовими характеристиками є аналіз ризиків на основі оцінок ресурсів, загроз і вразливостей ресурсів і контроль ризиків, який полягає в ідентифікації та виборі контрзаходів (табл. 3.1).

Таблиця 3.1

Характеристика оцінки та діагностики інформаційної безпеки підприємства на основі методики CRAMM [узагальнено на основі 9; 41; 48; 52; 53; 54; 57]

Методика оцінки та діагностики ІБ	Характеристика методики	Алгоритм проведення оцінки та діагностики	Сфера застосування
CRAMM (CCTA Risk Analysis and Management Method)	- Оцінка ризиків функціонування інформаційної системи; - обстеження інформаційної системи та розробка супровідної документації на всіх етапах проведення; - здійснення аудиту згідно зі стандартом BS 7799: 1995 «Code of Practice for Information Security Management»; - формування політики безпеки, та її інформаційної складової, розробка заходів стратегії розвитку	Для кожного етапу визначається набір вихідних даних, послідовність заходів, анкети для проведення інтерв'ю і набір звітних документів: етап I – ідентифікація та визначення цінності ресурсів, що захищаються; етап II – ідентифікація та оцінка загроз у сфері інформаційної безпеки; пошук і оцінка вразливостей системи, яка підлягає захисту; етап III – генерування варіантів комплексу заходів протидії виявленим ризикам. Розробка рекомендацій загального характеру; конкретні рекомендації для об'єктів захисту; приклади того, як можна організувати захист у конкретній ситуації	Орієнтована на різні типи підприємств

Методика FRAP відрізняється від попередньої тим, що вона базується на концепції, суть якої полягає в тому, що на початковому етапі оцінки слід дотримуватися припущення, що система інформаційної безпеки не має жодних засобів захисту для інформаційної системи, а корпоративна система є незахищеною. Основними перевагами методики FRAP є детальний опис можливостей системи інформаційної безпеки та отримання даних про систему та її вразливості (табл. 3.2).

Таблиця 3.2

Характеристика оцінки та діагностики інформаційної безпеки підприємства на основі методики FRAP [узагальнено на основі 9; 53; 54; 57; 78]

Методика оцінки та діагностики ІБ	Характеристика методики	Алгоритм проведення оцінки та діагностики	Сфера застосування
FRAP (Facilitated Risk Analysis Process)	- Оцінка рівня ризику незахищеної ІС, що надалі дозволяє визначити ефект від упровадження засобів захисту інформації; - кількісна оцінка ризику через числове значення, (наприклад, розмір очікуваних річних втрат і оцінка повернення інвестицій); - оцінка вигоди від упровадження фізичних, технічних, програмних та інших засобів і механізмів захисту	Процедура оцінки: етап I – визначення активів, зокрема інформаційних, які потребують захисту, через опитувальні листи, вивчення документації, інтерв'ювання, використання інструментів автоматизованого аналізу (сканування) мереж; етап II – ідентифікація загроз, на якому можливе застосування декількох підходів: - попередньо підготовлені переліки загроз експертами (checklists); - аналіз статистики подій в інформаційній системі (частота їх виникнення); «мозковий штурм»; етап III – визначення імовірності виникнення загрози інформаційній безпеці; оцінка можливого збитку внаслідок виникнення загрози	Орієнтована на різні розміри виробничих і комерційних підприємств

Методика OCTAVE має високий ступінь гнучкості, що досягається шляхом вибору критеріїв, які підприємство може використовувати в ході адаптації методології під власні потреби (табл. 3.3).

На відміну від розглянутих методика NIST базується на процедурі оцінки ризику, яка є фундаментальним компонентом процесу управління ризиком на підприємстві відповідно до NIST SP 800-39 [71], поряд із

визначенням, обробкою і моніторингом ризиків.

Таблиця 3.3

Характеристика оцінки та діагностики інформаційної безпеки підприємства на основі методики OSTATE [узагальнено на основі 41; 53; 54; 57]

Методика оцінки та діагностики ІБ	Характеристика методики	Алгоритм проведення оцінки та діагностики	Сфера застосування
OSTATE	• Формування профілю загроз, який передбачає інвентаризацію та оцінку цінності активів; • ідентифікація вимог законодавства та нормативної бази; • визначення системи організаційних заходів з підтримки режиму інформаційної безпеки; • в ході оцінки ризику ця методика оцінює тільки очікуваний збиток, але не оцінює вірогідність	Передбачає три фази аналізу ризику: фаза I – розробка профілю загроз, пов'язаних з активами підприємства; фаза II – ідентифікація інфраструктурних вразливостей; фаза III – розробка стратегії та планів безпеки, в тому числі інформаційної безпеки	Орієнтована на різні розміри та типи підприємств

Процедури оцінки ризиків використовуються для ідентифікації, оцінки та пріоритезації ризиків, що виникають унаслідок функціонування інформаційної системи, операційної діяльності підприємства, виконання функцій працівниками.

Цілями оцінки ризиків є інформування ОПР і підтримка процесу реагування на ризик шляхом ідентифікації актуальних загроз як власне підприємству, так і опосередковано іншим організаціям, внутрішніх і зовнішніх вразливостей інформаційного середовища, потенційного збитку підприємства з урахуванням можливостей експлуатації вразливостей загрозами та ймовірності виникнення цих збитків (табл. 3.4).

Більш адаптованою та зручною до практичного використання є методика MSAT, яка запропонована корпорацією Майкрософт і спрямована на управління безпекою інфраструктури підприємства. Ця методика заснована на досвіді фахівців підприємства і замовників та орієнтована на співробітників ІТ-підрозділів аграрних підприємств.

Таблиця 3.4

Характеристика оцінки та діагностики інформаційної безпеки підприємства на основі методики NIST [узагальнено на основі 6; 9; 48; 52; 54; 57; 71]

Методика оцінки та діагностики ІБ	Характеристика методики	Алгоритм проведення оцінки та діагностики	Сфера застосування
NIST (National Institute of Standards and Technology)	• Взаємопов'язана із формуванням стратегії управління ризикам; • є базисом для розроблення власної системи управління ризиками; • процес оцінювання ризику інформаційної безпеки представлений у вигляді таблиці, що відображає залежність ризику від двох вхідних змінних: потенційного збитку та імовірності можливого інциденту; • значення кожної змінної, зокрема ризику, оцінюється за трирівневою шкалою	Передбачає етапи: етап I – опис характеристик системи; етап II – ідентифікація загроз; етап III – ідентифікація вразливостей; етап IV – аналіз наявних засобів/заходів захисту; етап V – визначення значення імовірності; етап VI – аналіз впливу; етап VII – визначення значення ризику; етап VIII – вибір засобів/заходів захисту; етап IX – документування отриманих результатів	Орієнтована на різні розміри та типи підприємств

Результатом визначення ризиків інформаційної безпеки підприємства за методикою MSAT є список проблем, розставлених за пріоритетами, і список рекомендацій щодо мінімізації цих загроз (табл. 3.5).

Окрім розглянутих кількісних методик досить розповсюдженою є методика на основі стандарту ISO 17799 – методика COBRA.

За допомогою цієї методики можливо в автоматизованому режимі виконати найпростіший варіант оцінювання інформаційних ризиків будь-якого підприємства на основі спеціальних електронних баз даних і процедури логічного висновку. Перелік вбудованих вимог до рівня інформаційної безпеки можна доповнити різними нормативними вимогами регіонального рівня, галузевого та рівня підприємств для отримання більш логічних та ефективних висновків і рекомендацій щодо управління інформаційним захистом.

Методика COBRA представляє вимоги стандарту ISO 17799 у вигляді тематичної анкети («check list's»). Введені відповіді автоматично обробляються, і за допомогою відповідних правил логічного висновку формується підсумковий звіт із поточними оцінками інформаційних ризиків

підприємства та рекомендаціями щодо їх управління.

Таблиця 3.5

Характеристика оцінки та діагностики інформаційної безпеки підприємства на основі методики MSAT [узагальнено на основі 9; 41; 42; 48; 52; 53]

Методика оцінки та діагностики ІБ	Характеристика методики	Алгоритм проведення оцінки та діагностики	Сфера застосування
MSAT (Microsoft Security Assessment Tool)	• Дозволяє отримати якісну оцінку ризиків порушення інформаційної безпеки за чотирма характеристиками ІКС: інфраструктура, програмне забезпечення, функціонування, персонал; • для кожної характеристики визначені якісні оцінки ризиків інформаційної безпеки; • оцінка ризиків інформаційної безпеки проводиться за трибальною шкалою	Процес оцінки ризиків інформаційної безпеки передбачає заповнення полів бази даних експертної системи. На основі цього експертна система формує звіт з переліком якісних оцінок ризиків інформаційної безпеки ІКС та пропозицій стосовно покращення організації системи захисту інформації	Орієнтована на підприємства середніх розмірів і різні типи підприємств

Особливості та алгоритм проведення діагностики інформаційної безпеки за методикою COBRA детально наведено у табл. 3.6.

Digital Security Office 2006 – система управління інформаційними ризиками та оцінки відповідності системи управління інформаційної безпеки міжнародним, національним і корпоративним стандартам. Методика складається із системи аналізу ризиків ГРИФ і системи оцінки відповідності системи управління інформаційною безпекою вимогам стандартів – КОНДОР.

Система ГРИФ дозволяє побудувати наближену модель інформаційної системи, що містить найбільш критичні ресурси та основні загрози й вразливості з урахуванням імовірності їх реалізації. Отримана модель показує найбільш вразливі місця інформаційної системи, рівень збитку, до якого може привести кожна вразливість, а також дозволяє прийняти рішення про те, які контрзаходи будуть найбільш ефективними. Характеризована система є гнучкою, максимально простою у використанні, що дає можливість ІТ-менеджеру самостійно (без залучення сторонніх експертів) оцінити рівень

ризиків в інформаційній системі й ефективність існуючої практики забезпечення безпеки підприємства [67].

Таблиця 3.6

Характеристика оцінки та діагностики інформаційної безпеки підприємства на основі методики COBRA [узагальнено на основі 48; 50; 52; 54]

Методика оцінки та діагностики ІБ	Характеристика методики	Алгоритм проведення оцінки та діагностики	Сфера застосування
COBRA (Consultative Objective and BiFunctional Risk Analysis)	- Комплект програмного забезпечення передбачає наявність модулів COBRA ISO 17799 Security Consultant, COBRA Policy Compliance Analyst и COBRA Data Protection Consultant, а також менеджер модуля COBRA, який призначений для налаштування та зміни наявної бази знань; - дозволяє виконати в автоматизованому режимі найпростіший варіант оцінювання інформаційних ризиків будь-якого підприємства; - надає оцінку відносної важливості усіх загроз і уразливостей; - генерує відповідні рішення та рекомендації	Передбачає три фази аналізу ризиків: фаза I – розробка профілю загроз, пов'язаних із активом; фаза II – ідентифікація інфраструктурних уразливостей; фаза III – розробка стратегії та планів безпеки. Методика пропонує скласти профіль загроз і дерево варіантів. Профіль загрози включає в себе вказівки на актив (asset), тип доступу до активу (access), джерело загрози (actor), тип порушення або мотив (motive), результат (outcome) і посилання на описи загрози в загальнодоступних каталогах	Орієнтована на різні розміри та типи підприємств

Цей комплекс оцінює ризики стосовно різних інформаційних ресурсів, вираховує сумарний ризик, а також веде підрахунок співвідношення збитків і сумарного ризику, визначаючи недоліки існуючої політики безпеки (табл. 3.7).

На основі узагальнення розглянутих методик головні етапи ризик-орієнтованої оцінки інформаційної безпеки можна представити у такій послідовності: формування профілю загроз інформаційній безпеці; ідентифікація ризиків порушення інформаційної безпеки; характеристика існуючої системи управління інформаційною безпекою, зокрема інформаційними ризиками; формування критеріїв оцінки ризиків порушення

інформаційної безпеки, оцінка та вимірювання ризик-факторів інформаційної безпеки підприємства; формування звіту; розробка стратегії, політики та планів інформаційної безпеки (ризикозахищеності).

Таблиця 3.7

Характеристика оцінки та діагностики інформаційної безпеки підприємства на основі методики Digital Security Office 2006 [узагальнено на основі 9; 41; 48; 52; 53; 54; 57; 67]

Методика оцінки та діагностики ІБ	Характеристика методики	Алгоритм проведення оцінки та діагностики	Сфера застосування
Digital Security Office 2006	- Дає можливість ІТ-менеджеру самостійно оцінити рівень ризиків в інформаційній системі; - оцінка ефективності існуючої практики щодо забезпечення безпеки підприємства	Алгоритм складається з таких етапів: етап I – опитування з метою визначення повного списку інформаційних ресурсів, які є цінними для підприємства; етап II – введення в систему всіх цінних видів інформації; етап III – визначення збитку по кожній групі цінної інформації, розташованої на відповідних ресурсах, за всіма видами загроз; етап IV – визначення всіх видів користувальницьких груп та інформації на ресурсах, до якої має доступ кожна з груп користувачів; етап V – визначення видів (локальний або віддалений) і права (читання, запис, видалення) доступу користувачів до всіх ресурсів, що містять цінну інформацію; етап VI – визначення засобів захисту інформації. В систему вводиться інформація про разові витрати на придбання всіх засобів захисту інформації та щорічні витрати на їх технічну підтримку, а також – щорічні витрати на супровід системи інформаційної безпеки підприємства; етап VII – опитування користувачів відповідно до списку питань з політики безпеки, реалізованої в системі, що дозволяє оцінити реальний рівень захищеності системи і деталізувати оцінки ризиків; етап VIII – формування звіту про систему	Орієнтована на різні розміри та типи підприємств

Грунтуючись на характеристиках розглянутих ризико-орієнтованих методик оцінки та діагностики інформаційної безпеки, на ринку

інформаційних технологій ці методики можна поділити на дві великі групи: програми, що застосовують якісну (наприклад, «високий», «середній», «низький» чи за шкалою від 1 до 10) та кількісну оцінку ризиків (через числове значення, наприклад, розмір очікуваних річних втрат). До першої групи належать, наприклад, COBRA, FRAP, КОНДОР+, Proteus, до другої, – наприклад, RiskWatch, OCTAVE. Проте є комплекси, що об'єднують ці два підходи (наприклад, CRAMM, MSAT, ГРИФ, NIST, Buddy System) [48].

Розглянуті вище моделі оцінки й діагностики інформаційної безпеки базуються на процесній моделі та містять якісні й кількісні показники оцінювання інформаційних ризиків.

В оцінюванні інформаційної безпеки підприємства доцільно звернути увагу на матричний підхід. Матричний підхід в естиметології інформаційної безпекології поки що широко не застосовується. Причини цього вбачаються у складності підготовки вихідної інформації, зокрема якісного опису співвідношення змінних, що мають використовуватися для оцінок інформаційної безпеки підприємства, а також у традиційній недовірі до якісних оцінок, які дуже часто страждають суб'єктивністю. Як правило, до кількісних оцінок довіра є більшою, навіть тоді, коли такі оцінки насправді є квазікількісними або умовними, наприклад, кількість балів або рівень у частках одиниці [35].

Якщо показник має якісне вираження, то цю якісну характеристику інтерпретують через чисельну шкалу й вимірюють через кількісний показник.

Найбільш класичною формулою (3.1) оцінювання ризику (R) є його оцінка через добуток двох факторів: імовірність реалізації загрози ($P_{\text{реалізації}}$) і розмір збитку (D):

$$R = P_{\text{реалізації}} \cdot D. \quad (3.1)$$

Деталізація імовірності реалізації загрози можлива через вираження імовірності виникнення загрози та ймовірність появи вразливості за формулою (3.2):

$$P_{\text{реалізації}} = P_{\text{загрози}} \cdot P_{\text{вразливості}}. \quad (3.2)$$

В основу різних методик визначення рівня ризиків інформаційної безпеки покладені модифікації наведених вище формул. Наприклад, ризик по всій системі – це сума ризиків по всіх активах і кожній загрозі; ефект від вжитих контрзаходів – це різниця між сумою запланованих витрат на

контрзаходи та сумарною оцінкою збитків при визначеному рівні ризику по всій системі [53].

Вирізняється методика, за якої експерти визначають імовірність виникнення кожного виду ризику порушення інформаційної безпеки та розміри пов'язаних із ним втрат Y (вартість збитку), а також допустимий залишковий ризик $R_{\text{залишковий}}$. Усі оцінки ризиків представлені у вигляді матриці [53; 59; 78] (табл. 3.8).

Таблиця 3.8

Матриця ризиків інформаційної безпеки підприємства [59]

Імовірність атаки (P)	Збиток		
	Низький $0 < Y \leq 10$ (%)	Середній $10 < Y \leq 50$ (%)	Високий $50 < Y \leq 100$ (%)
Висока ($0,5 < P \leq 1$)	Низький $5 < R \leq 10$ (%)	Середній $10 < R \leq 50$ (%)	Високий $50 < R \leq 100$ (%)
Середня ($0,1 < P \leq 0,5$)	Низький $1 < R \leq 5$ (%)	Середній $5 < R \leq 25$ (%)	Середній $10 < R \leq 50$ (%)
Низька ($0 < P \leq 0,1$)	Низький $0 < R \leq 1$ (%)	Низький $0 < R \leq 5$ (%)	Низький $0 < R \leq 10$ (%)

У розглянутій матриці ризиків вартісна міра збитку визначається у відсотках від цінності інформаційного ресурсу на i -му компоненті.

Залишковий ризик обчислюється за формулою (3.3):

$$R_{\text{залишковий}} = P \cdot Y, \quad (3.3)$$

де P – імовірність впливу атак;

Y – вартість збитку.

Оцінка $R_{\text{залишковий}}$ буде достовірною тільки за умови врахування одночасної дії всіх атак на всі компоненти інформаційної системи від усіх категорій злоумисників. Нехай на i -й компонент ($i = \overline{1, I}$, де I – кількість вразливих до атак компонентів інформаційної системи) впливає j -та атака ($j = \overline{1, J}$, де J – кількість можливих атак злоумисника на об'єкт) в l -й зоні компонента з боку порушника k -ї категорії ($k = \overline{1, K}$, K – чисельність категорій порушників).

Відповідно до цієї методики, запропонованої А. Сьомкіною та А. Цибуліним, вірогідність P_{ijkl} впливу j -ї атаки на i -й компонент через l -ну зону уразливості. При цьому вірогідність несанкціонованого доступу до інформації на i -му компоненті інформаційної системи шляхом проведення j -ї атаки через l -ну зону буде дорівнювати похідній атак від k -го злоумисника згідно з формулою (3.4):

$$P_{ikj} = Y_l^{Pijkl}, \quad (3.4)$$

де $l = \overline{1, L_k}$, L_k – кількість захисних зон компонента для k -го зловмисника.

Імовірність впливу атак з боку k -го зловмисника визначається за формулою (3.5):

$$P_{ik} = \sum_{j=1}^J P_{ikj}. \quad (3.5)$$

Тоді ймовірність несанкціонованого отримання інформації на i -му компоненті з боку всіх потенційних зловмисників підраховується за формулою (3.6):

$$P_i = \sum_{k=1}^K P_{ik}. \quad (3.6)$$

Імовірність несанкціонованого доступу до інформації в інформаційній системі аграрного підприємства загалом визначається за формулою (3.7):

$$P = \sum_{i=1}^I P_i. \quad (3.7)$$

При цьому вартість збитку для всієї інформаційної системи аграрного підприємства визначається за формулою (3.8):

$$Y = \sum_{i=1}^I Y_i. \quad (3.8)$$

Отримана формула (3.9) загального залишкового ризику для всієї інформаційної системи аграрного підприємства:

$$R_{\text{залишковий}} = \sum_{i=1}^I P_i \cdot \sum_{i=1}^I Y_i. \quad (3.9)$$

А в разі невиконання умови $R_{\text{залишковий}} \leq R_{\text{залишковий додатовий}}$ вважається, що система не захищена і необхідно оновити механізми захисту [59].

Напрямок оцінки інформаційної безпеки на основі економічних показників є найбільш прийнятним і практично корисним для підприємців аграрного ринку. Для проведення оцінки як критерії ефективності використовуються такі показники: сукупної вартості володіння (Total Cost of Ownership): очікуваних витрат (ALE), який обчислюється як співвідношення між частотою виникнення потенційної загрози та величиною можливих втрат, яка визначається на підставі ступеня тяжкості порушення; економічного ефекту від упровадження системи інформаційної безпеки, який визначається як різниця між показником

збережених ресурсів за рахунок функціонування системи інформаційної безпеки аграрного підприємства та витратами на її створення (функціонування); рентабельності витрат на формування системи інформаційної безпеки тощо. Також використовуються групові та приватні показники економічної оцінки інформаційної безпеки. Групові показники оцінки інформаційної безпеки підприємства агропродовольчої сфери утворюють структуру напрямів оцінки, деталізуючи оцінки поточного рівня інформаційної безпеки підприємства, системи управління нею менеджменту та рівня усвідомлення інформаційної безпеки [19; 58; 65].

На основі узагальнення пропонованих напрямів і методик оцінки та діагностики рівня інформаційної безпеки аграрного підприємства [7; 8; 12; 15; 18; 27; 51; 61; 62; 66; 68; 69], використання переваг кожної з розглянутих методик пропонується концепція авторської методології оцінювання та діагностики інформаційної безпеки підприємств агропродовольчої сфери (рис. 3.1).

Пропонована концепція розробки методології економічного оцінювання та діагностики інформаційної безпеки підприємств агропродовольчої сфери враховує переваги розглянутих напрямів і методичних підходів діагностики та оцінювання рівня інформаційної безпеки аграрних підприємств. Зокрема враховано переваги етапності ризик-орієнтованих напрямів і методик оцінки інформаційної безпеки і в межах пропонованої методології визначено 6 основних етапів проведення оцінки та прогнозування рівня інформаційної безпеки підприємств агропродовольчої сфери.

Напрямок і метод оцінки інформаційної безпеки за еталоном у межах пропонованої методології дозволив уніфікувати та визначити ключові складові системи інформаційної безпеки підприємства агропродовольчої сфери, визначити та згрупувати основні фактори впливу на загрози інформаційної безпеки та визначити наслідки їх настання.

Діагностування системи інформаційної безпеки підприємства агропродовольчої сфери передбачає здійснення оцінки системи управління безпекою підприємства на відповідність встановленим зразковим характеристикам з визначенням ступеню відхилення від них.

Після проведення оцінки інформаційної безпеки повинна бути сформована оцінка ступеня відповідності системи інформаційної безпеки підприємства еталону, за який можуть бути прийняті (в сукупності та окремо) вимоги законодавства, галузеві вимоги до забезпечення інформаційної безпеки, вимоги нормативних, методичних та організаційно-розпорядчих документів щодо забезпечення інформаційної безпеки, вимоги національних і міжнародних стандартів у сфері інформаційної безпеки.

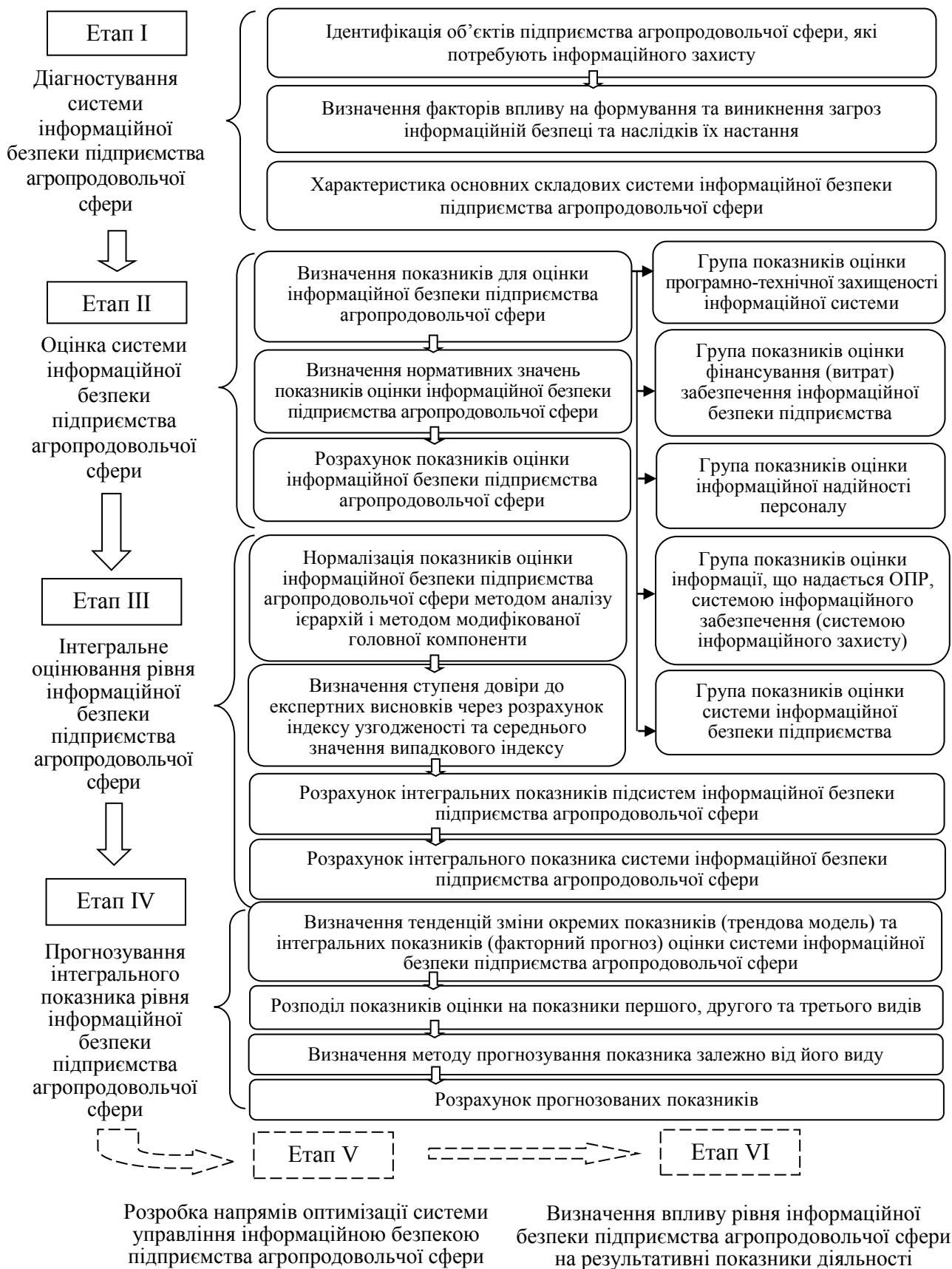


Рис. 3.1. Структурно-логічна схема методології оцінювання та діагностики інформаційної безпеки підприємств агропродовольчої сфери [авторська розробка]

Методичні підходи до оцінки якісних характеристик або кількісних показників захисту інформації / інформаційної системи / системи інформаційної безпеки / політики інформаційної безпеки в поєднанні з методичними підходами, що базуються на економічних показниках оцінки інформаційної безпеки підприємств за допомогою методу аналогії, дозволили в межах запропонованої концепції методології запропонувати 5 груп показників, які дають можливість провести кількісну та якісну оцінку інформаційної безпеки та комплексно оцінити захист інформаційного середовища підприємства, а отже, є підґрунтям для визначення інтегральних показників рівня інформаційної безпеки та дозволяють визначити вплив інтегральних показників на результативні показники діяльності суб'єктів аграрного бізнесу.

Використання переваг матричних методів у межах запропонованої методології забезпечує нормалізацію показників оцінки інформаційної безпеки підприємства агропродовольчої сфери методами аналізу ієрархій і модифікованої головної компоненти й визначенням індексу узгодженості та ступеня довіри до експертних висновків.

Діагностування системи інформаційної безпеки підприємства агропродовольчої сфери, що відповідає першому етапові структурно-логічної схеми методології оцінювання та діагностики інформаційної безпеки, було проведено в підрозділах 2.2 та 2.3 монографії, а також визначено групи показників, які розкривають рівень інформаційної безпеки та їх нормативні значення (див. додаток Я), і на основі яких надано характеристику рівня інформаційної безпеки підприємств агропродовольчої сфери Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей. Водночас усереднені дані одиничних показників не дають змоги зробити найбільш об'єктивні висновки та, відповідно, розробити актуальні та доречні рекомендації. Вищезазначене зумовило необхідність розрахунків інтегральних показників за кожною із розглянутих груп і загального інтегрального показника рівня інформаційної безпеки підприємств аграрного ринку.

3.2. Методологічні підходи до інтегральної оцінки рівня інформаційної безпеки підприємств агропродовольчої сфери України

Встановлення динаміки інтегрального індексу інформаційної безпеки припускає наявність відповідної методології, здатної максимально забезпечити адекватну діагностику рівня інформаційної безпеки

підприємства з можливістю порівняння з інтегральними пороговими (оптимальними) значеннями. Важливого значення набуває можливість прогнозування рівня інформаційної безпеки підприємства на середньо- та довгострокову перспективу. Для цього потрібні моделі, виходом яких стануть прогнозні показники для обчислення прогнозних індикаторів, за якими й можна отримати прогноз рівня інформаційної безпеки [24].

Відповідно до пропонованої методології оцінки інформаційної безпеки підприємств після розрахунків одиничних показників для отримання об'єктивних даних доцільно розрахувати інтегральні показники, які характеризуватимуть рівень інформаційної безпеки підприємств агропродовольчої сфери Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей.

У попередніх розділах було визначено, що інформаційна безпека підприємства являє собою складне синтетичне поняття, а для її оцінювання потрібно сформулювати систему показників, що із достатньою повнотою відображають різні її аспекти. Оскільки переважна більшість науковців виокремлюють в інформаційній системі підприємства функціональні компоненти й різні види забезпечення її діяльності, з-поміж яких найважливішими в контексті інформаційної безпеки є інформаційне, технічне, програмне, організаційне, фінансове, правове та кадрове, то система показників для оцінювання інформаційної безпеки підприємства повинна включати підмножини, які відповідають видам забезпечення відповідної інформаційної системи.

Для цього через X позначено множину всіх показників для оцінювання інформаційної безпеки підприємства, а її підмножини – через X_i . Звідси рівність (3.10):

$$X = \bigcup_{i=1}^n X_i, \quad (3.10)$$

де n – кількість виділених підмножин.

На основі визначених груп показників оцінки інформаційної безпеки (див. додаток Я) доцільно виокремити підмножини показників оцінки:

X_1 – програмно-технічної захищеності інформаційної системи;

X_2 – фінансування забезпечення інформаційної безпеки підприємства;

X_3 – інформаційної надійності персоналу;

X_4 – інформації, що надається ОПР системою інформаційного забезпечення (системою інформаційного захисту);

X_5 – системи інформаційної безпеки підприємства.

Множина X_1 включає показники технічного та програмного

забезпечення інформаційної системи, які доцільно включити до однієї підмножини, оскільки технічне та програмне забезпечення тісно пов'язані між собою. Множина X_2 включає показники фінансового забезпечення, X_3 – кадрового та правового, X_4 – інформаційного, X_5 – організаційного забезпечення діяльності інформаційної системи. Отже, запропонована декомпозиція множини показників для оцінювання інформаційної безпеки підприємства відповідає реально існуючій структурі інформаційної системи.

Через x_{ij} j -й позначаємо показник у множині X_i . Тоді $X_i = \{x_{ij}\}_{j=1}^{m_i}$, де m_i – кількість показників в i -й підмножині, а $X = \left\{ \{x_{ij}\}_{j=1}^{m_i} \right\}_{i=1}^n$.

З метою визначення впливу одиничних показників на рівень інформаційної безпеки їх розподілено на два види: стимулятори, збільшення яких сприяє зміцненню інформаційної безпеки, та дестимулятори, зменшення яких сприяє зміцненню інформаційної безпеки. Обраним показникам надано умовне позначення та визначено їх вид. Отже, група показників оцінки програмно-технічної захищеності інформаційної системи відповідає підмножині показників оцінки програмно-технічної захищеності інформаційної системи (табл. 3.9).

Таблиця 3.9

Підмножина показників оцінки програмно-технічної захищеності інформаційної системи (X_1) [побудовано автором]

Позначення	Назва показника	Зміст показника	Вид показника
X_{11}	Коефіцієнт технічного захисту інформаційної системи	Співвідношення кількості відвернутих інформаційних атак до загальної кількості інформаційних атак за певний проміжок часу	Стимулятор
X_{12}	Коефіцієнт програмної захищеності інформаційної системи	Співвідношення часу безперебійного функціонування інформаційної системи до нормативного часу функціонування інформаційної системи	Стимулятор
X_{13}	Коефіцієнт автоматизації програмно-технічної захищеності інформаційної системи	Співвідношення автоматизованих процесів, спрямованих на програмно-технічний захист інформації, до загальної кількості процесів, спрямованих на програмно-технічний захист інформації	Стимулятор
X_{14}	Коефіцієнт інноваційності (новітності) програмно-технічної захищеності інформаційної системи	Співвідношення використання новітніх (які, перебувають на ринку менше року) програмно-технічних засобів захисту інформаційної системи до загальної кількості програмно-технічних засобів захисту	Стимулятор

За аналогією з попередньою групою, група показників оцінки фінансування (витрат) забезпечення інформаційної безпеки підприємства відповідає множині показників оцінки фінансування забезпечення інформаційної безпеки підприємства та має відповідні позначення (табл. 3.10).

Таблиця 3.10

Підмножина показників оцінки фінансування забезпечення інформаційної безпеки підприємства (X_2) [побудовано автором]

Позначення	Назва показника	Зміст показника	Вид показника
1	2	3	4
X_{21}	Коефіцієнт фінансування інформаційної безпеки	Співвідношення витрат на забезпечення інформаційної безпеки підприємства до загальних витрат підприємства	Стимулятор
X_{22}	Коефіцієнт фінансування інформаційних служб підприємства	Співвідношення витрат утримання інформаційної служби підприємства до загальних витрат підприємства	Стимулятор
X_{23}	Коефіцієнт фінансування програмно-технічної захищеності інформації	Співвідношення витрат на програмно-технічний захист інформаційних ресурсів, до загальних витрат підприємства	Стимулятор
X_{24}	Коефіцієнт фінансування інформаційної безпеки фінансової підсистеми підприємства	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист фінансової підсистеми підприємства, до загальних витрат на інформаційну безпеку	Стимулятор
X_{25}	Коефіцієнт фінансування інформаційної безпеки виробничої підсистеми підприємства	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист виробничої підсистеми підприємства, до загальних витрат на інформаційну безпеку	Стимулятор
X_{26}	Коефіцієнт фінансування інформаційної безпеки комерційної, інноваційної та продовольчої підсистем підприємства	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист комерційної, інноваційної та продовольчої підсистем, до загальних витрат на інформаційну безпеку	Стимулятор
X_{27}	Коефіцієнт фінансування програмної захищеності інформації	Співвідношення вартості програмного забезпечення, яке застосовується для створення інформаційного захисту, до загальних витрат на інформаційну безпеку	Стимулятор
X_{28}	Коефіцієнт фінансування технічної захищеності інформації	Співвідношення вартості технічного забезпечення, яке застосовується для створення інформаційного захисту, до загальних витрат на інформаційну безпеку	Стимулятор

1	2	3	4
X ₂₉	Коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист фізичних об'єктів підприємства, до загальних витрат на інформаційну безпеку	Стимулятор
X ₂₁₀	Коефіцієнт фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист персоналу підприємства, до загальних витрат на інформаційну безпеку	Стимулятор

Група показників оцінки інформаційної надійності персоналу відповідає підмножині показників оцінки інформаційної надійності персоналу та має позначення від X₃₁ до X₃₇ (табл. 3.11).

Таблиця 3.11

Підмножина показників оцінки інформаційної надійності персоналу (X₃) [побудовано автором]

Позначення	Назва показника	Зміст показника	Вид показника
1	2	3	4
X ₃₁	Коефіцієнт обізнаності працівників підприємства з політикою інформаційної безпеки	Співвідношення чисельності працівників, які ознайомлені з політикою інформаційної підприємства до загальної чисельності працівників підприємства	Стимулятор
X ₃₂	Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства	Співвідношення чисельності працівників, маючих доступ до комерційної таємниці (баз даних, банків даних тощо), що працюють на підприємстві більше одного року до загальної чисельності працівників, що мають доступ до комерційної таємниці (баз даних, банків даних тощо)	Стимулятор
X ₃₃	Коефіцієнт ненадійності персоналу, що забезпечує інформаційну безпеку підприємства	Співвідношення чисельності працівників, звільнених за причиною витоку інформації до загальної чисельності звільнених працівників	Дестимулятор
X ₃₄	Коефіцієнт невідповідності персоналу до розпізнавання загроз інформаційній безпеці	Співвідношення чисельності працівників, ненавмисні дії яких призвели до витоку інформації через низький рівень компетентності персоналу та невміння розпізнавання загроз інформаційній безпеці до загальної чисельності працівників, що мають доступ до закритої інформації	Дестимулятор
X ₃₅	Коефіцієнт освіченості персоналу системи управління інформаційною безпекою	Співвідношення чисельності працівників системи управління інформаційною безпекою, які мають відповідну спеціальність та кваліфікацію, до загальної чисельності працівників системи управління інформаційною безпекою підприємства	Стимулятор

1	2	3	4
X ₃₆	Коефіцієнт правової незахищеності інформації	Співвідношення обсягу інформації, розголошення якої може спричинити негативні наслідки для підприємства до загального обсягу юридично захищеної інформації	Дестимулятор
X ₃₇	Коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку	Співвідношення інформаційних загроз (інформаційних атак), які відвернуті через дії персоналу, який забезпечує інформаційну безпеку до загальної кількості інформаційних атак за певний проміжок часу	Стимулятор

Наступна група показників оцінки інформації, що надається ОПР системою інформаційного забезпечення (системою інформаційного захисту), є відображенням підмножини показників-стимуляторів оцінки інформації, що надається ОПР системою інформаційного забезпечення (системою інформаційного захисту), а їх розподіл за видами відображений у табл. 3.12.

Таблиця 3.12

Підмножина показників оцінки інформації, що надається особам, які приймають рішення, системою інформаційного забезпечення (системою інформаційного захисту) (X₄) [побудовано автором]

Позначення	Назва показника	Зміст показника	Вид показника
X ₄₁	Коефіцієнт повноти інформації	Співвідношення обсягу інформації, що є в розпорядженні ОПР, до обсягу інформації, необхідної для ухвалення обґрунтованого рішення	Стимулятор
X ₄₂	Коефіцієнт точності інформації	Співвідношення обсягу релевантної інформації до загального обсягу наявної в розпорядженні ОПР інформації	Стимулятор
X ₄₃	Коефіцієнт суперечливості інформації	Співвідношення кількості незалежних свідчень на користь ухвалення рішення до загальної кількості незалежних свідчень у сумарному обсязі релевантної інформації	Стимулятор
X ₄₄	Коефіцієнт своєчасності надання інформації	Співвідношення обсягу своєчасно наданої ОПР інформації до обсягу інформації, необхідної для ухвалення обґрунтованого рішення	Стимулятор
X ₄₅	Коефіцієнт надійності інформації	Співвідношення обсягу інформації, наданої ОПР з перевірених джерел, до загального обсягу наданої ОПР інформації	Стимулятор
X ₄₆	Коефіцієнт коректності форми подання інформації	Співвідношення обсягу інформації, наданої ОПР у коректній і зручній формі для ефективного та швидкого прийняття рішення, до загального обсягу наданої ОПР інформації	Стимулятор

Група показників оцінки системи інформаційної безпеки підприємства відображається підмножиною показників оцінки системи інформаційної безпеки підприємства та містить дестимулятор – ступінь інформаційного ризику (табл. 3.13).

Таблиця 3.13

Підмножина показників оцінки системи інформаційної безпеки підприємства (X₅) [побудовано автором]

Позначення	Назва показника	Зміст показника	Вид показника
1	2	3	4
X ₅₁	Коефіцієнт керованості системи інформаційної безпеки підприємства	Співвідношення компетентостей, якими володіє керівний персонал системи інформаційної безпеки до загальних компетентностей, якими повинен володіти керівник відповідного рівня	Стимулятор
X ₅₂	Коефіцієнт власного програмного забезпечення	Співвідношення програмного забезпечення, розробленого працівниками підприємства, яке задіяне для забезпечення інформаційної безпеки підприємства, до загального програмного забезпечення, яке використовується для захисту інформаційної системи	Стимулятор
X ₅₃	Коефіцієнт власних технічних засобів	Співвідношення технічних засобів, розроблених працівниками підприємства, що задіяні для забезпечення інформаційної безпеки підприємства, до загальної чисельності технічних засобів, які використовуються для захисту ІС	Стимулятор
X ₅₄	Ступінь інформаційного ризику	Відсоток втрат (у грошовому вираженні), спричинених пошкодженням інформаційної цілісності підприємства, до загальних втрат від порушення безпеки	Дестимулятор
X ₅₅	Гнучкість системи інформаційної безпеки підприємства	Здатність системи управління інформаційною безпекою швидко адаптувати організаційну структуру до зовнішніх і внутрішніх потреб	Стимулятор
X ₅₆	Наявність і актуальність нормативно-правового забезпечення системи інформаційної безпеки підприємства	(від 0 до 1, де 0 – нормативно-правове забезпечення системи інформаційної безпеки підприємства відсутнє; 0,33 – наявне застаріле та неактуальне частково формалізоване нормативно-правове забезпечення системи інформаційної безпеки; 0,66 – наявне неактуальне повністю формалізоване нормативно-правове забезпечення системи інформаційної безпеки; 1 – наявне актуальне повністю формалізоване нормативно-правове забезпечення системи інформаційної безпеки)	Стимулятор

1	2	3	4
X ₅₇	Наявність на підприємстві політики інформаційної безпеки	(від 0 до 1, де 0 – політика інформаційної безпеки відсутня; 0,5 – політика інформаційної безпеки наявна, але не формалізована; 1 – наявна дієва та ефективна політика інформаційної безпеки на підприємстві)	Стимулятор
X ₅₈	Наявність на підприємстві стратегії інформаційної безпеки	(від 0 до 1, де 0 – стратегія інформаційної безпеки відсутня; 0,33 – стратегія інформаційної безпеки наявна, але не формалізована; 0,67 – визначена стратегія інформаційної безпеки підприємства; 1 – визначена стратегія інформаційної безпеки підприємства, яка інтегрована у загальну стратегію розвитку підприємства)	Стимулятор
X ₅₉	Наявність на підприємстві підрозділу управління інформаційною безпекою	(від 0 до 1, де 0 – підрозділ управління інформаційною безпекою на підприємстві відсутній; 0,5 – політика інформаційної безпеки наявна, але не формалізована; 1 – сформований та організаційно закріплений підрозділ управління інформаційною безпекою підприємства)	Стимулятор

Отже, підмножини X_i визначають підсистеми системи забезпечення інформаційної безпеки підприємства: множині X_1 відповідає підсистема програмно-технічного, множині X_2 – фінансового, множині X_3 – кадрового, множині X_4 – інформаційного, множині X_5 – організаційного забезпечення.

Надалі для кожної з підмножини X_i визначається інтегральна оцінка відповідної підсистеми в системі інформаційної безпеки підприємства. Інформаційною основою таких оцінок є значення показників x_{ij} протягом певного періоду часу на досліджуваних підприємствах агропродовольчої сфери Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей. Отже, через $x_{ij}(t, r)$ виражатиметься значення показника x_{ij} в період часу t на досліджуваних підприємствах агропродовольчої сфери області r . Для дослідження обрано період 2009–2018 рр. Параметру t надано значення від $t = 1$ в 2009 р. до $t = 10$ в 2018 р. Параметр r має такі значення:

$r = 1$ – досліджувані підприємства агропродовольчої сфери Полтавської області;

$r = 2$ – досліджувані підприємства агропродовольчої сфери Кіровоградської області;

$r = 3$ – досліджувані підприємства агропродовольчої сфери Сумської області;

$r = 4$ – досліджувані підприємства агропродовольчої сфери Харківської

області;

$r = 5$ – досліджувані підприємства агропродовольчої сфери Луганської області.

Для одержання інтегральної оцінки потрібно привести показники до порівняльного виду через нормалізацію показників кожної підмножини X_i .

Для показників-стимуляторів нормалізація здійснюється через рівність (3.11):

$$y_{ij}(t, r) = \frac{x_{ij}(t, r) - x_{ij}^{\min}}{x_{ij}^{\max} - x_{ij}^{\min}}, \quad (3.11)$$

а для показників-дестимуляторів – через рівність (3.12):

$$y_{ij}(t, r) = \frac{x_{ij}^{\max} - x_{ij}(t, r)}{x_{ij}^{\max} - x_{ij}^{\min}}, \quad (3.12)$$

де $y_{ij}(t, r)$ – нормалізоване значення показника x_{ij} в t -й період часу для досліджуваних підприємств агропродовольчої сфери r -ї області;

$x_{ij}(t, r)$ – відповідне початкове значення цього показника, $x_{ij}^{\min}$, $x_{ij}^{\max}$ – відповідно найменше та найбільше значення цього показника за всіма досліджуваними підприємствами агропродовольчої сфери всіх досліджуваних областей та періодів.

Отже, інтегральна оцінка підсистеми в системі інформаційної безпеки підприємства, що визначається підмножиною X_i , обчислюється за формулою (3.13):

$$V_i(t, r) = \sum_{j=1}^{m_i} \alpha_{ij} y_{ij}(t, r), \quad (3.13)$$

де $V_i(t, r)$ – значення інтегральної оцінки підсистеми, яке визначається підмножиною X_i , для досліджуваних підприємств агропродовольчої сфери r -ї області в період часу t ;

$y_{ij}(t, r)$ – нормалізоване значення показника x_{ij} в t -й період часу для досліджуваних підприємств агропродовольчої сфери r -ї області;

α_{ij} – ваговий коефіцієнт показника x_{ij} у множині показників X_i ;

m_i – кількість показників у цій множині.

Отже, обчислення інтегральної оцінки зводиться до визначення вагових коефіцієнтів α_{ij} . Для визначення цих коефіцієнтів (див. рис. 3.1) запропоновано використовувати два методи: метод аналізу ієрархій [58] і

метод модифікованої головної компоненти [5]. Кожен із цих методів має свої переваги та недоліки. Метод аналізу ієрархій використовує експертне оцінювання попарних переваг одних показників над іншими. Цей метод не вимагає накопичення статистичних даних, він дає можливість використати знання та досвід експертів. Водночас використання експертних оцінок вносить у процес інтегрального оцінювання певний елемент суб'єктивізму. Метод модифікованої головної компоненти заснований на дослідженні статистичних даних щодо відібраних показників. Цей метод є об'єктивним, оскільки він враховує взаємозв'язки між показниками, але його застосування можливе лише за наявності достатньої кількості статистичних даних.

У процесі застосування методу аналізу ієрархій першим етапом є складання матриці попарних порівнянь показників. Зазначену матрицю для підмножини показників X_i позначено через Q_i . Ця матриця є квадратною і містить m_i рядків та стовпців. Елемент $q_{j_1 j_2}^i$ цієї матриці, що знаходиться на перетині j_1 -го рядка та j_2 -го стовпця, визначається за такими правилами:

1) якщо показники x_{ij_1} та x_{ij_2} однаково впливають на інтегральну оцінку підсистеми, що визначається множиною показників X_i , то приймаємо $q_{j_1 j_2}^i = 1$. Очевидно, це означає, що на головній діагоналі матриці Q_i розміщені одиниці;

2) якщо показник x_{ij_1} дещо важливіший, ніж x_{ij_2} , але його перевага є незначною, то $q_{j_1 j_2}^i = 3$;

3) якщо показник x_{ij_1} значно важливіший, ніж x_{ij_2} , то $q_{j_1 j_2}^i = 5$;

4) якщо показник x_{ij_1} явно важливіший, ніж x_{ij_2} , то $q_{j_1 j_2}^i = 7$;

5) якщо показник x_{ij_1} за своєю значущістю абсолютно переважає показник x_{ij_2} , то $q_{j_1 j_2}^i = 9$;

6) якщо експерти не цілком впевнені у виборі між двома сусідніми значеннями, які вказані в попередніх правилах, то для оцінювання переваг можна використати числа 2, 4, 6, 8 ;

7) якщо показник x_{ij_1} менш важливий, ніж x_{ij_2} , то приймають

$$q_{j_1 j_2}^i = \frac{1}{q_{j_2 j_1}^i} \quad [58].$$

Для одержаної матриці Q_i визначено добутки $\prod_{j'=1}^{m_i} q_{jj'}^i$, $j = \overline{1, m_i}$ елементів кожного рядка. Із кожного з цих добутків добутий корінь степені m_i та здійснено їх нормалізацію, тобто поділено кожен із них на їх суму. Одержані

значення прийнято за вагові коефіцієнти α_{ij} .

Отже, наявна рівність (3.14):

$$\alpha_{ij} = \frac{\sqrt[m_i]{\prod_{j'=1}^{m_i} q_{jj'}^i}}{\sum_{j=1}^{m_i} \sqrt[m_i]{\prod_{j'=1}^{m_i} q_{jj'}^i}} \quad (3.14)$$

При застосуванні методу модифікованої головної компоненти визначається коваріаційна матриця K_i нормалізованих показників u_{ij} , елементами якої є коефіцієнти коваріації $k_{j_1 j_2}^i = \text{cov}(y_{ij_1}, y_{ij_2})$. Ці коефіцієнти визначаються на основі наявних статистичних даних. Далі визначаються максимальне власне значення $\lambda_i^{\max}$ матриці K_i та відповідний власний вектор A_i , для яких виконується рівність $K_i A_i = \lambda_i^{\max} A_i$. Вагові коефіцієнти α_{ij} показників u_{ij} в інтегральній оцінці V_i пропорційні квадратам компонент вектора A_i , [5] тобто наявна рівність (3.15):

$$\alpha_{ij} = \frac{a_{ij}^2}{\sum_{j=1}^{m_i} a_{ij}^2}, \quad j = \overline{1, m_i}. \quad (3.15)$$

Надавши формалізований вигляд зазначеним методам, доцільно перейти до визначення інтегральних оцінок кожної підсистеми, що визначаються підмножинами X_i методом аналізу ієрархій і методом модифікованої головної компоненти.

Для підмножини X_1 матриця переваг має вигляд, наведений у табл. 3.14

Таблиця 3.14

**Матриця переваг на основі методу аналізу ієрархій для підмножини X_1
[побудовано автором]**

	x_{11}	x_{12}	x_{13}	x_{14}
x_{11}	1	0,33	3	3
x_{12}	3	1	2	4
x_{13}	0,33	0,5	1	2
x_{14}	0,33	0,25	0,5	1

Сформовано на основі опитування

Вагові коефіцієнти показників визначені в табл. 3.15.

Таблиця 3.15

Вагові коефіцієнти показників підмножини X_1 , визначені методом аналізу ієрархій [побудовано автором]

Показник	$\sqrt[4]{\prod_{j'=1}^4 q_{jj'}^1}$	α_{1j}
y_{11}	1,3160740	0,277590
y_{12}	2,2133638	0,466849
y_{13}	0,7598357	0,160267
y_{14}	0,4518010	0,095295
Σ	4,7410745	1,000000

Інтегральна оцінка підсистеми програмно-технічної захищеності інформаційної системи, одержана методом аналізу ієрархій, визначається рівністю: $V_1 = 0,27759 y_{11} + 0,466849 y_{12} + 0,160267 y_{13} + 0,095295 y_{14}$.

Коваріаційна матриця нормалізованих показників цієї підсистеми представлена у табл. 3.16.

Таблиця 3.16

Коваріаційна матриця нормалізованих показників підмножини X_1 , визначена методом модифікованої головної компоненти [побудовано автором]

	y_{11}	y_{12}	y_{13}	y_{14}
y_{11}	0,074443	0,058157	0,033779	0,037099
y_{12}	0,058157	0,067980	0,035980	0,028577
y_{13}	0,033779	0,035980	0,042697	0,048979
y_{14}	0,037099	0,028577	0,048979	0,110400

Її максимальне власне значення $\lambda_1^{\max} = 0,1983$. Вагові коефіцієнти показників визначені в табл. 3.17.

Таблиця 3.17

Вагові коефіцієнти показників підмножини X_1 , визначені методом модифікованої головної компоненти [побудовано автором]

Показник	Компонента a_{1j} власного вектора A_1	α_{1j}
y_{11}	0,5098	0,259896
y_{12}	0,4702	0,221088
y_{13}	0,4066	0,165324
y_{14}	0,5947	0,353668
Σ	1,9813	1,000000

Отже, інтегральна оцінка підсистеми програмно-технічної захищеності інформаційної системи, одержана методом модифікованої головної

компоненти, визначається за рівністю: $V_1 = 0,259896 y_{11} + 0,221088 y_{12} + 0,165324 y_{13} + 0,353668 y_{14}$.

Для підмножини X_2 матриця переваг має вигляд, наведений у табл. 3.18

Таблиця 3.18

Матриця переваг на основі методу аналізу ієрархій для підмножини X_2 [побудовано автором]

	X_{21}	X_{22}	X_{23}	X_{24}	X_{25}	X_{26}	X_{27}	X_{28}	X_{29}	X_{210}
X_{21}	1	4	4	2	5	5	3	3	6	4
X_{22}	0,25	1	0,25	2	3	3	0,33	0,33	4	0,5
X_{23}	0,25	4	1	4	6	6	2	3	7	3
X_{24}	0,5	0,5	0,25	1	2	3	0,33	0,33	4	0,33
X_{25}	0,2	0,33	0,17	0,5	1	3	0,25	0,33	3	0,33
X_{26}	0,2	0,33	0,17	0,33	0,33	1	0,33	0,25	2	0,33
X_{27}	0,33	3	0,5	3	4	6	1	2	6	2
X_{28}	0,33	3	0,33	3	3	4	0,5	1	4	2
X_{29}	0,17	0,25	0,14	0,25	0,33	0,5	0,17	0,25	1	0,25
X_{210}	0,25	2	0,33	3	3	3	0,5	0,5	4	1

Сформовано на основі опитування

Вагові коефіцієнти показників визначені в табл. 3.19.

Отже, інтегральна оцінка підсистеми фінансування забезпечення інформаційної безпеки підприємства, одержана методом аналізу ієрархій, визначається рівністю: $V_2 = 0,249652 y_{21} + 0,065069 y_{22} + 0,199276 y_{23} + 0,055983 y_{24} + 0,038712 y_{25} + 0,026736 y_{26} + 0,146971 y_{27} + 0,110079 y_{28} + 0,020644 y_{29} + 0,086877 y_{210}$.

Таблиця 3.19

Вагові коефіцієнти показників підмножини X_2 , визначені методом аналізу ієрархій [побудовано автором]

Показник	$\sqrt[10]{\prod_{j'=1}^{10} q_{jj'}^2}$	α_{2j}
y_{21}	3,340061	0,249652
y_{22}	0,870551	0,065069
y_{23}	2,666081	0,199276
y_{24}	0,748984	0,055983
y_{25}	0,517925	0,038712
y_{26}	0,357702	0,026736
y_{27}	1,966307	0,146971
y_{28}	1,472733	0,110079
y_{29}	0,276198	0,020644
y_{210}	1,162308	0,086877
Σ	13,37885	1,000000

Коваріаційна матриця нормалізованих показників цієї підсистеми

представлена в табл. 3.20.

Таблиця 3.20

Коваріаційна матриця нормалізованих показників підмножини X_2 , визначена методом модифікованої головної компоненти [побудовано автором]

	y_{21}	y_{22}	y_{23}	y_{24}	y_{25}	y_{26}	y_{27}	y_{28}	y_{29}	y_{210}
y_{21}	0,0911	0,0907	0,0901	0,0566	0,0584	0,0497	0,0523	0,0491	0,0260	0,0449
y_{22}	0,0907	0,1095	0,0769	0,0519	0,0513	0,0438	0,0466	0,0420	0,0214	0,0381
y_{23}	0,0901	0,0769	0,0987	0,0593	0,0620	0,0520	0,0551	0,0525	0,0280	0,0480
y_{24}	0,0566	0,0519	0,0593	0,0559	0,0564	0,0455	0,0573	0,0545	0,0246	0,0465
y_{25}	0,0584	0,0513	0,0620	0,0564	0,0792	0,0559	0,0692	0,0647	0,0309	0,0569
y_{26}	0,0497	0,0438	0,0520	0,0455	0,0559	0,0748	0,0663	0,0704	0,0233	0,0549
y_{27}	0,0523	0,0466	0,0551	0,0573	0,0692	0,0663	0,0904	0,0793	0,0287	0,0662
y_{28}	0,0491	0,0420	0,0525	0,0545	0,0647	0,0704	0,0793	0,0824	0,0271	0,0621
y_{29}	0,0260	0,0214	0,0280	0,0246	0,0309	0,0233	0,0287	0,0271	0,0400	0,0279
y_{210}	0,0449	0,0381	0,0480	0,0465	0,0569	0,0549	0,0662	0,0621	0,0279	0,0599

Максимальне власне значення $\lambda_2^{\max} = 0,5593$. Вагові коефіцієнти показників наведені в табл. 3.21.

Таблиця 3.21

Вагові коефіцієнти показників підмножини X_2 , визначені методом модифікованої головної компоненти [побудовано автором]

Показник	Компонента a_{2j} власного вектора A_2	α_{2j}
y_{21}	0,3542	0,125458
y_{22}	0,3342	0,111690
y_{23}	0,3617	0,130827
y_{24}	0,2923	0,085439
y_{25}	0,3349	0,112158
y_{26}	0,3077	0,094679
y_{27}	0,3502	0,122640
y_{28}	0,3341	0,111623
y_{29}	0,1508	0,022741
y_{210}	0,2877	0,082771
Σ	3,1078	1,000000

Отже, інтегральна оцінка підсистеми фінансування забезпечення інформаційної безпеки підприємства, одержана методом модифікованої головної компоненти, визначається рівністю: $V_2 = 0,125458 y_{21} + 0,11169 y_{22} + 0,130827 y_{23} + 0,085439 y_{24} + 0,112158 y_{25} + 0,094679 y_{26} + 0,12264 y_{27} + 0,111623 y_{28} + 0,022741 y_{29} + 0,082771 y_{210}$.

Для підмножини X_3 матриця переваг має вигляд, наведений у табл. 3.22.

Таблиця 3.22

Матриця переваг на основі методу аналізу ієрархій для підмножини X_3 [побудовано автором]

	X_{31}	X_{32}	X_{33}	X_{34}	X_{35}	X_{36}	X_{37}
X_{31}	1	6	2	3	6	3	2
X_{32}	0,17	1	0,17	0,5	2	0,5	0,33
X_{33}	0,5	6	1	3	6	4	2
X_{34}	0,33	2	0,33	1	3	2	0,5
X_{35}	0,17	0,5	0,17	0,33	1	0,5	0,5
X_{36}	0,33	2	0,25	0,5	2	1	0,33
X_{37}	0,5	3	0,5	2	2	3	1

Сформовано на основі опитування

Вагові коефіцієнти показників підмножини, визначені методом аналізу ієрархій, відображені в табл. 3.23.

Таблиця 3.23

Вагові коефіцієнти показників підмножини X_3 , визначені методом аналізу ієрархій [побудовано автором]

Показник	$\sqrt[7]{\prod_{j'=1}^7 q_{jj'}}$	α_{3j}
y_{31}	2,783927	0,309935
y_{32}	0,463988	0,051656
y_{33}	2,379566	0,264918
y_{34}	0,943722	0,105065
y_{35}	0,380626	0,042375
y_{36}	0,661722	0,073670
y_{37}	1,368738	0,152382
Σ	8,982288	1,000000

Інтегральна оцінка підсистеми інформаційної надійності персоналу, одержана методом аналізу ієрархій, визначається рівністю: $V_3 = 0,309935 y_{31} + 0,051656 y_{32} + 0,264918 y_{33} + 0,105065 y_{34} + 0,042375 y_{35} + 0,073670 y_{36} + 0,152382 y_{37}$.

Коваріаційна матриця нормалізованих показників підсистеми інформаційної надійності персоналу представлена в табл. 3.24.

Таблиця 3.24

Коваріаційна матриця нормалізованих показників підмножини X_3 , визначена методом модифікованої головної компоненти [побудовано автором]

	y_{31}	y_{32}	y_{33}	y_{34}	y_{35}	y_{36}	y_{37}
1	2	3	4	5	6	7	8
y_{31}	0,0824	0,0645	0,0200	0,0467	0,0619	0,0298	0,0669
y_{32}	0,0645	0,0702	0,0300	0,0466	0,0475	0,0424	0,0707

Продовж. табл. 3.24

1	2	3	4	5	6	7	8
y ₃₃	0,0200	0,0300	0,1330	0,0168	0,0281	0,0143	0,0347
y ₃₄	0,0467	0,0466	0,0168	0,0543	0,0456	0,0365	0,0440
y ₃₅	0,0619	0,0475	0,0281	0,0456	0,0759	0,0302	0,0465
y ₃₆	0,0298	0,0424	0,0143	0,0365	0,0302	0,0682	0,0455
y ₃₇	0,0669	0,0707	0,0347	0,0440	0,0465	0,0455	0,0794

Максимальне власне значення матриці становить $\lambda_3^{\max} = 0,3368$.

Вагові коефіцієнти показників підсистеми інформаційної надійності персоналу визначені в табл. 3.25.

Таблиця 3.25

Вагові коефіцієнти показників підмножини X₃, визначені методом модифікованої головної компоненти [побудовано автором]

Показник	Компонента a _{3j} власного вектора A ₃	α_{3j}
y ₃₁	0,4374	0,191319
y ₃₂	0,4295	0,184470
y ₃₃	0,2834	0,080316
y ₃₄	0,3299	0,108834
y ₃₅	0,3841	0,147533
y ₃₆	0,2953	0,087202
y ₃₇	0,4476	0,200346
Σ	2,6072	1,000019

Отже, інтегральна оцінка підсистеми інформаційної надійності персоналу, одержана методом модифікованої головної компоненти, визначається рівністю: $V_3 = 0,191319 y_{31} + 0,18447 y_{32} + 0,080316 y_{33} + 0,108834 y_{34} + 0,147533 y_{35} + 0,087202 y_{36} + 0,200346 y_{37}$.

Для підмножини показників оцінки інформації, що надається ОПР системою інформаційного забезпечення (системою інформаційного захисту) (X₄), матриця переваг представлена в табл. 3.26.

Таблиця 3.26

Матриця переваг на основі методу аналізу ієрархій для підмножини X₄ [побудовано автором]

	X ₄₁	X ₄₂	X ₄₃	X ₄₄	X ₄₅	X ₄₆
X ₄₁	1	0,5	3	0,5	0,33	3
X ₄₂	2	1	3	2	0,5	3
X ₄₃	0,33	0,33	1	0,25	0,17	0,5
X ₄₄	2	0,5	4	1	0,5	2
X ₄₅	3	2	6	2	1	3
X ₄₆	0,33	0,33	2	0,5	0,33	1

Сформовано на основі опитування

Вагові коефіцієнти показників підмножини показників оцінки інформації, що надається ОПР, визначені в табл. 3.27.

Таблиця 3.27

Вагові коефіцієнти показників підмножини X_4 , визначені методом аналізу ієрархій [побудовано автором]

Показник	$\sqrt[6]{\prod_{j'=1}^6 q_{jj'}^4}$	α_{4j}
y_{41}	0,953184	0,131974
y_{42}	1,618870	0,224142
y_{43}	0,363708	0,050357
y_{44}	1,259921	0,174443
y_{45}	2,449490	0,339146
y_{46}	0,577350	0,079937
Σ	7,222524	1,000000

Рівняння інтегральної оцінки підсистеми інформаційного забезпечення ОПР, одержаної методом аналізу ієрархій, матиме такий вигляд: $V_4 = 0,131974 y_{41} + 0,224142 y_{42} + 0,050357 y_{43} + 0,174443 y_{44} + 0,339146 y_{45} + 0,079937 y_{46}$.

Коваріаційна матриця нормалізованих показників підсистеми X_4 має від'ємні значення (табл. 3.28).

Таблиця 3.28

Коваріаційна матриця нормалізованих показників підмножини X_4 , визначена методом модифікованої головної компоненти [побудовано автором]

	y_{41}	y_{42}	y_{43}	y_{44}	y_{45}	y_{46}
y_{41}	0,0685	-0,0368	-0,0465	-0,0400	-0,0424	-0,0476
y_{42}	-0,0368	0,0620	0,0461	0,0459	0,0503	0,0440
y_{43}	-0,0465	0,0461	0,0655	0,0503	0,0591	0,0566
y_{44}	-0,0400	0,0459	0,0503	0,0507	0,0547	0,0469
y_{45}	-0,0424	0,0503	0,0591	0,0547	0,0718	0,0550
y_{46}	-0,0476	0,0440	0,0566	0,0469	0,0550	0,0931

Проте її максимальне власне значення становить $\lambda_4^{\max} = 0,3115$, а вагові коефіцієнти показників оцінки інформації, що надається ОПР системою інформаційного забезпечення (системою інформаційного захисту), визначені в табл. 3.29.

Інтегральна оцінка підсистеми інформаційного забезпечення ОПР, одержана методом модифікованої головної компоненти, визначається за

такою рівністю: $V_4 = 0,134469 y_{41} + 0,138161 y_{42} + 0,182158 y_{43} + 0,143187 y_{44} + 0,193072 y_{45} + 0,209032 y_{46}$.

Таблиця 3.29

Вагові коефіцієнти показників підмножини X_4 , визначені методом модифікованої головної компоненти [побудовано автором]

Показник	Компонента a_{4j} власного вектора A_4	α_{4j}
y_{41}	0,3667	0,134469
y_{42}	0,3717	0,138161
y_{43}	0,4268	0,182158
y_{44}	0,3784	0,143187
y_{45}	0,4394	0,193072
y_{46}	0,4572	0,209032
Σ	2,4402	1,000000

Останньою є група показників оцінки системи інформаційної безпеки підприємства, яка відповідає підмножині X_5 . За аналогією будується матриця переваг на основі методу аналізу ієрархій (табл. 3.30).

Таблиця 3.30

Матриця переваг на основі методу аналізу ієрархій для підмножини X_5 [побудовано автором]

	X_{51}	X_{52}	X_{53}	X_{54}	X_{55}	X_{56}	X_{57}	X_{58}	X_{59}
X_{51}	1	6	6	4	2	2	0,5	0,5	3
X_{52}	0,17	1	2	0,5	0,33	0,25	0,14	0,17	0,5
X_{53}	0,17	0,5	1	0,33	0,33	0,25	0,14	0,17	0,33
X_{54}	0,25	2	3	1	0,5	0,33	0,17	0,25	0,5
X_{55}	0,5	3	3	2	1	0,5	0,25	0,33	2
X_{56}	0,5	4	4	3	2	1	0,5	0,33	2
X_{57}	2	7	7	6	4	2	1	0,5	4
X_{58}	2	6	6	4	3	3	2	1	4
X_{59}	0,33	2	3	2	0,5	0,5	0,25	0,25	1

Сформовано на основі опитування

Вагові коефіцієнти показників підмножини системи інформаційної безпеки підприємства наведені в табл. 3.31.

Таблиця 3.31

Вагові коефіцієнти показників підмножини X_5 , визначені методом аналізу ієрархій [побудовано автором]

Показник	$\sqrt[9]{\prod_{j'=1}^9 q_{jj'}^5}$	α_{5j}
1	2	3
y_{51}	1,962598	0,162962
y_{52}	0,380033	0,031556

1	2	3
y ₅₃	0,297710	0,024720
y ₅₄	0,557571	0,046297
y ₅₅	0,968541	0,080422
y ₅₆	1,360790	0,112992
y ₅₇	2,763756	0,229485
y ₅₈	3,017422	0,250548
y ₅₉	0,734867	0,061019
Σ	12,043289	1,000000

Інтегральна оцінка підсистеми організаційного забезпечення інформаційної безпеки підприємства, одержана методом аналізу ієрархій, визначається такою рівністю: $V_5 = 0,131974 y_{51} + 0,224142 y_{52} + 0,050357 y_{53} + 0,174443 y_{54} + 0,339146 y_{55} + 0,079937 y_{56} + 0,050357 y_{57} + 0,174443 y_{58} + 0,339146 y_{59}$.

Для оцінки показників підмножини X_5 за методом модифікованої головної компоненти визначена коваріаційна матриця нормалізованих показників підсистеми організаційного забезпечення інформаційної безпеки підприємства, що представлена у табл. 3.32.

Таблиця 3.32

Коваріаційна матриця нормалізованих показників підмножини X_5 , визначена методом модифікованої головної компоненти [побудовано автором]

	y ₅₁	y ₅₂	y ₅₃	y ₅₄	y ₅₅	y ₅₆	y ₅₇	y ₅₈	y ₅₉
1	2	3	4	5	6	7	8	9	10
y ₅₁	0,0785	0,0444	0,0408	0,0527	0,0295	0,0363	0,0370	0,0367	0,0402
y ₅₂	0,0444	0,0494	0,0358	0,0396	0,0495	0,0353	0,0380	0,0359	0,0599
y ₅₃	0,0408	0,0358	0,0381	0,0337	0,0347	0,0293	0,0313	0,0284	0,0411
y ₅₄	0,0527	0,0396	0,0337	0,0579	0,0365	0,0423	0,0425	0,0433	0,0593
y ₅₅	0,0295	0,0495	0,0347	0,0365	0,1600	0,0627	0,0600	0,0793	0,1360
y ₅₆	0,0363	0,0353	0,0293	0,0423	0,0627	0,0679	0,0475	0,0660	0,0821
y ₅₇	0,0370	0,0380	0,0313	0,0425	0,0600	0,0475	0,0700	0,0499	0,0960
y ₅₈	0,0367	0,0359	0,0284	0,0433	0,0793	0,0660	0,0499	0,0795	0,0977
y ₅₉	0,0402	0,0599	0,0411	0,0593	0,1360	0,0821	0,0960	0,0977	0,2176

Максимальне власне значення коваріаційної матриці нормалізованих показників підмножини X_5 дорівнює $\lambda_5^{\max} = 0,5498$. Вагові коефіцієнти показників за методом модифікованої головної компоненти визначені в табл. 3.33.

Таблиця 3.33

Вагові коефіцієнти показників підмножини X_5 , визначені методом модифікованої головної компоненти [побудовано автором]

Показник	Компонента a_{5j} власного вектора A_5	α_{5j}
y_{51}	0,2126	0,045199
y_{52}	0,2305	0,053130
y_{53}	0,1785	0,031862
y_{54}	0,2363	0,055838
y_{55}	0,4447	0,197758
y_{56}	0,2952	0,087143
y_{57}	0,3012	0,090721
y_{58}	0,3338	0,111422
y_{59}	0,5717	0,326841
Σ	2,8045	1,000000

Інтегральна оцінка підсистеми організаційного забезпечення інформаційної безпеки підприємства, одержана методом модифікованої головної компоненти, визначається рівністю: $V_5 = 0,045199 y_{51} + 0,05313 y_{52} + 0,031862 y_{53} + 0,055838 y_{54} + 0,197758 y_{55} + 0,087143 y_{56} + 0,090721 y_{57} + 0,111422 y_{58} + 0,326841 y_{59}$.

Визначивши інтегральні оцінки підсистеми, що визначаються підмножиною показників X_i , пропонується інтегральну оцінку, одержану методом аналізу ієрархій, позначити V_i^A , а інтегральну оцінку цієї підсистеми, одержану методом модифікованої головної компоненти, – через V_i^G . Тоді загальна інтегральна оцінка цієї підсистеми визначатиметься рівністю (3.16):

$$W_i = \gamma V_i^A + (1 - \gamma) V_i^G \quad (3.16)$$

Коефіцієнт γ відображає ступінь довіри до експертних висновків, які отримані за допомогою методу аналізу ієрархій. Цей коефіцієнт змінюється в межах від 0 до 1. Якщо $\gamma = 0$, то експертні висновки не беруться до уваги, а лише інтегральна оцінка, отримана методом модифікованої головної компоненти. Якщо $\gamma = 1$, то експертні висновки вважаються абсолютно достовірними, і береться до уваги інтегральна оцінка, отримана методом аналізу ієрархій. Для визначення величини коефіцієнта γ використано поняття індексу узгодженості [58], який обчислюється за формулою (3.17):

$$I = \frac{\lambda^{\max} - n}{n - 1}, \quad (3.17)$$

де $\lambda^{\max}$ – максимальне власне значення матриці попарних порівнянь, одержаної за допомогою методу аналізу ієрархій;
 n – порядок цієї матриці.

Індекс узгодженості порівнюється із середнім значенням $J(n)$ випадкового індексу, який визначається як індекс узгодженості згенерованої випадковим чином матриці попарних порівнянь порядку n . Перелік значень $J(n)$, що відповідають різним значенням n , наведений у роботі Сааті [58]. Якщо величина індексу узгодженості I не перевищує 10 % від величини $J(n)$, то результати експертного оцінювання попарних переваг вважаються узгодженими і їх можна використати для інтегрального оцінювання методом аналізу ієрархій. Інакше результати експертного оцінювання слід переглянути.

З огляду на це за показник якості експертного оцінювання обчислюється за формулою (3.18):

$$\gamma = 1 - \frac{I}{0,1J(n)}. \quad (3.18)$$

Показник якості експертного оцінювання використано для визначення загальної інтегральної оцінки підсистем системи забезпечення інформаційної безпеки підприємства. Результати визначення показника γ наведено в табл. 3.34.

Таблиця 3.34

Визначення показника γ для підмножин X_i [побудовано автором]

Підмножина показників	X_1	X_2	X_3	X_4	X_5
Кількість показників у множині (n)	4	10	7	6	9
$\lambda^{\max}$	4,22	10,85	7,24	6,22	9,3
Індекс узгодженості (I)	0,0733	0,0947	0,04	0,0424	0,0377
$J(n)$	0,9	1,49	1,32	1,24	1,45
γ	0,19	0,36	0,7	0,66	0,74

Для визначення інтегральної оцінки системи інформаційної безпеки підприємства використано рівність (3.19):

$$W = \sum_{i=1}^n \beta_i W_i, \quad (3.19)$$

де W_i – інтегральні оцінки підсистем системи інформаційної безпеки підприємства;

β_i – вагові коефіцієнти, що визначаються методом аналізу ієрархій або методом модифікованої головної компоненти.

Аналогічно до визначення вагових коефіцієнтів підмножин запропоновано визначення вагових коефіцієнтів β_i методом аналізу ієрархій. Відповідно, матриця $Q = (q_{ii'})$ переваг підсистем, що визначаються підмножинами показників X_i , матиме вигляд, відображений в табл. 3.35.

Таблиця 3.35

Матриця переваг підсистем, отримана на основі методу аналізу ієрархій [побудовано автором]

	X_1	X_2	X_3	X_4	X_5
X_1	1	6	6	4	2
X_2	0,17	1	2	0,5	0,33
X_3	0,17	0,5	1	0,33	0,33
X_4	0,25	2	3	1	0,5
X_5	0,5	3	3	2	1

Сформовано на основі опитування

Для одержаної матриці Q_i визначено добутки $\prod_{i'=1}^5 q_{ii'}$, $i = \overline{1,5}$ елементів кожного рядка. Із кожного з цих добутків добуто корінь 5-го степеня та здійснено їх нормалізацію через ділення кожного з них на їх суму. Одержані значення прийнято за вагові коефіцієнти β_i . Зазначене вище визначило рівність (3.20):

$$\beta_i = \frac{\sqrt[5]{\prod_{i'=1}^5 q_{ii'}}}{\sum_{i=1}^5 \sqrt[5]{\prod_{i'=1}^5 q_{ii'}}}. \quad (3.20)$$

А вагові коефіцієнти підсистем, визначені на основі методу аналізу ієрархій, відображені в табл. 3.36.

Таблиця 3.36

Вагові коефіцієнти підмножин, визначені методом аналізу ієрархій [побудовано автором]

Підмножина показників	$\sqrt[5]{\prod_{i'=1}^5 q_{ii'}}$	β_i
X_1	0,698827	0,121075
X_2	0,425142	0,073658
X_3	1,515717	0,262606
X_4	1,084472	0,187890
X_5	2,047673	0,354770
Σ	5,771829	1,000000

Отже, інтегральна оцінка системи інформаційної безпеки підприємства, одержана методом аналізу ієрархій, визначається такою рівністю: $W = 0,121075 W_1 + 0,073658 W_2 + 0,262606 W_3 + 0,187890 W_4 + 0,354770 W_5$.

На її основі визначено вагові коефіцієнти β_i методом модифікованої головної компоненти, а коваріаційна матриця інтегральних оцінок підсистем має такий вигляд (табл. 3.37):

Таблиця 3.37

Коваріаційна матриця нормалізованих показників підмножин, визначена методом модифікованої головної компоненти [побудовано автором]

	W_1	W_2	W_3	W_4	W_5
W_1	0,0785	0,0444	0,0408	0,0527	0,0295
W_2	0,0444	0,0494	0,0358	0,0396	0,0495
W_3	0,0408	0,0358	0,0381	0,0337	0,0347
W_4	0,0527	0,0396	0,0337	0,0579	0,0365
W_5	0,0295	0,0495	0,0347	0,0365	0,1600

Максимальне власне значення матриці $\lambda^{\max} = 0,2287$, а вагові коефіцієнти показників наведені в табл. 3.38.

Таблиця 3.38

Вагові коефіцієнти підмножин, визначені методом модифікованої головної компоненти [побудовано автором]

Інтегральна оцінка підсистеми	Компонента a_i власного вектора A	β_i
W_1	0,4529	0,205118
W_2	0,5043	0,254318
W_3	0,4494	0,20196
W_4	0,3166	0,100236
W_5	0,4883	0,238437
Σ	2,2115	1

Отже, інтегральна оцінка системи інформаційної безпеки підприємства, одержана методом модифікованої головної компоненти, визначається такою рівністю: $W = 0,205118 W_1 + 0,254318 W_2 + 0,254318 W_3 + 0,254318 W_4 + 0,254318 W_5$.

Інтегральна оцінка системи інформаційної безпеки підприємства, одержана методом аналізу ієрархій, позначена через w^A , а інтегральна оцінка, одержана методом модифікованої головної компоненти, через w^G . Отже, загальна інтегральна оцінка цієї системи визначається рівністю (3.21):

$$W = \gamma W^A + (1 - \gamma) W^G, \quad (3.21)$$

де коефіцієнт γ відображає ступінь довіри до експертних висновків, що використані при застосуванні методу аналізу ієрархій, і обчислюється аналогічно до подібних коефіцієнтів для інтегральних оцінок підсистем. Для оцінки системи $n = 5$, $\lambda^{\max} = 5,1339$, індекс узгодженості $I = 0,033475$, $J(n) = 1,12$, коефіцієнт $\gamma = 0,7011$. Отже, інтегральна оцінка системи інформаційної безпеки підприємства визначається такою рівністю: $W = 0,7011W^A + 0,2989W^G$.

Відповідно до пропонованої методології розраховано інтегральні показники оцінки системи інформаційної безпеки та її підсистем для досліджуваних підприємств агропродовольчої сфери Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей.

Рівень системи інформаційної безпеки аграрних підприємств і її підсистем пропонується визначати за такою шкалою:

$$\begin{cases} 0 \leq P_{i6} \leq 0,33 & \text{– недостатній рівень інформаційної безпеки;} \\ 0,34 \leq P_{i6} \leq 0,66 & \text{– помірний рівень інформаційної безпеки;} \\ 0,67 \leq P_{i6} \leq 1 & \text{– високий рівень інформаційної безпеки.} \end{cases}$$

Аналіз інтегральних показників оцінки системи інформаційної безпеки підприємств агропродовольчої сфери Полтавської області (табл. 3.39) свідчить про позитивну динаміку.

Таблиця 3.39

Інтегральні оцінки системи інформаційної безпеки підприємств агропродовольчої сфери Полтавської області за 2009–2018 рр. [побудовано автором]

Підсистеми системи інформаційної безпеки	Роки									
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Підсистема програмно-технічного забезпечення	0,2807	0,3787	0,3395	0,3715	0,4685	0,5725	0,5534	0,8872	0,9612	0,9212
Підсистема фінансового забезпечення	0,2800	0,3028	0,3925	0,4745	0,5277	0,5558	0,8078	0,9107	0,8869	0,9816
Підсистема кадрового забезпечення	0,4608	0,5577	0,6117	0,5930	0,7994	0,8028	0,8859	0,9075	0,9158	0,9741
Підсистема інформаційного забезпечення	0,4804	0,5565	0,5755	0,6350	0,7148	0,7223	0,7842	0,7200	0,7864	0,7786
Підсистема організаційного забезпечення	0,2865	0,3257	0,3275	0,4059	0,4450	0,6118	0,7494	0,8275	0,8513	0,9651
Рівень інформаційної безпеки	0,3590	0,4249	0,4474	0,4926	0,5895	0,6638	0,7673	0,8488	0,8771	0,9327

Зокрема показники підсистеми програмно-технічного забезпечення

(0,2807), підсистеми фінансового забезпечення (0,2800), підсистеми організаційного забезпечення (0,2865), будучи мінімальними у 2009 р., досягли значень високого рівня у 2018 р. Інші підсистеми, зокрема кадрового забезпечення та інформаційного забезпечення, які мали помірний рівень, теж досягли високого рівня у 2018 р., що і забезпечило значне зростання показника рівня інформаційної безпеки аграрних підприємств Полтавської області із середнього значення у 2009 р. майже до максимального у 2018 р.

Інтегральні показники оцінки системи інформаційної безпеки підприємств агропродовольчої сфери Сумської області відображені в табл. 3.40.

Таблиця 3.40

Інтегральні оцінки системи інформаційної безпеки підприємств агропродовольчої сфери Сумської області за 2009–2018 рр. [побудовано автором]

Підсистеми системи інформаційної безпеки	Роки									
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Підсистема програмно-технічного забезпечення	0,2763	0,2520	0,3292	0,3360	0,4521	0,4327	0,5769	0,7591	0,7597	0,7448
Підсистема фінансового забезпечення	0,2760	0,2714	0,3172	0,4246	0,4798	0,6086	0,5836	0,8023	0,8027	0,7668
Підсистема кадрового забезпечення	0,5346	0,5898	0,5522	0,5883	0,5645	0,6507	0,7085	0,8747	0,9108	0,9343
Підсистема інформаційного забезпечення	0,5586	0,6086	0,6082	0,5306	0,6490	0,6859	0,7387	0,7378	0,8116	0,8366
Підсистема організаційного забезпечення	0,2844	0,2983	0,3033	0,3318	0,3293	0,4347	0,7415	0,8477	0,8643	0,8721
Рівень інформаційної безпеки	0,3880	0,4100	0,4194	0,4392	0,4757	0,5501	0,6891	0,8179	0,8441	0,8498

Доцільно відзначити, що як і на підприємствах Полтавської області більшість інтегральних показників, які характеризують підсистеми інформаційної безпеки (програмно-технічного, фінансового, організаційного забезпечення), і які мали значення на початок аналізованого періоду – 0,2763, 0,2760 та 0,2844 відповідно, досягли значень 0,7448, 0,7668 та 0,8721 у 2018 р.

Підсистема кадрового забезпечення демонструє найвищий рівень – 0,9343 у 2018 р. Дещо меншим є значення рівня інтегрального показника підсистеми інформаційного забезпечення – 0,8366 у 2018 р. Інтегральні показники цих підсистем мали помірний рівень у 2009 р. Рівень інформаційної безпеки аграрних підприємств Сумської області має суттєві тенденції до зростання – 0,8498 у 2018 р., на відміну від 0,3880 у 2009 р.

Як і значення усереднених показників, аналізованих у розділі 2

монографії, інтегральні показники оцінки системи інформаційної безпеки підприємств агропродовольчої сфери Кіровоградської області є нижчими, ніж у вищезазначених областей (табл. 3.41).

Таблиця 3.41

**Інтегральні оцінки системи інформаційної безпеки підприємств агропродовольчої сфери Кіровоградської області за 2009–2018 рр.
[побудовано автором]**

Підсистеми системи інформаційної безпеки	Роки									
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Підсистема програмно-технічного забезпечення	0,2284	0,1927	0,2590	0,2949	0,3194	0,2922	0,3539	0,3632	0,3194	0,4147
Підсистема фінансового забезпечення	0,1161	0,1944	0,1916	0,2084	0,2426	0,2344	0,2753	0,2273	0,3856	0,4053
Підсистема кадрового забезпечення	0,4059	0,4249	0,4630	0,3206	0,4224	0,5071	0,3840	0,5548	0,7001	0,7148
Підсистема інформаційного забезпечення	0,4119	0,4282	0,4440	0,4891	0,4664	0,4981	0,4610	0,4737	0,5714	0,5841
Підсистема організаційного забезпечення	0,2594	0,2883	0,2764	0,2829	0,2879	0,3110	0,3186	0,5667	0,5694	0,8607
Рівень інформаційної безпеки	0,2975	0,3188	0,3361	0,3180	0,3487	0,3770	0,3574	0,4763	0,5422	0,6577

Цим підприємствам характерний низький рівень інтегральних показників підсистеми фінансового забезпечення – 0,1161, підсистеми програмно-технічного забезпечення – 0,2284, підсистеми організаційного забезпечення – 0,2594 у 2009 р. Помірне значення інтегральних показників на початковому часовому інтервалі дослідження мають підсистеми кадрового забезпечення – 0,4059 та інформаційного забезпечення – 0,4119.

На відміну від тенденцій, які демонструють підприємства агропродовольчої сфери вищезазначених областей, інтегральний показник підсистеми фінансового забезпечення зріс лише до помірної значення і становив 0,4053 у 2018 р., програмно-технічного забезпечення – 0,4147. Інтегральне значення підсистеми інформаційного забезпечення залишилось в межах категорії помірних значень і становило 0,5841 у 2018 р., а інтегральне значення підсистем кадрового та організаційного забезпечення системи інформаційної безпеки досліджуваних підприємств посилилось. Рівень інформаційної безпеки на кінець аналізованого періоду був помірним і становив 0,6577, хоча його значення у 2009 р. становило лише 0,2975.

Динаміка інтегральних показників оцінки системи інформаційної безпеки підприємств агропродовольчої сфери Харківської області відображена в табл. 3.42.

Таблиця 3.42

Інтегральні оцінки системи інформаційної безпеки підприємств агропродовольчої сфери Харківської області за 2009–2018 рр. [побудовано автором]

Підсистеми системи інформаційної безпеки	Роки									
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Підсистема програмно-технічного забезпечення	0,0774	0,1243	0,1484	0,1359	0,1778	0,0938	0,1709	0,4328	0,4720	0,5185
Підсистема фінансового забезпечення	0,1773	0,1491	0,1633	0,1403	0,1464	0,2328	0,2725	0,3281	0,4046	0,4240
Підсистема кадрового забезпечення	0,3350	0,4285	0,3125	0,3459	0,5663	0,4324	0,5483	0,6980	0,6645	0,7191
Підсистема інформаційного забезпечення	0,3963	0,4261	0,4828	0,4847	0,5119	0,5711	0,4437	0,4847	0,4299	0,5488
Підсистема організаційного забезпечення	0,2776	0,2765	0,2791	0,2743	0,2847	0,3008	0,3196	0,5449	0,7690	0,8308
Рівень інформаційної безпеки	0,2692	0,2999	0,2868	0,2890	0,3576	0,3383	0,3682	0,5290	0,5992	0,6609

Аналіз інтегральних показників аналізованих підсистем показав значне зростання показника підсистеми програмно-технічного забезпечення досліджуваних аграрних підприємств Харківської області з 0,0774 у 2009 р. до 0,5185 у 2018 р.; показника підсистеми організаційного забезпечення з 0,2776 у 2009 р. до 0,8308 у 2018 р.

Меншими темпами спостерігалось зростання інтегральних показників підсистеми фінансового забезпечення – з 0,1773 у 2009 р. до 0,4240 у 2018 р., показників підсистеми кадрового забезпечення – з 0,3350 у 2009 р. до 0,6645 у 2018 р. та показників підсистеми інформаційного забезпечення – з 0,3963 у 2009 р. до 0,5488 у 2018 р. На помірному рівні значення інтегрального показника системи інформаційної безпеки у 2018 р. – 0,6609, хоча його значення у 2009 р. становило лише 0,2692.

Надалі відображено динаміку інтегральних показників заключної групи підприємств – підприємств агропродовольчої сфери Луганської області, яка за усередненими показниками має найнижчий рівень інформаційної безпеки цих підприємств серед досліджуваних підприємств різних областей (табл. 3.43).

За даними розрахунків, майже мінімальними є інтегральні значення підсистем програмно-технічного забезпечення (0,0307), фінансового забезпечення (0,0463) та організаційного забезпечення (0,0265) у 2009 р. Їх показники у 2018 р. становили 0,3821, 0,1980 та 0,5935 відповідно, що свідчить про значне покращення показників зазначених підсистем у системі інформаційної безпеки.

Таблиця 3.43

Інтегральні оцінки системи інформаційної безпеки підприємств агропродовольчої сфери Луганської області за 2009–2018 рр. [побудовано автором]

Підсистеми системи інформаційної безпеки	Роки									
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Підсистема програмно-технічного забезпечення	0,0307	0,1011	0,1340	0,1809	0,1243	0,1217	0,1143	0,1677	0,4342	0,3821
Підсистема фінансового забезпечення	0,0463	0,0551	0,0789	0,0722	0,0577	0,0792	0,1019	0,1793	0,1696	0,1980
Підсистема кадрового забезпечення	0,3284	0,1852	0,1951	0,1647	0,1348	0,1678	0,2257	0,3663	0,3871	0,4121
Підсистема інформаційного забезпечення	0,2775	0,3324	0,3304	0,3701	0,2804	0,2203	0,1403	0,1277	0,1688	0,1255
Підсистема організаційного забезпечення	0,0265	0,0297	0,0449	0,0886	0,1700	0,1989	0,2111	0,1888	0,5455	0,5935
Рівень інформаційної безпеки	0,1443	0,1306	0,1453	0,1643	0,1585	0,1685	0,1753	0,2181	0,3819	0,3924

Інтегральна оцінка підсистеми кадрового забезпечення протягом аналізованого періоду зросла незначно – на 0,0837 і становила 0,4121 у 2018 р. Натомість зменшилося значення інтегрального показника підсистеми інформаційного забезпечення із 0,2775 у 2009 р. до 0,1255 у 2018 р.

Відповідно до проведених розрахунків та аналізу підсистем системи інформаційної безпеки підприємств агропродовольчої сфери, загальних тенденцій до зростання або зменшення інтегральних показників по окремії із підсистем не спостерігалось, а отже, і пропозиції слід розробляти, враховуючи специфіку недоліків системи інформаційної безпеки підприємств різних областей і визначаючи загальні стратегічні напрями забезпечення захисту інформації на досліджуваних підприємствах.

У ході розробки рекомендацій слід також враховувати тенденції зміни інтегральних показників і розрахунок їх прогностичних значень.

3.3. Прогнозування інтегрального показника рівня інформаційної безпеки підприємств агропродовольчої сфери України

Прогнозування впливу одиничних показників інформаційного захисту на рівень інформаційної безпеки підприємств агропродовольчої сфери є складним аналітично-розрахунковим процесом, що пов'язаний із дослідженням закономірностей зміни визначених коефіцієнтів підсистем інформаційної безпеки. Передбачення рівня інтегрального показника рівня

інформаційної безпеки з метою уникнення інформаційних ризиків, зниження рівня продовольчої та економічної безпеки держави в умовах глобалізації на стратегічному рівні потребує детального дослідження підходів до його прогнозування. Для прийняття ефективних управлінських рішень щодо забезпечення інформаційної безпеки підприємств важливо володіти інформацією не тільки про поточний стан її параметрів, але і про ймовірне значення показників інформаційної безпеки в майбутньому. Це стосується як первинних показників, так і інтегральної оцінки системи інформаційної безпеки та її підсистем. В межах пропонованої методології необхідно використовувати моделі та методи прогнозування. Математичні моделі прогнозування передбачають, що в майбутньому будуть із певною імовірністю продовжуватись тенденції розвитку досліджуваних явищ, які були виявлені в минулому та теперішньому часі [10; 14; 43; 46; 49; 63]. Таке припущення засноване на інерційності розвитку, який притаманний багатьом системам, серед яких і система інформаційної безпеки підприємства. Для ефективного прогнозування потрібна точна, достовірна та повна інформація про досліджувану систему, яка зібрана протягом достатньо тривалого ретроспективного періоду, тривалість якого має перевищувати тривалість періоду, на який здійснюється прогнозування, не менше ніж у 3–4 рази [14; 28; 43]. Інформаційним підґрунтям прогнозування динаміки показників інформаційної безпеки підприємств є значення цих показників за 10 років.

За видом функції, що використовується в прогнозних моделях, прогнози поділяють на факторні та трендові [34; 70]. При факторному прогнозі прогнозована величина розглядається як функція від інших величин, а при трендовому – як функція від часу [55]. Під час дослідження інформаційної безпеки підприємств використано обидва види прогнозів: майбутні значення окремих показників прогнозуються на основі трендових моделей, а динаміка інтегральних оцінок визначається за допомогою факторних прогнозів.

Для оцінювання імовірного стану інформаційної безпеки підприємств у 2020 р. здійснено прогноз показників, які визначають цей стан, тобто показників із множини $X = \left\{ \left\{ x_{ij} \right\}_{j=1}^{m_i} \right\}_{i=1}^5$. Ці показники по відношенню до прогнозування пропонується поділити на три види.

До першого належать ті показники, прогноз яких можна визначити безпосередньо з їх означення та відомих значень за попередні роки, взявши до уваги інерційність системи забезпечення інформаційної безпеки. Такими показниками є: x_{55} – гнучкість системи інформаційної безпеки підприємства, x_{56} – наявність та актуальність нормативно-правового забезпечення системи інформаційної безпеки підприємства, x_{57} – наявність на підприємстві

політики інформаційної безпеки, x_{58} – наявність на підприємстві стратегії інформаційної безпеки, x_{59} – наявність на підприємстві підрозділу управління інформаційною безпекою. Із означення цих показників випливає, що їх значення не може зменшитись порівняно із попереднім періодом, проте водночас немає підстав вважати, що ці значення можуть збільшитись. Тобто ймовірність значної зміни цих показників майже нульова. Таким чином доцільно вважати, що значення цих показників у наступному році збігаються з їх значеннями в попередньому. До цього ж виду включаємо показник x_{33} – коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку підприємства. Нульове значення цього показника протягом кількох останніх років дає підставу вважати, що воно залишиться нульовим і в прогнозованому році. Результати прогнозування майбутніх значень показників першого виду наведено в табл. 3.44.

Таблиця 3.44

Прогнозовані значення показників першого виду для досліджуваних підприємств агропродовольчої сфери Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей [побудовано автором]

Показник	Прогнозоване значення на 2020 р.
1	2
Підприємства агропродовольчої сфери Полтавської області	
x_{33}	0
x_{55}	1
x_{56}	0,67
x_{57}	1
x_{58}	0,67
x_{59}	0,5
Підприємства агропродовольчої сфери Сумської області	
x_{33}	0
x_{55}	1
x_{56}	0,67
x_{57}	0,5
x_{58}	0,67
x_{59}	0,5
Підприємства агропродовольчої сфери Кіровоградської області	
x_{33}	0
x_{55}	1
x_{56}	0,67
x_{57}	0,5
x_{58}	0,67
x_{59}	0,5
Підприємства агропродовольчої сфери Харківської області	
x_{33}	0
x_{55}	1

1	2
X ₅₆	0,67
X ₅₇	0,5
X ₅₈	0,67
X ₅₉	0,5
Підприємства агропродовольчої сфери Луганської області	
X ₃₃	0
X ₅₅	1
X ₅₆	0,67
X ₅₇	0,5
X ₅₈	0,67
X ₅₉	0,5

До показників другого виду запропоновано зарахувати показники, динаміка значень яких на досліджуваних підприємствах окремої області має тенденцію до збільшення або зменшення.

До третього виду відносяться показники, які не мають чітко вираженої тенденції до збільшення або зменшення їх значень. Тому одиничні показники можуть бути віднесені до другого виду показників у групі підприємств однієї області і до третього – в групі підприємств іншої області.

Щоб визначити другий вид показників, для кожного показника і для групи підприємств кожної області визначено рівняння парної лінійної регресії (3.22):

$$x_{ij}(t, r) = a_{ijr}t + b_{ijr}, \quad (3.22)$$

де i – номер підмножини, до якої належить показник;

j – номер показника в цій підмножині;

t – номер року;

r – номер групи підприємств області.

Отже, коефіцієнти a_{ijr} та b_{ijr} визначаються методом найменших квадратів [32]. Відповідно до цього методу значення коефіцієнтів визначаються із системи рівнянь (3.23):

$$\begin{cases} a_{ijr} \sum_{t=1}^T t^2 + b_{ijr} \sum_{t=1}^T t = \sum_{t=1}^T t x_{ij}(t, r) \\ a_{ijr} \sum_{t=1}^T t + b_{ijr} T = \sum_{t=1}^T x_{ij}(t, r) \end{cases} \quad (3.23)$$

де T – тривалість ретроспективного періоду. Оскільки відомі значення показників за 10 років, то приймаємо $T = 10$.

Після визначення коефіцієнтів регресії потрібно перевірити адекватність одержаного рівняння регресії початковим даним. Для цього слід визначити коефіцієнт детермінації за рівнянням (3.24):

$$R_{ijr}^2 = 1 - \frac{\sum_{t=1}^T (x_{ij}(t, r) - a_{ijr}t - b_{ijr})^2}{\sum_{t=1}^T (x_{ij}(t, r) - \overline{x_{ij}(r)})^2}, \quad (3.24)$$

де $\overline{x_{ij}(r)}$ – середнє значення показника x_{ij} у групі підприємств r -ї області протягом ретроспективного періоду.

Для подальшого прогнозування потрібно визначити фактичне значення критерію Фішера [11] для кожного показника i групи підприємств кожної області за формулою (3.25):

$$F_{ijr} = \frac{R_{ijr}^2}{1 - R_{ijr}^2} (T - 2). \quad (3.25)$$

Одержане значення порівняно із критичним значенням критерію Фішера $F(\alpha, k_1, k_2)$, де α – довірна імовірність, k_1 та k_2 – ступені свободи. Для парної лінійної регресії $k_1 = 1$, $k_2 = T - 2 = 8$. Прийнята імовірність $\alpha = 0,95$. Якщо є нерівність $F_{ijr} > F(\alpha, k_1, k_2)$, то рівняння регресії є адекватним, а відповідний показник відноситься до другого типу, тобто спостерігається чітко виражена тенденція його динаміки.

Підставляючи в рівняння регресії значення $t = 12$ (номер 2020 р.), одержимо прогнозне значення показника на зазначений рік. Якщо ж маємо нерівність $F_{ijr} < F(\alpha, k_1, k_2)$, то використовувати рівняння регресії для прогнозування не можна, а відповідний показник відноситься до третього виду, тобто в його динаміці немає чітко вираженої тенденції.

Відповідно до проведених розрахунків більшість показників оцінки інформаційної безпеки підприємства агропродовольчої сфери Полтавської області відносяться до другого виду, оскільки не мають стійких тенденцій зміни (табл. 3.45).

До цього виду показників відносяться всі показники групи оцінки програмно-технічної захищеності інформаційної системи, 8 із 10 показників групи показників оцінки фінансування (витрат) забезпечення інформаційної безпеки підприємства, 6 із 7 показників оцінки інформаційної надійності персоналу, 4 із 6 – групи показників оцінки інформації, що надається ОПР

системою інформаційного забезпечення (системою інформаційного захисту), та лише 3 із 9 показників оцінки системи інформаційної безпеки підприємства, оскільки більшість із них відноситься до показників першого виду.

Таблиця 3.45

Прогнозовані значення показників другого виду для досліджуваних підприємств агропродовольчої сфери Полтавської області [побудовано автором]

Показник	a_{ijr}	b_{ijr}	R^2_{ijr}	$F_{ijr} - F(\alpha, k_1, k_2)$	Прогноз на 2020 р.
X ₁₁	0,021515	0,658667	0,819339	30,964190	0,916848
X ₁₂	0,015818	0,758000	0,644079	9,159234	0,947818
X ₁₃	0,035333	0,042667	0,916259	82,214920	0,466667
X ₁₄	0,008061	-0,025330	0,631367	8,384127	0,071394
X ₂₁	0,009212	-0,008670	0,879549	53,099540	0,101879
X ₂₂	0,004061	-0,009330	0,751549	18,881810	0,039394
X ₂₃	0,005152	0,000667	0,757576	19,682340	0,062485
X ₂₄	0,028788	0,112667	0,978269	354,818000	0,458121
X ₂₅	0,016121	0,207333	0,877300	51,882020	0,400788
X ₂₇	0,009697	0,132667	0,529889	3,699605	0,249030
X ₂₈	0,006485	0,185333	0,463203	1,585571	0,263152
X ₂₁₀	0,013576	0,175333	0,791919	25,128950	0,338242
X ₃₁	0,035515	0,370667	0,849881	39,973300	0,796848
X ₃₂	0,022667	0,581333	0,850455	40,177870	0,853333
X ₃₄	-0,012000	0,140000	0,897281	64,564700	0,020000
X ₃₅	0,057879	0,116667	0,890802	59,943530	0,811212
X ₃₆	-0,004550	0,088000	0,707280	14,012240	0,033455
X ₃₇	0,030727	0,548000	0,920620	87,463070	0,916727
X ₄₂	0,033939	0,353333	0,959902	186,193800	0,760606
X ₄₃	0,021818	0,530000	0,561039	4,907197	0,791818
X ₄₄	0,025455	0,580000	0,876304	51,357040	0,885455
X ₄₅	0,014242	0,736667	0,662766	10,404760	0,907576
X ₅₂	0,010182	0,026000	0,703349	13,650090	0,148182
X ₅₃	0,006424	0,068667	0,583022	5,868009	0,145758
X ₅₄	-0,005030	0,136667	0,486614	2,265174	0,076303

Майже аналогічні показники оцінки інформаційної безпеки досліджуваних підприємств агропродовольчої сфери Сумської області відносяться до показників другого виду (табл. 3.46).

Це знову всі показники групи оцінки програмно-технічної захищеності інформаційної системи, 7 із 10 – групи показників оцінки фінансування (витрат) забезпечення інформаційної безпеки підприємства, 6 із 7 аналогічних показників, як і у підприємств Полтавської області, оцінки інформаційної надійності персоналу, 4 із 6 аналогічних показників, як і у підприємств Полтавської області, оцінки інформації, що надається ОПР

системою інформаційного забезпечення (системою інформаційного захисту), та 4 із 9 показників оцінки системи інформаційної безпеки підприємства, до яких, як і у попередніх підприємств, відносяться коефіцієнт власного програмного забезпечення, коефіцієнт власних технічних засобів, ступінь інформаційного ризику та новий показник – коефіцієнт керованості системи інформаційної безпеки підприємства.

Таблиця 3.46

Прогнозовані значення показників другого виду для досліджуваних підприємств агропродовольчої сфери Сумської області [побудовано автором]

Показник	a_{ijr}	b_{ijr}	R^2_{ijr}	$F_{ijr} - F(\alpha, k1, k2)$	Прогноз на 2020 р.
1	2	3	4	5	6
x_{11}	0,009879	0,722667	0,432628	0,782448	0,841212
x_{12}	0,016909	0,678000	0,822174	31,670230	0,880909
x_{13}	0,024424	0,026667	0,865088	45,980200	0,319758
x_{14}	0,007636	-0,022000	0,775953	22,389150	0,069636
x_{21}	0,007758	-0,004670	0,892958	61,419620	0,088424
x_{22}	0,003636	-0,008000	0,802139	27,114780	0,035636
x_{23}	0,004121	0,003333	0,854398	41,626510	0,052788
x_{24}	0,010485	0,203333	0,556746	4,730691	0,329152
x_{26}	0,003273	0,082000	0,401653	0,052511	0,121273
x_{27}	0,010545	0,096000	0,831028	34,027370	0,222545
x_{28}	0,007030	0,157333	0,563201	4,997408	0,241697
x_{31}	0,042303	0,293333	0,845382	38,422880	0,800970
x_{32}	0,023212	0,581333	0,803965	27,491340	0,859879
x_{34}	-0,007030	0,126667	0,554018	4,620307	0,042303
x_{35}	0,059394	0,073333	0,881910	54,427290	0,786061
x_{36}	-0,004670	0,092667	0,745505	18,117130	0,036667
x_{37}	0,030545	0,504000	0,831618	34,193310	0,870545
x_{42}	0,033636	0,350000	0,886849	57,384640	0,753636
x_{43}	0,010909	0,580000	0,409091	0,220806	0,710909
x_{44}	0,018788	0,596667	0,647138	9,354101	0,822121
x_{45}	0,023333	0,656667	0,812971	29,456540	0,936667
x_{51}	0,015152	0,596667	0,901876	68,211760	0,778485
x_{52}	0,003212	0,065333	0,423489	0,558914	0,103879
x_{53}	0,003273	0,072000	0,736364	17,027170	0,111273
x_{54}	-0,008550	0,162000	0,535515	3,905727	0,059455

Дещо менша кількість показників оцінки інформаційної безпеки підприємства агропродовольчої сфери Кіровоградської області була зарахована до другого виду (табл. 3.47).

З першої групи лише коефіцієнт автоматизації програмно-технічної захищеності інформаційної системи та коефіцієнт інноваційності (новітності)

програмно-технічної захищеності інформаційної системи не мають стійкої тенденції.

Таблиця 3.47

Прогнозовані значення показників другого виду для досліджуваних підприємств агропродовольчої сфери Кіровоградської області [побудовано автором]

Показник	a_{ijr}	b_{ijr}	R^2_{ijr}	$F_{ijr} - F(\alpha, k1, k2)$	Прогноз на 2020 р.
X ₁₃	0,010727	0,074000	0,479235	2,044347	0,202727
X ₁₄	0,003636	-0,010000	0,681818	11,825200	0,033636
X ₂₁	0,002485	0,009333	0,628881	8,238797	0,039152
X ₂₂	0,001091	0,000000	0,409091	0,220806	0,013091
X ₂₄	0,014121	0,099333	0,874599	50,477820	0,268788
X ₂₅	0,013758	0,141333	0,729325	16,238090	0,306424
X ₂₉	0,004061	0,030667	0,521189	3,390395	0,079394
X ₂₁₀	0,003091	0,144000	0,528981	3,666801	0,181091
X ₃₁	0,034848	0,245333	0,853329	41,226300	0,663515
X ₃₂	0,021697	0,416667	0,847242	39,052780	0,677030
X ₃₄	-0,008480	0,202667	0,642792	9,078232	0,100848
X ₃₅	0,028788	0,076667	0,802008	27,088090	0,422121
X ₃₇	0,027758	0,425333	0,819557	31,017700	0,758424
X ₄₂	0,008788	0,386667	0,417784	0,422959	0,492121
X ₄₃	0,017576	0,453333	0,509697	2,998785	0,664242
X ₄₄	0,014545	0,530000	0,601881	6,776833	0,704545
X ₄₆	0,010000	0,530000	0,804878	27,682340	0,650000
X ₅₁	0,011818	0,580000	0,667984	10,777580	0,721818
X ₅₂	0,005212	0,029333	0,875473	50,925690	0,091879
X ₅₃	0,006606	0,040667	0,499349	2,661526	0,119939
X ₅₄	-0,012120	0,194667	0,935279	110,289300	0,049212

З другої групи шість показників не мають стійкої тенденції: коефіцієнт фінансування інформаційної безпеки, коефіцієнт фінансування інформаційних служб підприємства, коефіцієнт фінансування інформаційної безпеки фінансової підсистеми підприємства, коефіцієнт фінансування інформаційної безпеки виробничої підсистеми підприємства, коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства, коефіцієнт фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства.

З третьої групи до другого виду показників слід зарахувати такі: коефіцієнт обізнаності працівників підприємства з політикою інформаційної безпеки, коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства, коефіцієнт невідповідності персоналу до розпізнавання загроз інформаційній безпеці, коефіцієнт освіченості

персоналу системи управління інформаційною безпекою та коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку.

Більша частина показників другого виду зарахована з четвертої групи, зокрема такі: коефіцієнт точності інформації, коефіцієнт суперечливості інформації, коефіцієнт своєчасності надання інформації та коефіцієнт коректності форми подання інформації.

З п'ятої групи показників також до другого виду зараховані коефіцієнт керованості системи інформаційної безпеки підприємства, коефіцієнт власного програмного забезпечення, коефіцієнт власних технічних засобів і ступінь інформаційного ризику.

Меншу кількість показників другого виду, тобто з невизначеною тенденцією, мають підприємства агропродовольчої сфери Харківської області – 19 із 36 визначених показників оцінки інформаційної безпеки підприємства агропродовольчої сфери (табл. 3.48).

Таблиця 3.48

Прогнозовані значення показників другого виду для досліджуваних підприємств агропродовольчої сфери Харківської області [побудовано автором]

Показник	a_{ijr}	b_{ijr}	R^2_{ijr}	$F_{ijr} - F(\alpha, k1, k2)$	Прогноз на 2020 р.
x_{13}	0,009394	0,091333	0,638063	8,785662	0,204061
x_{14}	0,007455	-0,024000	0,654001	9,803784	0,065455
x_{21}	0,005212	-0,004670	0,848944	39,642830	0,057879
x_{22}	0,002788	-0,007330	0,843700	37,866020	0,026121
x_{23}	0,002424	0,002667	0,757576	19,682340	0,031758
x_{24}	0,005394	0,143333	0,797443	26,177370	0,208061
x_{27}	-0,002480	0,080667	0,504350	2,822781	0,050848
x_{31}	0,046485	0,231333	0,957357	174,285200	0,789152
x_{32}	0,029333	0,382667	0,926235	95,135180	0,734667
x_{34}	-0,012480	0,234667	0,822212	31,679730	0,084848
x_{35}	0,027273	0,170000	0,864277	45,625740	0,497273
x_{37}	0,016364	0,460000	0,812166	29,273090	0,656364
x_{41}	-0,013330	0,503333	0,564103	5,035286	0,343333
x_{43}	0,013030	0,423333	0,514039	3,144588	0,579697
x_{44}	0,010303	0,553333	0,625541	8,046507	0,676970
x_{51}	0,007273	0,580000	0,727273	16,015680	0,667273
x_{52}	0,006545	0,032000	0,810676	28,937850	0,110545
x_{53}	0,006485	0,039333	0,746106	18,191590	0,117152
x_{54}	-0,004610	0,161333	0,717337	14,984630	0,106061

Отже, це:

лише 2 із 4 показників першої групи – оцінки програмно-технічної захищеності інформаційної системи, а саме: коефіцієнт автоматизації

програмно-технічної захищеності інформаційної системи та коефіцієнт інноваційності (новітності) програмно-технічної захищеності інформаційної системи;

половина показників другої групи – оцінки фінансування (витрат) забезпечення інформаційної безпеки підприємства: коефіцієнт фінансування інформаційної безпеки, коефіцієнт фінансування інформаційних служб підприємства, коефіцієнт фінансування програмно-технічної захищеності інформації, коефіцієнт фінансування інформаційної безпеки фінансової підсистеми підприємства;

майже вся група показників третьої групи – оцінки інформаційної надійності персоналу: коефіцієнт обізнаності працівників підприємства з політикою інформаційної безпеки; коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства; коефіцієнт ненадійності персоналу, що забезпечує інформаційну безпеку підприємства; коефіцієнт невідповідності персоналу до розпізнавання загроз інформаційній безпеці; коефіцієнт освіченості персоналу системи управління інформаційною безпекою; коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку;

половина показників четвертої групи – оцінки інформації, що надається ОПР системою інформаційного забезпечення (системою інформаційного захисту), а саме: коефіцієнт повноти інформації, коефіцієнт суперечливості інформації та коефіцієнт своєчасності надання інформації;

чотири показники п'ятої групи – оцінки системи інформаційної безпеки підприємства: коефіцієнт керованості системи інформаційної безпеки підприємства, коефіцієнт власного програмного забезпечення, коефіцієнт власних технічних засобів і ступінь інформаційного ризику.

Найменшу кількість показників другого виду мають підприємства агропродовольчої сфери Луганської області – 13 показників оцінки інформаційної безпеки підприємства агропродовольчої сфери (табл. 3.49).

У вищезазначених підприємств до другого виду показників зараховані такі:

перша група: коефіцієнт технічного захисту інформаційної системи, коефіцієнт програмної захищеності інформаційної системи, коефіцієнт автоматизації програмно-технічної захищеності інформаційної системи, коефіцієнт інноваційності (новітності) програмно-технічної захищеності інформаційної системи;

друга група: коефіцієнт фінансування інформаційної безпеки, коефіцієнт фінансування інформаційних служб підприємства, коефіцієнт фінансування програмно-технічної захищеності інформації, коефіцієнт фінансування

інформаційної безпеки фінансової підсистеми підприємства;

третя група: коефіцієнт обізнаності працівників підприємства з політикою інформаційної безпеки та коефіцієнт правової незахищеності інформації;

четверта група: коефіцієнт повноти інформації та коефіцієнт своєчасності надання інформації;

п'ята група: ступінь інформаційного ризику.

Таблиця 3.49

Прогнозовані значення показників другого виду для досліджуваних підприємств агропродовольчої сфери Луганської області [побудовано автором]

Показник	a_{ijr}	b_{ijr}	R^2_{ijr}	$F_{ijr} - F(\alpha, k1, k2)$	Прогноз на 2020 р.
x_{11}	0,008485	0,575333	0,505051	2,845610	0,677152
x_{12}	0,010606	0,558667	0,526991	3,595325	0,685939
x_{13}	0,003455	0,096000	0,437576	0,906483	0,137455
x_{14}	0,003879	-0,013330	0,484848	2,211757	0,033212
x_{21}	0,002727	0,002000	0,757576	19,682340	0,034727
x_{22}	0,001515	-0,003330	0,757576	19,682340	0,014848
x_{23}	0,001273	0,006000	0,636364	8,682345	0,021273
x_{24}	0,011333	0,068667	0,797341	26,157590	0,204667
x_{31}	0,014727	0,224000	0,858208	43,103010	0,400727
x_{36}	0,007515	0,072667	0,701716	13,502420	0,162848
x_{41}	-0,009390	0,496667	0,594310	6,401857	0,383939
x_{44}	-0,014550	0,530000	0,581818	5,812780	0,355455
x_{54}	-0,005880	0,211333	0,772686	21,875990	0,140788

Для показників третього виду, в динаміці яких тенденція не виявлена, застосовано метод експоненціального прогнозування [16; 60]. Особливістю цього методу є те, що при визначенні прогнозованих значень більша вага надається більш новим даним, одержаним за недавні періоди [16]. У ході застосування методу експоненціального прогнозування ряд динаміки, що містить значення прогнозованого показника протягом ретроспективного періоду, вирівнюється за допомогою зваженої ковзної середньої, де вага відповідає експоненціальному закону розподілу [79].

Експоненціальне прогнозування показників $x_{ij}(t, r)$ здійснюється за таким алгоритмом:

1) обирається значення α із інтервалу $[0,2; 0,6]$. Величина α відображає, наскільки більшу вагу матимуть новіші значення показника;

2) визначається поліном $z_t = \varepsilon_0 + \varepsilon_1 t + \varepsilon_2 \frac{t^2}{2!}$, що апроксимує значення прогнозованого показника. Коефіцієнти $\varepsilon_0, \varepsilon_1, \varepsilon_2$ визначаються методом

найменших квадратів [32].

3) для $t = 1$ визначається значення вирівняних рядів за рівностями (3.26):

$$\begin{cases} z_t^1 = \alpha_0 - \frac{1-\alpha}{\alpha} \cdot \varepsilon_1 + \frac{(1-\alpha) \cdot (2-\alpha)}{2 \cdot \alpha^2} \varepsilon_2; \\ z_t^2 = \alpha_0 - \frac{2(1-\alpha)}{\alpha} \cdot \varepsilon_1 + \frac{2(1-\alpha) \cdot (3-2\alpha)}{2 \cdot \alpha^2} \varepsilon_2; \\ z_t^3 = \alpha_0 - \frac{3(1-\alpha)}{\alpha} \cdot \varepsilon_1 + \frac{3(1-\alpha) \cdot (4-3\alpha)}{2 \cdot \alpha^2} \varepsilon_2. \end{cases} \quad (3.26)$$

4) для інших значень t значення вирівняних рядів визначається за рівностями (3.27–3.29):

$$z_t^1 = (1-\alpha)z_{t-1}^1 + \alpha z_t^1; \quad (3.27)$$

$$z_t^2 = (1-\alpha)z_{t-1}^2 + \alpha z_t^1; \quad (3.28)$$

$$z_t^3 = (1-\alpha)z_{t-1}^3 + \alpha z_t^2. \quad (3.29)$$

5. Для визначених z_t^1, z_t^2, z_t^3 визначаються $\varepsilon_0, \varepsilon_1, \varepsilon_2$ із рівностей (3.30):

$$\begin{cases} \varepsilon_0 = 3y_t^1 - 3y_t^2 + y_t^3; \\ \varepsilon_1 = \frac{\alpha}{2(1-\alpha)^2} [(6-5\alpha)y_t^1 - 2(5-4\alpha)y_t^2 + (4-3\alpha)y_t^3]; \\ \varepsilon_2 = \frac{\alpha^2}{(1-\alpha)^2} (y_t^1 - 2y_t^2 + y_t^3) \end{cases} \quad (3.30)$$

Значення $\varepsilon_0, \varepsilon_1, \varepsilon_2$, одержані для $t = T$, використані для визначення прогнозного значення показника, яке обчислюється за рівністю (3.31):

$$z = \varepsilon_0 + \varepsilon_1 t + \varepsilon_2 \frac{t^2}{2!}. \quad (3.31)$$

Оскільки визначається прогноз на 2020 р., а ретроспективний період закінчується 2018 р., то в цій рівності приймаємо $t = 2$, отже, $z = \varepsilon_0 + 2\varepsilon_1 + 2\varepsilon_2$.

Визначені вищезазначеним способом прогнозовані значення показників третього виду для досліджуваних підприємств агропродовольчої сфери Полтавської області наведено в табл. 3.50.

Таблиця 3.50

Прогнозовані значення показників третього виду для досліджуваних підприємств агропродовольчої сфери Полтавської області [побудовано автором]

Показник	Прогноз на 2020 р.
X ₂₆	0,148903
X ₂₉	0,061681
X ₄₁	0,335812
X ₄₆	0,703636
X ₅₁	0,726834

Для зазначених підприємств – це сукупність із п'яти показників другої, четвертої та п'ятої груп.

Прогнозовані значення показників третього виду для досліджуваних підприємств агропродовольчої сфери Сумської області наведено в табл. 3.51.

Таблиця 3.51

Прогнозовані значення показників третього виду для досліджуваних підприємств агропродовольчої сфери Сумської області [побудовано автором]

Показник	Прогноз на 2020 р.
X ₂₅	0,379868
X ₂₉	0,082130
X ₂₁₀	0,249035
X ₄₁	0,346874
X ₄₆	0,704676

Для зазначених підприємств – це п'ять показників другої (коефіцієнт фінансування інформаційної безпеки виробничої підсистеми підприємства; коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства; коефіцієнт фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства) та четвертої (коефіцієнт повноти інформації, коефіцієнт коректності форми подання інформації) груп.

Прогнозовані значення показників третього виду для досліджуваних підприємств агропродовольчої сфери Кіровоградської області наведено в табл. 3.52.

Таблиця 3.52

Прогнозовані значення показників третього виду для досліджуваних підприємств агропродовольчої сфери Кіровоградської області [побудовано автором]

Показник	Прогноз на 2020 р.
X ₁₁	0,759973
X ₁₂	0,709530
X ₂₃	0,036318
X ₂₆	0,080352
X ₂₇	0,074726
X ₂₈	0,121263
X ₃₆	0,102082
X ₄₁	0,437391
X ₄₅	0,813757

Для зазначених підприємств – це 9 показників: 2 з групи показників оцінки програмно-технічної захищеності інформаційної системи, 4 показники з групи оцінки фінансування (витрат) забезпечення інформаційної

безпеки підприємства, 1 показник із групи показників оцінки інформаційної надійності персоналу та 2 показники із групи оцінки інформації, що надається ОПР системою інформаційного забезпечення (системою інформаційного захисту).

Прогнозовані значення показників третього виду для досліджуваних підприємств агропродовольчої сфери Харківської області наведено в табл. 3.53.

Таблиця 3.53

Прогнозовані значення показників третього виду для досліджуваних підприємств агропродовольчої сфери Харківської області [побудовано автором]

Показник	Прогноз на 2020 р.
X ₁₁	0,727837
X ₁₂	0,681720
X ₂₅	0,237246
X ₂₆	0,070175
X ₂₈	0,088252
X ₂₉	0,050422
X ₂₁₀	0,160417
X ₃₆	0,147812
X ₄₂	0,481086
X ₄₅	0,718148
X ₄₆	0,649216

До третього виду показників для досліджуваних підприємств агропродовольчої сфери Харківської області слід зарахувати: коефіцієнт технічного захисту інформаційної системи, коефіцієнт програмної захищеності інформаційної системи (перша група), коефіцієнт фінансування інформаційної безпеки виробничої підсистеми підприємства, коефіцієнт фінансування інформаційної безпеки комерційної, інноваційної та продовольчої підсистем підприємства, коефіцієнт фінансування технічної захищеності інформації, коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства, коефіцієнт фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства (друга група), коефіцієнт правової незахищеності інформації (третя група), коефіцієнт точності інформації, коефіцієнт надійності інформації, коефіцієнт коректності форми подання інформації (четверта група).

Найбільша кількість показників третього виду у досліджуваних підприємств агропродовольчої сфери Луганської області. Їх прогноз на 2020 р. наведено в табл. 3.54.

Серед прогнозованих показників третього виду для досліджуваних підприємств Луганської області слід виділити показники:

Таблиця 3.54

Прогнозовані значення показників третього виду для досліджуваних підприємств агропродовольчої сфери Луганської області [побудовано автором]

Показник	Прогноз на 2020 р.
X ₂₅	0,169470
X ₂₆	0,038536
X ₂₇	0,048285
X ₂₈	0,062835
X ₂₉	0,040003
X ₂₁₀	0,107994
X ₃₂	0,336885
X ₃₄	0,171180
X ₃₅	0,327329
X ₃₇	0,311973
X ₄₂	0,298807
X ₄₃	0,352183
X ₄₅	0,426065
X ₄₆	0,529557
X ₅₁	0,391842
X ₅₂	0,041809
X ₅₃	0,032205

групи показників оцінки фінансування (витрат) забезпечення інформаційної безпеки підприємства: коефіцієнт фінансування інформаційної безпеки виробничої підсистеми підприємства, коефіцієнт фінансування інформаційної безпеки комерційної, інноваційної та продовольчої підсистем підприємства, коефіцієнт фінансування програмної захищеності інформації, коефіцієнт фінансування технічної захищеності інформації, коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства, коефіцієнт фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства;

групи показників оцінки інформаційної надійності персоналу: коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства, коефіцієнт невідповідності персоналу до розпізнавання загроз інформаційній безпеці, коефіцієнт освіченості персоналу системи управління інформаційною безпекою та коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку;

групи показників оцінки інформації, що надається ОПР системою інформаційного забезпечення (системою інформаційного захисту): коефіцієнт точності інформації, коефіцієнт суперечливості інформації, коефіцієнт надійності інформації та коефіцієнт коректності форми подання інформації;

групи показників оцінки системи інформаційної безпеки підприємства: коефіцієнт керованості системи інформаційної безпеки підприємства, коефіцієнт власного програмного забезпечення, коефіцієнт власних технічних засобів.

Визначивши прогнозовані значення показників, що відображають стан інформаційної безпеки досліджуваних підприємств, доцільно зробити прогноз інтегральних оцінок їх інформаційної безпеки та підсистем її забезпечення. Для кожного прогнозованого значення $x_{ij}(t, r)$ показника x_{ij} визначається відповідне значення нормалізованого показника $y_{ij}(t, r)$ і обчислюється прогнозоване значення інтегральної оцінки підсистеми, що визначається множиною показників X_i за рівністю (3.32):

$$W_i(r, t) = \gamma V_i^A(t, r) + (1 - \gamma) V_i^G(t, r), \quad (3.32)$$

де $V_i^A(t, r)$ та $V_i^G(t, r)$ – прогнозовані значення інтегральної оцінки вказаної підсистеми, визначені методами аналізу ієрархій і модифікованої головної компоненти,

γ – коефіцієнт, що відображає ступінь довіри до експертних висновків.

Методика визначення коефіцієнта γ і величин $V_i^A(t, r)$ та $V_i^G(t, r)$ описана в підрозділі 3.2 цього дослідження.

Одержані прогнозовані на 2020 р. значення інтегральних оцінок системи інформаційної безпеки підприємств і її підсистем наведено в табл. 3.55.

Таблиця 3.55

Інтегральні оцінки системи інформаційної безпеки досліджуваних підприємств агропродовольчої сфери та її підсистем на 2018 р. і їх прогноз на 2020 р. [побудовано автором]

Підсистеми системи інформаційної безпеки	Досліджувані підприємства агропродовольчої сфери									
	Полтавської області		Кіровоградської області		Сумської області		Харківської області		Луганської області	
	2018	2020	2018	2020	2018	2020	2018	2020	2018	2020
Підсистема програмно-технічного забезпечення	0,9212	1,0000	0,4147	0,4657	0,7448	0,8363	0,5185	0,5607	0,3821	0,3633
Підсистема фінансового забезпечення	0,9816	0,9889	0,4053	0,4034	0,7668	0,8278	0,4240	0,3702	0,1980	0,1937
Підсистема кадрового забезпечення	0,9741	0,9917	0,7148	0,7411	0,9343	0,9688	0,7191	0,7732	0,4121	0,3741
Підсистема інформаційного забезпечення	0,7786	0,8519	0,5841	0,6711	0,8366	0,8352	0,5488	0,5309	0,1255	0,1100
Підсистема організаційного забезпечення	0,9651	0,9745	0,8607	0,8638	0,8721	0,8801	0,8308	0,8346	0,5935	0,7043
Рівень інформаційної безпеки	0,9327	0,9644	0,6577	0,6865	0,8498	0,8816	0,6609	0,6718	0,3924	0,4129

Для порівняння в цій таблиці наведено відповідні інтегральні оцінки за 2018 р. За прогностичними даними програмно-технічна підсистема підприємств агропродовольчої сфери Полтавської області, інтегральне значення якої у 2018 р. становило 0,9212 і матиме тенденцію до зростання, а 2020 р. становитиме максимум 1,0. На підприємствах Кіровоградської області інтегральне значення цієї підсистеми підвищиться на 0,0510 і становитиме у прогнозованому періоді 0,4657. Щодо досліджуваних підприємств агропродовольчої сфери Сумської області, то інтегральне значення цієї підсистеми теж зросте і становитиме 0,8363, а на підприємствах Харківської області зростання становитиме 0,0422, а саме інтегральне значення – 0,5607. Лише на досліджуваних підприємствах Луганської області прогнозоване інтегральне значення аналізованої підсистеми зменшиться і становитиме 0,3633 у 2020 р.

Прогнозування інтегральних значень фінансової підсистеми системи інформаційної безпеки досліджуваних підприємств дозволило відмітити його зростання у прогнозованому році серед підприємств агропродовольчої сфери Полтавщини на 0,0730 (прогнозне значення у 2020 р. – 0,9889), Сумщини на 0,0610 (прогнозне значення у 2020 р. – 0,8278) та зменшення на підприємствах агропродовольчої сфери Кіровоградщини на 0,0190 (прогнозне значення у 2020 р. – 0,4043), Харківщини на 0,0538 (прогнозне значення у 2020 р. – 0,3702) та Луганщини на 0,0430 (прогнозне значення у 2020 р. – 0,1937), що свідчить про необхідність підвищення рівня фінансування забезпечення інформаційної безпеки.

Тенденції зростання інтегрального показника кадрової підсистеми системи інформаційної безпеки досліджуваних підприємств, зокрема на підприємствах Полтавської області з 0,9741 у 2018 р. до прогностичного 0,9917 у 2020 р., на підприємствах Кіровоградської області з 0,7148 у 2018 р. до прогностичного 0,7411 у 2020 р., на підприємствах Сумської області з 0,9343 у 2018 р. до прогностичного 0,9688 у 2020 р. і на підприємствах Харківської області з 0,7191 у 2018 р. до прогностичного 0,7732 у 2020 р., свідчать про достатність, кваліфікаційність і компетентність кадрів системи інформаційної безпеки. Водночас на підприємствах Луганської області інтегральне значення цієї підсистеми зменшується із 0,4121 у 2018 р. до прогностичного 0,3741 у 2020 р., що потребує залучення нових кваліфікованих кадрів або / та перепідготовки персоналу, задіяного у сфері інформаційного захисту.

Зростання інтегрального значення оцінки інформаційної складової простежується лише на підприємствах Полтавської та Кіровоградської областей з існуючих у 2018 р. – 0,7786 та 0,5841 до прогностичних у 2020 р. – 0,8519 та 0,9711 відповідно. Підприємства Сумської, Харківської та

Луганської областей мають тенденцію до зниження зазначеного інтегрального значення, а їх прогностні значення на 2020 р. становлять 0,8352, 0,5309 та 0,1100 відповідно, що зумовлює необхідність формування стратегічних заходів з посилення інформаційної складової системи інформаційної безпеки.

Інтегральні показники організаційної підсистеми свідчать про тенденцію зростання на всіх підприємствах усіх досліджуваних областей. Найбільші прогностні значення (до 2020 р.) мають підприємства Полтавської області – 0,9745, Кіровоградщини – 0,8638, Сумщини – 0,8801, Харківської області – 0,8346. Дещо менше прогностне значення інтегрального показника організаційної підсистеми мають досліджувані підприємства агропродовольчої сфери Луганської області – 0,7043, проте зростання становить 0,1108.

Прогноз зміни інтегрального показника рівня інформаційної безпеки підприємств агропродовольчої сфери Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей на 2020 р. порівняно з 2018 р. відображено на рис. 3.2.

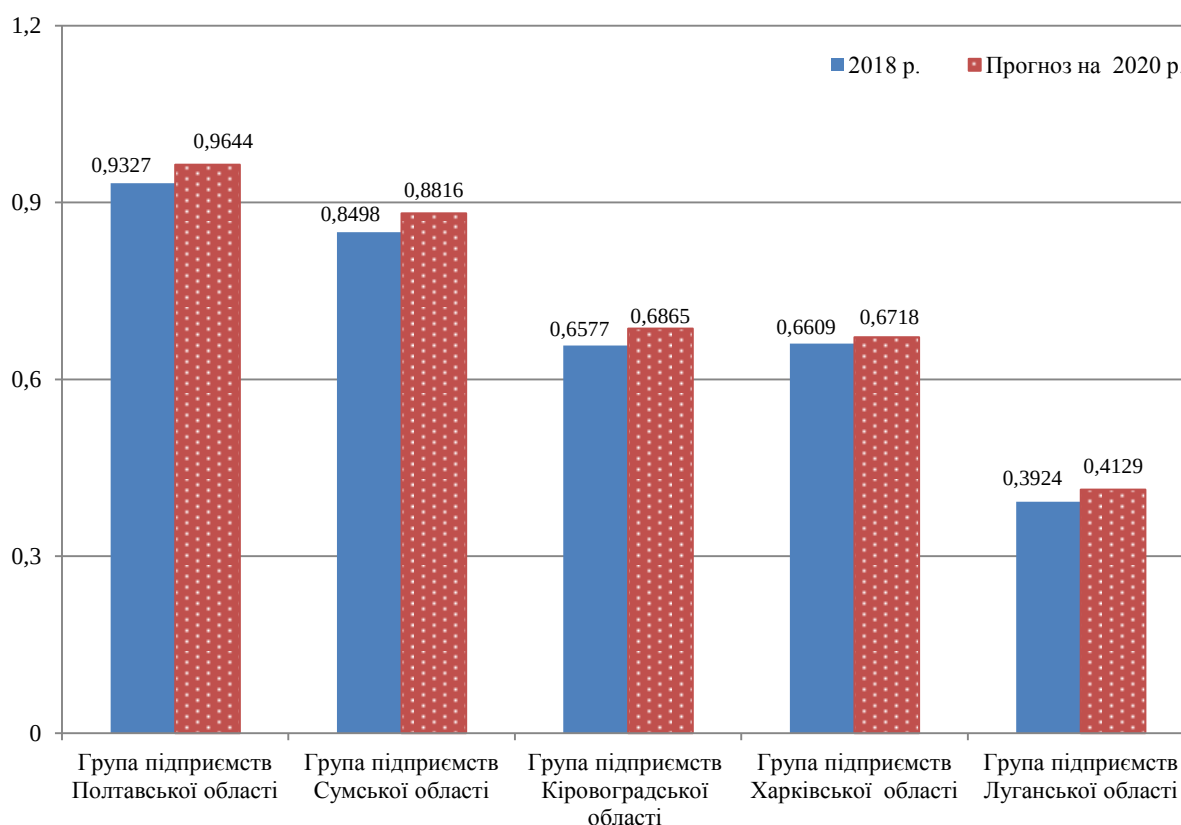


Рис. 3.2. Прогноз зміни інтегрального показника рівня інформаційної безпеки підприємств агропродовольчої сфери Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей на 2020 р. проти 2018 р. [побудовано автором]

Інтегральне значення рівня інформаційної безпеки досліджуваних підприємств агропродовольчої сфери свідчить про позитивну тенденцію та його зростання у прогнозованому періоді. Зокрема для досліджуваних підприємств Полтавщини, його прогнозне зростання становитиме 0,0317, Сумської області – 0,0318, Кіровоградської області – 0,0288, Харківщини – 0,0109, Луганської області – 0,0205.

Під час прогнозування було виявлено зменшення інтегральних показників окремих підсистем підприємств агропродовольчої сфери Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей.

Список використаних джерел до розділу 3

1. Department of Defense. Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, 1985 URL: <http://csrc.nist.gov/publications/history/dod85.pdf>

2. Канадські критерії безпеки комп'ютерних систем (Canadian Trusted Computer Product Evaluation Criteria. URL: https://www.researchgate.net/publication/3506169_The_Canadian_Trusted_Computer_Product_Evaluation_Criteria_CTCPEC.

3. Критерії оцінки безпеки інформаційних технологій (Information Technology Security Evaluation Criteria). URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile.

4. Федеральні критерії безпеки інформаційних технологій (Federal Criteria for Information Technology Security. URL: <https://www.commoncriteriaportal.org/files/ccfiles/ccpart1v2.3.pdf>.

5. Айвазян С. А. К методологии измерения синтетических категорий качества жизни населения. Экономика и математические методы. 2003. Т. 39, № 2. С. 33-53.

6. Андрианов В. В., Зефирова С. Л., Голованов В. Б., Голдуев Н. А. Обеспечение информационной безопасности бизнеса: 2-е издание, переработанное и дополненное. URL: <https://pqm-online.com/assets/files/lib/books/andrianov.pdf>.

7. Берко А. Ю., Висоцька В. А., Рішняк І. В. Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції. URL: <http://vlp.com.ua/files/03.pdf>.

8. Буркальцева Д. Д. Методологія розрахунку інтегральних показників безпеки за сферами економіки. *Збірник наукових праць Дніпропетровського національного університету залізничного транспорту імені академіка В.*

Лазаряна «Проблеми економіки транспорту». 2013. Вип. 6. С. 106–111.

9. Бучик С. С., Шалаєв В. О. Аналіз інструментальних методів визначення ризиків інформаційної безпеки інформаційно-телекомунікаційних систем. *Наукоємні технології*. 2017. № 3 (35). С. 2015–225.

10. Бобровська О. Ю. Еволюція прогнозування розвитку соціально-економічних процесів: стан і напрямки удосконалення. URL: [http://www.dridu.dp.ua/zbirnik/2011-02\(6\)/11boysnu.pdf](http://www.dridu.dp.ua/zbirnik/2011-02(6)/11boysnu.pdf).

11. Вальчук О. А., Матохнюк Л. О. Особливості застосування статистичного критерію фішера в психолого-педагогічних дослідженнях. URL: https://www.google.com.ua/%3DPDF%2FSitmn_2014_38_45.pdf&usg=AOvVaw1y4z37y-Qeoab_oxYtjrRV.

12. Вареник В. М. Аналіз методик розрахунку економічної безпеки України. *Академічний огляд*. 2016. № 1 (44). С. 70–79.

13. Велігура А. В. Оцінювання стану інформаційної безпеки підприємства. *Управління проектами та розвиток виробництва*. 2014. № 4 (52). С. 28–39.

14. Вертелева О. В. Математичне моделювання економічних процесів в умовах парадигмальних зрушень. *Інвестиції: практика та досвід*. 2019. № 12. С. 48–56.

15. Галахов Є. М., Собчук В. В. Розвиток моделей кібератак у площині інформаційної безпеки підприємства. *Телекомунікаційні та інформаційні технології*. 2019. № 4. С. 12–24.

16. Гаркуша Н. М., Цуканова О. В., Горошанська О. О. Моделі і методи прийняття рішень в аналізі та аудиті : навч. посіб. 2-ге вид. 2012. 591 с.

17. Грищук Р., Молодецька К. Метод прогнозування динаміки поширення контенту й запитів на нього за даними контент-аналізу повідомлень у соціальних інтернет-сервісах. *Системи управління, навігації та зв'язку*. 2015. № 4 (36), С. 85–92.

18. Дудат'єв А. В. Комплексна інформаційна безпека соціотехнічних систем: моделі впливу та захисту : моногр. Вінниця : ВНТУ, 2017. 128 с.

19. Дячков Д. В. Розробка методологічних засад оцінювання та діагностики інформаційної безпеки підприємств агропродовольчої сфери. *Український журнал прикладної економіки*. 2019. Том 4, № 3. С. 188–197.

20. Дячков Д. В. Способи оцінки інформаційної безпеки. *Менеджмент XXI століття: глобалізаційні виклики* : матер. III Міжнар. наук.-практ. конф. Полтава : ТОВ «Сімон», 2019. С. 338–340.

21. Дячков Д. В., Вибиванець А. Б. Особливості управління інноваціями промислових підприємств в умовах споживчих змін. *Економічний форум*. Луцьк : РВВ Луцького НТУ, 2019. № 1. С. 76–82.

22. Дячков Д. В., Германчук О. О. Система ризик менеджменту

підприємств, що здійснюють туристичну діяльність. *Управління туристичною індустрією: методологія і практика* : матер. II Міжнар. наук.-практ. конф., 08–09 жовтня 2015 р. Полтава : В-во «Сімон», 2015. С. 181–183.

23. Дячков Д. В., Германчук О. О. Формування системи ризик-менеджменту підприємства. *Економічний форум*. Луцьк : РВВ Луцького НТУ, 2015. № 4. С. 235–241.

24. Дячков Д. В., Кисіль І. Г. Сутність та значення ризику підприємства. *Управління ресурсним забезпеченням господарської діяльності підприємств реального сектору економіки* : матер. III Всеукр. наук.-практ. інтернет-конф., 31 жовтня 2018 р. Полтава : РВВ ПДАА, 2018. С. 56–57.

25. Дячков Д. В., Паскаль А. В. Система оцінки інформаційного забезпечення підприємства. *Управління ресурсним забезпеченням господарської діяльності підприємств реального сектору економіки* : матер. III Всеукр. наук.-практ. інтернет-конф., 31 жовтня 2018 р. Полтава : РВВ ПДАА, 2018. С. 193–195.

26. Дячков Д. В., Тур Є. І. Особливості формування механізму діагностики фінансового стану підприємства. *Східна Європа : економіка, бізнес та управління*. 2019. № 5. С. 59–66.

27. Єрмошин В. В., Хорошка В. О., Капустян М. В. Методика оцінки інформаційних ризиків системи управління інформаційною безпекою. *Науково-технічний журнал «Сучасний захист інформації»*. 2010. № 3. С. 95–104.

28. Жуков С. А., Солоха Д. В., Белякова О. В. Економічна інерційність промисловості України та формування інноваційного потенціалу галузі та регіону. *Актуальні проблеми економіки. Економічна теорія та історія економічної думки*. 2016. № 7 (181). С. 16–22.

29. Журавель М. Ю., Полозова Т. В., Стороженко О. В. Формування системи показників оцінки рівня інформаційної безпеки підприємства. *Вісник економіки транспорту і промисловості*. 2011. № 33. С. 171–177.

30. Зефіров С. Л., Алексеев В. М. Способы оценки информационной безопасности организации. *Труды Международного симпозиума «Надежность и качество»*. 2011. № 2. С. 407–409.

31. Зось-Кіор М. В., Дячков Д. В., Павлик Р. В. Система економічної безпеки підприємства: поняття, принципи, сутність. *Держава та регіони. Серія : Економіка та підприємництво*. 2019. № 5. С. 103–109.

32. Іванець Г. В., Євдокименко Ю. І., Марченко О. Г., Наконечний О. А. Алгоритм підвищення точності прогнозу економічних показників на основі багатофакторної лінійної моделі за рахунок передбачення похибок моделі і уточнення оцінок її параметрів на основі зваженого методу найменших квадратів. *Збірник наукових праць Харківського університету Повітряних Сил*.

2013. Вип. 2 (35). С. 94–97.

33. Ілляшенко С. М. Економічний ризик : навч. посіб. 2-ге вид., доп., перероб. К. : Центр навчальної літератури, 2004. 220 с.

34. Капленко Г. В. Деякі актуальні питання методології факторного прогнозування споживчого попиту. *Ефективна економіка*. 2015. № 12. URL: <http://www.economy.nayka.com.ua/?op=1&z=4670>

35. Козаченко А. В. Естиметологічний аспект в економічній безпекології. *Проблеми економіки*. 2016. № 1. С. 167–173.

36. Козаченко А. В., Буколова В. В. Концептуальні засади розроблення моделі оцінювання соціально-економічної безпеки регіону. в кн. : Економічна безпека : держава, регіон, підприємство : монографія; в 3-х т. Т. 3 / за заг. ред. В. О. Онищенко та Г. В. Козаченко. Полтава : ПолтНТУ, 2019. С. 178–212.

37. Козаченко А. В., Вахлакова В. В. Дезорганізація безпекозабезпечувальної діяльності підприємства: ознаки та причини. *Економіка : реалії часу*. 2017. № 3 (31). С. 27–34.

38. Козаченко А. В., Вахлакова В. В. Об'єкти та підходи в оцінюванні економічної безпеки підприємства як основні елементи оцінної системи. в кн. : Економічна безпека: держава, регіон, підприємство: монографія; в 3-х т. Т. 1 / за заг. ред. В. О. Онищенко та Г. В. Козаченко. Полтава : ПолтНТУ, 2016. С. 185–208.

39. Кононова В. О., Харкянен О. В., Грибков С. В. Оцінка засобів захисту інформаційних ресурсів. Вісник Національного університету «Львівська політехніка». *Комп'ютерні системи та мережі*. 2014. № 806. С. 99-105. URL: http://nbuv.gov.ua/UJRN/VNULPKSM_2014_806_18.

40. Кравчук О. Я., Кравчук П. Я. Діагностика рівня та критерії оцінки корпоративної безпеки суб'єктів господарювання. *Збірник наукових праць. Економічні науки. Серія «Економіка та менеджмент»*. Луцький державний технічний університет. Луцьк, 2004. Вип. 1. С. 85–109.

41. Куканова Н. Современные методы и средства анализа и управление рисками информационных систем компаний. URL: <http://citforum.ru/products/dsec/cramm/>.

42. Лютоев И. Microsoft Security Assessment Tool 4.0. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Microsoft-Security-Assessment-Tool-4.0.

43. Магас Т. Є. Класи економіко-математичних моделей та їх застосування. *Збірник наукових праць ВНАУ. Серія: Економічні науки*. 2011. № 1. С. 180–188.

44. Максименко В. Н., Ясюк Е. В. Основные подходы к анализу и оценке рисков информационной безопасности. *Экономика и качество систем святи*.

2017. № 2 / 2017. С. 42–48.

45. Маркіна І. А., Дячков Д. В. Економічна оцінка використання інформаційного потенціалу виробничого підприємства. *Потенціал економічного розвитку країни : теорія і практика* : колективна монографія у 2 т. / колектив авторів. Донецьк : Донбас ДонНУЕТ, 2014. Т.1. С. 18–32.

46. Математичні методи і моделі в управлінні економічними процесами : монографія / Л. М. Малярець, Є. Ю. Місюра, В. В. Койбічук та ін. Харків : ХНЕУ ім. С. Кузнеця, 2016. 420 с.

47. Морозова В. И., Врублевский К. Э. Защита информации в вычислительных системах : учеб. пособ. М. : МИИТ, 2008. 122 с.

48. Оксенюк В. Використання програмних засобів для оцінки та управління ризиками інформаційної безпеки. URL: http://elartu.tntu.edu.ua/bitstream/lib/30437/2/IMST_2019_Okseniuk_V-Use_of_software_for_information_75.pdf.

49. Перегудов Д. О., Селюков О. В., Крихта В. В., Краснік А. А. Аналіз особливостей застосування та класифікація методів прогнозування у сфері розвитку мереж та телекомунікаційних технологій. *Вісник ДУІКТ*. 2009. № 1 (7). С. 27–40.

50. Петренко С., Симонов С. Методики и технологии управления информационными рисками. *IT-Manager*. 2003. № 3. URL: <http://citforum.sk.ua/security/articles/risk/>.

51. Пілько А. Д., Савчук Н. В. Моделювання процесу оцінювання рівня економічної безпеки регіону. URL: http://www.businessinform.net/pdf/2015/8_0/77_84.pdf.

52. Пугин В. В., Губарева О. Ю. Обзор методик анализа рисков информационной безопасности информационной системы предприятия. *T-Comm*. 2012. № 6. С. 54–57.

53. Пузиренко О. Г., Івко С. О., Лаврут О. О., Климович О. К. Застосування моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах. *Системи обробки інформації*. 2015. Вип. 3 (128). С. 75–79.

54. Пузиренко О. Г., Івко С. О., Лаврут О. О. Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційно-телекомунікаційних систем. *Системи обробки інформації: Інфокомунікаційні системи*. 2014. Вип. 8 (124). С. 128–134.

55. Путренко В. В. Застосування трендових геопросторових статистичних моделей на основі інтелектуального аналізу даних. *Системні дослідження та інформаційні технології*. 2015. № 4. С. 7–9.

56. Реверчук Н. Й. Управління економічною безпекою підприємницьких

структур : монографія. Львів : ЛБІ НБУ, 2004. 195 с.

57. Родін Є. С. Процесні підходи до моделювання у сфері управління ризиками інформаційної безпеки. *Математичні машини і системи*. 2012. № 4. С. 142–148.

58. Саати Т., Кернс К. Аналитическое планирование. Организация систем : пер. с англ. М. : Радио и связь, 1991. 224 с.

59. Семкина А. А., Цыбулин А. М. Оценка уровня информационной безопасности предприятия через остаточный риск. *Вестник ВолГУ*. 2012. Вып. 6. Серия 10. С. 156–159.

60. Сенишин О. С. Екстраполяційні методи прогнозування як інструмент передбачення оптимальних обсягів споживання продукції вітчизняного продовольчого комплексу. URL: <https://core.ac.uk/download/pdf/32607853.pdf>.

61. Сухоруков А. І., Харазішвілі Ю. М. Теоретико-методологічний підхід до інтегральної оцінки рівня економічної безпеки держави. *Банківська справа*. 2011. № 4. С. 13–32.

62. Тимошенко О. В. Методичні підходи до оцінювання рівня економічної безпеки держави. URL: http://nbuv.gov.ua/j-pdf/binf_2014_6_6.pdf.

63. Трояновский В. М. Математическое моделирование в менеджменте : учеб. пособие. 2-е изд., испр. и доп. М., 2002. 250 с.

64. Хоффман Л. Дж. Современные методы защиты информации. М. : Советское радио, 1980. 264 с.

65. Цуканова О. А., Смирнов С. Б. Экономика защиты информации: учеб. пособие, 2-е издание, измененное и дополненное. СПб. : НИУ ИТМО, 2014. 79 с.

66. Чаплінський Ю. П. Одна реалізація знаннє-орієнтованої інформаційної системи з безпеки продуктів харчування. *Наукові праці національного університету харчових технологій*. 2018. Т. 24, № 4. С. 8–18.

67. Швалев И. С., Чусавитина Г. Н., Давлеткиреева Л. З. Сравнительная характеристика автоматизированных инструментальных средств управления информационными рисками. *Современные научные исследования и инновации*. 2012. № 11. URL: <http://web.snauka.ru/issues/2012/11/18524>.

68. Шушура О. М., Довбешко С. В., Золотухіна О. А., Асєєва Л. А. Фактори створення стратегії безпеки інформаційних технологій сучасного підприємства. *Телекомунікаційні та інформаційні технології*. 2019. № 2. С. 5–13.

69. Янчук В. О. Методика оцінювання стану захисту інформації локальних об'єктів системи електронного врядування. URL: <http://academy.gov.ua/ej/ej11/txts/10ivoseu.pdf>.

70. Яренко А. В. Систематизація кількісних методів прогнозування

кон'юнктури ринку в маркетингових дослідженнях. *Вісник КНУТД. Серія «Економічні науки»*. 2015. № 3 (87). С. 11–18.

71. Gallagher P., Locke G. NIST: National Institute of Standards and Technology. Managing information security risk organization, mission, and information system view. *Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg*. 2011. 88 p.

72. Aranchiy V. I., Markina I. A. Features of the enterprise's financial security system functioning. *Збірник наукових праць та тез наукових доповідей за матеріалами IV Міжнародної науково-практичної конференції : Наукові розробки, передові технології, інновації*. Прага-Барно-Київ, К.: НДІСР. 2017. С. 27–34.

73. Aranchiy V., Yasnolob I., Makhmudov H., Radionova Y. The developing of conceptual foundation of the process of organizing innovation activities at agro-industrial enterprise based on outsourcing and the program business process model and notation. *Economic Annals-XXI*. 2017. № 165(5-6). P. 84–89.

74. Markina I. A., Zos-Kior N. V., Diachkov D. V. Globalization and economic and social changes of makro-level indicators. *Проблеми й перспективи розвитку академічної та університетської науки* : зб. наук. пр. за матер. VII Всеукр. наук.-практ. конф., 09-12 грудня 2014 р. Полтава : ПолтНТУ, 2014. С. 114–117.

75. Markina I., Diachkov D. Information security audit specificity. *Modern Science – Moderi veda*. 2019. № 1. P. 31–38.

76. Markina I., Diachkov D., Somych M. Key problems of ensuring food security in the context of globalization. *Informational technologies, Management and Society* : The 16th International Conference Information Technologies and Management, 26-27 April 2018. ISMA University, Riga, 2018. P. 160–161.

77. Markina I., Safonov Yu., Zhylynska O., Diachkov D., Varaksina E. Defining the dimensions of national security, financial security and food supply chain in Ukraine. *International Journal of Supply Chain Management*. URL : <http://ojs.excelingtech.co.uk/index.php/IJSCM/article/view/2559>.

78. Stoneburner G., Goquen A., Feringa A. Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology. Gaithersburg. USA, 2002. 55 p.

79. Метод ковзного середнього. Wiki ТНТУ. URL: https://wiki.tntu.edu.ua/Метод_ковзного_середнього

РОЗДІЛ 4

ОПТИМІЗАЦІЯ ОРГАНІЗАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ АГРОПРОДОВОЛЬЧОЇ СФЕРИ УКРАЇНИ

4.1. Організаційні засади створення віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу

Формування конкурентоспроможного аграрного виробництва потребує відтворення інформаційного потенціалу аграрних підприємств та домогосподарств на якісно новій основі. Тому процеси інноваційної діяльності в аграрному виробництві повинні мати комплексний характер по всьому циклу цієї діяльності: від освіти й науки до впровадження інноваційного продукту в реальне виробництво, а не зводитися до впровадження окремих інноваційних заходів. Саме впровадження новітніх технологій в системи інформаційного захисту забезпечує удосконалення та оновлення і продуктивне відтворення економічного, виробничо-ресурсного та інформаційного потенціалів. Крім того, важливу роль у впровадженні нововведень відіграє управлінська діяльність, яка повинна згладжувати можливі протиріччя між технологічним рівнем виробництва та організацією управління на підприємстві, що підвищить ефективність інноваційних процесів.

Система інформаційної безпеки підприємства в таких умовах не може обмежуватись тільки організацією кібербезпеки, а повинна досліджуватись комплексно, з урахуванням впливу процесу «цифровізації» на всі напрями розвитку аграрного бізнесу, враховуючи безпеку ІТ-трансформації системи безпеки загалом.

Цифрова трансформація сприяє сталому розвитку одночасного підвищення ефективності управлінських і виробничих процесів, оскільки з'являється можливість оперативного обміну цінною актуальною інформацією. Створення віртуальних об'єднань і цифрових платформ полегшує обмін інформацією та сприяє ефектній взаємодії між представниками учасників агропродовольчого ринку різних рівнів і державних установ. Разом з тим інформатизація та цифровізація діяльності аграрних підприємств передбачає появу нових вразливостей для функціонування їх

підсистем, що в подальшому потребує забезпечення інформаційної безпеки підприємств агропродовольчої сфери. Проте не кожне підприємство має потрібну чисельність людських ресурсів з відповідним набором компетентностей і певним досвідом для вирішення питань забезпечення інформаційної безпеки, уникнення інформаційних ризиків і побудови системи управління інформаційною безпекою, що зумовлює доцільність застосування новітнього методу пошуку альтернатив управлінських рішень – краудсорсингу. Власне тому особливої актуальності набуває розробка, впровадження та ефективне використання віртуальних і цифрових платформ для розв'язання нагальних проблем управління підприємствами, зокрема із застосуванням новітніх форм управління таких як інтелектуальний краудсорсинг.

Питанням створення та впровадження цифрових і віртуальних платформ у діяльність підприємств агропродовольчої сфери присвячені праці таких зарубіжних і вітчизняних авторів, як І. Білан [68], С. Євсєєв [60], О. Король [60], С. Огнівцев [59], С. Остапов [60], П. Смертенко [68], Л. Чернишев [68], А. Шабанов [77], Ю. Ярмоленко [79] та інших. Ефективність застосування краудсорсингу та визначення його особливостей розкриті у працях Н. Коршикової [35], О. Марченко [53], А. Хусаїнової [75] та інших науковців.

В умовах розвитку цифрових технологій широкого застосування набувають віртуальні системи та платформи, що являють собою сучасну форму організації співпраці, яка дозволяє інтегрувати знання, вміння, навички та досвід управління суб'єктів різних рівнів для виконання завдань певної предметної області. Застосування інтелектуальних віртуальних платформ в економіці та у сфері управління [59] співвідноситься із загальносвітовою тенденцією становлення економіки знань [41]. Важливим завданням інноваційного управління інформаційною безпекою є консолідація на базі віртуальної платформи інтелектуальних ресурсів організаційних систем державних органів, аграрних підприємств, їх об'єднань, підприємств ІТ-сфери, наукових організацій для виконання управлінських і господарських завдань забезпечення інформаційного захисту на рівні підприємства, регіону, агропродовольчої сфери та держави загалом [77].

Проте, на відміну від існуючих і реалізовуваних технологічних платформ [43; 68; 75; 77] та широкопропонованих цифрових платформ [59; 60; 77], в агропродовольчому секторі з метою вирішення нагальних питань управління інформаційною безпекою та захисту інформаційно-комунікаційної системи суб'єктів аграрної сфери пропонується формувати віртуальну платформу на засадах інтелектуального краудсорсингу.

Після узагальнення доробків авторів [5; 35; 53; 60; 75] було визначено

один із найбільш розповсюджених і ефективних підвидів краудсорсингу, яким є інтелектуальний, що у класичному вигляді являє собою технологію інтелектуальної співпраці поєднаних віртуальною системою або інформаційною мережею носіїв знань, діяльність яких спрямована на створення інтелектуального продукту для виконання важливих бізнес-завдань. Водночас це технологія мережної інтеграції неявних знань великої кількості людей («натовпу»), інтелектуальна взаємодія яких не має територіальних, соціальних, професійних та інших обмежень. Краудсорсинг наслідує базовий егалітарний принцип, що «кожна людина володіє особливим значенням і талантом, які можуть виявитися потрібними іншим людям... У більш широкому сенсі краудсорсинг передбачає формування зв'язків між людьми» [35].

Унаслідок еволюції краудсорсингу потенціал конкретного підприємства агропродовольчої сфери перестає бути обмеженим виключно його внутрішніми ресурсами та залучає до процесу виконання управлінських і виробничих завдань зовнішнє середовище. Доцільно відмітити, що для аграрного підприємства сутність краудсорсингу полягає у використанні інтелектуального потенціалу спільноти людей для виявлення нових напрямків щодо поліпшення окремих бізнес-процесів або їх групи [75]. Користувачі технології краудсорсингу можуть скористатися концентрованим інтелектуальним потенціалом спільноти людей, об'єднаних спільною метою, що в умовах відсутності необхідних знань або досвіду в одних працівників заміщається вміннями або навиками працівників іншого підприємства.

Отже, технологія краудсорсингу дозволяє забезпечити формування глобального віртуального простору для інтеграції знань суб'єктів-учасників віртуальної платформи, оскільки створюватиме умови не тільки для національного, а й міжнародного рівня інтелектуальної співпраці. Інформаційні та віртуальні мережі не мають територіальних кордонів, тому можна залучати наявні знання і досвід як фахівців із предметної області «управління інформаційною безпекою аграрних підприємств», так і людей, професійна діяльність яких не пов'язана з цією проблематикою, проте їх інтелектуальний капітал сприятиме розв'язанню проблемної ситуації [53].

Отже, віртуальна платформа «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу являтиме собою інформаційну систему, що забезпечуватиме багатосторонні взаємодії користувачів з обміну інформацією і цінностями, які сприятимуть зниженню загальних транзакційних витрат, оптимізації процесів захисту інформації, підвищенню ефективності системи управління інформаційною безпекою підприємств агропродовольчої сфери. Особливості

пропонованої віртуальної платформи полягають у взаємодії складових її технології здійснення (рис. 4.1).

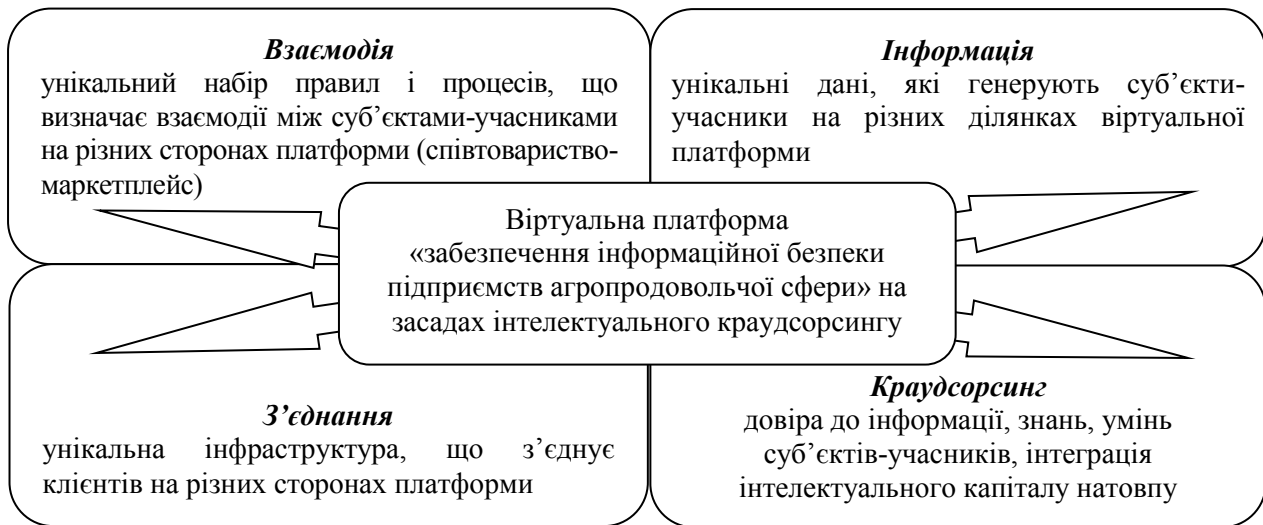


Рис. 4.1. Особливості пропонованої віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу [сформовано на основі 17; 57; 63; 95]

Процес створення пропонованої віртуальної платформи повинен передбачати проходження певної послідовності етапів (рис. 4.2).

Характеризуючи перший етап створення пропонованої платформи та визначаючи її основну мету, доцільно відзначити, що вона полягатиме в оперативному обміні інформацією з проблем управління інформаційною безпекою підприємств агропродовольчої сфери, обміні об'єктами інтелектуальної власності, ноу-хау, технологіями захисту тощо.

Учасниками віртуальної платформи є державні органи із забезпечення інформаційної безпеки на рівні країни та певна спільнота, створена у форматі «професійного клубу», до якого належать працівники агропідприємств, їх об'єднання, у тому числі і громадські, фермери, власники земельних ресурсів, споживачі аграрної продукції, інвестори, експерти компаній, які здійснюють розробку інформаційних технологій, інформаційних систем, програмних продуктів і апаратних засобів, фахівці у сфері інформаційної безпеки, наукова спільнота навчальних закладів та інші учасники. Ця платформа об'єднуватиме найактивніше ядро фахівців, відкритих для комунікацій, що дозволить їм обмінюватись досвідом, ефективним розв'язанням проблем, акумулювати практичні знання, створити надійну та оперативну комунікацію між виробництвом, споживанням, інвестиціями, інноваціями цифрової сфери.

Досягнення мети функціонування пропонованої платформи можливе в разі скоординованих дій її учасників.

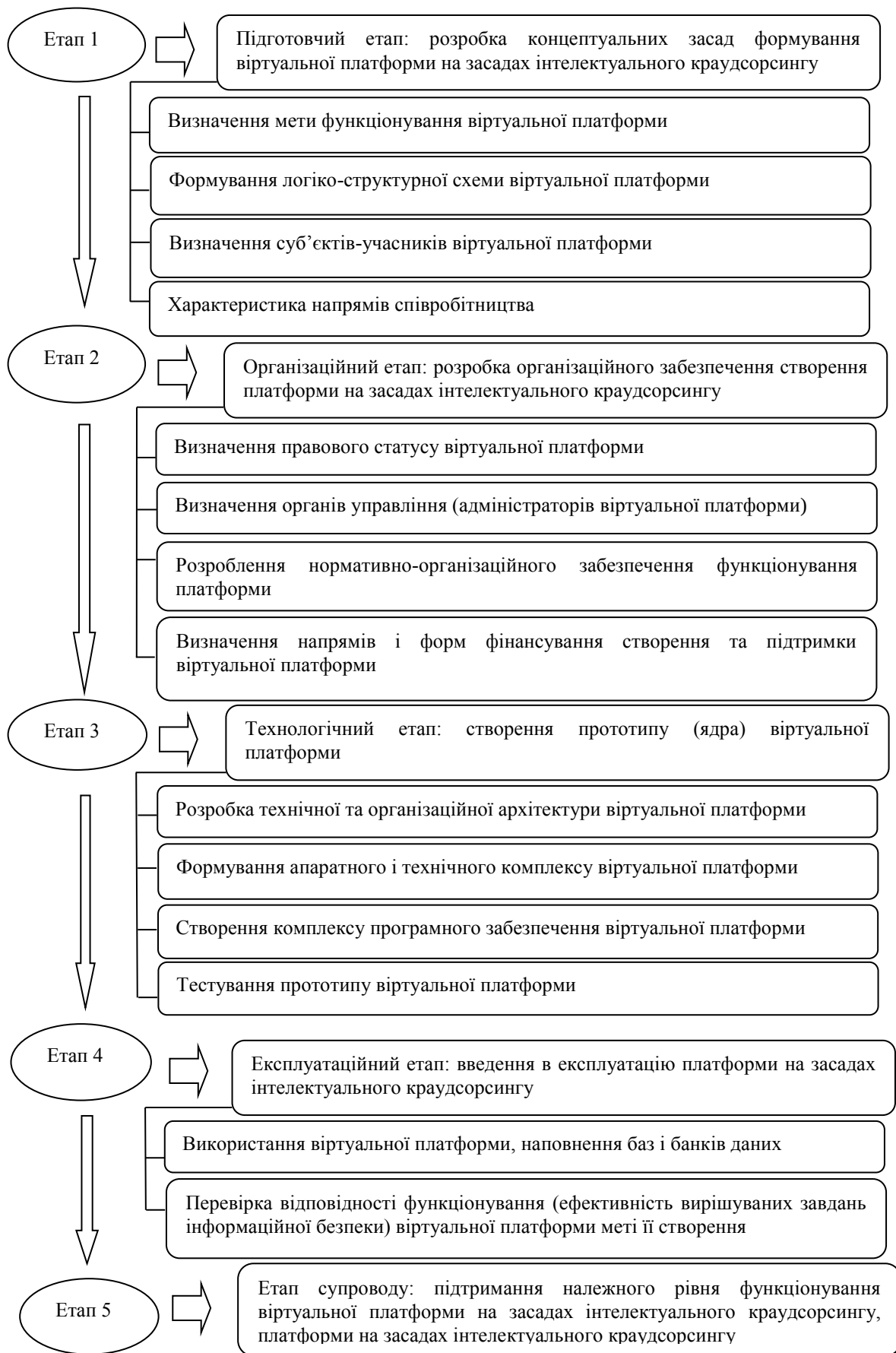


Рис. 4.2. Етапи формування віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу [авторська розробка]

Тому важливого значення набуває розподіл окремих функцій між працівниками управління (адміністрування) віртуальної платформи та основними групами учасників. Дії та функції, їх розподіл між суб'єктами-учасниками віртуальної платформи можуть залишатися незмінними протягом тривалого часу, а можуть змінюватись з різних причин, таких як зміна цілей функціонування платформи, адаптація функціонування платформи під нові умови зовнішнього середовища, оптимізація функціонування платформи під вимоги учасників-користувачів тощо.

Враховуючи те, що суб'єктами-учасниками пропонованої платформи є державні та регіональні органи управління, різноманітні об'єднання, підприємства агропродовольчого ринку, спеціалісти ІТ-сфери та інформаційної безпеки, інші зацікавлені сторони, а також органи управління (адміністрування) цією платформою, доцільно розмежувати дії зазначених суб'єктів і функції, які вони виконуватимуть. Водночас слід зазначити, що спеціалізація діяльності платформи передбачає виконання одних і тих же дій та функцій декількома суб'єктами одночасно. З цією метою пропонується не здійснювати розподіл повноважень, а використовувати систему ролей на основі матричної моделі.

Виокремлення ролі як альтернативи повноважень і обов'язків суб'єктів-учасників платформи виникає у зв'язку з потребою менеджменту в зниженні складності різних завдань організаційного проектування та в спрямованості на виконання однотипних завдань. Тому ефективно організований і реалізований рольовий опис повноважень у межах пропонованої віртуальної платформи дозволить таке:

- збільшити гнучкість, оскільки в разі змін потрібні менші зусилля для реорганізації системи обов'язків і повноважень суб'єктів-учасників;

- запровадити систему ролей, яка із меншою імовірністю (ніж система посадових інструкцій) буде містити суперечності й неточності, оскільки вона формується для окремих видів діяльності, де такі недоліки простіше відстежити і виключити;

- надати більші можливостей для точного опису горизонтальної взаємодії між суб'єктами-учасниками віртуальної платформи.

Формування системи ролей повинне відбуватись за найпростішим алгоритмом: ідентифікація системи ролей віртуальної платформи → оцінка системи ролей → оптимізація системи ролей. Вище зазначалось, що ідентифікацію системи ролей віртуальної платформи пропонується здійснити на основі матричної моделі. Для формування такої матричної моделі необхідна наявність хоча б простої моделі діяльності віртуальної платформи, в якій виділені власне види діяльності та визначені функції – структурні

елементи видів діяльності.

Наступний крок ідентифікації системи ролей полягає у відображенні в матричній моделі участі суб'єктів у виконанні окремих функцій. Якщо суб'єкт-учасник організації бере участь у виконанні певної функції, то у відповідній клітинці матриці робиться відмітка. Склад допустимих позначок потрібно встановлювати таким чином: Вик – виконує; Від – відповідальний; З – забезпечує; І – інформує про результати; К – контролює; Р – регулює; Уз – узгоджує рішення і (або) консультує. З-поміж груп ролей пропонується визначити такі: адміністративні ролі – здійснюють процесів управління віртуальною платформою; ролі користувачів-учасників – передбачають активну взаємодію між собою з метою поширення контенту на платформі; організаційно-управлінські ролі – інтеграція суб'єктів-учасників задля формування експертного професійного співтовариства за напрямками діяльності. Відповідно до визначених груп суб'єктів, ролей (функцій) суб'єктів-учасників запропонованої платформи та їх повноважень доцільно запропонувати такий розподіл ідентифікації ролей (функцій) суб'єктів-учасників віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на основі розглянутої матричної моделі (табл. 4.1).

Таблиця 4.1

Матрична модель ідентифікації ролей (функцій) суб'єктів-учасників віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» [авторська розробка]

	Суб'єкти віртуальної платформи													
Ролі (функції) суб'єктів віртуальної платформи	Органи управління віртуальною платформою (адміністратори)	Міністерство аграрної політики України	Міністерство цифрової трансформації України	Держава служба спеціального зв'язку та захисту інформації в Україні (територіальні відділення, інші підрозділи)	Національний координаційний центр кібербезпеки	Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України	Департамент кіберполіції національної поліції	Підприємства агропродовольчої сфери (об'єднання підприємств)	Громадські організації	Власники земельних ресурсів	Споживачі аграрної продукції	Інвестори в аграрну сферу	Спеціалісти сфери інформаційного захисту	Розробники програмного забезпечення та апаратних засобів
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Ролі адміністрування														
Керування доступом користувачів до інформаційних ресурсів	Від Вик К З												Уз	Уз
Захист даних, що передаються каналами зв'язку	Від Вик К З			З	З	З	З						Уз	Уз

Продовж. табл. 4.1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Реєстрація, збереження і наданих даних	Від Вик К З			З	З	З	З						Уз	Уз
Контроль за роботою користувачів	Від Вик К З												Уз	Уз
Контроль і підтримка цілісності критичних ресурсів системи захисту і середовища виконання прикладних програм	Від Вик К З			З	З	З	З						Уз	Уз
Забезпечення функціонування програмно-технічних комплексів	Від Вик К З												Уз	Уз
Керування та моніторинг засобів захисту інформації	Від Вик К З												Уз	Уз
Спільне виконання завдань із забезпечення інформаційної безпеки	Вик І К	Вик І	Вик І	Вик І	Вик І	Вик І	Вик І	Вик К	Вик К	Вик К	Вик К	Вик К	Вик	Вик
Ролі користування-участі														
Обговорення забезпечення інформаційної безпеки на дискусійних форумах; публікація, обговорення думок і досвіду	Вик І К	Вик Р	Вик Р	Вик Р	Вик Р	Вик Р	Вик	Вик	Вик	Вик	Вик	Вик	Вик	Вик
Створення програмних продуктів для забезпечення інформаційної безпеки	К І Р	Уз	Уз	Уз				Уз К	Уз	Уз	Уз	Уз	Вик	Вик
Створення нормативно-правового забезпечення систем управління інформаційною безпекою	Вик З К І Р	Уз	Уз	Уз	Уз			Вик К	Вик К	Вик К	Вик К	Вик К	Уз	Уз
Ролі організаційно-управлінські														
Формування експертного професійного співтовариства за напрямками діяльності	З К І Р							Від Вик І К						
Організація роботи над рішеннями в командах	Вик І Р							Вик З						

Продовж. табл. 4.1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Забезпечення ефективних комунікацій між учасниками при пошуку рішення	Від Вик І Р													
Здійснення відбору ідей силами учасників спільноти;	І	Уз						Вик	Вик	Вик	Вик	Вик	Уз	Уз
Використання механізмів фільтрації ідей за рейтингом (шляхом голосування учасників платформи)	Від Вик І З												Вик З	Вик З
Досягнення максимальної кількості активних учасників	Вик І К Р							Вик						

Умовні позначення: Вик – виконує; Від – відповідальний; З – забезпечує; І – інформує про результати; К – контролює; Р – регулює; Уз – узгоджує рішення і (або) консультує

Характерними особливостями матричної моделі ідентифікації ролей суб'єктів-учасників віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» будуть такі:

забезпечення взаємодій між суб'єктами віртуальної платформи онлайн є найважливішою передумовою, що перетворює технологію забезпечення інформаційної безпеки в краудсорсингову;

подолання бар'єрів часу та простору між суб'єктами за допомогою онлайн-середовища;

забезпечення користувачів можливостями здійснення операцій з контентом (створення, споживання та розповсюдження);

надання користувачам можливостей об'єднуватися в групи з метою виконання завдань щодо забезпечення інформаційної безпеки підприємств агропродовольчої сфери.

У разі чіткого розмежування та виконання зазначених ролей кожен учасник у межах платформи зможе діяти одночасно як споживач і як сервер, що забезпечить наскрізну цифровізацію всіх фізичних активів суб'єктів агропродовольчого ринку, надання та використання цифрових послуг, електронну обробку всіх видів інформації, підтримку інформаційної взаємодії, використання бізнес-аналітики на основі залучення штучного інтелекту, підтримку різних потреб, управління технологічними процесами, посилення міжгалузевої взаємодії та залучення в предметно-орієнтовані кластери.

Проте головним напрямом співпраці в межах пропонованої віртуальної

платформи повинен стати обмін інформацією щодо:

- тенденцій виникнення вразливостей інформаційно-комунікаційної системи підприємства;

- основних порушників і зловмисників у сфері інформаційної безпеки;

- нових видів здійснення злочинів і шахрайства в інформаційно-комунікаційній сфері;

- кількості та видів атак на інформаційно-комунікаційну систему підприємства;

- навчання, підвищення кваліфікації персоналу з питань інформаційної грамотності, освіченості;

- новітніх технічних, технологічних і програмних рішень захисту інформаційних активів, інформаційних ресурсів та інформаційних систем аграрного підприємства;

- проведення аудиту інформаційної безпеки та системи управління інформаційною безпекою;

- формування ефективної системи управління інформаційною безпекою;

- витрат на формування ефективної системи управління інформаційною безпекою;

- розробки та реалізації інформаційної політики підприємства, інформаційної стратегії підприємств та її взаємозв'язку із загальною стратегією бізнесу.

Запропоновані напрями співпраці в межах функціонування віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу є базовими та можуть бути доповнені або оптимізовані відповідно до потреб основних суб'єктів-учасників і впливів зовнішнього середовища (рис. 4.3).

Другий етап створення віртуальної платформи передбачає визначення її правового статусу, який, у свою чергу, залежить від територіального місця розташування основних технічних (апаратних) потужностей: серверів, комп'ютерів, мережного обладнання тощо. Існує декілька варіантів фізичного розміщення апаратних ресурсів віртуальної платформи. На початковому етапі, якщо не потрібні масове розгортання серверів, постійний контроль за продуктивністю фізичних серверів при навантаженні та високий ступінь їх доступності, доцільне розміщення віртуальної платформи на основі безкоштовних і недороговартісних інтернет-ресурсів агропродовольчої сфери: Agravery [97], AgroPortal [98], Landlord [99], Latifundist [100], ProAgro [101].

У разі збільшення кількості серверів і високого ступеня їх консолідації потрібно застосовувати потужні засоби управління й обслуговування віртуальної інфраструктури.

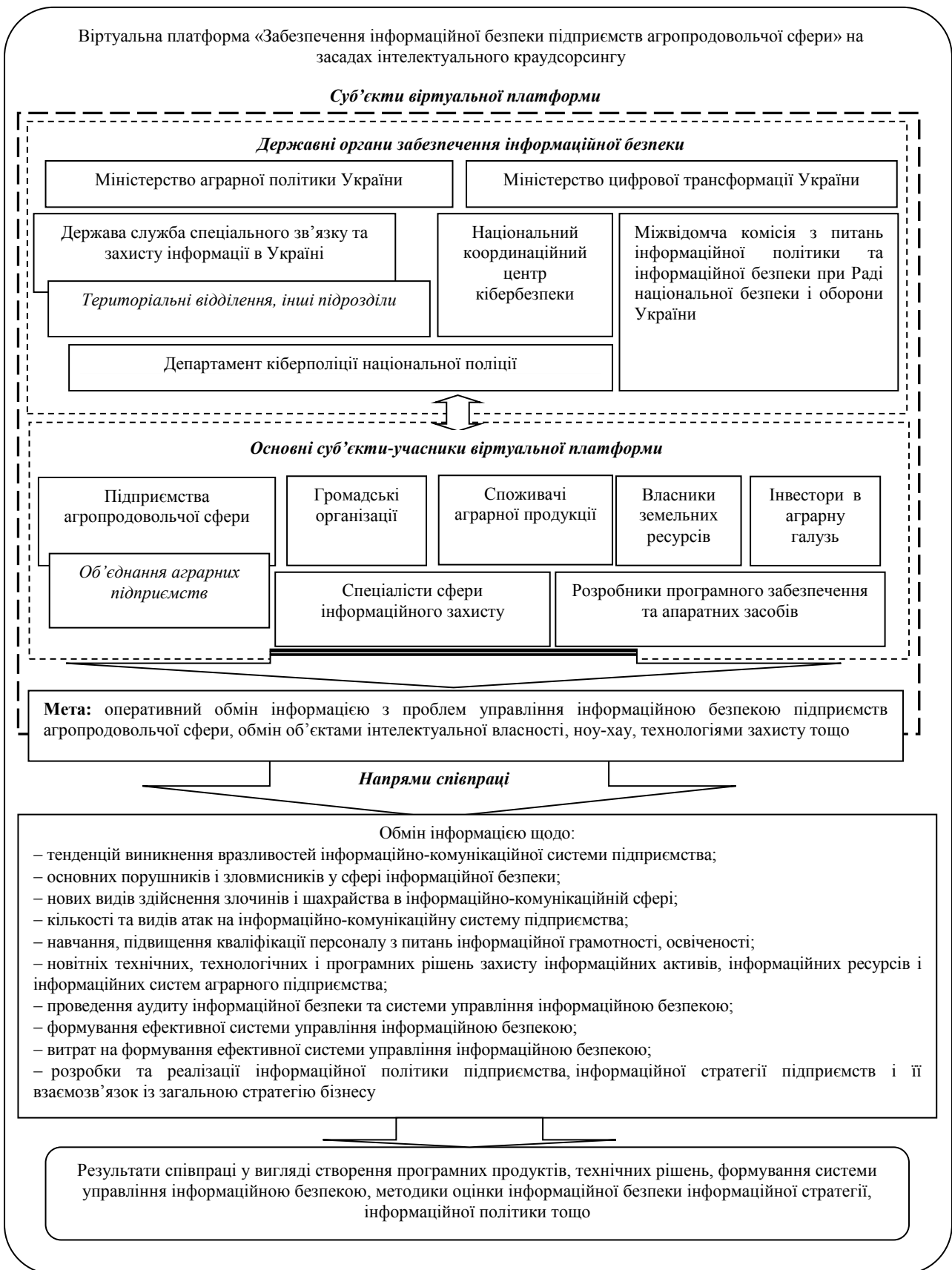


Рис. 4.3. Логіко-структурна схема віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу [авторська розробка]

Проте в разі виникнення потреби використання різних систем і мереж зберігання даних, наприклад, Storage Area Network (SAN), засобів резервного копіювання та відновлення після збоїв і необхідності «гарячої» міграції запущеної віртуальної платформи на інше обладнання, можливостей інтернет-ресурсів агропродовольчої сфери не вистачить.

Доцільно відзначити, що вказані інтернет-ресурси агропродовольчої сфери постійно оновлюються і набувають нових функцій, що розширює сферу їх використання. Отже, важливим аспектом створення пропонованої віртуальної платформи є технічна підтримка.

Open Source, де є працівники, які займаються доопрацюванням продукту і його підтримкою. Цей варіант передбачає активну участь користувачів у розвитку продукту, складання ними звітів про помилки та не гарантує розв'язання проблем при використанні платформи [67].

Існує підхід, коли кожен сервер використовується одним додатком. Така структура допомагає гарантовано забезпечити додаток потрібними ресурсами та ізолювати від інших додатків, щоб його збої не впливали на роботу системи, проте потребує залучення додаткових ресурсів.

Пропоновану платформу можна також створити на базі технічно потужного аграрного підприємства (об'єднання підприємств) або ж на базі новоствореної юридичної особи. Натомість, щодо органів управління, а саме адміністраторів платформи, то, на нашу думку, це повинні бути фахівці спеціальної кваліфікації, які володітимуть компетентностями для забезпечення функціонування віртуальної платформи.

Безкоштовні платформи віртуалізації існують або в рамках спільноти

Розроблення нормативно-організаційного забезпечення функціонування платформи на початковому етапі її формування та запуску повинні здійснювати органи управління платформи, спеціалісти провідних аграрних підприємств і фахівці ІТ-сфери та інші учасники, що вказані в матриці розподілу ролей із метою врахування специфіки різних напрямів, які поєднуються в цій платформі. Надалі організаційно-нормативне забезпечення можна корегувати та оптимізувати з урахуванням інтересів усіх суб'єктів-учасників платформи, тобто на засадах інтелектуального краудсорсингу.

Цей етап також передбачає визначення напрямів і форм фінансування, створення та підтримки віртуальної платформи. На нашу думку, фінансування діяльності платформи повинні забезпечувати безпосередньо учасники цієї платформи, а основні кошти на розробку прототипу та введення його в експлуатацію повинні надавати державні органи, зокрема Міністерство аграрної політики України та Міністерство цифрової трансформації України. Подальше фінансування платформи повинно

відбуватися за кошт усіх суб'єктів-учасників віртуальної платформи та добровільних внесків.

Технологічний етап передбачає створення прототипу (ядра) віртуальної платформи. Технологічно віртуальна платформа повинна являти собою інформаційну систему для накопичення, обміну й управління даними в структурованому вигляді, а також для виклику бізнес-функцій із підключеними до неї через технологічні інтерфейси інформаційними системами учасників платформи. Правила і порядок обміну інформацією з використанням платформи (а значить, і інтерфейси взаємодії – API і структури баз даних) визначаються регулятором на основі еталонної галузевої моделі даних і еталонного опису бізнес-процесів. Пропонована віртуальна платформа забезпечує так звану «горизонтальну» інтеграцію інформаційних систем учасників, при цьому підключатися до неї можуть як інформаційні системи окремих суб'єктів, так і групи користувачів.

Програмне забезпечення необхідно розробляти з урахуванням таких вимог: забезпечувати реалізацію всіх напрямів співпраці в межах віртуальної платформи, мати зручний інтерфейс, бути легким у використанні та фінансово доступним для всіх учасників проектованої платформи.

Архітектоніку пропонованої віртуальної платформи захисту інформаційних ресурсів аграрних підприємств наведено на рис. 4.4.

Основою вказаної архітектоніки віртуальної платформи є її інформаційна система на базі технологічних засобів, програмних продуктів, засобів комунікації та управлінського персоналу, який здійснює процеси адміністрування. На основі обміну інформацією, знаннями, досвідом, уміннями, навичками, ноу-хау, об'єктами інтелектуальної власності формується база даних щодо окремих напрямів формування забезпечення інформаційної безпеки підприємств агропродовольчої сфери, яка доступна всім користувачам платформи.

На основі бази даних функціонує банк моделей, що дозволяє визначити найбільш оптимальний варіант вирішення відповідно до конкретних умов заданої ситуації порушення інформаційної безпеки. Банк моделей повинен функціонувати на основі:

статистично-математичних методів, що допомагають вирахувати оптимальний сценарій подолання певної інформаційної загрози за існуючих умов і обмежень;

даних, які надійшли від інших суб'єктів учасників, які мали подібні прецеденти, та інформація про які раніше надходила до віртуальної платформи, що дозволить використати існуючий позитивний досвід;

експертних оцінок фахівців-учасників, які нададуть суб'єктивності

оцінці запропонованих банком моделей рішення та допоможуть вибрати із них найбільш оптимальний варіант.

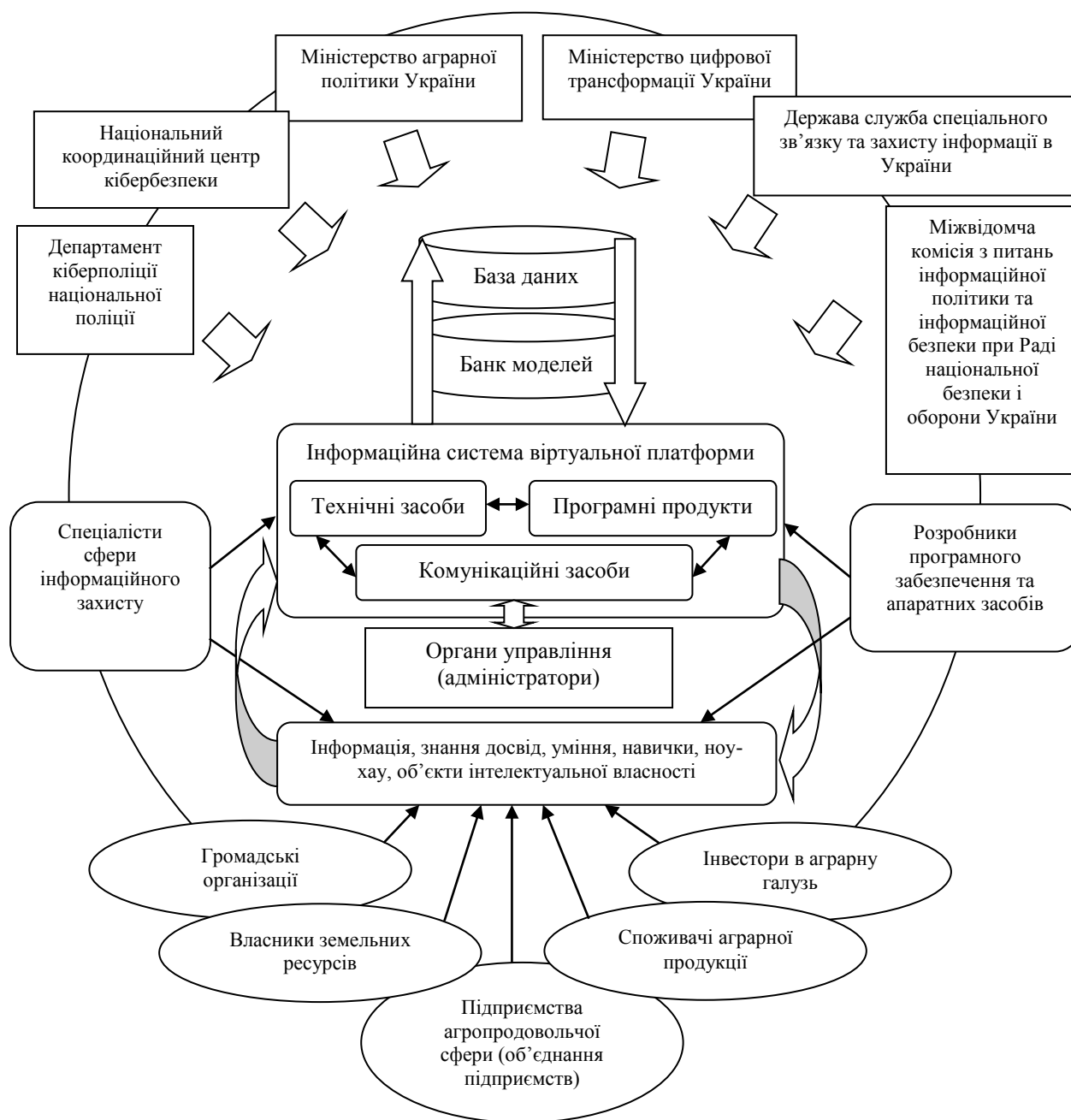


Рис. 4.4. Архітектура віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу [авторська розробка]

Поєднання цих методів дозволяє отримувати найбільш об'єктивні дані для формування рішень відносно окремих напрямів функціонування системи інформаційної безпеки підприємства аграрного сектора економіки України.

Основним завданням суб'єктів макрорівня відповідно до пропонованої технологічної архітектури віртуальної платформи є сприяння формуванню достовірної найбільш повної бази даних і, відповідно, банку моделей.

Суб'єкти макрорівня теж наповнюють бази даних, консультують, спільно розробляють заходи і, відповідно, є користувачами віртуальної платформи.

Дещо специфічними суб'єктами є спеціалісти сфери інформаційного захисту та розробники програмного забезпечення і апаратних засобів, які, крім основних напрямів діяльності платформи, забезпечують і її програмну та технічну підтримку.

Інші етапи формування віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу передбачають виконання дій, що відповідають власне назвам цих етапів, зокрема введення в експлуатацію платформи (використання віртуальної платформи, наповнення баз і банків даних, перевірка відповідності функціонування платформи меті її створення) та на етапі супроводу – підтримання належного рівня функціонування віртуальної платформи.

Процес створення та функціонування віртуальної платформи повинен відповідати основним принципам, таким як законність; економічна обґрунтованість; перспективність та орієнтація на існуючі вітчизняні й міжнародні відкриті стандарти; безперервність функціонування; забезпечення відмовостійкості, надійності, доступності та коректності функціонування організаційних, програмних і технічних елементів віртуальної платформи; безперервність удосконалення; персональна відповідальність; контроль; рівнодоступність ресурсів для всіх учасників.

Пропонована віртуальна платформа «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу організована вищезазначеним чином матиме ряд переваг:

- наявність відкритих захищених інтерфейсів для інформаційної взаємодії із зовнішнім оточенням;

- надання віртуальних майданчиків для комунікації суб'єктів-учасників;

- збереження, поширення і обробка величезних обсягів даних;

- надання консультацій суб'єктам-учасникам, розподіленим на великій території;

- шмарний характер послуг, надання послуг у реальному часі;

- формування активів інноваційного характеру – це нові інноваційні розробки та ідеї у сфері інформаційної безпеки;

- повна автоматизація практично всіх видів діяльності;

- необмеженість кількості виконуваних завдань у рамках ключової проблеми забезпечення інформаційної безпеки;

використання біометрії, двофакторної аутентифікації через мобільні телефони й додатки для ідентифікації користувача, що забезпечує необхідний рівень інформаційної безпеки;

збільшення кількості користувачів, їх ролей і функцій не вимагає модернізації, і водночас підвищує цінність інформаційного ресурсу;

конструювання нових суспільних відносин і процесів обміну, створення нової суспільної цінності;

кількість користувачів, що реалізують різні функції при схожості ключової взаємодії, не обмежена;

ця віртуальна платформа може об'єднуватись із іншими віртуальними платформами у віртосистему («кущ платформ») за допомогою загального механізму приєднання;

до створення можуть залучатися державні та приватні суб'єкти, що передбачає застосування різних механізмів державно-приватного партнерства;

з метою проведення фінансових операцій можна застосувати одну або кілька моделей монетизації;

функціонал можна використовувати та розширювати, виходячи з галузевих потреб і логіки розвитку віртуальної платформи;

архітектура віртуальної платформи масштабується на основі відкритих стандартів;

суб'єкт-користувач може виконувати одночасно кілька ролей, що орієнтує задоволення потреб усіх груп суб'єктів-учасників, в інтересах яких спроектовані всі сервіси віртуальної платформи;

накопичуються дані, включаючи ті, що одержуються ззовні за рахунок аналізу поведінки користувачів [19; 71].

Отже, віртуальна платформа «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу є масштабним інструментом, що формує та регулює процеси забезпечення інформаційної безпеки агропродовольчого ринку, робить прозорими відносини між діючими суб'єктами зазначеного ринку за рахунок технологій безпечної участі, репутаційних оцінок і зрозумілого механізму співпраці, зокрема в межах захисту інформації.

Використання пропонованої віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу є своєрідним драйвером інноватизації та цифровізації діяльності підприємств агропродовольчої сфери, з одного боку, та дозволить створити надійну систему захисту інформаційних активів та ефективну систему управління інформаційною безпекою – з іншого.

Однією з основних умов функціонування пропонованої віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу є наявність на зазначених підприємствах сформованої ефективної системи управління інформаційною безпекою.

4.2. Створення системи менеджменту інформаційної безпеки підприємства агропродовольчої сфери України

Сучасний етап розвитку інформаційної безпеки потребує комплексного підходу до розробки та впровадження методів і засобів захисту ресурсів інформаційно-комунікаційних систем та мереж як на технічному, так і організаційному рівні, тобто реалізації комплексного процесу. Комплексний процес організації безпеки в першу чергу має включати заходи управління інформаційною безпекою. Зазначений процес забезпечує механізми та методи, які дозволяють реалізувати комплексну політику інформаційної безпеки підприємства.

Інформаційна безпека – реалізація процесу захисту інформації від широкого діапазону загроз (внутрішніх та зовнішніх), що здійснюється з метою забезпечення ефективності та надійності функціонування системи управління підприємством.

Сучасні інформаційні системи призначені для забезпечення працездатності інформаційної інфраструктури сільськогосподарського підприємства, надання різних видів інформаційних сервісів, автоматизації фінансової та виробничої діяльності, а також підтримки бізнес-процесів, завдяки їм можна скоротити як фінансові, так і трудові витрати. В інформаційних системах сучасних підприємств агропродовольчої сфери продукуються, обробляються, передаються та зберігаються значні обсяги інформаційних ресурсів різного ступеня конфіденційності, що формує необхідність захисту цих інформаційних систем підприємства та інформаційного середовища загалом від різних загроз безпеці інформації.

У ході аналізу управління інформаційною безпекою підприємств агропродовольчої сфери було визначено, що процес успішного функціонування суб'єктів аграрного ринку залежить від прийняття якісних і своєчасних управлінських рішень, які формуються на основі ретельного відбору й аналізу інформації, що надходить із внутрішнього та зовнішнього середовища. У зв'язку з розвитком інформаційних технологій, загальною інформатизацією і цифровізацією економічних відносин суб'єктів аграрного

ринку підвищується вагомість інформації та інформаційних ресурсів не тільки для економіки, але і для суспільства загалом. Інформація набула значення найбільш важливого управлінського ресурсу порівняно з людськими, фінансовими та матеріальними. З підвищенням ролі інформації сформувався інформаційний простір, який необхідно захищати від несанкціонованого або навіть ненавмисного впливу на рівні держави, регіону й окремих підприємств. В економічній діяльності захист інформації істотно підвищує рівень конкурентоспроможності підприємства, що дає можливість отримувати більші прибутки, укладати нові вигідні контракти з контрагентами, а отже, – значно підвищити ефективність діяльності сільськогосподарської організації загалом.

Зазначені передумови визначають провідну роль формування системи інформаційної безпеки підприємства агропродовольчої сфери та визначення особливостей управління нею. Цим питанням присвячені праці В. Андріанова [15], А. Гладких [21], Ю. Гарасима [66], Ю. Гатчина [20], Н. Голдуєва [15], В. Голованова [15], С. Євсєєва [60], Д. Жмурова [58], С. Зефірова [15], Л. Кауспадієнльє [87]; Є. Климової [20], Р. Коржа [66], О. Король [60]; Н. Куканової [46]; Н. Кухарської [47]; А. Лагуна [47]; А. Моїсєєва [58], С. Остапова [60]; В. Ромака [66] та інших науковців.

Доробки світової та вітчизняної наукової спільноти та практика функціонування підприємств агропродовольчої сфери щодо формування системи інформаційної безпеки підприємства агропродовольчої сфери, управління нею свідчать про дуалістичність поглядів на цей процес, з одного боку, обов'язкові вимоги національних уповноважених органів (стандарти, нормативи, процеси ліцензування) [2; 3; 4; 5; 6; 7; 8; 9; 10; 11; 12; 13], з іншого – розуміння власником аграрного бізнесу або вищим керівництвом організації необхідності впровадження комплексів захисту інформації. Тому для менеджменту та власників аграрного бізнесу головна проблема – відповідність встановленим вимогам до захисту інформації, а головний спосіб її розв'язання – з мінімальними витратами забезпечити надійний захист інформаційного середовища. Складність полягає в тому, як, незважаючи на неможливість охоплення всіх існуючих видів діяльності та умов їх реалізації, а також істотні відмінності цілей діяльності підприємств агропродовольчої сфери, запропонувати універсальний набір вимог до формування систем інформаційної безпеки. Тому інформаційна безпека розглядалася як самодостатня сутність, інваріантна до діяльності, цілей, умов, а також істотно звужувалася її змістовність для досягнення універсальності [15; 21; 66].

Аналізовані системи інформаційної безпеки підприємств агропродовольчої сфери Полтавської, Сумської, Кіровоградської, а особливо Харківської та Луганської областей, не відповідають існуючим реаліям господарювання, а власники та керівники цих підприємств характеризують їх дещо викривлено. Так, основні недоліки діяльності із забезпечення інформаційної безпеки пов'язані з використанням традиційної моделі інформаційної безпеки, яка передбачає обов'язкову наявність зловмисника, що прагне завдати шкоди активам (інформації), та, відповідно, технічній і програмній частинам, орієнтованим на захист інформації від дій такого суб'єкта (групи суб'єктів). Доцільно відзначити, що інциденти, пов'язані, наприклад, зі штатними змінами прикладного програмного забезпечення, порушення процедур роботи з інформацією персоналом підприємства, низький рівень технічного захисту інформаційної, не пов'язані із діями зловмисника. Основні причини зазначеного – низький рівень ефективності менеджменту та невідповідна програмно-технологічна база. Власне неефективність менеджменту аграрних підприємств, відсутність органів управління системою інформаційної безпеки на підприємстві є основним джерелом проблем, які ігноруються через неможливість доведення причетності до них дій зловмисника. Усвідомлення важливості інформаційного впливу на виробничі та управлінські бізнес-процеси, ефективності їх захисту та захисту інформаційних активів та інформаційних продуктів підприємства є ефективнішим заходом, ніж вплив інших факторів, що перетворює процеси інформаційного захисту в один із ключових інструментів конкурентної боротьби підприємств агропродовольчої сфери, а це, в свою чергу, актуалізує першочергову необхідність формування ефективної системи управління інформаційною безпекою, яка повинна бути інтегрована з основними бізнес-процесами суб'єкту господарювання.

Тому важливим аспектом дослідження системи управління інформаційною безпекою є визначення сучасного розуміння поняття «інформаційна безпека», його значення для реалізації основних бізнес-процесів. Проведений у попередніх розділах монографії аналіз дав змогу визначити, що найбільш розповсюдженим є визначення інформаційної безпеки як певного рівня захищеності інформації від незаконного ознайомлення, перетворення і знищення, а також захищеності інформаційних ресурсів від впливів, спрямованих на порушення їх працездатності. Природа цих впливів може бути найрізноманітнішою – це і спроби проникнення зловмисників, і помилки персоналу, і відмова апаратних засобів і програмних продуктів, і стихійні лиха та інші фактори [15; 21; 58; 69].

Інша група науковців розглядає це поняття з погляду бізнесу та визначає інформаційну безпеку підприємства як стан захищеності інтересів (цілей) організації в умовах загроз її інформаційній сфері та інформаційному середовищу. Інформаційну сферу розуміють як сукупність інформації, інформаційної інфраструктури, суб'єктів, які здійснюють збір, формування, розповсюдження, зберігання та використання інформації, а також системи регулювання відносин, які при цьому виникають [20; 47; 66].

Відповідно до зазначених підходів і показників оцінки рівня інформаційної безпеки аграрних підприємств роль інформаційної безпеки в бізнесі сучасної аграрної організації є незначною, оскільки її власники та керівництво розглядають інформаційну безпеку як «звичайну страховку» від можливих проблем і неприємностей: «...заплатив гроші, впровадив рішення і можеш спокійно зосередитися на основній діяльності...» [104].

Водночас розвиток ринку, інформатизація сфер діяльності суб'єктів господарювання аграрного ринку, зростання кількості загроз і засобів забезпечення безпеки призводять до принципово іншого розуміння ролі інформаційної безпеки. В умовах глобальної інформатизації її не можна сприймати виключно як захист або «страховку» – вона переростає в щось більше, а саме в один із ключових бізнес-активів сучасного суб'єкта агропродовольчого ринку. На думку фахівців аналітичного центру компанії Perimetrix, упровадження технологій інформаційної безпеки може сприяти зростанню прибутковості або загальної ефективності бізнесу безпосередньо, а не тільки за рахунок мінімізації ризиків [104].

За даними дослідження Ernst & Young, основними драйверами сучасного ринку інформаційної безпеки для 67 % респондентів є необхідність відповідності різним нормативним актам. Цей пункт очолює список із 2005 р. [103]. При цьому більшість нормативних актів мають рекомендаційний характер і регулюють питання забезпечення інформаційної безпеки опосередковано. Наприклад, основна мета закону SOX – забезпечити прозорість внутрішнього контролю і коректність інформації у звітах, а завдання нормативу Basel II – спонукати фінансові компанії резервувати операційні ризики [11; 13]. Ні той, ні інший не стосуються інформаційної безпеки безпосередньо, проте значною мірою на неї впливають, причому, за інформацією Ernst & Young, 80 % опитаних вважають, що відповідність нормативним актам позитивно впливає на інформаційну безпеку [103]. Фахівці аналітичного центру компанії Perimetrix вважають це питання надзвичайно актуальним і для українських підприємств. До 2005 р. серед факторів, що стимулюють розвиток інформаційної безпеки, перше місце посідали технічні загрози, зокрема класичні віруси та мережні «черв'яки».

Позитивною тенденцією формування та впровадження системи інформаційної безпеки на підприємстві є захист приватних і корпоративних даних – так вважають відповідно 43 і 59 % фахівців [104].

Вітчизняні суб'єкти господарювання аграрного ринку демонструють доволі різні показники (рис. 4.5).

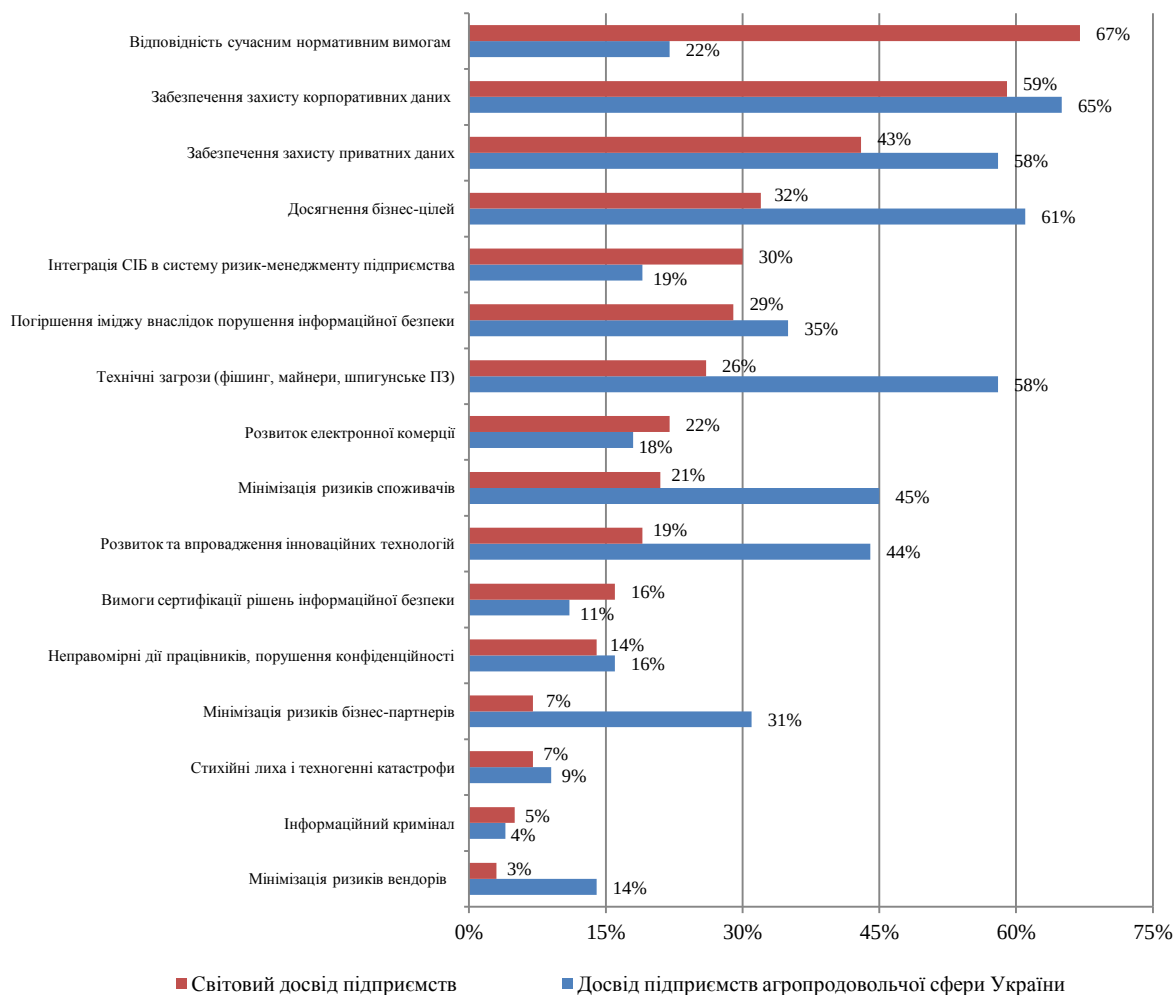


Рис. 4.5. Драйвери формування системи інформаційної безпеки підприємства (світовий досвід і досвід підприємств агропродовольчої сфери України) [сформовано на основі 21; 47; 89; 91; 94; 103; 104]

Драйвери формування системи інформаційної безпеки вітчизняних підприємств агропродовольчої сфери відрізняються від світових тенденцій через специфіку їх діяльності. Головною метою створення системи інформаційної безпеки вітчизняних аграрних підприємств є забезпечення захисту корпоративних даних, досягнення бізнес-цілей, забезпечення захисту приватних даних, протидія технічним загрозам інформаційній безпеці (фішингу, майнерам, шпигунському програмному забезпеченню тощо), мінімізація ризиків бізнес-партнерів і споживачів, розвиток і впровадження

інноваційних технологій, особливо у виробничих процесах вирощування сільськогосподарських культур, погіршення іміджу внаслідок порушення інформаційної безпеки. Це свідчить про практичну орієнтацію необхідності створення системи інформаційної безпеки підприємств аграрного ринку, а не про номінальну або ж законодавчу необхідність її формування та підтримки.

Розглянуті підходи до визначення інформаційної безпеки та визначені драйвери формування системи інформаційної безпеки підприємства зумовлюють доцільність формування системи менеджменту інформаційної безпеки на основі ризик-орієнтованого підходу, який ґрунтується на припущенні, що оцінка ризику уможливорює вирішення питань, пов'язаних із інформаційними активами організації: актуальні загрози і їх джерела – фактори ризику; можливість і періодичність виникнення загроз; визначення інформаційних активів (їх кількісний аналіз), які можуть підлягати впливу у разі виникнення загрози [15].

Аналіз наукових праць у цій сфері показав, що стандартній системі управління інформаційною безпекою підприємства притаманні всі загальні для систем менеджменту елементи. При цьому досвід використання стандартизованих вимог до системи менеджменту інформаційної безпеки визначив основні напрями забезпечення інформаційної безпеки на сучасному аграрному підприємстві, такі як:

- розробка стратегії інформаційної безпеки, цілей та заходів, що відображають цілі бізнесу аграрного суб'єкта господарювання;

- актуалізація політики інформаційної безпеки, яка передбачає дотримання правил і норм забезпечення інформаційної безпеки підприємства агропродовольчої сфери;

- поширення настанов (інструкцій) з політики та стандартів інформаційної безпеки серед всіх керівників, службовців та інших контрагентів;

- підхід і структура реалізації, підтримки моніторингу та вдосконалення інформаційної безпеки, узгоджуються з культурою організації;

- підтримка і прихильність керівництва всіх рівнів;

- розуміння вимог інформаційної безпеки, оцінка ризику та наявність ризик-менеджменту;

- формування системи ефективні заходи щодо формування компетентності з питань інформаційної безпеки для належного усвідомлення;

- забезпечення фінансування заходів менеджменту інформаційної безпеки;

- забезпечення відповідної інформованості, навчання і освіти;

- встановлення ефективного процесу менеджменту інцидентів інформаційної безпеки;

оцінювання системи, яке використовується для оцінки ефективності функціонування менеджменту інформаційної безпеки та пропозицій щодо вдосконалення.

Реалізація системи менеджменту інформаційної безпеки підприємства може бути організована як сукупність управління цільовими (профільними) процесами діяльності, що ініціюються і завершуються за прийнятими для них критеріями (за часом або подією) на основі циклу Шухарта – Демінга (цикл PDCA).

З огляду на вищезазначене зауважимо, що вітчизняні нормативно-правові акти та стандарти мають більш декларативний характер і не враховують специфіку інформатизації діяльності окремих суб'єктів господарювання. Практично всі міжнародні стандарти системи менеджменту методологічно сумісні, що дозволяє виокремлювати і підтримувати уніфіковані завдання, наприклад, робота з персоналом організації відносно користування інформацією та її захисту, реєстрації та збору інформації, формування інформаційних систем, використання засобів автоматизації тощо. У такому разі процедури для реалізації і управління системою менеджменту інформаційної безпеки можуть бути організовані як дерево процесів.

Під час прийняття підприємством рішення про вибір підходу до формування системи менеджменту інформаційної безпеки доцільно враховувати рекомендації ISO / IEC 27003 [13]. Положення цього міжнародного стандарту ґрунтуються на методології процесного підходу, включаючи специфікацію всіх формальних атрибутів можливих процесів системи менеджменту інформаційної безпеки [12].

На основі поєднання положень міжнародних стандартів системи менеджменту інформаційної безпеки, моделі побудови системи менеджменту інформаційної безпеки підприємства на основі циклу Демінга та враховуючи запропоновані організаційні заходи щодо створення віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу та специфіку діяльності підприємств аграрного ринку запропоновано модель побудови системи управління інформаційною безпекою підприємства агропродовольчої сфери, яка на відміну від існуючих передбачає забезпечення інформаційної безпеки підприємства на основі поєднання функцій управління з циклом організаційного управління Демінга в площині організаційного забезпечення та програмних продуктів, у площині технічного забезпечення, апаратних засобів і технічної підтримки, а також у площині людських ресурсів, що дозволяє розробити найбільш оптимальну систему менеджменту інформаційною безпекою кожному окремому суб'єкту господарювання (рис. 4.6).

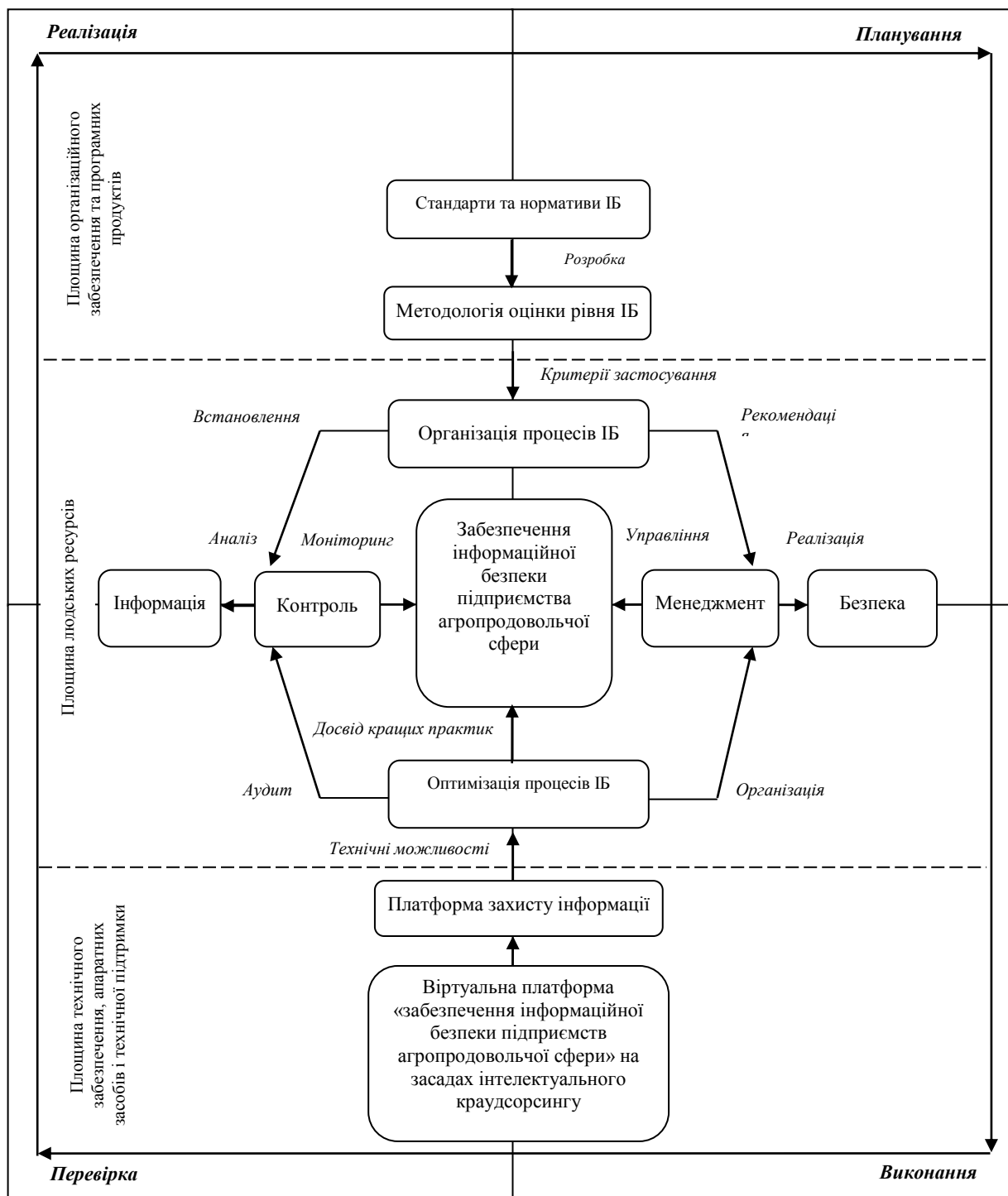


Рис. 4.6. Модель побудови системи управління інформаційною безпекою підприємства агропродовольчої сфери на основі циклу Демінга [розроблено на основі 12; 13; 46; 87]

Відповідно до зазначеної моделі на основі міжнародних і вітчизняних стандартів та внутрішніх нормативів з інформаційної безпеки формується методологія оцінки рівня інформаційної безпеки і визначаються необхідні програмні продукти для організації процесів управління безпекою підприємства. Зазначені процеси реалізуються завдяки платформі захисту

інформації, яка в поєднанні із віртуальною платформою «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу дозволяє реалізувати та в разі необхідності оптимізувати процеси захисту інформаційних ресурсів. Платформа захисту інформації являє собою сукупність апаратних і технічних засобів, фізичних інструментів для забезпечення інформаційної безпеки. Ефективність функціонування платформи захисту інформації залежить від технічних і технологічних можливостей підприємств агропродовольчої сфери та здатності їх управлінського персоналу системи менеджменту інформаційної безпеки правильно використовувати інструменти захисту.

Надалі запропонована модель передбачає проведення аудиту використання програмних та апаратних засобів для забезпечення процесів інформаційного захисту та ефективність функціонування діяльності системи менеджменту інформаційної безпеки підприємства загалом.

На основі моніторингу та подальшого аналізу визначаються недоліки захисту інформаційних ресурсів і розробляються заходи щодо їх усунення, які передбачають оптимізацію нормативів з інформаційної безпеки, методології оцінки рівня інформаційного захисту та програмного забезпечення. Отже, запропонована модель має циклічний характер, який забезпечує її гнучку адаптацію, що, в свою чергу, виступає основою для визначення послідовності етапів формування системи менеджменту інформаційної безпеки підприємства агропродовольчої сфери.

У загальному вигляді послідовність формування системи менеджменту інформаційної безпеки та завдань може включати етапи, реальне наповнення яких корегує саме підприємство залежно від масштабів і спеціалізації його діяльності (рис. 4.7).

За поданою схемою, етапи з першого по восьмий відповідають за здійснення компонента організаційного управління циклу Демінга – «планування» («plan»). На першому етапі передбачене визначення основної сфери діяльності системи менеджменту інформаційної безпеки відповідно до специфіки діяльності підприємства агропродовольчої сфери. Тобто залежно від масштабів підприємства, його спеціалізації (виробництво сільськогосподарської продукції рослинництва чи тваринництва, переробка, сільськогосподарське і харчове машинобудування, заготівля, зберігання, транспортування і реалізація продукції), основних видів продукції або послуг, завдань інформаційного захисту, рівня людських і фінансових ресурсів та інших факторів (переважно внутрішнього середовища) визначаються вимоги до майбутньої системи менеджменту інформаційної безпеки суб'єкта аграрного ринку.

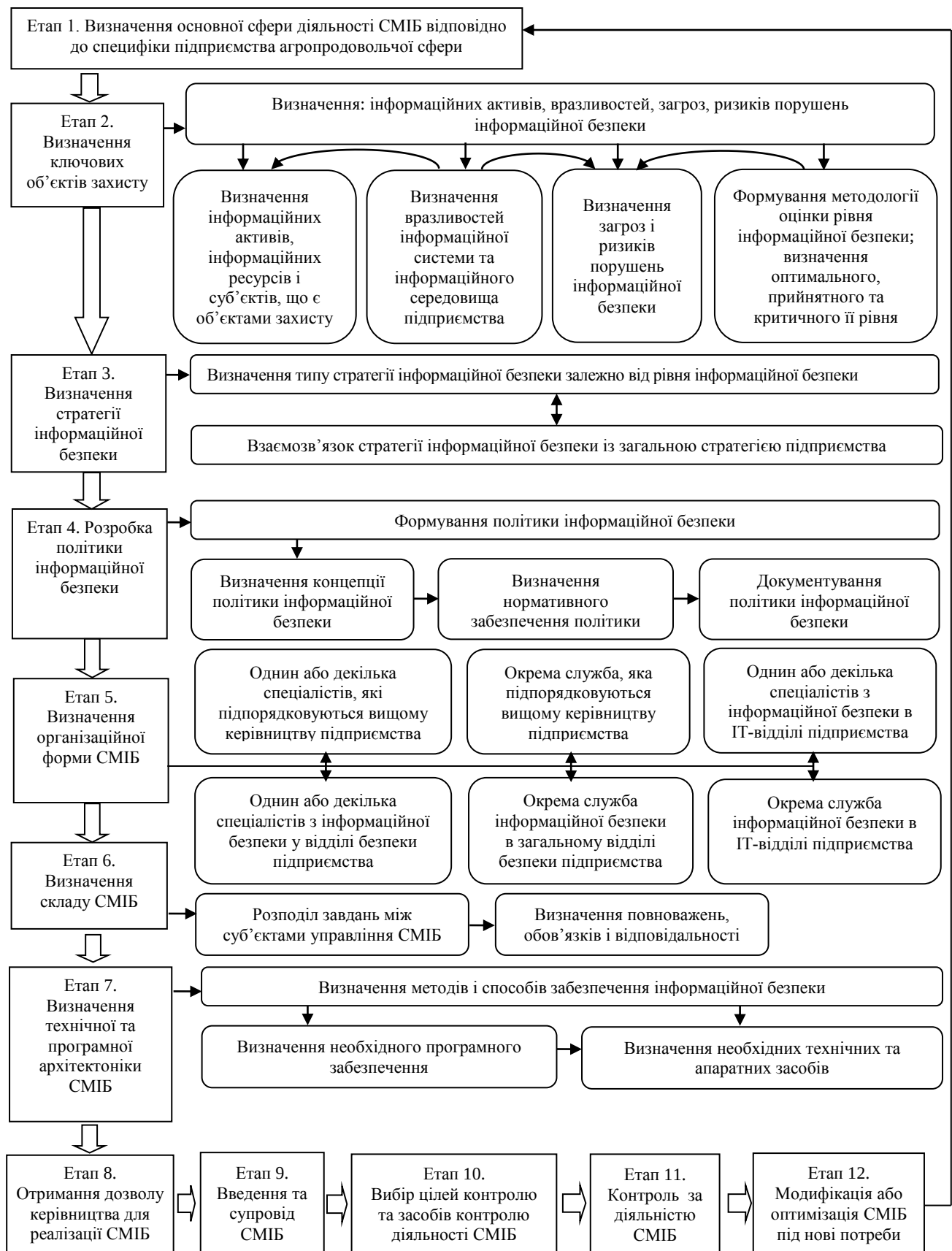


Рис. 4.7. Послідовність етапів формування системи менеджменту інформаційної безпеки підприємства агропродовольчої сфери [авторська розробка]

На другому етапі передбачене визначення інформаційних активів, вразливостей, загроз, ризиків порушення інформаційної безпеки. Фактично цілями цього етапу формування системи менеджменту інформаційної безпеки є:

проведення інвентаризації активів, особливо інформаційних, та інформаційних ресурсів;

здійснення категоризації інформаційних активів та інформаційних ресурсів, що підлягають захисту;

проведення технологічного аудиту захищеності інформаційної системи з виявленням загроз і вразливостей інформаційного середовища;

оцінка інформаційних ризиків підприємства;

формування методології оцінки інформаційної безпеки;

визначення прийнятного та критичного рівня інформаційної безпеки.

Основна складність цього етапу полягає у тому, що фахівці аграрного підприємства зазвичай не можуть визначити вартість інформації, інформаційних ресурсів та інформаційний активів.

Тобто фахівці з інформаційної безпеки мають пояснювати провідним фахівцям, які працюють з різною інформацією, інформаційними ресурсами та активами, яким чином потрібно здійснювати оцінку і підбивати підсумки цього процесу, а також розробити методики і критерії категоризації інформації. Зауважимо, що визначення вартості активів, дійсно, дуже складний процес. Проте для оцінки інформаційних ризиків досить оцінити вартість активів приблизно, тобто проранжувати ресурси відносно один одного. Для цього можна, наприклад, використовувати шкалу з трьох-п'яти рівнів [46; 47; 69]. Під час визначення загроз і вразливостей інформаційної системи підприємства агропродовольчої сфери можна використовувати трирівневу шкалу для ймовірності, тому що визначити рівень ймовірності реалізації (низький, середній або високий) набагато простіше, ніж визначити ймовірність реалізації у відсотках. Залежно від розміру аграрного підприємства, спеціалізації та масштабів його діяльності для більшої деталізації можна використовувати ще й проміжні етапи шкали (нижче середнього, вище середнього тощо). Крім цього, ймовірність уразливості можна поділити на параметри, її складові, тоді оцінка буде простішою. Наприклад, ймовірність реалізації вразливості оцінюється також і на основі простоти реалізації вразливості та доступності ресурсу, в якому існує ця вразливість.

На третьому етапі передбачене визначення стратегії інформаційної безпеки підприємства, яку буде реалізовувати та захищати створена система менеджменту інформаційної безпеки, а також її взаємозв'язок із загальною стратегією бізнесу. Оскільки стратегія інформаційної безпеки є

функціональною стратегією, то вона взаємопов'язана та взаємозумовлена загальною стратегією агропродовольчого підприємства.

На четвертому етапі передбачена розробка політики інформаційної безпеки, результат якої полягає у формуванні ефективного нормативного забезпечення інформаційної безпеки та документаційному затвердженні політики інформаційної безпеки, з якою обов'язково слід ознайомитися не тільки керівництву підприємства та працівникам системи інформаційного захисту, але й іншим працівникам.

Під час встановлення сфери застосування і політики системи менеджменту інформаційної безпеки необхідно розглянути стратегічні питання бізнесу, організаційні аспекти, місце розташування (географічне і фізичне), активи (зокрема інформаційні), технології.

На п'ятому етапі передбачене визначення організаційної форми системи менеджменту інформаційної безпеки підприємства агропродовольчої сфери, яка залежить від багатьох внутрішніх факторів, зазначених на першому етапі.

Найбільш важливим є шостий етап, на якому передбачене визначення складу системи менеджменту інформаційної безпеки підприємства, тобто визначення чисельності працівників цієї системи, розподіл завдань між ними, визначення їх повноважень, обов'язків і відповідальності, що, в свою чергу, передбачає, щонайменше, розробку посадових інструкцій [44]. На цьому етапі важливо сформулювати вимоги до працівників системи менеджменту інформаційної безпеки, до їх освіти, компетентностей, досвіду роботи та інші. На цьому етапі також визначаються взаємовідносини між працівниками пропонованої системи та іншими провідним фахівцями підприємства агропродовольчої сфери.

На сьомому етапі визначається технічна та програмна архітектура системи менеджменту інформаційної безпеки, перш за все програмні додатки, основним завданням яких є формування систем інформаційного захисту, моніторинг інформаційних атак, визначення вразливостей і загроз інформаційному середовищу, захист інформаційних активів та інформаційних ресурсів підприємства за різними напрямками діяльності або за різними бізнес-процесами, сповіщення про відбиття в автоматичному режимі інформаційних атак, проектування можливих сценаріїв дій в разі виникнення загрози інформаційній безпеці тощо. Відповідно до програмних продуктів і вимог для їх ефективного функціонування створювана система забезпечується технічними та апаратними засобами. Відповідним чином формується архітектура апаратно-програмного забезпечення.

Проходження вищенаведених етапів забезпечує необхідний рівень інформаційної безпеки агропродовольчого підприємства, який досягається

завдяки застосуванню відповідного набору засобів управління, включаючи методику оцінки рівня інформаційної безпеки, інформаційну стратегію, політику, процедури, організаційну структуру, програмне та апаратне забезпечення з метою захисту ідентифікованих інформаційних активів та інформаційних ресурсів. Визначені на цих етапах заходи управління інформаційною безпекою мають бути проаналізовані, реалізовані, перевірені, і в разі необхідності поліпшені, щоб гарантувати, що рівень інформаційної безпеки забезпечує умови досягнення бізнес-цілей підприємства агропродовольчої сфери.

Наступним і заключним у цьому блоці етапом є отримання схвалення власниками і керівництвом підприємства формування спроектованої системи менеджменту інформаційної безпеки та визначення організаційних, людських і фінансових витрат. Доцільно відзначити необхідність залучення керівництва в процес розробки та впровадження системи менеджменту інформаційної безпеки. Роль керівництва полягає як у постановці завдання забезпечення та управління системою менеджменту інформаційною безпекою, контролю за ефективністю її функціонування, так і в належній мотивації працівників зазначеної системи.

Потрібно враховувати, що тільки вище керівництво підприємства повинно мати повноваження щодо визначення порогового рівня інформаційної безпеки у сфері забезпечення інформаційної безпеки, які є специфічними для кожної організації аграрного ринку. Це зумовлено тим, що саме керівництво несе остаточну відповідальність за інвестиції в систему менеджменту інформаційної безпеки та її ефективність. Не менш важливу роль у формуванні зазначеної системи відіграє дотримання вимог державних і міжнародних нормативно-правові актів і стандартів у цій сфері. За цих умов стандарти є можливим еталоном дій, але не незмінною константою. Керівництво, в певному сенсі, перебуває в багатовимірному просторі, де повинно зорієнтуватися, оцінити кожен вектор і прийняти необхідне рішення відносно дотримання стандартів і положень інформаційної безпеки.

Наступному компоненту циклу Демінга – «виконання» («do») – відповідає дев'ятий етап пропонованої моделі формування системи менеджменту інформаційної безпеки, на якому передбачено її ведення та супровід. Особливість цієї системи полягає в тому, що вона є симбіозом інформаційної системи та системи управління, тому в процесі свого функціонування керується одночасно принципами кібернетики та менеджменту і передбачає розвиток і вдосконалення інформаційних технологій та економіко-математичних методів захисту інформаційних ресурсів для ефективного здійснення економічної та управлінської

діяльності.

Одним із найбільш ефективних способів захисту від інформаційних ризиків, пов'язаних із перебоями в роботі або зниженням продуктивності критично важливих програмних додатків, є послуги із супроводу системи менеджменту інформаційної безпеки, а точніше її програмно-апаратного комплексу, на якому такі програми виконуються. Загалом зазначений супровід складається із комплексу таких заходів, як:

- технічна підтримка (відновлення працездатності інформаційної системи та системи інформаційної безпеки у працездатній задовільній конфігурації);

- зміна конфігурації інформаційного комплексу, окремих його елементів або системи інформаційної безпеки (інсталяція нового програмного забезпечення, апаратного й технічного устаткування, їх конфігурація та налаштування, застосування нових технологій, алгоритмів інформаційного захисту тощо);

- проведення технічних консультацій для провідних фахівців підприємства агропродовольчої сфери та загального персоналу;

- оптимізація роботи інформаційного комплексу (наприклад, підвищення загальної продуктивності діяльності системи інформаційного захисту, досягнення оптимального використання дискового простору та хмарного простору систем зберігання, удосконалення протоколів захисту, скорочення часу резервного копіювання та післяаварійного відновлення даних тощо);

- ведення технічної документації (паспортизація програмно-технічного комплексу системи менеджменту інформаційної безпеки та інформаційних технологій, регламентація робіт з відновлення працездатності інформаційної системи після настання загроз, її профілактика тощо);

- профілактичні заходи, зокрема визначення відповідності використовуваного програмного забезпечення, апаратно-технічних заходів та інформаційних технологій захисту виробничих і управлінських процесів цілям системи менеджменту інформаційної безпеки та бізнес-цілям підприємства агропродовольчої сфери;

- підвищення кваліфікації за напрямками менеджменту та інформаційного захисту персоналу системи менеджменту інформаційної безпеки.

Десятий та одинадцятий етапи формування системи менеджменту інформаційної безпеки підприємства агропродовольчої сфери відповідають компоненту організаційного управління циклу Демінга – «контроль» («check»). Питання реалізації системи менеджменту інформаційної безпеки на практиці невіддільні від відповідних процедур контролю, організованих в окремому блоці вимог системи менеджменту інформаційної безпеки.

Етап вибору цілей контролю та засобів контролю за діяльністю системи

менеджменту інформаційної безпеки суб'єкта агропродовольчої сфери передбачає визначення складових контролю. Доцільним є виділення таких трьох важливих складових контролю за системою менеджменту інформаційної безпеки: операційний контроль, внутрішній аудит, аналіз з боку керівництва.

Операційний контроль має передбачати поточний контроль з боку безпосередніх працівників системи менеджменту інформаційної безпеки. Наприклад, виконання періодичного сканування на наявність вразливостей інформаційної системи та автоматизованих процесів виробництва й управління у сфері рослинництва або тваринництва, визначення інформаційних загроз у сфері зберігання або збуту продукції та інше.

Внутрішній аудит полягає в періодичній перевірці ефективності процесів операційного контролю. Аудитор здійснює аналіз діяльності системи менеджменту інформаційної безпеки загалом (бізнес-процеси, які підлягають захисту, рівень їх захисту, інформація про кількість інцидентів інформаційної безпеки, чисельність кібератак, кількість відвернутих атак, функціонування програмно-апаратної частини, обсяг фінансування, перерозподіл фінансових ресурсів усередині системи інформаційного захисту тощо) та власне процесів операційного контролю за певний період, на основі чого формується висновок про результативність її діяльності.

Аналіз з боку керівництва передбачає оцінку результатів проведених аудитів (як внутрішніх, так і зовнішніх), розробку та прийняття рішень щодо подальшого функціонування системи менеджменту інформаційної безпеки.

Відповідно до пропонованої моделі побудови системи менеджменту інформаційної безпеки підприємства агропродовольчої сфери головними завданнями органів управління цієї системи є моніторинг і контроль. Формально зміст робіт контролю за інформаційною безпекою підприємства повинен включати:

моніторинг та перевірку процедур і інших засобів контролю за інформаційними ризиками (захисних заходів) для швидкого виявлення помилок у результатах обробки, швидкої ідентифікації порушень безпеки, надання керівництву інформації, сприяння виявленню подій небезпеки та запобігання виникненню інцидентів загроз інформаційній та іншим видам безпеки підприємства за допомогою відповідної системи критеріїв;

перегляд оцінки рівня інформаційної безпеки через заплановані інтервали часу, а також визначення залишкових ризиків та ідентифікацію прийнятних рівнів ризику відповідно до змін на аграрному підприємстві та в його операційному і бізнес-середовищі;

регулярні перевірки ефективності системи менеджменту інформаційної безпеки (зокрема дотримання політики та досягнення цілей системи

менеджменту інформаційної безпеки, засобів контролю безпеки), враховуючи результати аудитів безпеки, інцидентів, результати вимірювань ефективності, пропозиції усіх зацікавлених сторін;

внутрішні аудити діяльності системи менеджменту інформаційної безпеки;

перевірку керівництвом системи менеджменту інформаційної безпеки для підтвердження адекватності сфери її дії і ефективності заходів з удосконалення системи менеджменту інформаційної безпеки тощо.

Останній, дванадцятий етап формування системи менеджменту інформаційної безпеки підприємства агропродовольчої сфери – її модифікація або адаптація під нові потреби – відповідає компоненту «реалізація» («act») циклу Демінга.

Забезпечення інформаційної безпеки, як і будь-який інший процес, потребує постійного адаптування до умов зовнішнього середовища та вимог внутрішньої системи підприємства. Оскільки норми та принципи складних процесів використовуються для їх концептуальної перебудови, зокрема і для забезпечення ефективності процесів інформаційної безпеки, то її можливо вдосконалити за допомогою реінжинірингу [22; 23; 40; 61; 73; 74; 82].

Інформаційна безпека підприємства агропродовольчої сфери передбачає такий рівень розвитку інформаційної діяльності, який би забезпечував безперебійне й стабільне функціонування, а також оптимальне використання наявних інформаційних ресурсів при мінімізації впливів загроз. Тому головною причиною реінжинірингу системи інформаційної безпеки є розбіжність між вимогами до цієї системи з боку користувачів і її дійсними характеристиками.

Існуючі дослідження в галузі вдосконалення інформаційної безпеки переважно стосувалися оцінок часу ефективного функціонування в рамках життєвого циклу [22; 23; 40; 48; ; 61; 73; 74; 82; 85]. Передбачалося, що після закінчення життєвого циклу система інформаційної безпеки замінюється новою, або її відновлюють. У сучасних умовах розвитку інформаційних технологій необхідне й можливе гнучке вдосконалення: або поступове, протягом нормального функціонування системи інформаційної безпеки, або інтенсивне (реінжиніринг), після того, як значно знизилась її ефективність.

На відміну від відомих методологій пропонується технологія гнучкого реінжинірингу являє собою процес побудови та послідовного перетворення узгоджених моделей на всіх етапах життєвого циклу. Це дозволяє, по-перше, розширити період життєвого циклу системи менеджменту інформаційної безпеки; по-друге, на початковому етапі зниження рівня інформаційної безпеки запропонувати конкретні способи її модернізації.

Особливість пропонованої технології полягає у варіативності процедур реінжинірингу системи менеджменту інформаційної безпеки за горизонтально-вертикальними схемами, що уможливлюють реалізацію вимог на різних ступенях перепроєктування, зокрема програмному, організаційному, процедурному та процесному рівнях і комплексному їх поєднанні (рис. 4.8).

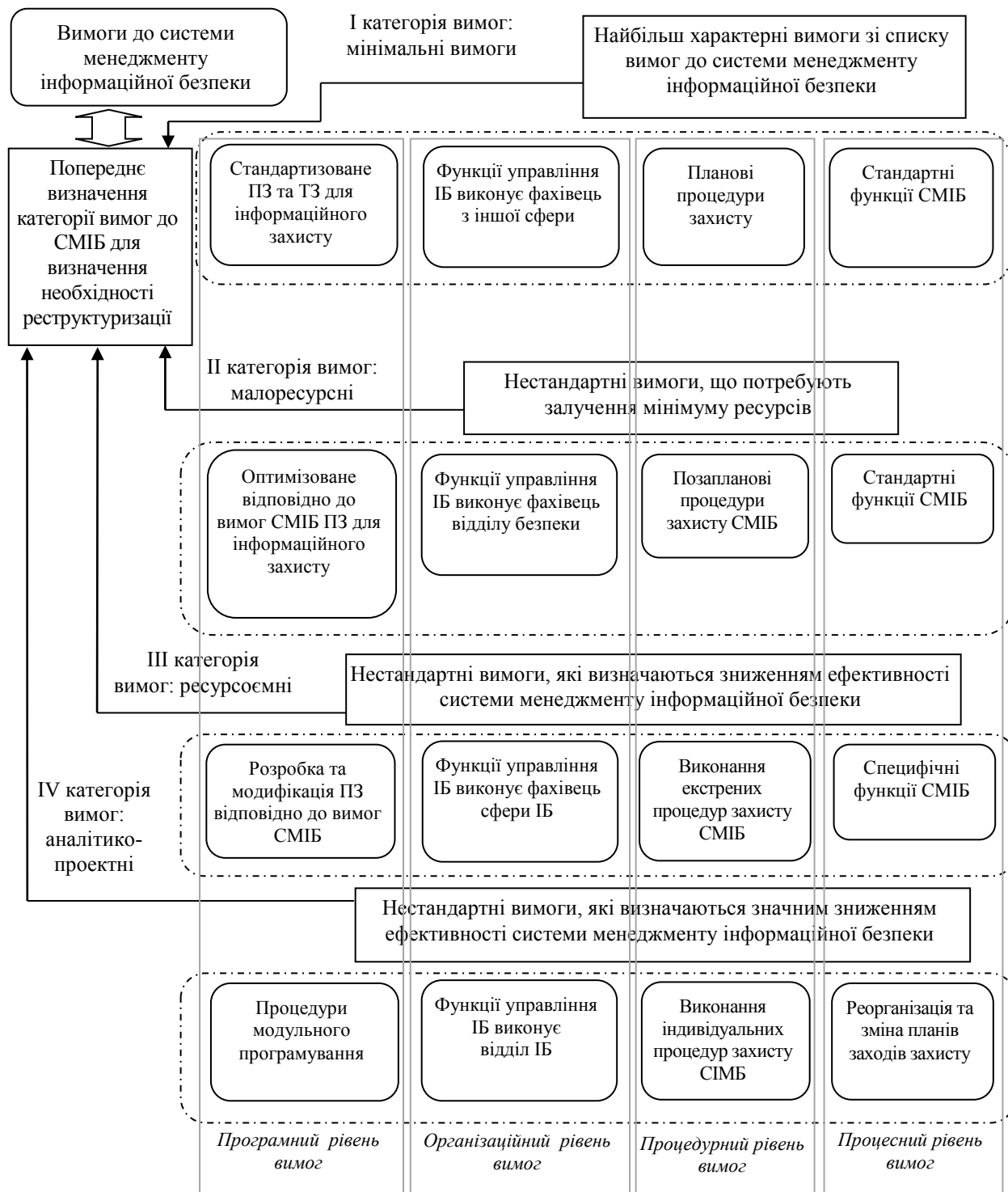


Рис. 4.8. Специфіка вимог до реінжинірингу системи менеджменту інформаційної безпеки підприємства агропродовольчої сфери [розроблено на основі 22; 23]

Отже, пропонується ідея специфікації вимог, яка містить три рівні – програмний, функціональний та організаційний, і чотири категорії, а саме: I – мінімальні вимоги, II – малоресурсні, III – ресурсоемні, IV – аналітико-проектні.

За типами вимог для проведення реінжинірингу інформаційної безпеки, їх доцільно класифікувати таким чином:

- найбільш характерні вимоги зі списку вимог до системи менеджменту інформаційної безпеки;

- нестандартні вимоги, що потребують залучення мінімуму ресурсів;

- нестандартні вимоги, які визначаються зниженням ефективності системи менеджменту інформаційної безпеки;

- нестандартні вимоги, які визначаються значним зниженням ефективності системи менеджменту інформаційної безпеки, або вимоги, пов’язані з необхідністю розширення цілей системи.

Сучасній системі менеджменту інформаційної безпеки підприємств агропродовольчої сфери притаманні процеси постійного вдосконалення та реінжинірингу. Проте умови сьогодення визначають необхідність пошуку новітніх технологій модифікації систем і процесів. З цією метою запропоновано технологію вдосконалення системи менеджменту інформаційної безпеки з використанням процесів гнучкого реінжинірингу, яка передбачає поєднання горизонтально-вертикальних схем, які уможливають реалізацію вимог на різних ступенях перепроєктування, зокрема на програмному, організаційному, процедурному та процесному рівнях і комплексному їх поєднанні, та враховують життєвий цикл системи інформаційної безпеки.

Отже, на основі визначених драйверів формування системи інформаційної безпеки підприємств агропродовольчої сфери, специфіки їх діяльності, враховуючи базові положення міжнародних і вітчизняних стандартів і нормативів щодо формування системи менеджменту інформаційної безпеки, концептуальні принципи циклу Демінга та запропоновані організаційні заходи щодо створення віртуальної платформи на засадах інтелектуального краудсорсингу, розроблено модель побудови системи управління інформаційною безпекою підприємства агропродовольчої сфери, яка, на відміну від існуючих, передбачає забезпечення інформаційної безпеки поєднанням функцій управління з циклом організаційного управління в площинах: організаційного забезпечення та програмних продуктів; технічного забезпечення, апаратних засобів і технічної підтримки; людських ресурсів, що дозволяє сформувати найбільш оптимальну систему менеджменту

інформаційної безпеки для кожного окремого суб'єкта господарювання агропродовольчої сфери.

З огляду на запропоноване вище, розроблено логіко-структурну схему послідовності формування системи менеджменту інформаційної безпеки підприємства агропродовольчої сфери, яка ґрунтується на послідовному проходженні дванадцяти основних етапів, кожен із яких має набір завдань, наповнення яких корегує саме підприємство залежно від масштабів і спеціалізації його діяльності. Відповідно до визначеної послідовності етапів етапи з першого по восьмий відповідають за здійснення компонента організаційного управління циклу Демінга – «планування», дев'ятий етап передбачає ведення та супровід системи менеджменту інформаційної безпеки – «виконання», десятий та одинадцятий етапи – здійснення компонента організаційного управління циклу – «контроль», дванадцятий етап – модифікація або адаптація під нові потреби – відповідає компоненту «реалізація» циклу Демінга. В межах останнього етапу запропоновано технологію гнучкого реінжинірингу системи менеджменту інформаційної безпеки підприємства, яка полягає у варіативності процедур реінжинірингу зазначеної системи по горизонтально-вертикальних схемах, що уможливають реалізації вимог на різних ступенях перепроєктування, зокрема програмному, організаційному, процедурному, процесному рівнях і комплексному їх поєднанні.

Слід відмітити, що ефективність системи менеджменту інформаційної безпеки та системи захисту інформаційних ресурсів та інформаційних активів підприємств агропродовольчої сфери значною мірою залежить від обраної моделі захисту. Тому наступним етапом є розробка пропозицій щодо формування моделі захисту інформації підприємств агропродовольчої сфери.

4.3. Адаптація моделі захисту інформації підприємства агропродовольчої сфери

Протягом останніх десятиліть спостерігається тенденція мінімізації участі людського фактора в різних виробничих та управлінських процесах, що реалізується за допомогою масового впровадження автоматизованих систем. Людино-машинні комплекси на даний момент є найбільш поширеною і продуктивною моделлю здійснення діяльності. На поточному етапі розвитку технологій процес автоматизації людської діяльності є тільки проміжною ланкою на шляху до повного виключення людського втручання. Даний напрямок є найбільш актуальним для систем, які несуть потенційну і

реальну загрозу здоров'ю і життю людини або системи, загрозою яким є людина. До другої групи слід віднести сферу інформаційної безпеки. Зазначене визначає необхідність в переході на наступний рівень виключення людського фактора – впровадження адаптивних моделей інформаційної безпеки, які дозволять перенести процес захисту інформації в зовсім іншу площину.

В умовах глобалізації економіки успішне ведення бізнесу передбачає наявність у підприємств інформації про ринкову кон'юнктуру, фінансове становище конкурентів, новітні розробки, тенденції розвитку в конкретних сферах науки і виробництва. Водночас практика діяльності аграрних суб'єктів господарювання повсякденно свідчить про їх підвищену вразливість від незаконних та інших посягань злочинних організацій та окремих осіб із метою викрадення інформаційних ресурсів, знищення або пошкодження програмного та техніко-технологічного забезпечення, розкриття комерційної таємниці тощо. Тому забезпечення інформаційної безпеки, збереження конкурентних переваг стає важливою необхідністю, одним із базових принципів функціонування сучасних суб'єктів агропродовольчої сфери.

Щоб побудувати ефективну систему менеджменту інформаційної безпеки, необхідно реалізувати комплексний підхід, найважливішим елементом якого є формування і реалізація політики інформаційної безпеки, що, в свою чергу, зумовлює необхідність пошуку оптимальної моделі захисту інформації підприємств агропродовольчої сфери.

Важливу роль у забезпеченні інформаційної безпеки суб'єкта будь-якого рівня відіграє політика безпеки. Визначивши політику інформаційної безпеки, потрібно вирішити питання стосовно технології, яка буде використана для її реалізації, а для цього необхідно створити релевантну модель формування політики інформаційної безпеки.

Проблематика забезпечення інформаційної безпеки, зокрема в аспектах формування моделі захисту інформації, відображені в працях С. Богомолу [16], Д. Зегджи [40], А. Івашка [39], К. Мезенцевої [54], М. Мельника [54], Н. Мілославської [55], Г. Нікітіна [54], А. Петрова [62], В. Степанова [70], А. Толстої [55], С. Чурубрової [76] та інших науковців.

Інформаційні операції можуть проводитися на різних рівнях управління інформаційною безпекою: рівні окремої особи (групи осіб), одного підприємства, групи підприємств, галузі промисловості, регіону та держави загалом. Ефективність здійснення інформаційних операцій і функціонування інформаційної системи загалом, від якої, в свою чергу, залежить соціо-економіко-технічний стан діяльності окремого об'єкта, обґрунтовано

потребує формування не тільки системи інформаційної безпеки, а й дієвої та прийнятної моделі захисту інформації. Тому розробка такої моделі, зокрема і для підприємств агропродовольчої сфери, є актуальним завданням.

Формування ефективної та релевантної моделі політики інформаційної безпеки обґрунтовує необхідність характеристики існуючих моделей для виявлення їх сильних сторін і побудови найбільш оптимальної, універсальної, ефективної, придатної для застосування на різних підприємствах агропродовольчої сфери, моделі.

Найбільш відомою є модель захисту інформації, яка реалізується в межах політики інформаційної безпеки – Bell-LaPadula (BLP) [54]. Ця модель захисту інформації заснована на політиці конфіденційності та стала першою моделлю політики безпеки, яка в зміненому вигляді застосовується для інформаційних технологій аж до сьогодні.

Згідно з політикою безпеки в моделі Bell-LaPadula кожному суб'єкту і об'єкту призначаються рівні секретності, які утворюють ієрархію «від найвищого до найнижчого». Для надання доступу до певного об'єкта рівень секретності суб'єкта порівнюється з рівнем секретності цього об'єкта. Тому в цій моделі безпека розуміється як такий стан системи, при якому забезпечується конфіденційність інформації, тобто такий стан системи (суб'єктів та об'єктів), при якому виключається несанкціонований доступ.

Як вхідні впливи на систему використовують операції доступу суб'єктів «читати» й «записувати». Внаслідок цих дій система може переходити як в безпечний стан, так і в стан небезпеки. Наприклад, якщо внаслідок виконання будь-якої операції дані стають доступними для суб'єктів із більш низьким рівнем допуску (став можливим несанкціонований доступ), то це означає, що система перейшла в небезпечний стан. Ця модель є повністю математично формалізованою [62].

Наступна модель має назву «модель Viba» [55]. В цій моделі основа безпеки полягає в цілісності інформації. Аналогічно до попередньої моделі вона оперує суб'єктами й об'єктами, які також розподіляються на ієрархічно організовані рівні. Проте замість рівнів секретності визначаються рівні цілісності: чим вищий рівень цілісності об'єкта (наприклад, документа), тим більший рівень довіри повинен бути до суб'єкта, який має доступ до цього об'єкта, тим вища ймовірність, що він містить точні дані, тим суворіші правила доступу суб'єкта до операцій із цими даними; чим вищий рівень ієрархії доступу суб'єкта, тим вищий рівень доступу до інформаційних ресурсів та інформаційних активів підприємства [62; 96].

Набір правил моделі Clark-Wilson (CW) [2] розроблений таким чином, щоб у повній мірі забезпечувати безпеку та підзвітність переходів у системі

за рахунок вибору необхідного для такої ситуації режиму роботи з даними. Головне досягнення цих правил порівняно з моделлю Biba – поділ процедур перевірки цілісності та процедур зміни, завдяки яким можна запобігти або виправити більшість нелегальних дій, які здійснюються зсередини підприємства [62].

Згідно з моделлю Clark-Wilson дані поділяються на підмножини, які повинні бути максимально захищені (CDI), і підмножини, для яких такий захист не потрібний (UDI). Користувачі не можуть безпосередньо змінювати критичні дані CDI, а повинні пройти аутентифікацію у відповідній частині програмного забезпечення, а програмні процедури (TP) виконують необхідні операції від імені цих користувачів.

Доцільно виділити три основних мети моделі Clark-Wilson: запобігання виконанню змін неуповноваженими користувачами; запобігання виконанню некоректних змін уповноваженими користувачами (розподіл обов'язків); забезпечення внутрішньої та зовнішньої узгодженості (правильні транзакції).

Дискреційна модель являє собою визначені правила доступу суб'єктів системи до об'єктів. Такі правила зазвичай записані у вигляді матриці доступів. Класична дискреційна модель Харрісона – Руззо – Ульмана (ХРУ) складається з таких елементів (4.1):

$$\{O; S; M; R\}, \quad (4.1)$$

де O – множина об'єктів системи;
 S – множина суб'єктів системи, O – підмножина безлічі;
 R – множина прав доступу суб'єктів до об'єктів. Ці права передбачають виконання таких операцій володіння (own), запис (write), читання (read);
 M – матриця доступів, рядки якої відповідають суб'єктам, а стовпці – об'єктам.

Елементами матриці M є підмножини множини прав доступу.

Забезпечення захисту інформації у системі передбачає зміни в матриці доступів. Можливі зміни визначаються набором примітивних операторів.

Для довільних систем ХРУ завдання перевірки безпеки є алгоритмічно невиконуваним. Тому дискреційні моделі наповнюються обмеженнями, завдяки яким можна гарантувати безпеку моделі.

Щоб досягти зручності адміністрування, в модель включають такі елементи, як ролі та групи суб'єктів, організовують домени безпеки, які пов'язують із підмножиною множини об'єктів набори допустимих прав. У разі великої кількості суб'єктів поширенням прав доступу в такій системі управляти складно. Зменшення кількості контрольованих об'єктів

відбувається завдяки покладанню відповідальності за поширення доступу до об'єкта на суб'єкта, який є власником об'єкта [45].

Основою реалізації управління доступом за цієї моделі є аналіз ряду матриці доступу за зверненням «суб'єкт – об'єкт».

Перевагою зазначеної моделі та інших матричних моделей є наочність і гнучкість налаштувань політики доступу до об'єктів. Водночас головним недоліком є зайвий деталізований рівень опису відносин «суб'єкт – об'єкт», що призводить до підвищення складності адміністрування системи захисту інформації під час встановлення параметрів і їх підтримки в актуальному стані, особливо при включенні до схеми розмежування доступу нових елементів (об'єктів або суб'єктів, або ж і тих і інших одночасно), через що виникає ризик допущення помилок адміністрування системи інформаційної безпеки.

У разі значної чисельності користувачів традиційним підсистемам управління доступом необхідне адміністрування за допомогою об'єктно-орієнтованих рішень, завдяки яким можна дещо спростити цей процес. Це необхідний захід, оскільки кількість зв'язків пропорційна добутку чисельності користувачів на кількість об'єктів, що робить процес адміністрування надскладним завданням. Є кілька різновидів об'єктно-орієнтованих рішень, наприклад, рольове управління доступом, яке реалізується шляхом додання проміжних ролей користувачам, що дозволяє в різні проміжки часу мати різні права завдяки зміні ролі. Тобто один користувач може мати кілька ролей. У разі використання рольового доступу можна спростити процес адміністрування системи, оскільки збільшення його складності у разі зростання кількості користувачів відбувається значно повільніше. Це досягається завдяки абстрагуванню від конкретних видів і способів перевірки прав користувачів і встановленню зв'язків між ролями. Ролей у такому разі потрібно значно менше, ніж користувачів. Відповідно кількість зв'язків, які потрібно адмініструвати, стає пропорційною сумі, а не добутку кількості користувачів і об'єктів [62].

Модель Адепт-50 – одна з перших моделей безпеки, у якій розглядаються 4 групи об'єктів безпеки: користувачі, завдання, термінали та файли. Кожен об'єкт безпеки описується вектором (А, С, F, М), що включає такі параметри безпеки:

А – компетенція – елемент з набору впорядкованих універсальних положень безпеки, які включають можливі, апріорно задані в інформаційній системі характеристики об'єкта безпеки, наприклад, категорії конфіденційності об'єкта: не таємно, конфіденційно, таємно, цілком таємно;

С – категорія – рубрикатор (тематична класифікація). Рубрики є незалежними від рівня компетенції. Приклад набору рубрик: фінансова, політична, банківська тощо;

Е – повноваження – перелік користувачів, які мають право на доступ до окремого об'єкта;

М – режим – набір видів доступу, дозволених для певного об'єкта або здійснюваних об'єктом. Приклад: читати дані, записувати дані, виконати програму (виконання програм розуміється як породження активного компонента з певного об'єкта, як правило, виконуваного файлу) [16; 70].

Достатньо своєрідною є модель «MITER ATT & СК™», яка являє собою доступну в усьому світі базу знань про тактики та методи формування інформаційної політики, засновані на реальних спостереженнях. База знань ATT & СК використовується як підґрунтя для розробки конкретних моделей і методологій загроз для приватного сектора користувачів та уряду.

Ця модель передбачає використання матриці, яка формується на основі показників, таких як ступінь доступу, система реалізації програмних додатків, наполегливість, ескалація привілеїв, ухилення від захисту, доступ до перевірених даних, відкриття, додаткові дії, збір, управління та адміністрування, ексфільтрація, вплив тощо [76; 92].

Досить оригінальною моделлю захисту інформації є «модель алмазу» («Diamond Model»). Модель визначає політику інформаційної безпеки об'єкта на основі аналізу чотирьох ознак: зловмисника (супротивника), інформаційної інфраструктури, можливостей (здатностей персоналу) та об'єкта впливу (жертви) [64]. Зазначені елементи розташовані у формі ромба, що і визначає назву моделі, а також додаткові мета-функції для підтримки конструкцій вищого рівня, таких як пов'язування подій у потоки діяльності та подальше злиття подій потоків у групи інформаційної активності (рис. 4.9).

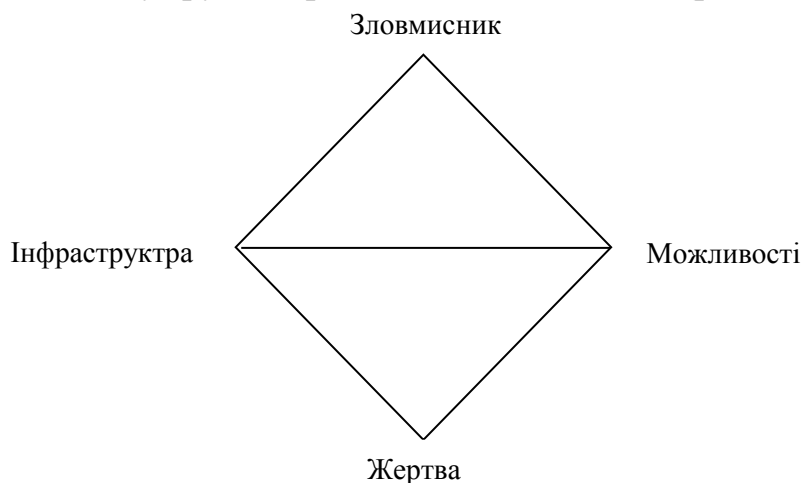


Рис. 4.9. Формування політики інформаційної безпеки на основі моделі «Алмаз» [92]

Ця модель ґрунтується на формальному методі, в рамках якого застосовуються наукові принципи аналізу вразливостей або загроз, методи їх вимірювання, встановлення достовірності та повторюваності, забезпечуючи комплексний метод синтезу та кореляції діяльності відносно забезпечення інформаційної безпеки об'єкта [92].

Ще однією незвичною моделлю формування політики інформаційної безпеки є застосування «піраміди болю» («The Pyramid of Pain») (рис. 4.10).



Рис. 4.10. Формування моделі захисту інформації на основі «Піраміди болю» [81; 92]

Аналітик у сфері інформаційної безпеки Д. Б'янка розробив методику під назвою «піраміда болю». В основі піраміди знаходяться хеш-коди. Файли, що мають відомі хеш-коди, легко визначаються, але також легко і замінюються зловмисником. Те саме стосується і IP-адрес, хоча при цьому потрібно трохи більше часу як для пошуку, так і для їх заміни зловмисником, тому вони займають дещо вищий сегмент піраміди. Домени потребують більших зусиль для їх зміни, мережні артефакти є ще складнішими і т. д. Найбільш цінні відомості – це тактика, методи та процедури захисту інформації, оскільки зловмисникові складно їх змінити. Їх виявлення часто є найбільш складною і трудомісткою частиною процесу, здебільшого тому, що потребує порівняння точок даних з різних наборів даних і створення зв'язків

насамперед там, де ці відносини не є очевидними.

Ефект цієї піраміди полягає в тому, що в процесі руху вгору по піраміді зловмисники витрачають більше ресурсів і часу на проникнення в інформаційну систему, що ускладнює цей процес і зменшує імовірність успіху. Кінцева мета «піраміди болю» полягає в тому, щоб змінюючись, інформаційна система стала настільки складною для проникнення, що зловмисникам довелося б відмовитися від своїх намірів.

На рис. 4.10 зображений взаємозв'язок між типами показників, які використовуються для виявлення діяльності порушника інформаційної безпеки, і ступінь «болю», який він їм заподіє.

В існуючій літературі акцентується увага на описі структури та змісту моделі захисту інформації, але зазвичай не описує детально процеси розробки такої моделі.

Зважаючи на відсутність настанов, розробники такої моделі часто використовують політику, розроблену іншими організаціями, доступні джерела або шаблони. Проте модель захисту інформації, отримана в результаті використання таких методів, не забезпечить належного рівня інформаційної безпеки підприємства, зокрема й агропродовольчої сфери [102].

Завдяки основним перевагам різень моделей захисту (рис. 4.11) можливо сформулювати найбільш оптимальну й ефективну модель захисту інформації.

Слід зазначити, що моделі захисту інформації, так само як і стандарти інформаційної безпеки, не є обов'язковими для впровадження не тільки тому, що їх потрібно періодично переглядати з метою максимально однозначного відображення в рамках реального об'єкта захисту, а й тому, що загалом їх потрібно застосовувати згідно із визначеними завданнями інформаційного захисту, цілями функціонування підприємства агропродовольчої сфери, його спеціалізацією та специфікацією, інформаційними загрозами та інформаційними ресурсами й активами, які потребують захисту і, безумовно, змінюються з часом.

Прийняття рішення про використання конкретної моделі також обумовлено вимогами зовнішніх процесів, які постачають інформацію для завдань або приймають дані, які є результатами роботи.

Водночас розглянуті моделі захисту інформації можливо застосовувати в процесі формування політики інформаційної безпеки аграрного підприємства або системи менеджменту інформаційної безпеки.

З метою забезпечення належного рівня інформаційної безпеки аналізованих підприємств агропродовольчої сфери запропоновано для реалізації модель, яка узагальнює позитивні надбання зазначених моделей захисту інформації та базується на концепції «глибинного захисту».

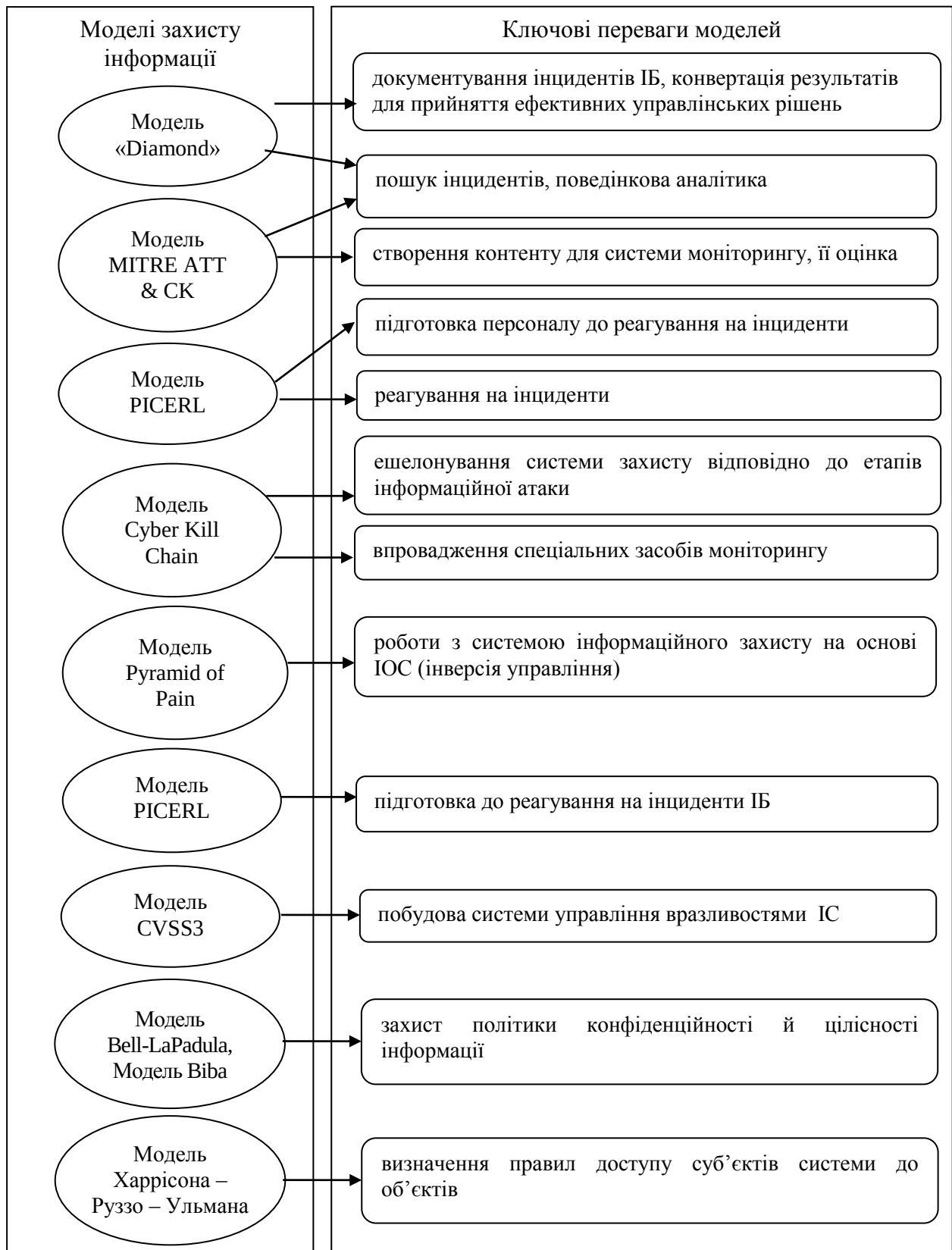


Рис. 4.11. Ключові переваги моделей захисту інформації на підприємствах [сформовано автором на основі 21; 42; 55; 62; 81; 82; 85; 88; 102]

Класичний вигляд моделі захисту інформації на основі концепції «глибинного захисту» відображений на рис. 4.12.



Рис. 4.12. Класична побудова моделі захисту інформації на основі концепції «глибинного захисту» [62; 80; 92; 102]

Концепція «глибинного захисту» походить від воєнної стратегії, яка прагне затримати наступ атаки завдяки розшаруванню військ, а не перемогти її однією сильною лінією оборони. Принцип протидії «глибинного захисту» відомий як простота в захисті, тобто, що занадто багато заходів безпеки можуть створити проблеми або прогалини, якими можуть скористатися зловмисники. Загалом «глибинний захист» полягає в забезпеченні захисту інформації на основі поетапного шарування захисних механізмів, оскільки багаторазові надмірні оборонні заходи, ефективні заходи моніторингу та контролю інформаційної безпеки або заходи нейтралізації загроз і вразливостей призводять лише до додаткових труднощів під час відбиття атак або нейтралізації наслідків.

Інформацію необхідно захищати протягом усього її життєвого циклу – від початкового створення даних до їх знищення. Тому кожен компонент моделі «глибинного захисту» повинен мати свої захисні методи для адекватного захисту інформації протягом усього її життєвого циклу. Захист у глибині означає розбудову та накладення заходів безпеки.

Концепція «глибинного захисту» полягає в тому, що механізми інформаційної безпеки розшаровані, і таким чином підвищують безпеку системи загалом. Якщо атака спричиняє збій одного механізму захисту, інші механізми все ще можуть забезпечити необхідний рівень безпечності для захисту системи [102]. Багаторівнева структура дозволяє створити високоефективний багаступеневий захист, який буде відповідати найсучаснішим вимогам.

Переважна більшість спеціалістів стверджує, що не варто використовувати готову модель «глибинного захисту», оскільки висока ймовірність її неефективності, наприклад, вона може виявитися надто складною і не буде враховувати специфіку роботи підприємства, для якого необхідна індивідуальна модель «глибокоешелонного захисту», а розробка «з нуля» може виявитися більш ефективною, ніж трансформація моделі іншого підприємства.

Для досліджуваних підприємств агропродовольчої сфери запропоновано застосовувати модель захисту інформації, яка базується на поєднанні концепції «глибинного захисту», що інтегрує ключові переваги вищерозглянутих моделей (Diamond, MITRE ATT & CK, PICERL, Cyber Kill Chain, Pyramid of Pain, PICERL, CVSS3, Bell-LaPadula, Biba, Харрісона – Руззо – Ульмана та інших) та концепції «mind map», яка як «карта розуму» дозволяє визначити наповнення кожного «шару» моделі «глибинного захисту» компонентами, які відповідатимуть потребі формування ефективної системи інформаційної безпеки підприємства.

На рис. 4.13 зображена пропонована модель формування політики інформаційної безпеки на основі концепції «глибинного захисту» у вигляді карти «mind map», яка впорядковує основні категорії як організаційного, так і технічного аспектів захисту та водночас враховує функціонал ключових елементів: людей, політику, моніторинг, показники безпеки та інше.

З метою ефективної імплементації пропонованої моделі захисту інформації на підприємствах агропродовольчої сфери охарактеризовано її основні складові. Політика інформаційної безпеки та процедури забезпечення інформаційного захисту передбачає перш за все те, що підприємству аграрної сфери потрібно визначити необхідні та доцільні положення міжнародних, вітчизняних галузевих стандартів і нормативів, політик, найкращих практик, які будуть використані для формування та реалізації політики інформаційної безпеки та методів, процедур і протоколів її забезпечення на конкретному підприємстві або в організації (рис. 4.14).

Окрім основних положень, політика інформаційної безпеки має передбачати сценарій, який дозволить кожному працівникові ознайомитись із особливостями захисту інформації, правилами та нормами інформаційної безпеки, а також передбачати алгоритм, відповідальних осіб за забезпечення ефективності діяльності системи менеджменту інформаційної безпеки та протоколи процедур реінжинірингу цієї системи в разі виникнення такої необхідності.

Щоб уникнути серйозних інцидентів інформаційної безпеки на рівні фізичної безпеки, потрібно однозначно ідентифікувати все, що фізично потрапляє на підприємство, починаючи з людей (особливо якщо вони не є

співробітниками) і закінчуючи технічними засобами. Для персоналу потрібно запровадити процеси ідентифікації та рольове управління доступом до інформації.

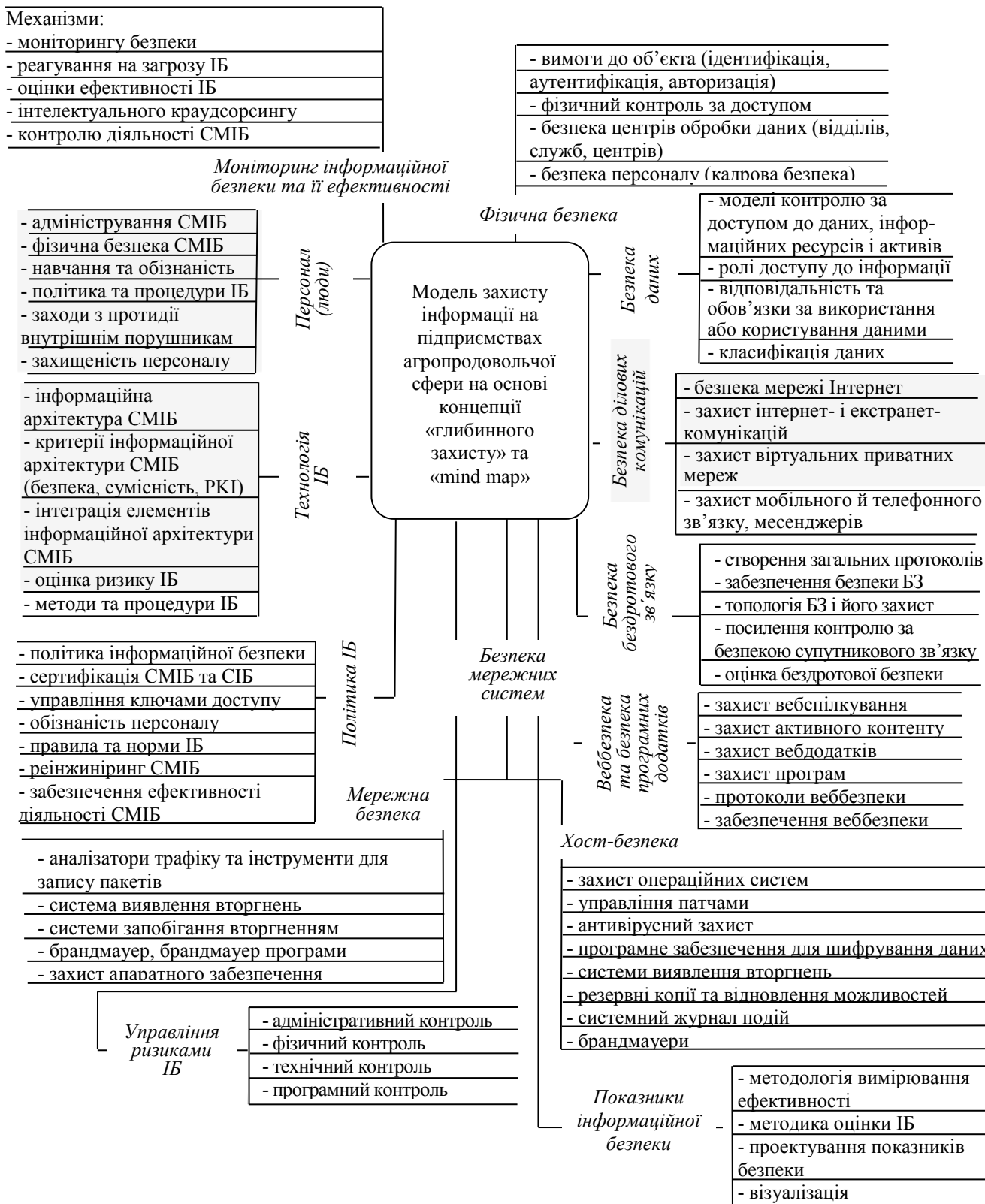


Рис. 4.13. Формування моделі захисту інформації підприємства агропродовольчої сфери на основі концепцій «глибинного захисту» та «mind map» [розроблено на основі 81; 102]

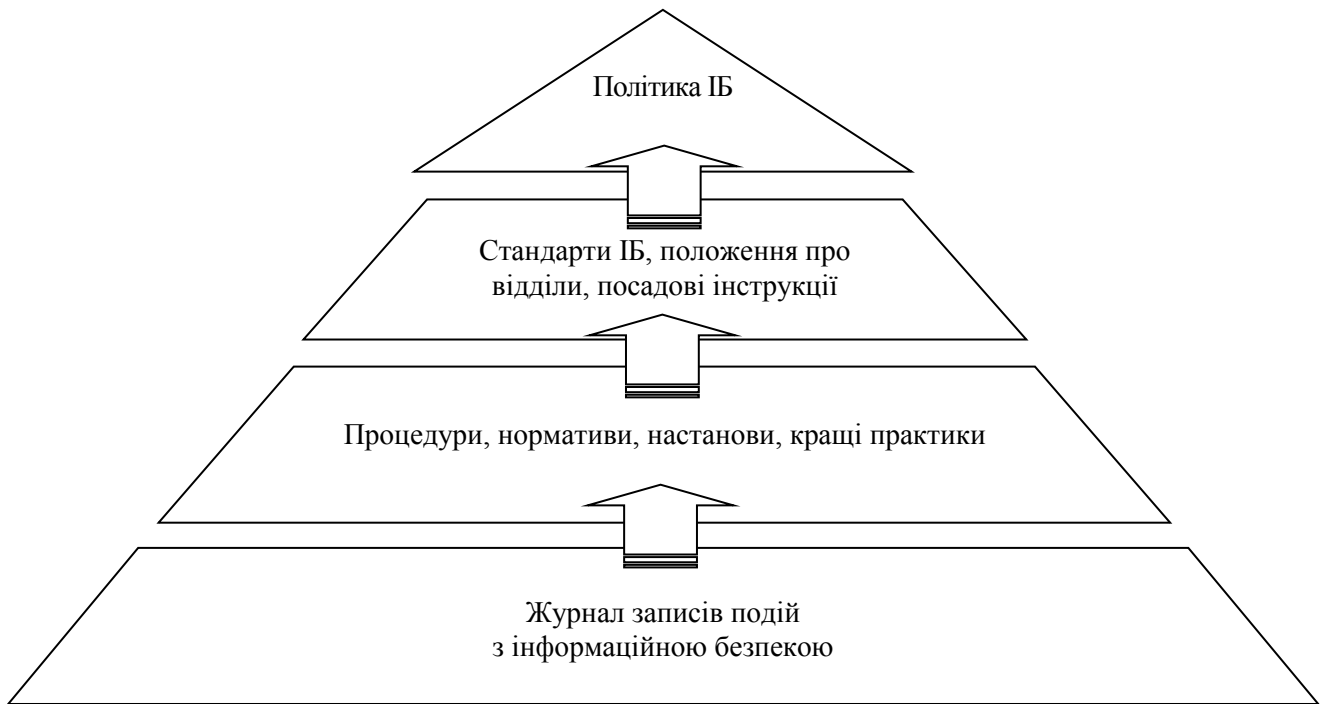


Рис. 4.14. Схема формування політики інформаційної безпеки та процедур забезпечення інформаційного захисту підприємства [авторська розробка]

Основними комунікаційними каналами підприємств агропродовольчої сфери залишаються внутрішні та зовнішні мережі, а їх захист є однією із головних умов забезпечення інформаційного захисту підприємства. Він передбачає як покриття мережної архітектури проти відомих і очевидних атак, так і забезпечення хост-безпеки.

Периметр мережного трафіку необхідно відфільтрувати й захистити за допомогою брандмауерів, механізмів виявлення вторгнень, ідентифікації зловмисних програм, блокувальних технологій, програм фільтрації небезпечного вмісту тощо. Захист хостів передбачає захист операційних систем, управління патчами, антивірусний захист, програмне забезпечення для шифрування даних, системи виявлення вторгнень, резервні копії та відновлення можливостей, системний журнал подій, використання брандмауерів тощо. У разі правильного налаштування цей рівень захищає інформаційні активи підприємств агропродовольчої сфери, дозволяючи лише ті дії, які необхідні для продовження ділових операцій.

Архітектура системи інформаційної безпеки залишається незавершеною без належної системи моніторингу та реєстрації. Операції з мережею та безпекою необхідно постійно контролювати щодо ознак можливого вторгнення. Ефективні сповіщення та сигнали тривоги можуть створюватися лише при належному здійсненні моніторингу засобів контролю. Зазначений рівень у межах пропонованої моделі захисту інформації, на відміну від її класичної версії, передбачає наявність системи моніторингу рівня

інформаційної безпеки, механізму реагування на загрозу інформаційній безпеці, прийнятної методики оцінки ефективності інформаційної безпеки та визначення способу імплементації системи інтелектуального краудсорсингу в процес адміністрування інформаційної безпеки та систем і видів контролю за діяльністю системи менеджменту інформаційної безпеки підприємства.

Оскільки більшість виробничих і управлінських бізнес-процесів у сільськогосподарській діяльності передбачають використання засобів Інтернету та технологій, які базуються на основі використання цих засобів, а також інших програмних додатків, то наступним видозміненим шаром моделі захисту інформації на основі концепції «глибинного захисту» – «Додатки, програмне забезпечення управління інформацією» є веббезпека та безпека програмних додатків. Хоча вебдодатки мають більшу кількість переваг, проте вони мають і деякі значні недоліки порівняно з настільними додатками, оскільки не запускаються безпосередньо з операційної системи, мають обмежений доступ до системних ресурсів, а отже, й ускладнюють процедури їх захисту. Як зазначалося вище, більшість програмних продуктів, які використовують підприємства агропродовольчої сфери, пов'язані з використанням інтернет-технологій (GPS, GIS, датчики для дистанційних вимірів і бортові датчики для приведення в дію різних частин машинного агрегату, безпілотні технології, датчик smartfirmer для точної посадки, робототехніка тощо), тому основу захисту на цьому шарі становлять захист вебспілкування, активного контенту, вебдодатків, програм і протоколи веббезпеки.

Основу запропонованої моделі, як і в класичній моделі «глибинного захисту», становить шар «захист даних». Проте, на відміну від класичної моделі, цей рівень захисту передбачає захист даних, інформації, інформаційних ресурсів та інформаційних активів, що було визначено основою захисту в системі менеджменту інформаційної безпеки. Такий захист у межах пропонованої моделі передбачає класифікацію даних, інформації, інформаційних ресурсів, наявність моделей контролю за доступом до даних, інформаційних ресурсів та активів (відповідно до аналогії з моделями Bell-LaPadula, Biba, Харрісона – Руззо – Ульмана), ролі доступу до інформації, визначення обов'язків та відповідальності за використання або користування даними.

Водночас запропонована модель включає інші компоненти, які посилюють рівні захисту, з-поміж яких технологія інформаційної безпеки, персонал, безпека ділових комунікацій, безпека бездротового зв'язку, управління ризиками інформаційною безпекою, показники інформаційної безпеки – як ключові компоненти забезпечення інформаційного захисту.

Одним із пропонованих компонентів, що посилюватиме захист інформації в межах пропонованої моделі «глибинного захисту», є концепція інформаційної безпеки, яку пропонується визначити як окремий рівень, що включатиме інформаційну архітектуру системи інформаційної безпеки, критерії інформаційної архітектури цієї системи, тобто її якісні характеристики та компетентності персоналу, який здійснює управління цією системою, інтеграцію елементів інформаційної архітектури цієї системи в інформаційне середовище підприємства агропродовольчої сфери та в загальну систему управління підприємством, методику оцінки інформаційного ризику та відповідно методи й процедури забезпечення інформаційної безпеки.

Наступний компонент моделі – персонал, який, як було визначено в процесі дослідження, є основою забезпечення інформаційної безпеки будь-якого суб'єкта. Його теж пропонується виокремити в самостійний рівень, головними елементами якого стануть: процес адміністрування інформаційної безпеки, забезпечення фізичної безпеки працівникам системи менеджменту інформаційної безпеки, навчання та обізнаність працівників аграрного суб'єкта господарювання, формування політики інформаційної безпеки, захищеність персоналу та заходи протидії внутрішнім порушникам.

В умовах автоматизації виробничих бізнес-процесів у сільському господарстві рівень моделі «безпеки мережних систем» пропонується посилити такими двома складовими, як:

безпека ділових комунікацій, що передбачає захист інтернет- і екстранет-комунікацій, забезпечення безперебійного та безпечного доступу та роботи в мережі Інтернет, захист віртуальних приватних мереж і обов'язковий захист мобільного й телефонного зв'язку, а також месенджерів;

безпека бездротового зв'язку, що передбачає топологію бездротового зв'язку, забезпечення оптимального рівня його безпеки, створення загальних протоколів його захисту, посилення контролю за безпекою супутникового зв'язку та оцінку бездротової безпеки.

Будь-яка модель захисту інформації потребує оцінки її рівня. З цією метою до складу пропонованої моделі включають модуль показників інформаційної безпеки, який передбачатиме визначення методології вимірювання ефективності діяльності цієї моделі, методику оцінки рівня інформаційної безпеки, проектування показників інформаційної безпеки та візуалізацію результатів для прийняття ефективних управлінських рішень.

Ще одним модулем, який пропонується ввести до складу моделі, є управління ризиками інформаційної безпеки, які мають передбачати захист на чотирьох основних рівнях: адміністративному, програмному, технічному та фізичному (рис. 4.15).

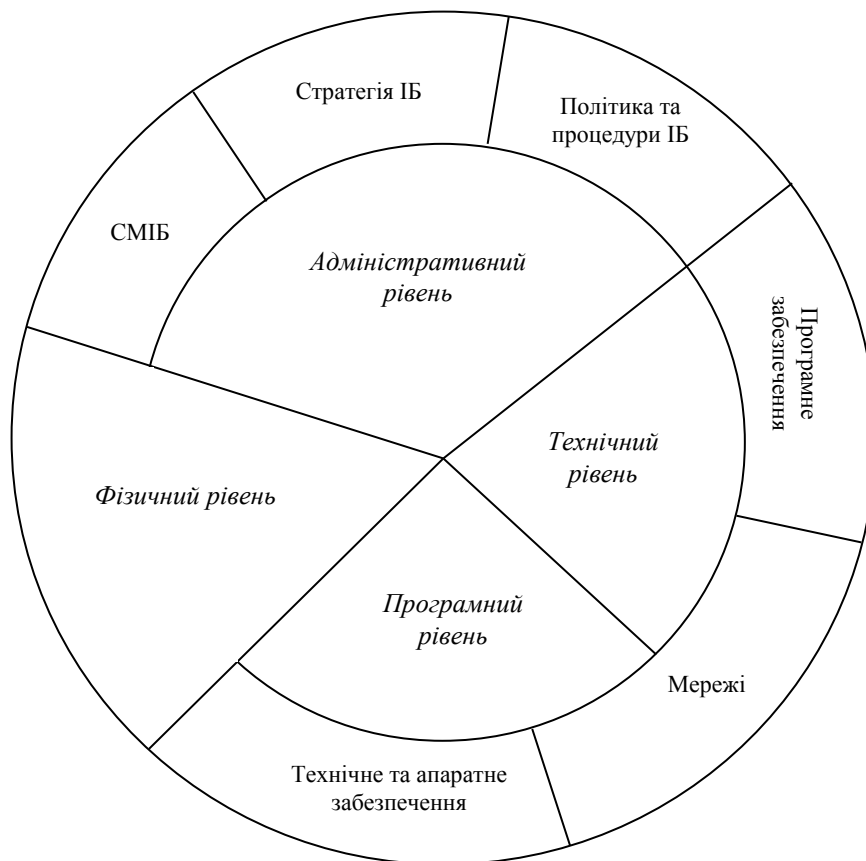


Рис. 4.15. Рівні управління ризиками інформаційної безпеки моделі захисту інформації підприємства агропродовольчої сфери на основі концепцій «глибинного захисту» та «mind map» [авторська розробка]

Фізичний рівень визначає заходи щодо обмеження фізичного доступу до ІТ-інфраструктури неавторизованих осіб, що передбачає наявність охорони, систем СКУД, камер відеоспостереження, сигналізації, телекомунікаційних шаф тощо.

Технічний рівень включає всі хардверні засоби захисту інформації, а також засоби, які призначені для контролю за мережним доступом до об'єктів інформаційної системи.

Програмний рівень передбачає програмні продукти та додатки, спрямовані на забезпечення інформаційного захисту, міжмережний екран, засоби антивірусного захисту робочих станцій, проксі-сервери, системи аутентифікації та авторизації тощо.

Адміністративний рівень включає всі політики та процедури інформаційної безпеки, стратегію інформаційної безпеки, положення про систему менеджменту інформаційної безпеки, документаційне забезпечення, що регулює управління захистом, розподілом і обробкою критичної інформації, використання програмних і технічних засобів, а також взаємодію співробітників з інформаційною системою, сторонніми організаціями та

іншими зовнішніми суб'єктами.

Усі перераховані види та заходи управління ризиками інформаційної безпеки забезпечують основу захисних механізмів, призначених для захисту інформаційного середовища підприємства від неправомірного втручання в процеси їх функціонування і несанкціонованого доступу до інформації зокрема, та передбачають обов'язковий набір процедур: ідентифікацію, аутентифікацію користувачів інформаційної системи; розмежування доступу користувачів до ресурсів системи і авторизацію (привласнення повноважень користувачем); реєстрацію та оперативне оповіщення про події, що відбуваються в системі; криптографічне закриття (шифрування) даних, що зберігаються і передаються каналами зв'язку; контроль за цілісністю та автентичністю (справжністю авторства) даних; резервування та створення резервних копій; фільтрацію трафіку і трансляцію адрес; виявлення вторгнень (атак) тощо.

Враховуючи пропоновані модифікації моделі захисту інформації на основі «глибинного захисту» для підприємств агропродовольчої сфери, вона матиме вигляд, відображений на рис. 4.16.



Рис. 4.16. Модифікована модель захисту інформації підприємства агропродовольчої сфери на основі концепції «глибинного захисту» [авторська розробка]

Хоча концепція «глибинного захисту» при формуванні моделі інформаційної безпеки передбачає створення і реалізацію вичерпного плану захисту, проте хибно вважати, що застосовування цієї концепції здійснюється за принципом «все або нічого». Насправді, для досягнення швидких результатів з мінімальними витратами доцільно дотримуватися покрокового підходу під час її побудови.

Зазначена модель захисту інформації матиме ряд переваг, таких як:

диверсифікація: кожен шар моделі має різноманітні механізми, методи, процедури, об'єкти, що дозволяє оптимізувати та налаштувати захист інформації під потреби кожного суб'єкта агропродовольчої сфери та підвищити рівень інформаційної безпеки;

практична апробація: модель випробувана та перевірена підприємствами різних країн, галузей, сфер діяльності;

масштабованість і прийнятність: цей багат шаровий підхід настільки гнучкий, що може легко адаптуватися до нових загроз шляхом включення нового рівня безпеки. Також цю модель можна застосовувати як на малих, так і на великих підприємствах;

комплексність та інтегрованість: модель об'єднує переваги багатьох моделей інформаційного захисту та має адаптивний механізм інтеграції в систему інформаційної безпеки різних за масштабом і напрямом діяльності підприємств.

Проаналізовані моделі захисту інформації загалом призводять до результатів, які у багатьох відношеннях корелюють із тим, на що пропонується звернути увагу при використанні концепцій «глибинного захисту» та «mind map». Різниця полягає в тому, що в моделі політики інформаційної безпеки на основі концепції «глибинного захисту» увага зосереджується на всіх рівнях і напрямках захисту інформаційних ресурсів, а використання «mind map» дозволяє визначити та обрати той набір процедур, правил та інструментів, які забезпечать реалізацію найбільш відповідної та оптимальної політики інформаційної безпеки.

Список використаних джерел до розділу 4

1. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. Дата оновлення: 21.02.2019. URL: <https://zakon.rada.gov.ua/laws/show/254>.
2. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. *Верховна Рада України*. URL <http://zakon5.rada.gov.ua/laws/show/80/94-вр>

3. Про захист персональних даних : Закон України від 1 червня 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34.

4. Про прийняття за основу проекту Закону України Про Концепцію державної інформаційної політики : Постанова Верховної Ради України від 11.01.2011 № 2897-VI. URL: <http://zakon1.rada.gov.ua>.

5. Про затвердження Концепції технічного захисту інформації в Україні: постанова Кабінету Міністрів України від 08.10.1997 р. № 1126, із змінами. URL: <https://zakon.rada.gov.ua/laws/show/1126-97-п>.

6. Європейські стандарти безпеки ISO 15408 (Common Criteria for Information Technology Security Evaluation. URL: <https://www.sans.org/reading-room/whitepapers/standards/common-criteria-iso-iec-15408-insight-thoughts-questions-issues-545>.

7. Канадські критерії безпеки комп'ютерних систем (Canadian Trusted Computer Product Evaluation Criteria). URL: https://www.researchgate.net/publication/3506169_The_Canadian_Trusted_Computer_Product_Evaluation_Criteria_CTCPEC.

8. Критерії безпеки комп'ютерних систем (Trusted Computer System Evaluation Criteria). URL: <https://www.cs.clemson.edu/course/cpsc420/material/Evaluation/TCSEC.pdf>.

9. Критерії оцінки безпеки інформаційних технологій (Information Technology Security Evaluation Criteria). URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile.

10. Стандарты информационной безопасности: государственные и международные. URL: <http://tvoi.biz/biznes/informatsionnaya-bezopasnost/prakticheskaya-polza-standartov-info.html>.

11. ISO 17799: Code of Practice for Information Security Management. URL: http://www.iso.org/iso/catalogue_detail?csnumber=39612.

12. ISO/IEC 27000:2014. Information technology – Security techniques – Information security management systems – Overview and vocabulary. URL: <https://www.iso.org/standard/63411.html>.

13. ISO/IEC 27003 : 2010 Information technology – Security techniques – Information security management system implementation guidance. URL: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27003:ed-1:v1:en>.

14. Алетдинова А. А. Инновационное развитие аграрного сектора на основе цифровизации и создания технологических платформ. *Инновационный электронный научный журнал*. 2017. № 4 (33). URL: <http://www.innov.ru/science/tech/innovatsionnoe-razvitie-agrarnogo-s/>.

15. Андрианов В. В., Зефиоров С. Л., Голованов В. Б., Голдуев Н. А.

Обеспечение информационной безопасности бизнеса : 2-е издание, переработанное и дополненное. URL: <https://pqm-online.com/assets/files/lib/books/andrianov.pdf>.

16. Богомолов С. А. Модели типовых политик безопасности. 2016. URL: <https://infourok.ru/lekcija-po-zaschite-informacii-modeli-bezopasnosti-927637.html>

17. Большаков С. Н., Лескова И. В., Большакова Ю. М. Цифровая экономика как составляющая технологической платформы государственной политики и управления. *Вопросы управления*. 2017. № 1 (25). С. 64–70.

18. Висоцький В. В. Аутсорсинг як технологія менеджменту інформаційної безпеки підприємства. *Вісник Хмельницького національного університету*. 2010. № 2, Т. 3. С. 62–64.

19. Воробьев А. И., Колбанёв М. О. Инфокоммуникация и архитектура цифровой экономики. URL: https://www.alley-science.ru/domains_data/files/024April18/INFOKOMMUNIKACIYa%20I%20ARNITEKTURA%20CIFROVOY%20EKONOMIKI.pdf.

20. Гатчин Ю. А., Климова Е. В. Основы информационной безопасности: учеб. пособие. СПб : СПбГУ ИТМО, 2009. 84 с.

21. Гладких А. А., Дементьев В. Е. Базовые принципы информационной безопасности вычислительных сетей : учебное пособие для студентов. Ульяновск : УлГТУ, 2009. 156 с.

22. Доронина Ю. В. Реинжиниринг информационных систем : монографія. Издательство «Спутник +», 2015. 170 с.

23. Доронина Ю. В. Реинжиниринг мониторинговых информационных систем циклического типа. *Східно-європейський журнал передових технологій*. 2012. № 1 / 2 (55). С. 12–14.

24. Дячков Д. В. Комплексна система інформаційної безпеки. *Менеджмент ХХІ століття : глобалізаційні виклики*: матер. II Міжн. наук.-практ. конф., 19 травня 2018 р. Полтава : ПП «Астроя», 2018. С. 243–246.

25. Дячков Д. В. Краудсорсинг як сучасна технологія управління натовпом. *Проблеми управління економічною безпекою підприємства, регіону, країни* : матер. Міжнар. наук.-практ. інтернет-конф., 13 травня 2015 р. Полтава : ПолтНТУ, 2015. С. 113–114.

26. Дячков Д. В. Нейронні мережі в управлінні організацією. *67-а наукова конференція професорів, викладачів, наукових працівників, аспірантів та студентів університету*, 02 квітня – 22 травня 2015 р. Полтава : ПолтНТУ, 2015. Т. 2. С. 214–216.

27. Дячков Д. В. Основи формування системи менеджменту інформаційної безпеки. *Управління ресурсним забезпеченням господарської*

діяльності підприємств реального сектору економіки : матер. Всеукр. наук.-практ. Інтернет-конф., 28 жовтня 2016 р. Полтава : РВВ ПДАА, 2016. С. 34–36.

28. Дячков Д. В. Особливості захисту локального та «хмарного» ІТ-оточення сучасної організації. *Економіка і культура України в світових глобалізаційних процесах: позиціювання і реалії* : тези доповідей III Міжн. наук.-практ. конф., 21-22 березня 2018 р. К. : Вид. центр КНУКіМ., 2018. Ч. 3. С. 247–250.

29. Дячков Д. В. Формування моделі політики інформаційної безпеки на основі концепцій «глибинного захисту». *Підприємництво і торгівля : збірник наукових праць*. Львів : Видавництво Львівського торговельно-економічного університету, 2019. Вип. 25. С. 116–122.

30. Дячков Д. В., Батура В. Ю., Сокирко І. А. Формування організаційно-економічного механізму управління економічною безпекою підприємства. *Вчені записки ТНУ імені В. І. Вернадського. Серія : Економіка та управління*. К. : ВД «Гельветика», 2019. Т. 30 (69), № 5, Ч. 2. С. 31–36.

31. Дячков Д. В., Вовк М. О. Економічна сутність реструктуризації підприємства. *Економічний розвиток : теорія, методологія, управління* : матер. Міжн. наук.-практ. конф., 26–28 листопада 2018 р. Прага, 2018. С. 20–26.

32. Дячков Д. В., Вовк М. О. Принципи реструктуризації підприємств в умовах глобалізації них. *Нові виклики для аграрного сектору України в умовах глобалізації* : матер. Міжн. наук.-практ. конф., 14 листопада 2018 р. К. : НУБіП України, 2018. С. 90–92.

33. Дячков Д. В., Вовк М. О. Реструктуризація підприємства як метод конкурентної боротьби в умовах трансформаційних змін. *Управління розвитком соціально-економічних систем* : матер. Міжн. наук.-практ. конф., 08–09 листопада 2018 р. Харків : ХНТУСГ, 2018. С. 44–46.

34. Дячков Д. В., Кіт В. В., Паскаль А. В. Технологія забезпечення інформаційної безпеки підприємства. *Економічний форум*. Луцьк : РВВ Луцького НТУ, 2018. № 4. С. 157–162.

35. Дячков Д. В., Коршикова Н. В. Крауд-концепція як ефективний інструмент управління. *Економіка і організація управління*. 2014. 1 (17) – 2 (18). 2014. С. 333–338.

36. Дячков Д. В., Маховка В. М. Інформаційна складова управління туристичними підприємствами як рушійний фактор їх розвитку. *Стратегічні перспективи туристичної та готельно-ресторанної індустрії в Україні : теорія, практика та інновації розвитку* : матер. Всеукр. наук.-практ. інтернет-конф., 30 жовтня 2015 р. Умань, 2015. С. 77–78.

37. Дячков Д. В., Навагіна А. М., Рогова В. В. Assessment center – сучасний метод управління персоналом підприємства. *Менеджмент у*

XXI сторіччя : методологія і практика : матер. III Міжнар. наук.-практ. конф., 14–15 травня 2015 р. Полтава : В-во «Сімон», 2015. С. 193–195.

38. Дячков Д. В., Простак О. С., Тенянюк А. О. Напрями підвищення ефективності управління інноваціями на сільськогосподарських підприємствах. *Економічний форум*. Луцьк : РВВ Луцького НТУ, 2019. № 3. С. 122–129.

39. Зегджа Д. П., Ивашко А. М. Основы безопасности информационных систем. М. : Горячая линия – Телеком, 2000. 452 с.

40. Зиндер Е. З. Бизнес-реинжиниринг и технологии системного проектирования. Центр Информационных Технологий, 1996. 236 с.

41. Зянько В. В., Єпіфанова І. Ю., Зянько В. В. Інноваційна діяльність підприємств та її фінансове забезпечення в умовах трансформаційних змін економіки України : монографія. Вінниця : ВНТУ, 2015. 168 с.

42. Иода Е. В. О концепции открытых инноваций. *Социально-экономические явления и процессы*. № 8. С. 96–101.

43. Киристюк С. В. Диверсифікація економічної діяльності агровиробників: деякі висновки з досвіду ЄС. *Економіка і суспільство*. 2017. Вип. № 12. С. 44–51.

44. Князюк Н. Ф., Кицул И. С. Моделирование системы менеджмента информационной безопасности медицинской организации. *Врач и информационные технологии*. 2015. № 1. С. 62–70.

45. Кубышкин А. С. Разработка модели разграничения прав доступа для автоматизированных систем технологического управления. *Вестник НГУ. Серия : Информационные технологии*. 2012. Т. 10, Вип. 3. URL: <https://nsu.ru/xmlui/bitstream/handle/nsu/238/03.pdf>.

46. Куканова Н. Сертификация системы управления ИБ обеспечит эффективное управление информационными рисками. *Cnews. Аналитика*. URL: <https://cnews.ru/reviews/free/security2007/articles/certification.shtml>.

47. Лагун А., Кухарська Н. Ризики інформаційної безпеки IT-підприємства. URL: http://www.google.com.ua/url?url=http://sci.ldubgd.edu.ua:8080/bitstream/handle/123456789/750/11.doc%3Fsequence%3D1%26isAllowed%3Dy&rct=j&q=&esrc=s&sa=U&ved=0ahUKEwjz_823xfrPAhVB2SwKHbpaA5wQFggZMAE&usg=AFQjCNGIfE5rDW5CCFrQNLL5Ha42UVvO3g.

48. Литвинская О. С., Сальников И.И. Обобщённая структура принятия решения для метода выбора средств реализации проектируемой информационной технической системы. *«Искусственный интеллект»*. Пенза : ПГТУ, 2010. № 4. С. 404–414.

49. Лихачев Е. Ф. Краудсорсинг, как новое явление в экономике. Его социоинновационная природа и классификация. *Интернет-журнал «Наукovedение»*. 2016. №6. Том 8. URL: <http://naukovedenie.ru/PDF/76EVN116.pdf>

50. Маркіна І. А., Дячков Д. В. Основи формування системи менеджменту інформаційної безпеки підприємства. *Проблеми і перспективи розвитку підприємництва* : зб. наук. пр. Харківського національного автомобільно-дорожнього університету. Харків : ХНАДУ, 2016. № 3 (14), Т. 1. С. 80–88.

51. Маркіна І. А., Дячков Д. В. Організаційні засади створення віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу. *Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка : Економічні науки*. Вип. 202. С. 450–461.

52. Маркіна І. А., Дячков Д. В. Реінжиніринг бізнес-процесів маркетингової сфери промислових підприємств. *Технологія вдосконалення інформаційної безпеки на основі процесів гнучкого реінжинірингу* : монографія / за заг. ред. д. е. н., проф. Л. М. Таранюка, Суми : СНАУ, 2018. С. 176–183.

53. Марченко О. С. Інтелектуальний краудсорсинг як категорія інформаційного суспільства. *Strategiczne pytania światowej nauki 2013: Materiały IX Międzynarodowej naukowo-praktycznej konferencji. Przemysł: Nauka i studia, 2013. Ekonomiczne nauki*. Vol. 8. P. 51–53.

54. Мельник М. О., Нікітін Г. Д., Мезенцева К. О. Аналіз побудови моделі політики інформаційної безпеки підприємства. *Системи обробки інформації*. 2017. Вип. 2 (148). С. 126–128.

55. Милославская Н. Г., Толстой А. И. Интрасети: доступ в Internet, защита : учеб. пособие для вузов. М. : ЮНИТИ-ДАНА, 2000. 527 с.

56. Мингалева Ж. А. Формирование эффективных бизнес-моделей открытых инноваций на примере Apple, Nintendo, Nokia. *Инновации*. 2010. № 7. С. 18–20.

57. Минзов А. С., Невский А. Ю., Баронов О. Ю. Информационная безопасность в цифровой экономике. *ИТНОУ : информационные технологии в науке, образовании и управлении*. 2018. № 3 (7). С. 52–59.

58. Моисеев А. И., Жмуров Д. Б. Информационная безопасность распределённых информационных систем : учеб. Самара : Изд-во Самар. гос. аэрокосм. ун-та, 2013. 180 с.

59. Огневцев С. Б. Концепция цифровой платформы агропромышленного комплекса. *Международный сельскохозяйственный журнал*. 2018. № 2. С. 16–22.

60. Остапов С. Е., Євсєєв С. П., Король О. Г. Технології захисту інформації : навч. посіб. Х. : ХНЕУ, 2013. 476 с.

61. Петров А. А. Компьютерная безопасность. Криптографические

методы защиты информации. М. : ДМК, 2000. 448 с.

62. Петров Ю. К. JAM-инструментальное средство разработки приложений в информационных системах архитектуры «клиент / сервер», построенных на базе PCУБД. CitForum. «СУБД», 1995. URL: <http://citforum.ru/database/kbd96/612.shtml>.

63. Раунио М., Нордлинг Н., Каутонен М. Платформы открытых инноваций как инструмент «треугольника знаний» : опыт Финляндии. *Форсайт*. 2018. Т. 12. № 2. С. 62–76.

64. Ревнивых А. В., Федотов А. М. Обзор политик информационной безопасности. *Вестник НГУ. Серия : Информационные технологии*. 2012. № 3. URL: <https://cyberleninka.ru/article/n/obzor-politik-informatsionnoy-bezopasnosti>.

65. Резник А. Развивающиеся системы. *Knowledge-dialogue-solutions: International conference*. 2007. URL: <http://www.foibg.com/conf/ITA2007/KDS2007/PDF/KDS07-Reznik1.pdf>.

66. Ромака В. А., Корж Р. О., Гарасим Ю. Р. Менеджмент у сфері захисту інформації. Львів : ЗУКЦ, 2013. 462 с.

67. Самойленко А. Бесплатные серверные платформы виртуализации. URL: <https://www.ixbt.com/cm/virtualization-servers-free.shtml>

68. Смертенко П. С., Чернишев Л. І., Білан І. І. Кластери і технологічні платформи як механізми розвитку економіки України. *Вісник Національної академії наук України*. 2014. № 3. С. 67–76.

69. Соколов А. Н. Безопасность информационного пространства : сборник трудов XIII Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных. Челябинск : Издательский центр ЮУрГУ, 2015. 246 с.

70. Степанов В. Ю. Інформаційна безпека як складова державної інформаційної політики. *Державне будівництво*. 2016. № 2. URL: <http://www.kbuara.kharkov.ua/e-book/db/2016-2/doc/1/02.pdf>.

71. Стырин Е. М., Дмитриева Н. Е., Синятуллина Л. Х. Государственные цифровые платформы : от концепта к реализации. *Вопросы государственного и муниципального управления*. 2019. № 4. С. 31–60.

72. Схиртладзе А. Основные принципы и приемы реинжиниринга бизнес-процессов. Центр дистанционного образования «Элитариум». 2014. URL: <https://www.cfin.ru/management/strategy/change/foundations.shtml>.

73. Тельнов Ю. Ф. Реинжиниринг бизнес-процессов : компонентная методология. Финансы и статистика, 2004. 320 с.

74. Унижаев Н. В. Модель формирования или реинжиниринга принципов системы обеспечения экономической безопасности организации.

Вестник университета «Экономика: проблемы, решения и перспективы». 2016. № 3. С. 107–112.

75. Хусаинова А. В. Перспективы использования краудсорсинговой технологии управления в сельском хозяйстве. *Вестник АПК Верхневолжья. Трибуна молодых ученых*. 2014. № 4 (28). С. 89–93.

76. Чуруброва С. М. Політика інформаційної безпеки в системах інформаційно-аналітичного забезпечення підтримки прийняття організаційних рішень. *Проблеми програмування*. 2016. № 4. С. 97–103.

77. Шабанов А. П. Инновационное управление цифровыми платформами в экономике знаний. *Системы управления, связи и безопасности*. 2018. № 3. С. 106–135.

78. Яковлев Г. О., Батетников И. А. Обеспечение безопасности сторонних компонентов веб приложений. *Вестник науки и образования*. 2019. № 9-2 (63). С. 6–9.

79. Ярмоленко Ю. О. Формування економічного механізму сталого розвитку аграрного виробництва в умовах цифровізації : монографія. Київ : ТОВ «Сік груп Україна», 2018. 328 с.

80. Ярочкин В. И. Служба безопасности коммерческого предприятия. М. : Ось-89, 1995. 144 с.

81. Caballero A. Information security essentials for it managers : protecting mission-critical systems. Syngress, 2013. URL: https://booksite.elsevier.com/samplechapters/9781597495332/02~Chapter_1.pdf.

82. Davenport T. H. Process innovation: reengineering work. Through information technology. Boston : Harvard Business School Press, 1993. 352 p.

83. Diachkov D., Babich O., Reutska V. International problems of management and leadership. *International problems of management and leadership* : International scientific and practical conference of students and young scientists, December 1st, 2017. Lutsk, 2018. P. 9–11.

84. Diachkov D., Potapiuk I. Usage of social networks in modern business environment. *Information technologies and management 2016* : the 14th International scientific conference. Riga, 2016. P. 157–158.

85. Hammer M. Reengineering work : Don't automate, obliterate. *Harvard Business Review*. 1990. P. 104–112. URL: <https://maaw.info/ArticleSummaries/ArtSumHammer1990.htm>.

86. Jacobson I., Ericsson M., Jacobson A. The object advantage. Business process reengineering with object technology. N-Y : Addison-Wesley Publishing Company, 1995. 368 p.

87. Kaušpadienė L. Information security management framework for small and medium enterprise : doctoral diss. / Technological sciences, informatics

engineering. Vilnius, 2019. 140 p.

88. Shamim A., Fayyaz B., Balakrishnan V. Layered defense in Depth Model for IT organizations. *Innovations in Engineering and Technology*: 2nd International Conference (ICCET'2014), 19-20 September, 2014. 2014. Penang : Malaysia. URL: http://iieng.org/images/proceedings_pdf/8285E0914047.pdf.

89. Державна служба спеціального зв'язку та захисту інформації України. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=92368&cat_id=48306.

90. Європейські технологічні платформи та створення платформ в Україні. URL: <http://cstei.lviv.ua/ua/item/719>.

91. Инсайдерские угрозы безопасности. URL: http://www.perimetrix.ru/downloads/rp/PTX_Insider_Security_Threats_in_Russia_2014.pdf.

92. Модели в информационной безопасности. URL: <https://habr.com/ru/post/467269/>.

93. Система помощи принятия решений для аграриев. URL: <https://agplatform.ru/#partners>.

94. Сільське, лісове та рибне господарство. *Державна служба статистики України*: веб-сайт. URL: http://www.ukrstat.gov.ua/druk/publicat/kat_u/publ7_u.htm.

95. Что такое цифровая платформа? URL: https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2017/09_Tashkent/Presentations/ITU%20Workshop%2019.09%20-%20Nikolay%20Kovtun%20presentation%203.pdf.

96. Формальные модели безопасности управления доступом. Модель Биба, Белла-ЛаПадулы. URL: https://www.olifer.co.uk/new_rus/CN-5ed/cn5-additions/formal-models.htm#_ftn1.

97. Офіційний сайт : Agravery. URL: <https://agravery.com>.

98. Офіційний сайт : AgroPortal. URL: <http://agroportal.ua>.

99. Офіційний сайт : Landlord. URL: <https://landlord.ua>.

100. Офіційний сайт : Latifundist. URL: <https://latifundist.com>.

101. Офіційний сайт : ProAgro. URL: <http://www.proagro.com.ua>.

102. Defense in Depth : A Practical Strategy for Achieving Information Assurance in Today's Highly Networked Environments. National Security Agency, Information Assurance Solutions Group-STE 6737.

103. Ernst & Young. Британская аудиторско-консалтинговая компания. URL: <http://www.ey.com/ua/uk/home>.

104. Perimetrix. URL: <http://www.perimetrix.com/>.

РОЗДІЛ 5

СТРАТЕГІЧНІ НАПРЯМИ ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ АГРОПРОДОВОЛЬЧОЇ СФЕРИ УКРАЇНИ

5.1. Розробка стратегій управління інформаційною безпекою підприємств агропродовольчої сфери України

У сучасних умовах розвитку світових ринків ключовим фактором, який визначає конкурентоспроможність підприємства, виступає наявність у нього унікального інформаційного ресурсу. Унікальність його полягає в тому, що він відображає специфіку саме цього конкретного підприємства. З розвитком суспільства і подальшою його трансформацією в суспільство інформаційне, із переходом від національних економік в економіки цифрові і, зрештою, з їх інтеграцією, інформаційний ресурс стає самим головним фактором впливу на соціальноекономічний і політичний розвиток суспільства. Боротьба за володіння інформацією конкурента стає пріоритетною. Для забезпечення успіху в цій війні розробляються спеціальні інформаційно-комунікаційні технології, які нерідко, використовуються як стратегії інформаційної діяльності. Створюючи системи захисту на підприємстві, необхідно враховувати, що, по-перше, для ефективного захисту інформаційних ресурсів потрібна реалізація цілої низки різноманітних заходів, які можна розподілити на три групи: юридичні, організаційно-економічні й технологічні. По-друге, хоча розробкою заходів у кожній із трьох груп повинні займатися фахівці відповідних галузей знань, які застосовують свої способи і методи для досягнення заданих цілей, успіх значною мірою буде залежати від того, наскільки в рамках системного підходу вдасться визначити і реалізувати взаємні зв'язки між відповідними визначеннями, принципами, способами і механізмами захисту.

Сучасне аграрне підприємство не може існувати без чітко сформованої та деталізованої стратегії. Основне завдання розробки стратегії полягає в пошуку способів подолання конкуренції на ринку, забезпеченні високих темпів економічного розвитку підприємства. Водночас розвиток інформаційних технологій і пов'язаний із ним процес цифровізації відкривають для сучасних підприємств значні можливості оптимізації бізнесу, підвищення конкурентоспроможності, ефективності та швидкості прийняття управлінських рішень тощо. Проте є й інший бік медалі, коли з новими

можливостями з'являються і нові не повністю вивчені ризики, пов'язані з інформаційною безпекою. Тому забезпечення інформаційної безпеки аграрних підприємств в умовах швидкої зміни факторів зовнішнього середовища є важливою передумовою їх ефективного функціонування, а процес формування стратегії бізнесу суб'єктів агропродовольчої сфери обґрунтовує необхідність інтеграції стратегії їх інформаційної безпеки. В умовах глобалізації та інформатизації соціально-економічних відносин процеси забезпечення безпеки перетворюються в один із найважливіших елементів підтримки бізнесу. Проте увага фахівців у сфері інформаційної безпеки, ІТ-безпеки та кібербезпеки переважно спрямована на формування політики інформаційної безпеки, визначення рівня інформаційної безпеки та заходів щодо відвернення кібератак, використання новітніх технічних засобів і впровадження програмних продуктів із метою захисту інформації. Водночас питання формування та реалізації стратегії інформаційної безпеки залишаються поза увагою як науковців, так і практиків у сфері інформаційного захисту. Проведений аналіз показав, що у багатьох підприємств агропродовольчої сфери існує реальна необхідність у розробленні окремих, незалежних від ІТ-стратегій, стратегій управління інформаційною безпекою, які могли б, поряд із необхідним рівнем захисту, забезпечити належну підтримку бізнес-процесів підприємств і їх ефективний розвиток.

Варто відзначити, що окремі аспекти стратегічних напрямів захисту інформації та інформаційної стратегії розглянуті у працях А. Апетик [9], В. Аранчій [10], В. Ахрамовича [13], Е. Андерсона [55], А. Атіфа [56], В. Бірюкова [14], М. Вільямсона [62], С. Євсєєва [27], С. Кавуна [31], Дж. Кларка [61], Я. Левкова [34], Н. Лихарева [14], С. Мейнарда [56], С. Парка [56], Т. Перуна [41], Дж. Тапаіадора [61], Р. Чаплигіна [50], А. Чередниченка [51; 52], Дж. Чобінеха [55] та інших науковців. Проте особливості реалізації інформаційної стратегії підприємств, зокрема підприємств агропродовольчої сфери, їх типізація, взаємозумовленість із загальною стратегією, висвітлені у працях зарубіжних і вітчизняних учених фрагментарно.

Інформаційна архітектура сучасного аграрного підприємства, яка пронизує його виробничі та управлінські процеси, потребує надійного та своєчасного захисту. Вищезазначене обґрунтовує необхідність формування політики захисту інформації та розробки й реалізації ефективної інформаційної стратегії, яка повинна бути поєднана із загальною стратегією підприємства. З цією метою запропоновано модель визначення стратегії інформаційної безпеки підприємства, яка б відповідала вищезазначеним вимогам (рис. 5.1).

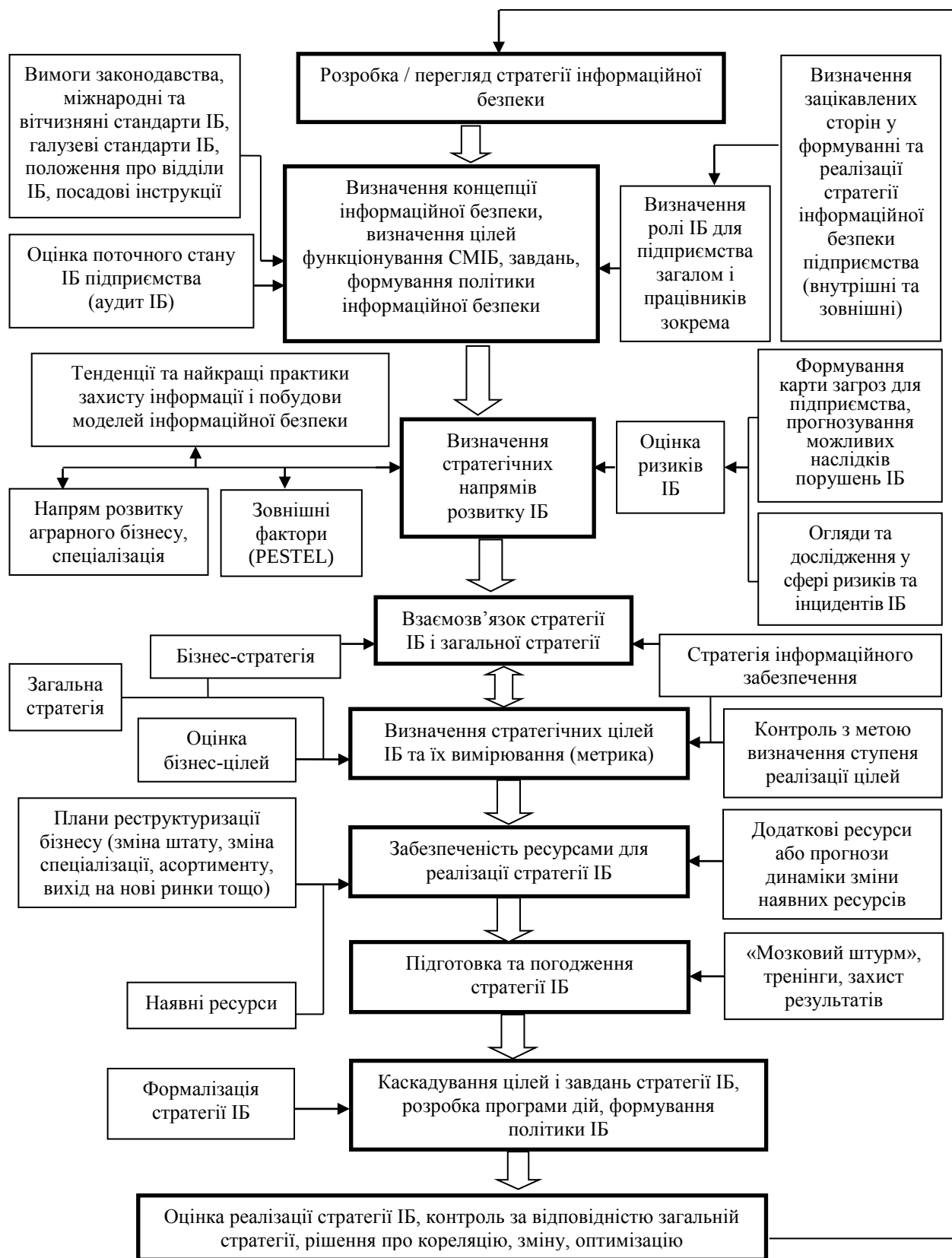


Рис. 5.1. Модель визначення стратегії інформаційної безпеки підприємства [розроблено на основі 1; 6; 13; 27; 31; 55; 56; 70; 71]

В основі комплексу заходів щодо захисту інформації має бути стратегія інформаційної безпеки, яка б визначала цілі, критерії, принципи та процедури,

необхідні для побудови надійної системи захисту. В умовах всеохоплюючої інформатизації стратегія захисту інформації в найзагальнішому вигляді може бути визначена як пошук оптимального компромісу між потребами в захисті і необхідними для цих цілей ресурсами. У контексті бізнесу інформаційні технології є інструментом, який підтримує існуючі бізнес-процеси, відповідно, на кінцевий стан інформаційної безпеки аграрного підприємства насамперед впливає бізнес-стратегія підприємства.

Отже, процес формування стратегії захисту інформації має бути тісно взаємопов'язаним із основною метою бізнесу підприємства та його загальною стратегією (рис. 5.2).



Рис. 5.2. Взаємозв'язок стратегії інформаційної безпеки з бізнес-стратегією підприємства [сформовано на основі 6; 27; 31; 55; 70]

Відповідно до запропонованої моделі формування стратегії інформаційної безпеки на основі взаємозв'язку з бізнес-стратегією підприємства підґрунтям зазначеного процесу є визначення базових елементів забезпечення інформаційної безпеки підприємства, таких як: перелік недоліків і вразливостей відповідно до проведеного контролю, перелік напрямів розвитку бізнесу, перелік дій відповідно до внутрішніх факторів, результати визначення ролі та пріоритетності інформаційної безпеки підприємства, результати оцінки інформаційних ризиків, актуальні тенденції та найкращі практики розвитку інформаційної безпеки, вплив зацікавлених сторін. На основі визначення та взаємного врахування бізнес-направів розвитку підприємства та напрямів розвитку інформаційної безпеки окреслюються стратегічні напрями управління інформаційною безпекою та мета в межах кожного напрямку (мета М). В разі, якщо досягнення мети призводить до отримання надочікуваного ефекту, то в такому разі вона визначається як «надмета» (мета М+1).

Визначення особливостей формування стратегії інформаційної безпеки підприємств агропродовольчої сфери необхідно починати з виявлення суб'єктів, зацікавлених у забезпеченні своєчасного доступу до необхідного масиву інформації, конфіденційності певної частини інформації, достовірності інформації, захисту частини інформації від незаконного її тиражування, розмежування відповідальності за порушення прав інших суб'єктів інформаційних відносин і встановлених правил поведінки з інформацією, можливості здійснення безперервного контролю і управління процесами обробки та передачі інформації. Стейкхолдерів розробки та реалізації інформаційної стратегії підприємств агропродовольчої сфери потрібно розподілити на внутрішніх, до яких слід зарахувати вище керівництво, IT-підрозділи, систему управління ризиками, бізнес-підрозділи (основні підрозділи, задіяні у виробництві сільськогосподарської продукції) та персонал підприємства агропродовольчої сфери, та зовнішніх, таких як акціонери, інвестори, партнери, споживачі, конкуренти, постачальники.

Як зазначалося вище, базовим і важливим елементом формування стратегії захисту інформаційних об'єктів є використання перевірених практик і актуальних тенденцій розвитку інформаційної безпеки підприємств, серед яких слід виокремити власне тенденції розвитку інформаційної безпеки, заходи, спрямовані на підвищення рівня інформаційної безпеки, та технології, спрямовані на підвищення рівня інформаційної безпеки (рис. 5.3).

Наразі найбільш розповсюдженим є підхід до визначення стратегії інформаційної безпеки, який ґрунтується на побудові матриці з урахуванням

двох критеріїв. Згідно з першим критерієм класифікації процеси захисту інформації значною мірою залежать від великої кількості випадкових і важкопередбачуваних факторів, таких як поведінка зловмисника, вплив природних явищ, збоїв і помилки в процесі функціонування елементів системи обробки інформації тощо. Згідно з другим критерієм класифікації серед засобів захисту значне місце посідають організаційні заходи, пов'язані з дією персоналу.



Рис. 5.3. Практики оптимізації та актуальні тенденції розвитку системи інформаційної безпеки підприємства [сформовано на основі 50; 56; 63]

Обґрунтування змісту необхідних стратегій у межах розглянутого підходу здійснюється за двома критеріями: визначення необхідного рівня захисту та визначення ступеня свободи дій у ході організації захисту.

Значення першого формалізується безліччю загроз, щодо яких має бути забезпечений захист:

- від найбільш небезпечних із уже відомих загроз;
- від усіх відомих загроз;
- від усіх потенційно можливих загроз.

Другий критерій вибору стратегій захисту зводиться до того, що організатори та виконавці процесів захисту мають відносно повну свободу розпоряджатися методами й засобами захисту, а також певний ступінь свободи втручання в архітектурну структуру системи обробки інформації та в організацію і забезпечення технології її функціонування. Відповідно, виокремлюють і три основні ступені свободи:

будь-яке втручання в систему обробки інформації недопустиме. Така вимога може бути висунута до вже функціонуючих систем обробки інформації, а порушення процесу їх функціонування для установки механізмів захисту не дозволяється;

до архітектурної побудови системи обробки інформації та технології її функціонування допускається висування неконцептуальних вимог, тобто допускається припинення процесу функціонування системи обробки інформації для встановлення деяких механізмів захисту;

вимоги будь-якого рівня, обумовлені потребами захисту інформації, приймаються як обов'язкові умови при побудові системи обробки інформації, організації та забезпеченні її функціонування [70].

Відповідно, доцільно виокремити три основні стратегії (табл. 5.1).

Таблиця 5.1

Матриця визначення стратегії захисту інформації підприємства [70]

Загрози, що враховуються	Вплив на систему обробки інформації		
	Відсутній	Частковий	Повний
Найбільш небезпечні	Захисна стратегія		
Усі відомі		Наступальна стратегія	
Усі потенційно можливі			Попереджувальна стратегія

Проте динамічність інформаційного середовища, формування глобального інформаційного простору, міжнародна взаємодія у сфері інформаційно-комунікаційних технологій висувають на передній план формування більш адаптивної моделі визначення стратегії інформаційної безпеки, яка б враховувала найрізноманітніші фактори впливу як на

виробничі та управлінські бізнес-процеси, так і на інформаційну систему підприємства, а також враховувала цілі загальної стратегії підприємства.

У ході огляду літератури також було визначено два основні аспекти стратегій інформаційної безпеки аграрного підприємства – час і простір. У «часовому» аспекті стратегії можуть бути спрямовані на очікування нападу або реагування після нападу, в «просторовому» – стратегії захисту інформації можуть поділятися на спрямовані на захист усієї інформаційної системи або на захист окремих інформаційних об’єктів [56].

Враховуючи запропоновану модель визначення стратегії інформаційної безпеки, необхідність взаємозв’язку стратегії інформаційної безпеки з бізнес-стратегією підприємства агропродовольчої сфери, інтереси стейкхолдерів у формуванні та реалізації стратегії інформаційної безпеки та положення матричного підходу до визначення стратегії інформаційної безпеки, запропоновано матричний підхід, який базуватиметься на врахуванні рівня інформаційної безпеки аграрного суб’єкта господарювання та показника рентабельності аграрного підприємства (рис. 5.4).

Рівень інформаційної безпеки підприємства	Високий рівень ІБ 0,67–1,00	<i>Превентивна стратегія</i> Стратегія стримування (Deterrence)	<i>Превентивна стратегія</i> Профілактична стратегія (превентивна) (Prevention)	<i>Превентивна стратегія</i> Стратегія спостереження (Surveillance)
	Помірний рівень ІБ 0,34–0,66	<i>Наступальна стратегія</i> Стратегія виявлення (Detection)	<i>Наступальна стратегія</i> Стратегія реагування (відповіді) (Response)	<i>Наступальна стратегія</i> Стратегія відволікання (стратегія «обману») (Deception)
	Недостатній рівень ІБ 0,00–0,33	<i>Захисна стратегія</i> Стратегія захисту по периметру (Perimeter Defense)	<i>Захисна стратегія</i> Стратегія компартменталізації (Compartmentalization)	<i>Захисна стратегія</i> Стратегія шарування (Layer)
		< 15,0 %	15,0–40,0 %	> 40,0 %

Рівень рентабельності підприємства

Рис. 5.4. Матриця визначення стратегії інформаційної безпеки підприємств агропродовольчої сфери [авторська розробка]

Відповідно до запропонованої матриці стратегія інформаційної безпеки підприємства агропродовольчої сфери визначатиметься існуючим рівнем власне інформаційної безпеки та рівнем рентабельності, який свідчатиме одночасно про ефективність діючої інформаційної стратегії та стратегії захисту інформації та про можливість необхідного ресурсного забезпечення для реалізації визначеної або пропонованої до реалізації стратегії інформаційної безпеки.

Отже, для підприємств із низьким рівнем інформаційної безпеки, який у межах матриці визначений як «недостатній», запропоновано до реалізації одну із таких захисних стратегій інформаційної безпеки, як стратегія шарування, стратегія компартменталізації, стратегія захисту по периметру (табл. 5.2).

Таблиця 5.2

Характеристика превентивних стратегій інформаційної безпеки підприємства агропродовольчої сфери [сформовано на основі 50; 55; 56; 66]

Стратегія інформаційної безпеки аграрного підприємства	Характеристика стратегії
1	2
Стратегія стримування (Deterrence)	Стратегія базується на положенні, що основне джерело загроз інформаційній безпеці є людина (персонал) і передбачає планування та реалізацію захисних дій із метою впливу на поведінку людини (працівника) стосовно використання інформаційних активів підприємства. Хоча ця стратегія не передбачає суворого режиму розмежування прав доступу до інформаційних ресурсів та активів, однак однією з головних особливостей застосування стратегії стримування є реалізація політики інформаційної безпеки, яка передбачає конкретизацію покарання працівників, які не дотримуються правил інформаційної безпеки
Профілактична стратегія (превентивна) (Prevention)	Профілактика спрямована на захист інформаційних активів від нападу шляхом заборони несанкціонованого доступу до них, їх модифікації, знищення чи розголошення. Найчастіше використовується запобіжний контроль – автентифікація, що спрямована на обмеження доступу до авторизованих користувачів. Подальші профілактичні методи включають використання ПЗ яке регулює взаємодію користувачів із інформаційними активами, шифруючи інформацію, щоб запобігти витоку. Ця стратегія передбачає використання захисних механізмів, які спрямовані на чітке розмежування прав доступу до інформаційних ресурсів, визначення системи ролей в інформаційній системі
Стратегія спостереження (Surveillance)	Передбачає систематичний моніторинг інформаційного середовища безпеки, спрямований на формування ситуаційної обізнаності з метою адаптації до мінливих обставин і виникаючих загроз, що дає змогу вчасно

1	2
	попередити або уникнути інцидентів інформаційної безпеки та розробити більш ефективні засоби захисту. Моніторинг середовища інформаційної безпеки підприємства у фізичній і цифровій сферах за допомогою технічних і нетехнічних засобів – складне завдання. Стратегія передбачає реєстрацію доступу до обмежених фізичних і логічних просторів, де зберігається інформація про копіювання та програмне забезпечення тощо

Вибір підвиду цієї групи стратегії інформаційної безпеки залежить від рівня рентабельності: зі зростанням рівня рентабельності захисна стратегія зміщуватиметься із позиції менш витратної, а отже, і менш ефективної, до більш ефективної, але водночас і такої, що потребуватиме додаткового обсягу ресурсів для її реалізації.

Аналогічним чином визначається і група наступальних стратегій, які рекомендовані до реалізації підприємствам із помірним рівнем інформаційної безпеки. Зазначена група включатиме такі три основні стратегії інформаційної безпеки, як стратегія виявлення, стратегія реагування (відповіді), стратегія відволікання (або стратегія «обману») (табл. 5.3). Відповідно, перша стратегія потребуватиме залучення меншого обсягу ресурсів, а остання – значно більшого.

Таблиця 5.3

Характеристика наступальних стратегій інформаційної безпеки підприємства агропродовольчої сфери [сформовано на основі 41; 50; 55; 56; 66]

Стратегія інформаційної безпеки аграрного підприємства	Характеристика стратегії
1	2
Стратегія виявлення (Detection)	Стратегія виявлення – це наступальна стратегія, яку переважно застосовують фахівці аграрного підприємства, вона спрямована на виявлення конкретної небезпеки. Зазначена стратегія контрастує зі стратегією спостереження. Проте виявлення фокусується на конкретній події, тоді як спостереження спрямоване на визначення загальної ситуації інформаційної захищеності. Виявлення має різні форми: виявлення шкідливої або незвичної поведінки працівників, вторгнення чи несанкціоноване використання інформаційних ресурсів, програмних продуктів, апаратних засобів тощо
Стратегія реагування (відповіді) (Response)	Стратегія реагування передбачає реалізацію відповідних коригувальних дій щодо виявлених атак. Відповідь на напад можна розділити на дві фази: фаза реакції, під час якої виконуються відповідні дії проти нападника або атаки та фаза

1	2
	відновлення – пошкоджену інформаційну систему або її окремих елемент повертають до початкового стану. Ця стратегія є більш ефективною порівняно зі стратегією стримування, що дозволяє відокремити нападника або атаковану сферу від інших сфер інформаційного середовища підприємства
Стратегія відволікання (стратегія «обману») (Deception)	Стратегія «обману» спрямована на відволікання уваги зловмисника від критично важливих інформаційних активів, використовуючи «приманки», які змушують порушника витрачати час і ресурси, а систему захисту – створити додаткові умови для безпеки інформаційних ресурсів. Стратегія відволікання має два конструкти: пасивний обман та активний обман. Пасивний обман полягає в тому, щоб щось приховувати, тоді як активний – щось показати. В межах реалізації цієї стратегії виокремлюють два види приманок – програмні приманки та «медові горщики». Програмні приманки являють собою програмну оболонку, яка спілкується з процесами виклику від зловмисника від «імені» критичного програмного забезпечення, що дає змогу приховати насправді важливе програмне забезпечення, інформаційні ресурси та інформаційні активи. «Медові горщики» слугують своєрідною приманкою у вигляді цілісної інформаційної системи для зловмисників, насправді приховуючи та захищаючи від атаки справжню цінну інформаційну систему підприємства

Третю групу стратегій доцільно застосувати підприємствам із високим рівнем інформаційної безпеки. До її складу входять стратегії, які передбачають вживання превентивних заходів: стратегія стримування, профілактична стратегія (превентивна), стратегія спостереження. Їх зміщення відбувається як і у стратегій попередніх груп із зростанням або зменшенням рівня рентабельності суб'єкта господарювання агропродовольчої сфери України. Характерні особливості зазначених стратегій наведено у табл. 5.4.

Отже, на основі вищезазначеного доцільно відзначити, що стратегія інформаційної безпеки аграрних підприємств – це структурований і взаємопов'язаний набір виважених дій, спрямованих на довгострокову перспективу захисту інформаційних об'єктів підприємства.

Стратегію інформаційної безпеки варто розглядати як карту, яка визначає орієнтири досягнення безпечних умов протікання основних управлінських і виробничих процесів суб'єктів агропродовольчої сфери та допомагає забезпечити отримання економічного та соціального ефекту [50; 51; 71].

Водночас варто звернути увагу на те, що стратегія інформаційної безпеки підприємства агропродовольчої сфери не має бути статичною, і в міру зменшення фактора невизначеності з плином часу її необхідно

переглядати і в разі потреби коригувати, задаючи нові пріоритети прийняття тактичних рішень.

Таблиця 5.4

Характеристика захисних стратегій інформаційної безпеки підприємства агропродовольчої сфери [сформовано на основі 6; 50; 55; 56; 61; 66]

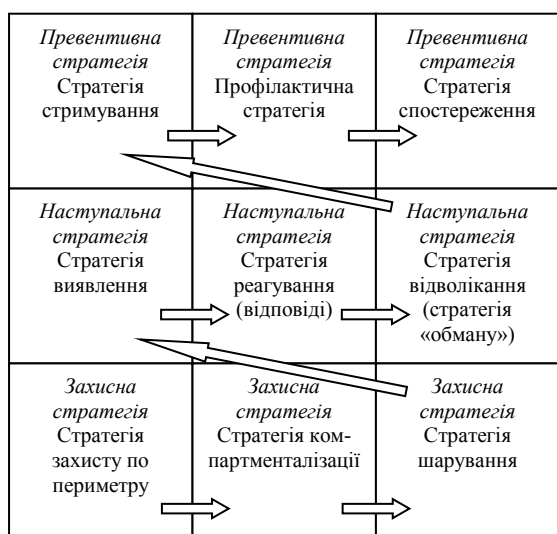
Стратегія інформаційної безпеки аграрного підприємства	Характеристика стратегії
Стратегія захисту по периметру (Perimeter Defense)	Захист периметра передбачає «оборону» фізичної та/або логічної межі інформаційного середовища, в межах якої визначена політика безпеки або застосовується архітектура безпеки. В умовах інформаційної безпеки захист периметра передбачає створення межі навколо інформаційних активів, яка забезпечується регулюванням трафіку на кожному вхідному та вихідному інформаційному каналі. Мережні брандмауери, механізми контролю доступу, механізми аутентифікації, контрзаходи щодо відмови програмного забезпечення або апаратних засобів, виявлення та відбиття кібер- та інформаційних атак – типові засоби управління, що реалізуються як основа стратегії оборони периметра
Стратегія компартменталізації (Compartmentalization)	Компартменталізація зменшує можливості зловмисників, поділяючи область інформаційної атаки на окремі захищені зони. У разі, якщо зловмисник, який подолав захист однієї зони, автоматично не має доступу до інших зон. Інформаційні активи класифікуються на категорії – таємні та надтаємні. Кожній одиниці персоналу призначаються права доступу до окремих категорій категорію інформації. Типовим прикладом цієї стратегії є DMZ (демілітаризована зона) або мережна зона, ізольована від внутрішньої мережі, але відкрита для загального доступу
Стратегія шарування (Layer)	Шарування використовує шари (рівні) контрзаходів, які функціонують незалежно один від одного, але підвищують загальну ефективність захисту в разі комплексної взаємодії. Пошаровий захист ґрунтується на переконанні, що єдиної стратегії недостатньо, тому потрібен складний набір інтелектуальних та інноваційних технологій інформаційного захисту

Перехід від реалізації однієї стратегії інформаційної безпеки до іншої може відбуватися двома основними способами:

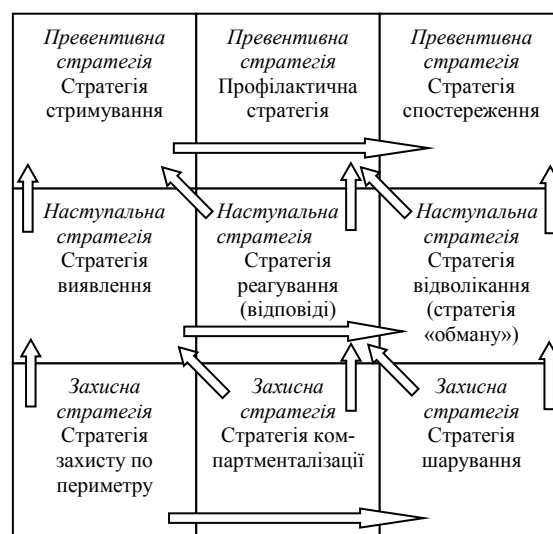
у разі досягнення мети управління інформаційною безпекою (мета М) – еволюційним (див. рис. 5.2);

у разі досягнення надмети управління інформаційною безпекою (отримання надочікуваного ефекту) (мета М+1) (див. рис. 5.2) – революційним (рис. 5.5). Революційний варіант зміни (розвитку) стратегії

інформаційної безпеки передбачає перехід від однієї до іншої стратегії, пропускаючи одну або дві проміжні стратегії.



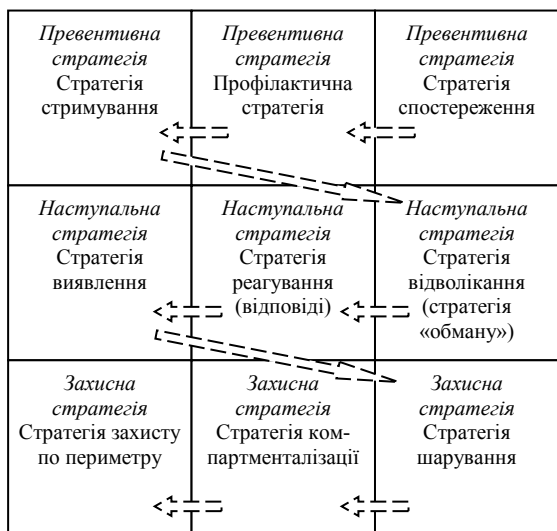
а) еволюційний варіант зміни (розвитку) стратегії інформаційної безпеки підприємства агропродовольчої сфери (умова досягнення мети М)



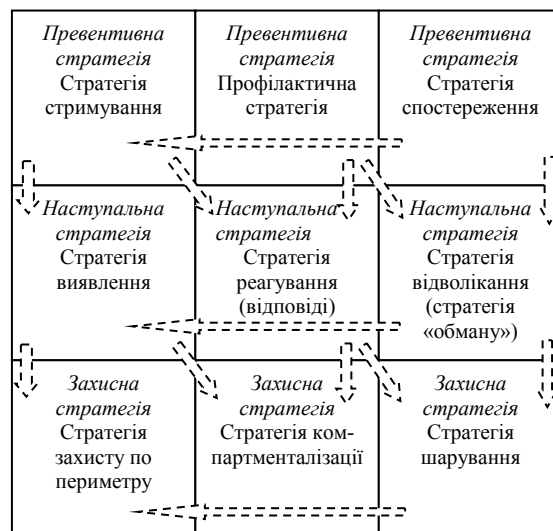
б) революційний варіант зміни (розвитку) стратегії інформаційної безпеки підприємства агропродовольчої сфери (умова досягнення мети «М + 1», ... «М + n»)

Рис. 5.5. Варіанти розвитку стратегії інформаційної безпеки підприємств агропродовольчої сфери [авторська розробка]

Аналогічним чином може відбуватися зміна стратегії і в бік регресу (рис. 5.6).



а) еволюційний варіант зміни (регресу) стратегії інформаційної безпеки підприємства агропродовольчої сфери (умова недосягнення мети М)



б) революційний варіант зміни (регресу) стратегії інформаційної безпеки підприємства агропродовольчої сфери (умова недосягнення мети «М+1», ... «М+n»)

Рис. 5.6. Варіанти регресу стратегії інформаційної безпеки підприємств агропродовольчої сфери [авторська розробка]

Вибір варіанта зміни стратегії інформаційної безпеки підприємства здійснюється експертним способом через встановлення досягнення / недосягнення мети інформаційного захисту (мета М або мета М + 1...М + n), проте слід зважати і на кількісні показники, які визначають стратегію інформаційної безпеки. Тому запропоновано використовувати метрику для визначення варіанта розвитку стратегії інформаційної безпеки, яка базується на темпах зміни показника рівня інформаційної безпеки та рентабельності.

Отже, еволюційний варіант зміни (розвитку) стратегії інформаційної безпеки підприємства агропродовольчої сфери слід обирати в тому разі, якщо: $\{0 \leq \Delta P_{IB} \leq 10\%; 0 \leq \Delta P_p \leq 30\%\}$;

революційний варіант зміни (розвитку) стратегії інформаційної безпеки підприємства агропродовольчої сфери, що передбачає перехід від однієї стратегії до іншої, пропускаючи одну проміжну стратегію, слід обирати в тому разі, якщо $\{\Delta P_{IB} > 10\%; 0 \leq \Delta P_p \leq 30\%\}$ або $\{0 \leq \Delta P_{IB} \leq 10\%; \Delta P_p > 30\%\}$;

революційний варіант зміни (розвитку) стратегії інформаційної безпеки підприємства агропродовольчої сфери, що передбачає перехід з однієї стратегії до іншої, пропускаючи дві проміжні стратегії, слід обирати в тому разі, якщо: $\{\Delta P_{IB} > 10\% \text{ та } \Delta P_p > 30\%\}$;

стратегію запропоновано не змінювати, в разі виконання умов: $\{-9\% \leq \Delta P_{IB} \leq 0; \Delta P_p > 0\}$; $\{\Delta P_{IB} > 0\%; -29\% \leq \Delta P_p \leq 0\}$;

еволюційний варіант зміни (регресії) стратегії інформаційної безпеки підприємства агропродовольчої сфери слід обирати в тому разі, якщо: $\{-9\% \leq \Delta P_{IB} \leq 0; -29\% \leq \Delta P_p \leq 0\}$;

революційний варіант зміни (регресії) стратегії інформаційної безпеки підприємства агропродовольчої сфери, що передбачає перехід від однієї стратегії до іншої, пропускаючи одну проміжну стратегію, слід обирати в тому разі, якщо: $\{-20\% \geq \Delta P_{IB} > -10\%; -50\% \geq \Delta P_p \geq -30\%\}$;

революційний варіант зміни (регресії) стратегії інформаційної безпеки підприємства агропродовольчої сфери, що передбачає перехід з однієї стратегії до іншої, пропускаючи дві проміжні стратегії, слід обирати в тому разі, якщо: $\{-20\% > \Delta P_{IB}; -50\% > \Delta P_p\}$, де P_{IB} – темп зміни показника рівня інформаційної безпеки, P_p – темп зміни показника рівня рентабельності, Δ – зміна показника.

Обов'язково слід зважати і на від'ємні показники значень рентабельності, які свідчать про необхідність регресії стратегії інформаційної безпеки.

Водночас доцільно відзначити, що можливе і в деяких випадках навіть доцільне використання одночасно декількох стратегій інформаційної безпеки, наприклад, для захисту внутрішнього інформаційного середовища

підприємства та для захисту від атак і вторгнень із зовнішнього середовища; для захисту управлінської сфери діяльності та виробничої сфери діяльності; як для захисту технічної частини інформаційної системи, так і для забезпечення інформаційної безпеки персоналу тощо.

Узагальнюючи розглянуті стратегії, доцільно відзначити, що головними напрямками захисту інформації у процесі реалізації будь-якого типу стратегії інформаційної безпеки підприємства агропродовольчої сфери мають стати:

основні принципи формування переліку критичних ресурсів, які потребують захисту, що формується в процесі проведення аудиту безпеки й аналізу ризиків. Цей перелік має включати в себе опис фізичних, програмних та інформаційних ресурсів з визначенням вартості ресурсів і ступеня їх критичності для підприємства;

основні принципи захисту, що визначають стратегію забезпечення інформаційної безпеки та перелік правил, якими необхідно керуватися при побудові системи забезпечення інформаційної безпеки підприємства;

модель порушника безпеки, яка визначається на основі обстеження ресурсів системи і способів їх використання;

модель загроз безпеці та оцінки ризиків, пов'язаних із їх здійсненням, що формується на основі переліку критичних ресурсів і моделі порушника, яка включає визначення імовірностей загроз і способів їх здійснення, а також оцінку можливих збитків;

вимоги безпеки, які визначаються за результатами аналізу ризиків;

заходи забезпечення безпеки організаційного та програмно-технічного рівня, що вживаються для реалізації перерахованих вимог;

відповідальність співробітників підприємства за дотримання встановлених вимог інформаційної безпеки під час експлуатації інформаційної системи підприємства [14; 34; 62].

Зважаючи на розвиток агропродовольчої сфери, її постійну інформатизацію, цифровізацію та автоматизацію, проблеми захисту інформації суб'єктів зазначеного сектора набувають стратегічного значення. У ході дослідження було визначено сутність інформаційної стратегії аграрних підприємств як структурованого і взаємопов'язаного набору виважених дій, спрямованих на довгострокову перспективу захисту інформаційних об'єктів підприємства. Базуючись на запропонованому матричному методі, що передбачає визначення рівня інформаційної безпеки та його зміну (Додаток АБ) і визначення рівня рентабельності та його зміну (Додаток АВ), окреслено стратегії інформаційної безпеки для аналізованих підприємств агропродовольчої сфери, а також спрогнозовано тип зміни (розвитку) цієї стратегії (табл. 5.5).

Таблиця 5.5

Стратегія інформаційної безпеки підприємств агропродовольчої сфери [авторська розробка]

Досліджувані підприємства	Рівень інформаційної безпеки (середнє значення за 2014–2018 рр.)	Рівень рентабельності (середнє значення за 2014–2018 рр.)	Стратегія інформаційної безпеки підприємства	Динаміка зміни рівня інформаційної безпеки	Динаміка зміни рівня рентабельності	Тип розвитку інформаційної стратегії	Прогнозована стратегія інформаційної безпеки підприємства
1	2	3	4	5	6	7	8
ПрАТ «ПОЕЗ Кернел-груп»	0,75	-4,29	ПС Стратегія стримування	2,23	26,92	ЕВ↑	ПС Профілактична стратегія
ФГ «Батьківщина»	0,17	18,62	ЗС Стратегія компарт-менталізації	13,39	-5,10	→	ЗС Стратегія компарт-менталізації
СК «Іскра»	0,17	19,24	ЗС Стратегія компарт-менталізації	5,98	392,94	РВ ₁ ↑	НС Стратегія виявлення
СТОВ «Мусіївське»	0,33	9,07	ЗС Стратегія захисту по периметру	-0,56	10,13	→	ЗС Стратегія захисту по периметру
ПрАТ «Агротон»	0,57	1,56	НС Стратегія виявлення	9,33	61,55	РВ ₁ ↑	НС Стратегія відволікання
ТОВ «РОСТ АГРО»	0,36	5,12	НС Стратегія виявлення	0,48	13,06	ЕВ↑	НС Стратегія відволікання
ПСП «Солоницьке»	0,20	41,40	ЗС Стратегія шарування	0,88	1,58	ЕВ↑	НС Стратегія виявлення
СТОВ «Агрофірма „Оржицька”»	0,15	9,95	ЗС Стратегія захисту по периметру	1,87	-17,61	→	ЗС Стратегія захисту по периметру
ТОВ «Агрофірма ім. Довженка»	0,70	30,51	ПС Профілактична стратегія	1,54	49,71	РВ ₁ ↑	ПС Стратегія спостереження
СТОВ «Агрофірма „Дружба”»	0,26	15,65	ЗС Стратегія компарт-менталізації	0,79	85,84	РВ ₁ ↑	НС Стратегія виявлення

1	2	3	4	5	6	7	8
ПП «Альтаір»	0,09	15,52	ЗС Стратегія захисту по периметру	11,81	80,50	PВ ₂ ↑	НС Стратегія виявлення
ФГ «Товсте»	0,18	27,26	ЗС Стратегія компарт-менталізації	29,49	11,00	PВ ₁ ↑	НС Стратегія виявлення
ПП «Надь»	0,23	16,81	ЗС Стратегія компарт-менталізації	13,66	264,10	PВ ₂ ↑	НС Стратегія виявлення
СФГ «Зеніт»	0,38	7,20	НС Стратегія виявлення	2,98	250,65	PВ ₁ ↑	НС Стратегія відволікання
ТОВ «АПК Докучаєвські чорноземи»	0,63	16,71	НС Стратегія реагування (відповіді)	6,00	1,80	ЕВ↑	НС Стратегія відволікання

НС – наступальна стратегія;

ЗС – захисна стратегія;

ПС – превентивна стратегія ;

ЕВ – еволюційний тип зміни стратегії;

PВ₁ – революційний тип зміни стратегії, що передбачає перехід від однієї стратегії до іншої, пропускаючи одну проміжну стратегію;

PВ₂ – революційний тип зміни стратегії, що передбачає перехід від стратегії однієї до іншої, пропускаючи дві проміжні стратегії;

↑ – зміна (розвиток) стратегії;

↓ – зміна (регресія) стратегії

Відповідно до проведеного аналізу доцільно відмітити, що більшість аналізованих підприємств агропродовольчої сфери (ФГ «Батьківщина», СК «Іскра», СТОВ «Мусіївське», ПСП «Солоницьке», СТОВ «Агрофірма „Оржицька”», СТОВ «Агрофірма „Дружба”», ПП «Альтаір», ФГ «Товсте», ПП «Надь») через низький рівень інформаційної безпеки реалізують захисні стратегії інформаційної безпеки, п'ять із них – стратегію компартменталізації, 3 – стратегію захисту по периметру та лише підприємство – стратегію шарування. Тільки три підприємства (ФГ «Батьківщина», СТОВ «Мусіївське», СТОВ «Агрофірма „Оржицька”») реалізують відповідну до їх можливостей стратегію інформаційної безпеки. ПСП «Солоницьке» потребує еволюційного варіанта зміни стратегії на наступальну стратегію, а саме стратегію виявлення, що доцільно здійснити шляхом застосування пропонованих сучасних тенденції розвитку сфери інформаційної безпеки, а також заходів і тенденцій, спрямованих на підвищення рівня інформаційної безпеки, зокрема таких, як забезпечення адміністрування ІТ-сфери, реалізація політики захисту інформаційних активів, забезпечення системи управління

інформаційною безпекою достатнім бюджетом і ресурсами, застосування показників ефективності інформаційної безпеки для її постійного моніторингу, впровадження засобів автоматизації управління інформаційною політикою, обізнаність персоналу з політикою інформаційної безпеки, навіть у тому разі, якщо вона не формалізована.

СК «Іскра», СТОВ «Агрофірма „Дружба”», ФГ «Товсте» запропоновано шляхом революційного варіанта розвитку стратегії, яким передбачено перехід від однієї стратегії до іншої, пропускаючи одну проміжну стратегію, перейти до реалізації наступальної стратегії – стратегії виявлення, що зумовлено малим розміром зазначених підприємств (це зменшує імовірність порушення інформаційної безпеки) та високим рівнем рентабельності. ПП «Альтаір», ПП «Надь» через ще менший розмір і надвисокий рівень рентабельності запропоновано шляхом революційного варіанту розвитку стратегії, яким передбачено перехід від однієї стратегії до іншої, пропускаючи дві проміжні стратегії, теж перейти до реалізації стратегії виявлення. З цією метою підприємствам цієї групи рекомендовано застосування метрик вимірювання рівня інформаційної безпеки для його ефективного моніторингу, методик управління інформаційними ризиками, технологій управління доступом до різного рівня інформаційних ресурсів та інформаційних активів підприємства, забезпечення контролю за периметром та міжмережним екрануванням.

Визначено, що наразі ПрАТ «Агротон», ТОВ «РОСТ АГРО», СФГ «Зеніт», ТОВ «АПК Докучаєвські чорноземи» реалізують наступальні стратегії, перші три підприємства – стратегію виявлення, а останнє – стратегію реагування (відповіді). Це переважно середні за розміром і масштабом діяльності підприємства, які мають значні обсяги інформаційних ресурсів і дороговартісні інформаційні активи, автоматизовані виробничі та управлінські процеси, використовують цифрові технології у виробництві.

Для ТОВ «РОСТ АГРО», ТОВ «АПК Докучаєвські чорноземи» запропоновано поступовий еволюційний перехід до реалізації наступальної стратегії – стратегії відволікання. Для ПрАТ «Агротон», СФГ «Зеніт» теж запропоновано реалізовувати цю стратегію, але на відміну від еволюційного розвитку, пропонованого для вищезазначених підприємств, їм необхідний революційний розвиток, яким передбачено перехід від однієї стратегії до іншої, пропускаючи одну проміжну стратегію. Щоб цього досягти, їм доцільно забезпечити стратегічне планування розвитку інформаційного середовища та системи інформаційної безпеки загалом, стратегічне управління інформаційною безпекою через інтеграцію з бізнес-стратегією, застосування метрик вимірювання рівня інформаційної безпеки та технологій

управління доступом до різного рівня інформаційних ресурсів та інформаційних активів підприємства, визначення професійного лідера з управління системою інформаційної безпеки, застосування системи централізованого управління доступом, системи GRC (управління, ризик, відповідність), системи управління процесами (BPM), системи запобігання витоку інформації (DLP).

ПрАТ «ПОЕЗ Кернел-груп», ТОВ «Агрофірма ім. Довженка» є значними за масштабами та видами діяльності підприємствами агропродовольчої сфери зі сформованою та ефективно діючою системою інформаційної безпеки, про що свідчить рівень інформаційної безпеки та рентабельність діяльності. Досліджувані підприємства реалізують превентивні стратегії – стратегії вищого щабля інформаційної безпеки, зокрема стратегію стримування та профілактичну стратегію, відповідно до зазначених підприємств. Згідно із проведеними розрахунками зміни показників, що визначають інформаційну стратегію, для ПрАТ «ПОЕЗ Кернел-груп» запропоновано еволюційний варіант розвитку, яким передбачено реалізацію профілактичної стратегії в межах групи превентивних стратегій, а для ТОВ «Агрофірма ім. Довженка» – стратегію спостереження – найвищого щабля розвитку стратегій інформаційної безпеки. Водночас для реалізації прогнозованих змін цим товариствам доцільно посилити захист хмарних технологій і програмних додатків, систему інформаційної безпеки інтелектуальними системами безпеки, а саме системою централізованого управління доступом, системою GRC (управління, ризик, відповідність), системою управління процесами (BPM), системою запобігання витоку інформації (DLP), а також забезпечити шифрування каналів зв'язку, баз даних, упровадити новітні засоби автоматизації управління інформаційною безпекою, визначити професійного лідера з управління системою інформаційної безпеки, забезпечити систему управління інформаційною безпекою висококваліфікованим персоналом, застосувати новітні метрики моніторингу рівня інформаційної безпеки та забезпечити створення форм звітності з інформаційної діяльності.

Аналіз діяльності вітчизняних суб'єктів агропродовольчої сфери показує, що в сучасних умовах потреба у формуванні та реалізації стратегії інформаційної безпеки, як правило, виникає в аграрних підприємств, які мають досить значні конкурентні позиції на ринку, визначили довгострокові перспективи власного розвитку та зіткнулися з такими викликами, як недостатній рівень інформаційної безпеки ключових бізнес-процесів підприємства, відсутність взаємозв'язку між стратегічними цілями підприємства і напрямками розвитку інформаційної безпеки, низька віддача від інвестицій у розвиток інформаційної безпеки.

Визначення основних елементів формування і реалізації інформаційної стратегії аграрних утворень, зацікавлених сторін у формуванні та реалізації стратегії інформаційної безпеки аграрного підприємства, характеристика типів інформаційних стратегій, актуальні тенденції та найкращі практики розвитку інформаційної безпеки підприємства – усе це дозволить аграрним підприємствам обрати оптимальну інформаційну стратегію, яка буде взаємообумовленою із загальною стратегією розвитку, та сформувати необхідний набір програмних, технічних, апаратних та організаційних інструментів захисту інформаційних ресурсів.

Особливим вираженням стратегії інформаційної безпеки підприємства є політика інформаційної безпеки, яка призначена для встановлення єдиних норм, правил і вимог до системи управління інформаційною безпекою підприємств агропродовольчої сфери. Основними цілями політики інформаційної безпеки є захист інформації та забезпечення ефективного інформаційного середовища у процесі діяльності підприємства агропродовольчої сфери. Водночас актуальність розробки політики інформаційної безпеки для зазначених підприємств пояснюється необхідністю створення механізму управління і планування інформаційною безпекою.

5.2. Формування політики інформаційної безпеки підприємства на основі концепції інформаційної культури

Розробка формальної моделі, що дає можливість ефективно програмувати на формальній мові, дозволяє реалізувати норми та правила політики безпеки, що сформульовані в термінах природної мови. Політику безпеки інформаційної системи необхідно формалізувати з метою опису поглядів керівництва підприємства на суть загроз інформаційній безпеці, а також на технології, за допомогою яких можна забезпечити безпеку її інформаційних ресурсів. Для політики безпеки можна визначити дві основні частини. Перша з них – загальні принципи роботи з інформаційними ресурсами (базами даних) для кожної із категорій користувачів. Друга – чітко визначені правила такої роботи. При побудові політики безпеки потрібно розуміти, що вона завжди буде компромісом між рівнем захищеності інформаційних ресурсів системи інформаційної безпеки і витратами, що необхідні для її експлуатації. В умовах глобалізації економіки успішне ведення бізнесу суб'єктами аграрних відносин передбачає наявність інформації про ринкову кон'юнктуру, фінансове становище конкурентів,

новітні розробки, тенденції розвитку в конкретних областях науки і виробництва. Як було з'ясовано в попередніх розділах, проблеми побудови та функціонування системи інформаційної безпеки суб'єкта господарської діяльності аграрного ринку є нагальними та потребують детального розгляду питань, які стосуються формування ефективної політики інформаційної безпеки цих суб'єктів, що є особливо актуальним завданням у сучасних умовах глобалізації та інтеграції цифрових технологій в соціально-економічні відносини, оскільки без організації ефективного та цілеспрямованого процесу протидії різним загрозам інформаційній системі та інформаційному простору неможливо створити умови для безпечного та сталого розвитку підприємств агропродовольчої сфери. Для побудови ефективної системи захисту інформації необхідно реалізувати комплексний підхід, найважливішим елементом якого є формування і реалізація політики інформаційної безпеки.

Аналіз доробків вітчизняних і зарубіжних науковців допоміг розглянути етимологічний і гносеологічний аспекти поняття політики інформаційної безпеки підприємства [15; 18; 28; 29; 30; 37; 38; 42; 44; 45; 46; 48; 54; 71].

Найбільш відома електронна бібліотека визначає політику інформаційної безпеки як набір вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в організації і спрямовані на досягнення та підтримку стану інформаційної безпеки організації [65].

Ю. Коваленко пропонує визначити політику безпеки підприємства як сукупність керівних принципів, правил, процедур і практичних прийомів сфери інформаційної безпеки, що регулюють управління, захист і розподіл цінної інформації на підприємстві [33].

Інша група авторів визначає дуалістичність політики інформаційної безпеки, першу частину якої вони визначають як загальні принципи роботи з інформаційними ресурсами (базами даних) для кожної із категорій користувачів, а другу – характеризують як чітко визначені правила такої роботи [18].

Сучасне підприємство агропродовольчої сфери повинно вміти належним чином будувати політику інформаційної безпеки, тобто розробляти й ефективно впроваджувати комплекс превентивних заходів щодо захисту конфіденційних даних та інформаційних процесів. Л. Власова вважає, що така політика передбачає відповідні вимоги до персоналу, менеджерів і технічних служб [17].

Зарубіжні вчені у політиці інформаційної безпеки вбачають досконалий стандарт, яким може бути виміряна доцільність і окупність витрат на захист ресурсів. Керівнику організації необхідно порівняти вигоди з витратами,

прописаними в політиці інформаційної безпеки, щоб визначити ефективність витрачання коштів [33].

Політика безпеки інформації в організації – це сукупність документованих правил, процедур, практичних прийомів або керівних принципів у сфері безпеки інформації, якими керується організація у своїй діяльності [32].

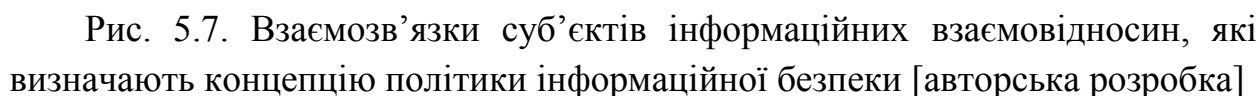
Зарубіжні дослідники стверджують, що політику безпеки інформації використовує керівництво для розмежування поведінки працівників – як дозволеної або забороненої [57].

Варто відмітити і те, як визначають політику інформаційної безпеки практикуючі суб'єкти господарювання. Так, керівництво одного з аграрних підприємств у програмі інформаційної безпеки визначає політику інформаційної безпеки як надійне забезпечення інформаційної безпеки підприємства, а отже, недопущення заподіяння матеріального, фізичного, морального чи іншого збитку внаслідок проектно-технологічної та інформаційної діяльності. Інша організація політику інформаційної безпеки розглядає як систему поглядів на проблему забезпечення інформаційної безпеки, яка являє собою систематизований виклад високорівневих цілей і завдань захисту, якими необхідно керуватись у своїй діяльності, а також основних принципів побудови системи управління інформаційною безпекою установи. Деякі підприємства як основу політики інформаційної безпеки використовують міжнародні стандарти, зокрема стандарт TCSEC (США), відомий як «Помаранчева книга» [5].

Отже, термін «політика інформаційної безпеки» може вживатися як у широкому, так і у вузькому значенні. У широкому значенні політика інформаційної безпеки визначається як система документованих управлінських рішень щодо забезпечення інформаційної безпеки організації, а у вузькому, – як локальний нормативний документ, у якому окреслені вимоги інформаційної безпеки, система заходів, або порядок дій, а також відповідальність співробітників підприємства і механізми контролю для забезпечення інформаційної безпеки.

Узагальнюючи вищенаведені визначення, доцільно відмітити три основні аспекти, які мають бути покладені в основу формування політики інформаційної безпеки підприємств агропродовольчої сфери: по-перше, політика інформаційної безпеки повинна являти собою набір законів, правил, практичних рекомендацій і практичного досвіду, що визначають управлінські та проектні рішення у сфері забезпечення інформаційної безпеки; по-друге, на її основі повинне здійснюватися управління, захист і розподіл інформації в системі; по-третє, вона повинна охоплювати всі особливості процесу

Підсумовуючи вищезазначене, доцільно відмітити, що важливою умовою для ефективного захисту інформаційних ресурсів підприємств агропродовольчої сфери має стати створення атмосфери, сприятливої для підтримки пріоритету інформаційної безпеки. Тому політику інформаційної безпеки підприємства необхідно розглядати не тільки з позиції формалізації – розробки документів, планів інформаційної безпеки, встановлення правил, методів тощо, але й з позиції формування інформаційних взаємовідносин і запровадження моделі поведінки користувачів інформаційної системи підприємства, основні групи яких відображені на рис. 5.7.



310

На інформаційні взаємовідносини серед внутрішніх суб'єктів найбільше впливають взаємовідносини між вищим керівництвом, системою менеджменту інформаційної безпеки та користувачами інформаційних ресурсів, а серед зовнішніх суб'єктів – державні органи, які регулюють окремі аспекти інформаційної і комунікаційної сфери діяльності; зовнішні користувачі інформаційних ресурсів, які потребують захисту інформації не тільки відносно взаємозв'язків з підприємством, а й інформації про власну економічну, фінансову, інноваційну, виробничу, торговельну та інші сфери діяльності; аудитори, які визначають недоліки інформаційного захисту та надають пропозиції щодо оптимізації системи інформаційної безпеки. Опосередковано, проте істотно впливають на політику інформаційної безпеки зловмисники – порушники інформаційної безпеки, власне дії яких і визначають види атак, способи, методи, механізми попередження, захисту, мінімізації ризиків і ліквідації наслідків настання подій порушення інформаційної безпеки. Доцільно враховувати й основні вимоги зазначених суб'єктів при розробці політики інформаційної безпеки і розподілити їх на внутрішні та зовнішні. До внутрішніх слід зарахувати вимоги керівництва щодо формування ефективної системи інформаційної безпеки, що забезпечить захист фінансово-економічної сфери виробничої та управлінської діяльності аграрних суб'єктів господарювання, залучення співробітників до процесу забезпечення інформаційної безпеки; надійність інформації та даних, які надаються користувачам, і зручність їх використання; економічну доцільність системи захисту інформації, формування інформаційної культури тощо. До зовнішніх вимог слід зарахувати такі: дії зловмисників, вимоги законодавства та стандартів, вимоги клієнтів і партнерів, необхідність сертифікації за стандартами, висновки аудиторів. Політика інформаційної безпеки є документом високого рівня, в якому описуються цілі та завдання заходів безпеки. Для побудови політики інформаційної безпеки підприємства застосовуються такі напрями захисту інформаційної системи: захист об'єктів інформаційної системи, захист процесів, процедур і програм обробки інформації, захист каналів зв'язку, управління системою захисту тощо. Водночас запропоновано звернути увагу на необхідність захисту не менш значимих елементів – інтелектуальних ресурсів і знань працівників підприємства. На основі зазначеного запропоновано функціональну модель формування політики інформаційної безпеки підприємства (рис. 5.8), засновану на адаптації загальних стандартів ISO 15408 та ISO 17799 з урахуванням запровадження інформаційної культури підприємства [3; 4; 67].

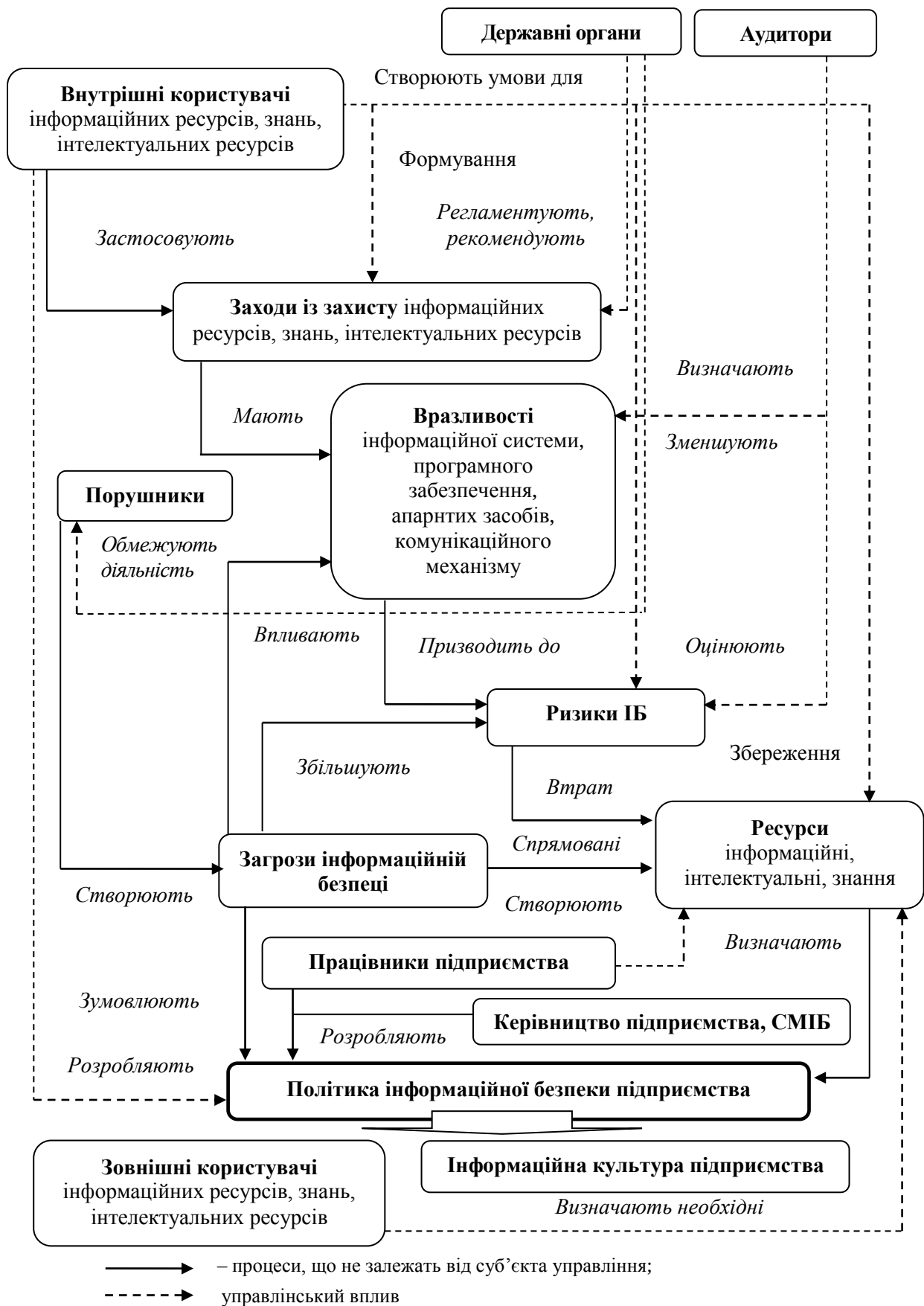


Рис. 5.8. Функціональна модель політики інформаційної безпеки підприємства [розроблено на основі 3; 4; 67; 67]

Зазначена функціональна модель формування політики інформаційної безпеки підприємства являє собою модель функціонального впливу зовнішніх і внутрішніх суб'єктів інформаційних відносин і їх вплив на стан елементів і властивостей інформаційної безпеки, на збереження матеріальних або інформаційних ресурсів. У цій моделі, на відміну від існуючих, увага зосереджується не тільки на елементах системи інформаційної безпеки та їх властивостях, але й на впливі зовнішніх і внутрішніх суб'єктів інформаційних взаємовідносин на ці елементи, їх властивості, їх зміну та ролі у формуванні політики інформаційної безпеки підприємства. Крім того, у запропонованій моделі передбачено запровадження інформаційної культури, зокрема й культури дотримання інформаційної безпеки.

Згідно з цією моделлю для ресурсів визначається їх цінність як із погляду пов'язаних із ними можливих фінансових втрат, так і в контексті загрози репутації підприємства, дезорганізації його діяльності, нематеріальної шкоди від розголошення конфіденційної інформації, на підставі чого здійснюється опис взаємозв'язків ресурсів, визначення небезпек та оцінка ймовірності їх реалізації.

Суб'єктами пропонованої моделі є внутрішні та зовнішні користувачі інформаційної системи, керівництво підприємства, його персонал, державні органи, аудитори, а також порушники інформаційної безпеки (внутрішні та зовнішні). Основними об'єктами є інформаційні ресурси, інтелектуальні ресурси та знання, для збереження безпеки яких визначаються вразливості інформаційної системи, програмного забезпечення, апаратних засобів і комунікаційного механізму та загрози інформаційній безпеці; встановлюється рівень і ймовірність виникнення ризиків інформаційній безпеці; формуються заходи щодо захисту зазначених об'єктів і, як наслідок, актуалізується політика інформаційної безпеки підприємства на основі інформаційної культури. Важливим елементом запропонованої моделі є визначення процесів, які здійснюються суб'єктом і впливають на об'єкти, або на складові системи інформаційної безпеки та процесів, які зумовлені взаємодією між об'єктами та складовими системи інформаційної безпеки.

На основі визначених взаємозв'язків обирається система заходів щодо захисту інформаційних, інтелектуальних ресурсів і знань, які знижують ризики до допустимих рівнів і мають найбільшу соціально-економічну ефективність. На відміну від існуючих систем захисту інформаційних ресурсів у межах пропонованої моделі формування політики інформаційної безпеки запропоновано включити рекомендації щодо проведення регулярних перевірок ефективності систем захисту (управління надійністю) та заходів з упровадження інформаційної культури. Отже, система заходів має

охоплювати групи заходів: управління доступом, процедур обмеження доступу, перетворення інформації, контролю загроз (із зупинкою функціонування інформаційної системи або окремих її компонентів у разі визначення системою безпеки атак, загроз та інших порушень цілісності системи), управління надійністю та формування інформаційної культури як моделі поведінки працівників у процесі роботи з інформаційними ресурсами.

Планування цих заходів здійснюється після завершення етапу аналізу ризиків інформаційної безпеки та їх вибору. Обов'язковою складовою моделі формування політики інформаційної безпеки підприємства є періодична перевірка відповідності поточного режиму інформаційної безпеки вимогам певного стандарту безпеки.

Політика інформаційної безпеки має бути еталоном, відповідно до якого можливо виміряти ступінь компетенції, ефективність виконання завдання і робочої дисципліни. По суті, політика має заздалегідь встановлювати високі стандарти інформаційної безпеки, а працівники системи менеджменту інформаційної безпеки стежити за тим, щоб персонал підприємства упорядкував відповідно до цих стандартів власні знання, навички, поведінку з інформаційними активами та роботу з інформаційною системою та повністю відповідав за інформаційну безпеку господарюючого суб'єкта, за наслідки власних дій.

Зарубіжний і вітчизняний досвід формування політики інформаційної безпеки підприємства свідчить, що для боротьби з усією сукупністю потенційно можливих загроз, пов'язаних із конфіденційною інформацією, захистом ноу-хау і підтриманням конкурентоспроможності господарюючого суб'єкта агропродовольчої сфери, необхідна злагоджена й цілеспрямована організація процесу протидії інформаційним загрозам.

Водночас організація цього процесу передбачає участь не тільки фахівців у сфері захисту інформації, а й керівництва, провідних співробітників підприємства, працівників, відповідальних за окремий напрям діяльності, та іншого персоналу, що зумовлює необхідність формування концепції поведінки працівників підприємства в ході виконання робіт з інформаційними та інтелектуальними ресурсами, використання програмного забезпечення, користування техніко-технологічними засобами та здійснення комунікаційного процесу.

Тому метою розробки політики інформаційної безпеки суб'єкта господарської діяльності у сфері інформаційної безпеки є визначення ефективного (з погляду організації) способу використання інформаційних,

інтелектуальних ресурсів і знань, а також розроблення процедур, що запобігають порушенню режиму безпеки або реагують на нього.

У межах запропонованої моделі складовими політики інформаційної безпеки вважаємо її функціональні підсистеми, які окреслюють і регулюють певні предметні області інформаційної діяльності (рис. 5.9).



Рис. 5.9. Складові політики інформаційної безпеки підприємства [авторська розробка]

Політика прийнятного використання (AUP) визначає обмеження дій працівників під час використання апаратних засобів, програмних додатків, внутрішньої мережі підприємства та мережі Інтернет, інших засобів і додатків.

Політикою контролю за доступом (ACP) передбачено розмежування та контроль за доступом до інформації, інтелектуальних активів, баз даних і баз знань підприємства.

Політика доступу до ідентичності та управління (IAM) визначає, як

ІТ-адміністратори авторизують системи та програми окремим працівникам, а співробітники створюють паролі, які б відповідали стандартам безпеки.

Політика віддаленого доступу окреслює прийнятні методи віддаленого підключення до внутрішніх мереж.

Політика безперервності бізнесу (BCP) координує зусилля підприємства, її використовують у разі катастрофи для відновлення бізнесу.

Політика реагування на інциденти (IR) регулює організаційні аспекти реагування системи менеджменту інформаційної безпеки та інших працівників підприємства на виникнення інцидентів порушення інформаційної безпеки та ліквідації їх наслідків.

Політика управління змінами визначає та регулює формальний процес внесення змін до інформаційного середовища підприємства, зокрема оптимізації інформаційної системи, системи захисту інформації, розробки програмного забезпечення, автоматизації бізнес-процесів тощо.

ІТ-операції та політика адміністрування описують взаємодію ІТ-відділів, системи менеджменту інформаційної безпеки та інших структурних підрозділів для забезпечення відповідності вимогам безпеки.

Політикою відновлення після стихійних лих передбачено організацію кібербезпеки та діяльності взаємодії ІТ-відділів, системи менеджменту інформаційної безпеки для реалізації загального плану забезпечення безперервного бізнесу.

Політикою класифікації даних передбачено інвентаризацію, аудит і класифікацію даних, інформаційних активів, інтелектуальних ресурсів і знань.

Політика безпеки даних окреслює технічні вимоги та прийнятні мінімальні стандарти щодо захисту даних відповідно до правил.

Політика конфіденційності визначає, яким чином підприємство дотримується норм, що призначені для захисту конфіденційності споживачів.

Політика електронної пошти, месенджерів, комунікації визначає, як працівники можуть використовувати обраний бізнес-канал зв'язку або обміну інформацією технічними засобами.

Політика щодо персональних і мобільних пристроїв визначає доцільність дозволу працівникам використовувати персональні пристрої для доступу до інформаційної інфраструктури підприємства та заходи зменшення інформаційного ризику.

Політика захисту «хмари» визначає рекомендації щодо використання засобів зберігання, обчислення, резервування, відновлення після збоїв, забезпечення безпеки, роботи з базами даних, які надають постачальники «хмарної» інфраструктури.

Процес формування, впровадження, виконання та актуалізації політики інформаційної безпеки підприємства, зокрема й агропродовольчої сфери (рис. 5.10), запропоновано здійснювати на основі її життєвого циклу, яким передбачено проходження таких етапів, як:



Рис. 5.10. Формування політики інформаційної безпеки підприємства агропродовольчої сфери [авторська розробка]

1. Оцінка ризику: на основі рівня ризику інформаційної безпеки визначається актуальність, оперативність, рівень упровадження політики інформаційної безпеки, а в її межах – предметна область інформаційного захисту, заходи захисту, а також рівень формалізації політики інформаційної безпеки: високорівнева політика інформаційної безпеки (задокументована політика інформаційної безпеки, яка обов'язково має бути затверджена керівництвом і доведена до відома всіх співробітників і зовнішніх контрагентів, до яких вона має відношення) або низькорівнева політика

інформаційної безпеки (частина корпоративної політики, приватна політика, якою передбачено правила захисту у конкретно визначеній області управління доступом, резервне копіювання, політика щодо персональних і мобільних пристроїв тощо).

2. Створення політики інформаційної безпеки – це перш за все визначення розділів і підрозділів документа. На основі узагальнення теоретичних положень і практик створення політик інформаційної безпеки [7; 12; 32; 55; 58; 59; 60] запропоновано в структуру політики інформаційної безпеки підприємств агропродовольчої сфери включити розділи, які б містили:

визначення об'єктів, щодо яких встановлюється режим інформаційної безпеки, їх ранжування за значимістю та встановлення необхідного й достатнього ступенів захисту;

опис загальних функцій системи менеджменту інформаційної безпеки, опис функцій кожного підрозділу, відповідального за обробку інформації та даних, їх захист, захист інформаційних ресурсів, знань та інтелектуальних ресурсів;

перелік діючих і потенційних загроз інформаційній безпеці, ранжування їх за ступенем впливу та ймовірністю виникнення;

формування карти впливу зовнішніх і внутрішніх факторів на виникнення загроз інформаційній безпеці аграрних підприємств;

визначення та характеристики зовнішніх і внутрішніх суб'єктів, які можуть стати джерелами потенційних загроз інформаційній безпеці;

опис моделі захисту інформації підприємства та технологій забезпечення інформаційної безпеки;

опис існуючих адміністративних заходів, документів, стандартів з інформаційної безпеки;

опис поняття «інцидент інформаційної безпеки», процедур повідомлення в разі його виникнення;

опис систем доступу до всіх інформаційних ресурсів підприємства, ранжування систем доступу до інформаційних активів, знань та інтелектуальних ресурсів, апаратних засобів, програмного забезпечення;

визначення рівнів доступу на призначення ролей доступу співробітникам підприємства;

опис обраної політики захисту від вірусних атак, програм-шкідників, можливих дій хакерів;

опис системи резервного копіювання важливих даних, його періодичності, моделей зберігання;

алгоритм проведення аварійних і відновлювальних робіт в разі

пошкодження апаратної частини у пожежі, проблем із електрозв'язком або з інших причин, що призвело до пошкодження апаратних засобів, носіїв інформації або власне баз даних;

алгоритм тестування, узгодження та атестації створеної системи інформаційної безпеки на відповідність встановленим вимогам діяльності підприємства;

опис системи розслідування інцидентів інформаційної безпеки власними силами чи із залученням компетентних організацій, правоохоронних органів;

план заходів із забезпечення безперебійності функціонування системи інформаційної безпеки, її оптимізації та реструктуризації.

Перелік розділів є узагальненим і визначається кожним окремим підприємством залежно від розмірів, специфіки діяльності, стратегії інформаційної безпеки, особливостей інформаційної системи та системи менеджменту інформаційної безпеки.

3. Упровадження політики інформаційної безпеки – визначення процедур доведення до відома персоналу та розповсюдження правил, норм поведінки з інформаційними ресурсами, комерційною таємницею, програмним забезпеченням та апаратними засобами. На цьому етапі створюються інформаційна культура та культура захисту інформації, що передбачає не тільки документаційне закріплення правил і їх дотримання як необхідність здійснення діяльності, а і їх сприйняття як норми поведінки. Тому інформаційна культура в межах інформаційної політики повинна відповідати головним базовим вимогам, таким як:

бути невід'ємною частиною повсякденної діяльності працівника;

до її складу мають входити не тільки знання (освіченість) у сфері інформаційної безпеки, але й цінності моделі інформаційної поведінки;

сприяти не тільки захисту інформації, а й захисту суб'єкта, який володіє інформацією, знаннями та інтелектуальними ресурсами;

сприяти не тільки захисту суб'єктів, які володіють інформацією, знаннями та інтелектуальними ресурсами, але і їх розвитку, інформаційному обміну між ними.

Виходячи з цих принципових положень, інформаційна культура та культура інформаційного захисту підприємства повинні передбачати такий спосіб організації інформаційної діяльності працівника, при якому знання і ціннісні моделі його поведінки забезпечують безпечне функціонування його та інших суб'єктів і, як наслідок, розвиток в інформаційному середовищі [12].

Як і Л. Астахова та С. Лушникова, вважаємо, що культуру інформаційної безпеки користувача інформаційної системи підприємства агропродовольчої сфери доцільно визначити як специфічний спосіб

організації інформаційної діяльності користувача, згідно з яким знання і ціннісні моделі його поведінки забезпечують йому та іншим користувачам безпечне функціонування і розвиток навичок і здібностей в інформаційному середовищі. Отже, при необхідному і достатньому рівні інформаційної культури користувач контролює створення і розповсюдження інформації, сприяючи захисту інформаційних ресурсів, інтелектуальних ресурсів і знань, захисту інших суб'єктів інформаційної діяльності як у межах підприємства, так і зовнішніх користувачів, таким чином, що це стає природним аспектом виконання його повсякденної діяльності. А культура інформаційної безпеки підприємства – це такий спосіб організації інформаційної діяльності підприємства, згідно з яким знання і ціннісні моделі поведінки його співробітників забезпечують йому безпечне функціонування і розвиток в інформаційно-технологічному середовищі [12].

З огляду на вищезазначене доцільно виокремити організаційні рішення, що сприятимуть формуванню інформаційної культури на підприємстві, такі як:

- культивування цінності інформаційної безпеки для бізнесу й активна підтримка її розвитку керівництвом і стейкхолдерами;

- наявність ціннісно-орієнтованої спрямованості політики інформаційної безпеки та інформаційної культури, які б містили закріплені морально-етичні установки моделі інформаційної поведінки співробітників підприємств агропродовольчої сфери;

- розвиток обізнаності, освіченості та розуміння співробітниками загроз інформаційній безпеці, встановлення різних видів відповідальності за порушення її правил. Важливий не тільки сам факт наявності програми підвищення обізнаності, але і якість та доступність її змісту;

- забезпечення актуальними нормативними, навчально-методичними та іншими матеріалами, їх постійне оновлення разом із застосуванням сучасних світових практик інформаційної культури та культури захисту інформації з метою підвищення рівня знань працівників у сфері інформаційної безпеки;

- організація зворотного зв'язку із працівниками, надання їм можливості висловити власну думку і внести пропозиції в політику інформаційної безпеки підприємства;

- розроблення та затвердження метрик для оцінки рівня культури інформаційної безпеки підприємства та здійснення її моніторингу. Метрики дозволять об'єктивно оцінити рівень культури, виявити слабкі й сильні сторони, а також зосередитися на питаннях, які необхідно оптимізувати.

4. Встановлення відповідності політики інформаційної безпеки, яка на цьому етапі вже формалізована та доведена до відома працівників підприємства. Крім документаційного вираження, основні положення

політики інформаційної безпеки імplementовані в корпоративну культуру підприємства. Важливою частиною цього етапу є встановлення того, наскільки дотримання прийнятої політики відповідає практиці поводження з інформаційними й інтелектуальними ресурсами та знаннями, вимогам функціонування системи інформаційної безпеки, очікуванням від упровадження політики інформаційної безпеки стейкхолдерами та працівниками підприємства.

5. Моніторинг політики інформаційної безпеки – встановлення рівня її дотримання працівниками підприємства з метою визначення найбільш слабких місць системи інформаційного захисту. В разі виявлення недотримання або грубих порушень політики інформаційної безпеки, здійснення опору або несприйняття окремих аспектів інформаційної культури та культури захисту інформації виникає потреба в аналізі причин цих відхилень, а відповідно, і перегляді та подальшій актуалізації політики інформаційної безпеки підприємства, зокрема і агропродовольчої сфери. Тому на рис. 5.12 акцентовано увагу на циклічному характері формування політики інформаційної безпеки підприємства агропродовольчої сфери. Водночас для запровадження більш ефективної політики інформаційної безпеки процес «роботи над помилками» має бути забезпечений перш за все підтримкою працівників і фахівців системи менеджменту інформаційної безпеки й обов'язковою підтримкою вищого керівництва та провідних фахівців підприємства.

Важливими аспектами зазначеного циклічного процесу формування політики інформаційної безпеки є врахування зміни драйверів політики інформаційної безпеки та її документаційне забезпечення. На ці аспекти, в свою чергу, впливають інформаційна культура та культура захисту інформації, які формуються під впливом моделі цінностей і поведінки працівника з інформаційними, інтелектуальними ресурсами, знаннями працівників підприємства. Ще однією особливістю процесу актуалізації політики інформаційної безпеки є врахування новітніх теорій та екстраполяція світових практик забезпечення політики інформаційного захисту.

Отже, запропоновані напрями актуалізації політики інформаційної безпеки підприємств агропродовольчої сфери на основі концепції інформаційної культури дозволять:

визначити основні вразливості інформаційного середовища та ризики інформаційної безпеки для формування ефективних механізмів захисту та правил їх застосування;

встановити вимоги до працівників щодо дотримання норм і правил

інформаційної безпеки;

побудувати систему контролю для захисту підприємства агропродовольчої сфери від зовнішніх і внутрішніх інформаційних загроз;

забезпечити ефективність механізму підтримки юридичних та етичних обов'язків захисту інформаційних ресурсів, інтелектуальних ресурсів і знань;

забезпечити перехід від документаційного регламентування правил інформаційної безпеки, чіткого дотримання очікуваної стейкхолдерами моделі поведінки працівника підприємства до формування у нього культурних цінностей щодо захисту інформації.

Важливим аспектом забезпечення інформаційної безпеки підприємства залишається не тільки захист ресурсів, але й вплив рівня інформаційної безпеки на зміну результатів діяльності підприємства агропродовольчої сфери.

5.3. Прогнозування результативних показників діяльності підприємств агропродовольчої сфери на основі рівня інформаційної безпеки

Характеристика інформаційної діяльності підприємства виражається через систему економічних та фінансових показників. В умовах ринкової економіки кожен суб'єкт господарювання самостійно визначає таку систему, виходячи з особливостей інформаційної активності, професіоналізму фахівців та інших факторів. В даний час забезпечення процесу інформаційної безпеки, а саме сукупність аналітичних показників, які задовольняли б вимогам об'єктивності та комплексності не відповідає потребам ефективного управління підприємством. У зв'язку з цим виникає необхідність удосконалення методичного інструментарію комплексної характеристики та оперативного прогнозування результативних показників діяльності підприємств агропродовольчої сфери на основі рівня інформаційної безпеки.

Одним із основних завдань діагностики соціально-економічного розвитку підприємств агропродовольчої сфери є визначення перспективних значень результативних показників. Важливим етапом запропонованої методології оцінювання та діагностики інформаційної безпеки підприємств агропродовольчої сфери (п. 3.1) є встановлення впливу рівня інформаційної безпеки на результативні показники діяльності підприємства агропродовольчої сфери. Результативними показниками для досліджуваних підприємств Полтавської, Сумської, Кіровоградської, Харківської та Луганської

областей було обрано обсяг виробництва продукції у грошовому вираженні (Додаток АГ) і продуктивність праці (Додаток АД).

Зміна показника обсягу виробництва продукції характеризуватиме вплив рівня інформаційної безпеки на рівень економічної та продовольчої складової підприємств агропродовольчої сфери, оскільки саме зростання обсягу виробленої продукції сільськогосподарського призначення свідчатиме про економічну ефективність діяльності та можливість забезпечити населення продуктами харчування. Зміна іншого показника – продуктивності праці – свідчатиме про ефективність діяльності кадрової складової досліджуваних підприємств. Не всі показники в межах визначених підмножин (п. 3.2) однаково впливають на інтегральний показник рівня інформаційної безпеки, а отже, і на результативні показники діяльності. Тому потрібно визначити взаємозв'язки між окремими показниками інформаційної безпеки, оцінити вплив кожного із цих показників на інтегральні оцінки відповідних підсистем, і, відповідно, вплив оцінок підсистем на інтегральну оцінку всієї системи інформаційної безпеки – все це дасть можливість виявити фактори, які першочергово впливають на підвищення рівня захисту інформації.

У підрозділі 3.2 було визначено, що підсистема системи інформаційної безпеки визначається множиною показників $X_i = \{x_{ij}\}_{j=1}^{m_i}$. Тому тіснота зв'язку між показниками x_{ij} та $x_{ij'}$ цієї множини характеризуватиметься значенням коефіцієнта кореляції [64], який визначається рівністю (5.1):

$$r_{jj'}^i = \frac{\sum_{r=1}^5 \sum_{t=1}^T (x_{ij}(t, r) - \bar{x}_{ij})(x_{ij'}(t, r) - \bar{x}_{ij'})}{\sqrt{\sum_{r=1}^5 \sum_{t=1}^T (x_{ij}(t, r) - \bar{x}_{ij})^2 \sum_{r=1}^5 \sum_{t=1}^T (x_{ij'}(t, r) - \bar{x}_{ij'})^2}}, \quad (5.1)$$

де $x_{ij}(t, r)$, $x_{ij'}(t, r)$ – значення показників x_{ij} та $x_{ij'}$ в рік t для групи досліджуваних підприємств агропродовольчої сфери r -ї області;

$\bar{x}_{ij}$, $\bar{x}_{ij'}$ – середні значення показників x_{ij} та $x_{ij'}$ усіх підприємств агропродовольчої сфери всіх досліджуваних областей за всі роки ретроспективного періоду.

Для кожної підсистеми, що визначається множинами X_i , визначено кореляційну матрицю, елементами якої є коефіцієнти кореляції $r_{jj'}^i$.

Щоб упевнитись, що визначені коефіцієнти кореляції відображають реальні статистичні зв'язки між показниками, застосовано критерій

Стюдента [73]. Для кожного коефіцієнта кореляції $r_{jj'}^i$ обраховано величину $t_{jj'}^i$ за формулою (5.2):

$$t_{jj'}^i = \frac{r_{jj'}^i}{\sqrt{1 - (r_{jj'}^i)^2}} \sqrt{N - 2}, \quad (5.2)$$

де N – кількість відомих значень показника x_{ij} .

Оскільки дані обрані за підприємствами п'яти областей за 10 років (2009–2018 рр.), то для формування задачі $N = 50$. Одержані значення $t_{jj'}^i$ порівняно із табличним значенням критерію Стюдента $t(\alpha, k)$, де α – довірча ймовірність, яку прийнято рівною 0,99, а k – кількість ступенів свободи, в цьому разі $k = N - 2 = 48$. Якщо $t_{jj'}^i > t(\alpha, k)$, то коефіцієнт кореляції є значимим, а статистичний зв'язок між відповідними показниками – доведеним.

Отже, для підсистеми програмно-технічного забезпечення захищеності інформаційної системи кореляційна матриця матиме такий вигляд (табл. 5.6):

Таблиця 5.6

Кореляційна матриця підсистеми програмно-технічного забезпечення захищеності інформаційної системи підприємства [побудовано автором]

	x_{11}	x_{12}	x_{13}	x_{14}
x_{11}	1,00000	0,81751	0,59915	0,40922
x_{12}	0,81751	1,00000	0,66784	0,32987
x_{13}	0,59915	0,66784	1,00000	0,71340
x_{14}	0,40922	0,32987	0,71340	1,00000

Критерій Стюдента підтверджує, що всі коефіцієнти кореляції в цій матриці є значимими. Найтісніше взаємозв'язок простежується між показниками x_{11} – коефіцієнт технічного захисту інформаційної системи та x_{12} – коефіцієнт програмної захищеності інформаційної системи. Коефіцієнт кореляції між ним дорівнює 0,81751.

Для підсистеми фінансового забезпечення захищеності інформаційної системи підприємства агропродовольчої сфери кореляційна матриця матиме такий вигляд (табл. 5.7):

Критерій Стюдента підтверджує, що всі коефіцієнти кореляції в цій матриці є значимими, крім коефіцієнта, що відображає зв'язок між

показниками x_{22} – коефіцієнт фінансування інформаційних служб підприємства та x_{29} – коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства.

Таблиця 5.7

Кореляційна матриця підсистеми фінансового забезпечення захищеності інформаційної системи підприємства [побудовано автором]

	x_{21}	x_{22}	x_{23}	x_{24}	x_{25}	x_{26}	x_{27}	x_{28}	x_{29}	x_{210}
x_{21}	1,00000	0,90833	0,94973	0,79333	0,68702	0,60170	0,57560	0,56593	0,42978	0,60778
x_{22}	0,90833	1,00000	0,73926	0,66375	0,55050	0,48381	0,46816	0,44197	0,32324	0,47074
x_{23}	0,94973	0,73926	1,00000	0,79818	0,70069	0,60551	0,58355	0,58199	0,44463	0,62466
x_{24}	0,79333	0,66375	0,79818	1,00000	0,84803	0,70281	0,80559	0,80253	0,52046	0,80285
x_{25}	0,68702	0,55050	0,70069	0,84803	1,00000	0,72573	0,81814	0,80030	0,54880	0,82642
x_{26}	0,60170	0,48381	0,60551	0,70281	0,72573	1,00000	0,80659	0,89611	0,42556	0,82020
x_{27}	0,57560	0,46816	0,58355	0,80559	0,81814	0,80659	1,00000	0,91852	0,47699	0,89904
x_{28}	0,56593	0,44197	0,58199	0,80253	0,80030	0,89611	0,91852	1,00000	0,47171	0,88299
x_{29}	0,42978	0,32324	0,44463	0,52046	0,54880	0,42556	0,47699	0,47171	1,00000	0,56935
x_{210}	0,60778	0,47074	0,62466	0,80285	0,82642	0,82020	0,89904	0,88299	0,56935	1,00000

Зв'язок між зазначеними показниками не підтверджений статистичними даними. Найтісніше пов'язані між собою показники x_{21} – коефіцієнт фінансування інформаційної безпеки та x_{23} – коефіцієнт фінансування програмно-технічної захищеності інформації (коефіцієнт кореляції дорівнює 0,94973), а також показники x_{21} – коефіцієнт фінансування інформаційної безпеки та x_{22} – коефіцієнт фінансування інформаційних служб підприємства (коефіцієнт кореляції дорівнює 0,90833).

Наступним етапом є побудова матриці кореляції для підсистеми кадрового забезпечення захищеності інформаційної системи (табл. 5.8).

Таблиця 5.8

Кореляційна матриця підсистеми кадрового забезпечення захищеності інформаційної системи підприємства [побудовано автором]

	x_{31}	x_{32}	x_{33}	x_{34}	x_{35}	x_{36}	x_{37}
x_{31}	1,00000	0,84907	-0,19117	-0,69928	0,78237	-0,39790	0,82755
x_{32}	0,84907	1,00000	-0,31038	-0,75597	0,65156	-0,61295	0,94696
x_{33}	-0,19117	-0,31038	1,00000	0,19815	-0,27981	0,15027	-0,33794
x_{34}	-0,69928	-0,75597	0,19815	1,00000	-0,71095	0,59965	-0,66978
x_{35}	0,78237	0,65156	-0,27981	-0,71095	1,00000	-0,41946	0,59874
x_{36}	-0,39790	-0,61295	0,15027	0,59965	-0,41946	1,00000	-0,61831
x_{37}	0,82755	0,94696	-0,33794	-0,66978	0,59874	-0,61831	1,00000

Критерій Стюдента підтверджує, що майже всі коефіцієнти кореляції в цій матриці є значимими, крім коефіцієнтів, що відображають зв'язки показника x_{33} – коефіцієнта ненадійності персоналу, що забезпечує інформаційну безпеку підприємства з усіма іншими показниками. Найтісніше пов'язані між собою показники x_{32} – коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства, та x_{37} – коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку (коефіцієнт кореляції дорівнює 0,94696).

Для подальшого аналізу побудовано кореляційну матрицю підсистеми інформаційного забезпечення захищеності інформаційної системи підприємства та встановлено тісноту взаємозв'язку між показниками в межах цієї підсистеми (табл. 5.9).

Таблиця 5.9

Кореляційна матриця підсистеми інформаційного забезпечення захищеності інформаційної системи підприємства [побудовано автором]

	x_{41}	x_{42}	x_{43}	x_{44}	x_{45}	x_{46}
x_{41}	1,00000	-0,56463	-0,69357	-0,67928	-0,60478	-0,59608
x_{42}	-0,56463	1,00000	0,72252	0,81844	0,75404	0,57822
x_{43}	-0,69357	0,72252	1,00000	0,87208	0,86214	0,72403
x_{44}	-0,67928	0,81844	0,87208	1,00000	0,90734	0,68266
x_{45}	-0,60478	0,75404	0,86214	0,90734	1,00000	0,67205
x_{46}	-0,59608	0,57822	0,72403	0,68266	0,67205	1,00000

Критерій Стюдента підтверджує, що всі коефіцієнти кореляції в цій матриці є значимими. Зв'язок між цими показниками не підтверджений статистичними даними. Найтісніше пов'язані між собою показники x_{44} – коефіцієнт своєчасності надання інформації та x_{45} – коефіцієнт надійності інформації (коефіцієнт кореляції дорівнює 0,90734).

Для підсистеми організаційного забезпечення захищеності інформаційної системи визначено тісноту взаємозв'язку коефіцієнтів в побудованій кореляційній матриці (табл. 5.10).

Критерій Стюдента підтверджує, що всі коефіцієнти кореляції в цій матриці є значимими, крім коефіцієнтів, що відображають зв'язки між показниками x_{51} – коефіцієнт керованості системи інформаційної безпеки підприємства та x_{55} – гнучкість системи інформаційної безпеки підприємства. Зв'язок між цими показниками не підтверджений статистичними даними. Найтісніше пов'язані між собою показники x_{56} – наявність і актуальність нормативно-правового забезпечення системи інформаційної безпеки

підприємства та x_{58} – наявність на підприємстві стратегії інформаційної безпеки (коефіцієнт кореляції дорівнює 0,89896).

Таблиця 5.10

Кореляційна матриця підсистеми організаційного забезпечення захищеності інформаційної системи підприємства [побудовано автором]

	x_{51}	x_{52}	x_{53}	x_{54}	x_{55}	x_{56}	x_{57}	x_{58}	x_{59}
x_{51}	1,00000	0,71209	0,74603	-0,78127	0,26318	0,49683	0,49906	0,46499	0,30753
x_{52}	0,71209	1,00000	0,82414	-0,74091	0,55698	0,60997	0,64594	0,57283	0,57728
x_{53}	0,74603	0,82414	1,00000	-0,71727	0,44407	0,57689	0,60682	0,51686	0,45109
x_{54}	-0,78127	-0,74091	-0,71727	1,00000	-0,37961	-0,67447	-0,66818	-0,63825	-0,52795
x_{55}	0,26318	0,55698	0,44407	-0,37961	1,00000	0,60221	0,56695	0,70302	0,72887
x_{56}	0,49683	0,60997	0,57689	-0,67447	0,60221	1,00000	0,68955	0,89896	0,67588
x_{57}	0,49906	0,64594	0,60682	-0,66818	0,56695	0,68955	1,00000	0,66869	0,77784
x_{58}	0,46499	0,57283	0,51686	-0,63825	0,70302	0,89896	0,66869	1,00000	0,74255
x_{59}	0,30753	0,57728	0,45109	-0,52795	0,72887	0,67588	0,77784	0,74255	1,00000

Аналогічним чином побудовано матрицю кореляції між інтегральними оцінками підсистеми системи забезпечення інформаційної безпеки підприємства (табл. 5.11).

Таблиця 5.11

Кореляційна матриця показників інтегральних оцінок підсистем системи забезпечення інформаційної безпеки підприємства [побудовано автором]

	X_1	X_2	X_3	X_4	X_5
X_1	1,00000	0,93394	0,87090	0,72085	0,88722
X_2	0,93394	1,00000	0,91907	0,83738	0,84084
X_3	0,87090	0,91907	1,00000	0,84285	0,86555
X_4	0,72085	0,83738	0,84285	1,00000	0,63291
X_5	0,88722	0,84084	0,86555	0,63291	1,00000

Критерій Стюдента підтверджує, що всі коефіцієнти кореляції в цій матриці є значимими. Найтісніше пов'язані між собою оцінка X_1 – підсистеми програмно-технічного забезпечення та X_2 – підсистеми фінансового забезпечення (коефіцієнт кореляції дорівнює 0,93394). Тісний зв'язок також наявний між оцінками X_2 – підсистеми фінансового забезпечення та X_3 – підсистеми кадрового забезпечення (коефіцієнт кореляції дорівнює 0,91907).

Наступним етапом є визначення та оцінка зв'язків між інтегральними оцінками підсистем системи забезпечення інформаційної безпеки підприємства та показниками, що відображають окремі елементи цих

підсистем. Така оцінка надасть можливість скласти рейтинг показників x_{ij} у множині X_i , яка визначає підсистему. Місця показників у рейтингу визначаються відповідно до абсолютних величин коефіцієнтів кореляції між цими показниками та інтегральною оцінкою підсистеми X_i .

Визначені коефіцієнти кореляції між показниками та інтегральною оцінкою підсистеми програмно-технічного забезпечення захищеності інформаційної системи підприємства та рейтинги показників у підсистемі наведено в табл. 5.12.

Таблиця 5.12

Рейтинги показників підсистеми програмно-технічного забезпечення захищеності інформаційної системи підприємства [побудовано автором]

Показник	Коефіцієнт кореляції	Рейтинг показника
x_{13} – коефіцієнт автоматизації програмно-технічної захищеності інформаційної системи	0,865134	1
x_{11} – коефіцієнт технічного захисту інформаційної системи	0,842366	2
x_{12} – коефіцієнт програмної захищеності інформаційної системи	0,815574	3
x_{14} – коефіцієнт інноваційності (новітності) програмно-технічної захищеності інформаційної системи	0,785753	4

Отже, відповідно до значення коефіцієнта кореляції в підсистемі програмно-технічного забезпечення захищеності інформаційної системи підприємства на інтегральне оціночне значення цієї підсистеми найбільший вплив має коефіцієнт автоматизації програмно-технічної захищеності інформаційної системи та коефіцієнт технічного захисту інформаційної системи. Дещо менше, але суттєво впливають коефіцієнт програмної захищеності інформаційної системи та коефіцієнт інноваційності програмно-технічної захищеності інформаційної системи.

За аналогією побудовано рейтинг показників підсистеми фінансового забезпечення інформаційної системи підприємства (табл. 5.13).

Таблиця 5.13

Рейтинги показників підсистеми фінансового забезпечення інформаційної системи підприємства [побудовано автором]

Показник	Коефіцієнт кореляції	Рейтинг показника
1	2	3
x_{24} – коефіцієнт фінансування інформаційної безпеки фінансової підсистеми підприємства	0,921119	1
x_{21} – коефіцієнт фінансування інформаційної безпеки	0,901625	2

1	2	3
x ₂₃ – коефіцієнт фінансування програмно-технічної захищеності інформації	0,886678	3
x ₂₅ – коефіцієнт фінансування інформаційної безпеки виробничої підсистеми підприємства	0,875456	4
x ₂₁₀ – коефіцієнт фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства	0,859498	5
x ₂₇ – коефіцієнт фінансування програмної захищеності інформації	0,853367	6
x ₂₈ – коефіцієнт фінансування технічної захищеності інформації	0,848787	7
x ₂₆ – коефіцієнт фінансування інформаційної безпеки комерційної, інноваційної та продовольчої підсистем підприємства	0,822578	8
x ₂₂ – коефіцієнт фінансування інформаційних служб підприємства	0,774830	9
x ₂₉ – коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства	0,542574	10

Відповідно до рейтингу на зазначену підсистему найбільший вплив мають коефіцієнт фінансування інформаційної безпеки фінансової підсистеми підприємства, коефіцієнт фінансування інформаційної безпеки, коефіцієнт фінансування програмно-технічної захищеності інформації, коефіцієнт фінансування інформаційної безпеки виробничої підсистеми підприємства.

На фінансове забезпечення дещо менше впливають коефіцієнт фінансування інформаційної безпеки виробничої підсистеми підприємства, коефіцієнт фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства, коефіцієнт фінансування програмної захищеності інформації, коефіцієнт фінансування технічної захищеності інформації, коефіцієнт фінансування інформаційної безпеки комерційної, інноваційної та продовольчої підсистем підприємства.

Менше, але теж вагомо впливають коефіцієнт фінансування інформаційних служб підприємства та коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства.

Наступним є аналіз рейтингу показників підсистеми кадрового забезпечення відповідно до отриманих коефіцієнтів кореляції (табл. 5.14).

Першими за рейтингом, а відповідно, за силою впливу на інтегральне значення показника підсистеми кадрового забезпечення системи інформаційної безпеки є коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства, коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку, коефіцієнт обізнаності працівників

підприємства з політикою інформаційної безпеки.

Таблиця 5.14

Рейтинги показників підсистеми кадрового забезпечення захищеності інформаційної системи підприємства [побудовано автором]

Показник	Коефіцієнт кореляції	Рейтинг показника
X ₃₂ – коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства	0,911376	1
X ₃₇ – коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку	0,904749	2
X ₃₁ – коефіцієнт обізнаності працівників підприємства з політикою інформаційної безпеки	0,868422	3
X ₃₅ – коефіцієнт освіченості персоналу системи управління інформаційною безпекою	0,775646	4
X ₃₄ – коефіцієнт невідповідності персоналу до розпізнавання загроз інформаційній безпеці	-0,766730	5
X ₃₆ – коефіцієнт правової незахищеності інформації	-0,583380	6
X ₃₃ – коефіцієнт ненадійності персоналу, що забезпечує інформаційну безпеку підприємства	-0,575010	7

Меншим за рейтингом і за впливом є коефіцієнт освіченості персоналу системи управління інформаційною безпекою. Найменше впливають коефіцієнт невідповідності персоналу до розпізнавання загроз інформаційній безпеці, коефіцієнт правової незахищеності інформації та коефіцієнт ненадійності персоналу, що забезпечує інформаційну безпеку підприємства. Не менш важливим залишається визначення рейтингів показників підсистеми інформаційного забезпечення захищеності інформаційної системи підприємства, які наведені в табл. 5.15.

Таблиця 5.15

Рейтинги показників підсистеми інформаційного забезпечення захищеності інформаційної системи підприємства [побудовано автором]

Показник	Коефіцієнт кореляції	Рейтинг показника
X ₄₅ – коефіцієнт надійності інформації	0,953174	1
X ₄₄ – коефіцієнт своєчасності надання інформації	0,938909	2
X ₄₃ – коефіцієнт суперечливості інформації	0,890985	3
X ₄₂ – коефіцієнт точності інформації	0,865202	4
X ₄₆ – коефіцієнт коректності форми подання інформації	0,771765	5
X ₄₁ – коефіцієнт повноти інформації	-0,573150	6

На інтегральний показник підсистеми інформаційного забезпечення у значній мірі впливають майже всі одиничні показники, зокрема коефіцієнт

надійності інформації, коефіцієнт своєчасності надання інформації, коефіцієнт суперечливості інформації та коефіцієнт точності інформації.

На інтегральне значення менше впливає коефіцієнт коректності форми подання інформації, а найменше – коефіцієнт повноти інформації, хоча це один із найважливіших показників оцінки інформації.

Наступним є рейтинги показників підсистеми організаційного забезпечення захищеності інформаційної системи підприємства (табл. 5.16).

Таблиця 5.16

Рейтинги показників підсистеми організаційного забезпечення захищеності інформаційної системи підприємства [побудовано автором]

Показник	Коефіцієнт кореляції	Рейтинг показника
X ₅₈ – наявність на підприємстві стратегії інформаційної безпеки	0,903677	1
X ₅₉ – наявність на підприємстві підрозділу управління інформаційною безпекою	0,876667	2
X ₅₆ – наявність і актуальність нормативно-правового забезпечення системи інформаційної безпеки підприємства та продовольчої підсистеми підприємства	0,869827	3
X ₅₇ – наявність на підприємстві політики інформаційної безпеки	0,863724	4
X ₅₅ – гнучкість системи інформаційної безпеки підприємства	0,784546	5
X ₅₂ – коефіцієнт власного програмного забезпечення	0,760954	6
X ₅₄ – ступінь інформаційного ризику	-0,756690	7
X ₅₃ – коефіцієнт власних технічних засобів	0,687498	8
X ₅₁ – коефіцієнт керованості системи інформаційної безпеки підприємства	0,609486	9

Менша частина показників цієї групи найбільше впливає на значення інтегрального показника підсистеми організаційного забезпечення, серед них: наявність на підприємстві стратегії інформаційної безпеки, наявність на підприємстві підрозділу управління інформаційною безпекою, наявність і актуальність нормативно-правового забезпечення системи інформаційної безпеки підприємства та продовольчої підсистеми підприємства, наявність на підприємстві політики інформаційної безпеки. Інша частина показників має менший, але теж тісний зв'язок із значенням інтегрального показника підсистеми, зокрема такі: гнучкість системи інформаційної безпеки підприємства, коефіцієнт власного програмного забезпечення, ступінь інформаційного ризику, коефіцієнт власних технічних засобів, коефіцієнт керованості системи інформаційної безпеки підприємства.

Отже, під час прийняття управлінських рішень щодо поліпшення інформаційної безпеки підприємства необхідно насамперед звернути увагу

на автоматизацію програмно-технічної захищеності інформаційної системи, фінансування інформаційної безпеки фінансової підсистеми підприємства, досвід роботи персоналу, що забезпечує інформаційну безпеку підприємства, надійність інформації та наявність на підприємстві стратегії інформаційної безпеки, оскільки відповідні показники мають найвищі рейтинги в своїх підсистемах і тісно пов'язані з іншими показниками інформаційної безпеки. Тому їх зростання сприятиме поліпшенню всієї системи забезпечення інформаційної безпеки підприємства. Потрібно зауважити, що інші показники теж достатньо тісно пов'язані із інтегральними оцінками відповідних підсистем, а отже, під час прийняття управлінських рішень їх теж потрібно брати до уваги.

Проаналізуємо зв'язки між інтегральними оцінками підсистем системи забезпечення інформаційної безпеки підприємства та загальною інтегральною оцінкою всієї системи, що дає можливість визначити рейтинг вказаних підсистем. Місця показників у рейтингу визначаються відповідно до абсолютних величин коефіцієнтів кореляції між інтегральними оцінками підсистем, що, у свою чергу, визначаються множинами показників X_i та інтегральною оцінкою всієї системи забезпечення інформаційної безпеки підприємства.

Визначені коефіцієнти кореляції між вказаними інтегральними оцінками та відповідні рейтинги підсистем наведено в табл. 5.17.

Таблиця 5.17

Рейтинги підсистем системи забезпечення інформаційної безпеки підприємств [побудовано автором]

Підсистема	Коефіцієнт кореляції	Рейтинг підсистеми
X_3 – кадрового забезпечення	0,968775	1
X_2 – фінансового забезпечення	0,952406	2
X_5 – організаційного забезпечення	0,943839	3
X_1 – програмно-технічного забезпечення	0,934605	4
X_4 – інформаційного забезпечення	0,829278	5

Найвищий рейтинг має підсистема кадрового забезпечення. Дещо меншими є коефіцієнти кореляції підсистем фінансового, організаційного та програмно-технічного забезпечення. На рівень інформаційної безпеки найменше впливають підсистеми інформаційного забезпечення захищеності інформаційної системи підприємства. Оскільки коефіцієнти кореляції між інтегральними оцінками підсистем і всієї системи є значними, то під час прийняття рішень щодо поліпшення захисту інформації в інформаційній

системі підприємства агропродовольчої сфери України потрібно приділяти увагу розвитку всіх підсистем.

Установивши рейтинги показників і підсистем, доцільно визначити вплив інтегральної оцінки інформаційної безпеки підприємств агропродовольчої сфери України на результативні показники їх діяльності. Як зазначалося, для дослідження вибрано такі показники: обсяг продукції сільського господарства підприємств Полтавської, Сумської, Харківської, Кіровоградської та Луганської областей (у постійних цінах 2010 р., млн грн), у 2009–2018 рр. і продуктивність праці в зазначених підприємствах (на одного зайнятого в сільськогосподарському виробництві, у постійних цінах 2010 р., грн). Зазначені показники позначено через P_1 та P_2 відповідно.

Коефіцієнти кореляції між показниками P_k та інтегральною оцінкою W інформаційної безпеки підприємства визначено за рівністю (5.3):

$$r_k = \frac{\sum_{r=1}^5 \sum_{t=1}^T (P_k(t, r) - \bar{P}_k)(W(t, r) - \bar{W})}{\sqrt{\sum_{r=1}^5 \sum_{t=1}^T (P_k(t, r) - \bar{P}_k)^2 \sum_{r=1}^5 \sum_{t=1}^T (W(t, r) - \bar{W})^2}}, \quad (5.3)$$

де $P_k(t, r)$ – значення показників P_k ($k = 1$ або $k = 2$) в рік t для r -ї групи підприємств агропродовольчої сфери досліджуваної області;

$\bar{P}_k$ – середні значення цих показників за всіма досліджуваними підприємствами агропродовольчої сфери всіх досліджуваних областей за всі роки ретроспективного періоду;

$W(t, r)$ – інтегральна оцінка системи інформаційної безпеки підприємств r -ї області за рік t ;

$\bar{W}(t, r)$ – середня інтегральна оцінка інформаційної безпеки підприємств за всіма досліджуваними підприємствами агропродовольчої сфери всіх досліджуваних областей за весь ретроспективний період;

T – тривалість ретроспективного періоду ($T = 10$).

Обчислення зазначених коефіцієнтів показало, що коефіцієнт кореляції між обсягом продукції сільськогосподарських підприємств та інтегральною оцінкою інформаційної безпеки цих підприємств становить $r_1 = 0,719225$, а коефіцієнт кореляції між продуктивністю праці та інтегральною оцінкою інформаційної безпеки підприємств – $r_2 = 0,656147$.

Для визначення значимості цих коефіцієнтів кореляції застосовано критерій Стюдента [73]. Для кожного коефіцієнта кореляції r_k визначено

величину за формулою (5.4):

$$t_k = \frac{r_k}{\sqrt{1-r_k^2}} \sqrt{N-2}, \quad (5.4)$$

де N – кількість відомих значень досліджених показників ($N = 50$). Одержані значення t_k порівняно із табличним значенням критерію Стюдента такі: $t(\alpha, N-2)$, де α – довірча імовірність, яку прийнято рівною 0,99, а $N-2 = 48$ – кількість ступенів свободи. Якщо $t_k > t(\alpha, N-2)$, то коефіцієнт кореляції вважається значимим, а статистичний зв'язок між відповідними показниками доведеним. Результати обчислень наведено в табл. 5.18.

Таблиця 5.18

Значимість коефіцієнтів кореляції між результативними показниками та інтегральною оцінкою інформаційної безпеки [побудовано автором]

k	Показник P_k	Коефіцієнт кореляції r_k	t_k	$t(\alpha, N-2)$	Висновок
1	Обсяг продукції сільськогосподарських підприємств	0,719225	7,171993	2,682204	Коефіцієнт значимий
2	Продуктивність праці в сільськогосподарських підприємствах	0,656147	6,023958	2,682204	Коефіцієнт значимий

Отже, доведено існування статистичного зв'язку інтегральної оцінки інформаційної безпеки досліджуваних підприємств агропродовольчої сфери із показниками обсягу продукції цих підприємств і продуктивністю праці. Для аналітичного відображення цих зв'язків записані рівняння парної лінійної регресії: $P_1 = p_{11}W + p_{10}$ (для показника обсягу продукції); $P_2 = p_{21}W + p_{20}$ (для показника продуктивності праці).

Для визначення коефіцієнтів p_{k1} та p_{k0} (де $k = 1$ або $k = 2$) розв'язано систему рівнянь (5.7):

$$\begin{cases} p_{k1} \sum_{r=1}^5 \sum_{t=1}^T W^2(t, r) + p_{k0} \sum_{r=1}^5 \sum_{t=1}^T W(t, r) = \sum_{r=1}^5 \sum_{t=1}^T P_k(t, r) W(t, r) \\ p_{k1} \sum_{r=1}^5 \sum_{t=1}^T W(t, r) + 50 p_{k0} = \sum_{r=1}^5 \sum_{t=1}^T P_k(t, r) \end{cases} \quad (5.7)$$

де $P_k(t, r)$ – значення показника P_k у групі підприємств агропродовольчої сфери досліджуваної r -ї області у t -й рік;

$W(t, r)$ – відповідне значення інтегральної оцінки W інформаційної безпеки.

Розв'язавши ці системи, одержали: $p_{11} = 10056,0427$; $p_{10} = 1913,4432$; $p_{21} = 215760,2610$; $p_{20} = 125399,2647$.

Отже, рівняння парної лінійної регресії для показника обсягу продукції сільськогосподарських підприємств має вигляд: $P_1 = 10056,0427 W + 1913,4432$, а для показника продуктивності праці в сільськогосподарських підприємствах має вигляд: $P_2 = 215760,2610 W + 125399,2647$.

Для перевірки адекватності одержаних рівнянь використано критерій Фішера [64].

Для цього визначено коефіцієнти детермінації за формулою (5.8):

$$R_k^2 = 1 - \frac{\sum_{t=1}^T \sum_{r=1}^5 (P_k(t, r) - p_{k1}W(r, t) - p_{k0})^2}{\sum_{t=1}^T \sum_{r=1}^5 (P_k(t, r) - \bar{P}_k)^2}, \quad (5.8)$$

де $\bar{P}_k$ – середнє значення показника P_k за всіма групами підприємств агропродовольчої сфери всіх досліджуваних областей і за всіма роками. Ці коефіцієнти дорівнюють $R_1^2 = 0,517284600$, $R_2^2 = 0,430524428$.

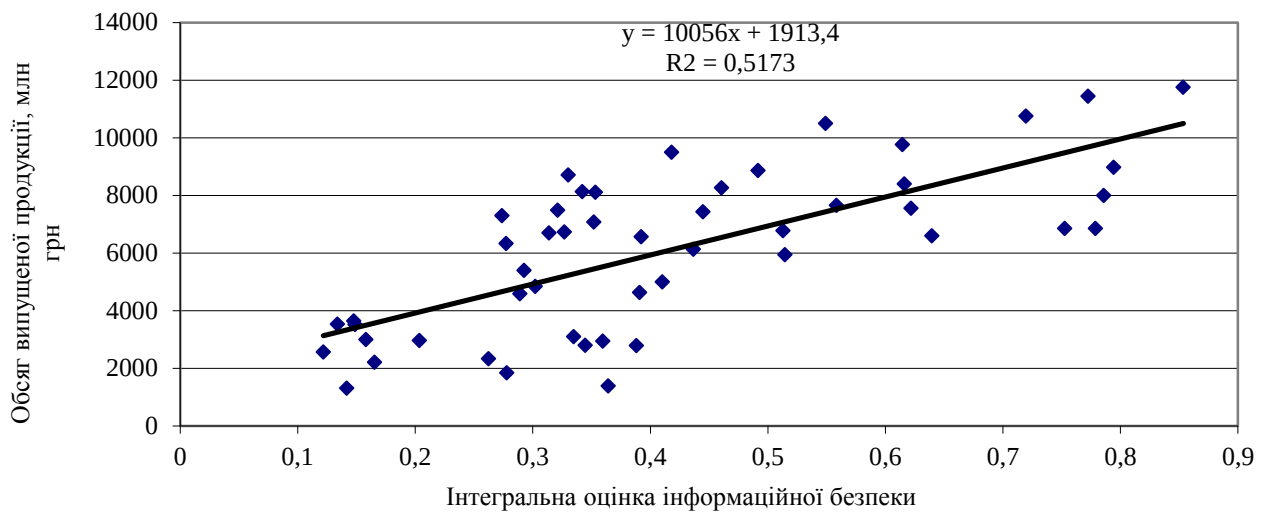
Потім визначено відповідні фактичні значення критерію Фішера за формулою (5.9):

$$F_k = \frac{R_k^2}{1 - R_k^2} (5T - 2), \quad (5.9)$$

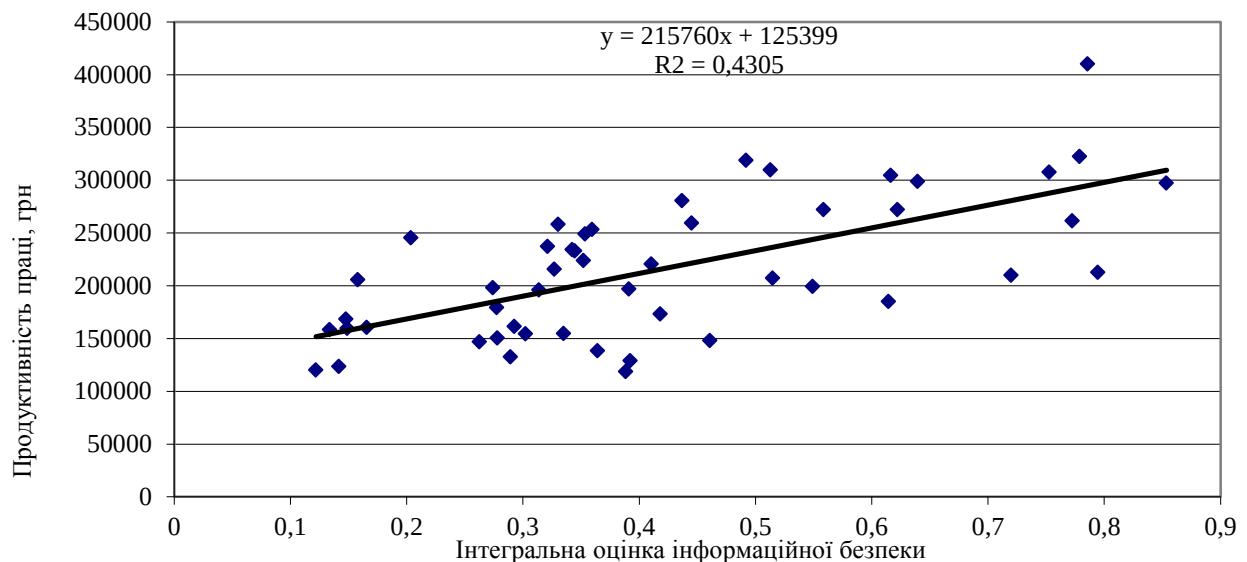
де $T = 10$.

Одержано $F_1 = 51,43748$, $F_2 = 36,28800$. Ці значення порівняно із критичним значенням критерію Фішера $F(\alpha, k_1, k_2)$, де α – довірча імовірність, k_1 та k_2 – ступені свободи. Для парної лінійної регресії $k_1 = 1$, $k_2 = 5T - 2 = 48$. Імовірність α прийнято рівною 0,99. Тоді $F(\alpha, k_1, k_2) = 7,19422$. Оскільки наявна нерівність $F_k > F(\alpha, k_1, k_2)$, то одержані рівняння регресії є адекватними. Залежність показників обсягів випущеної продукції та продуктивності праці на досліджуваних підприємствах показана на рис. 5.11.

Одержані рівняння регресії використано для прогнозування показників обсягів випущеної продукції та продуктивності праці на сільськогосподарських підприємствах на майбутні періоди. Для цього визначено прогнозовані значення інтегральної оцінки інформаційної безпеки підприємств досліджуваних областей за методикою, описаною у підрозділі 3.2.



а) залежність обсягу виробництва продукції від інтегральної оцінки інформаційної безпеки підприємств агропродовольчої сфери України



а) залежність продуктивності продукції від інтегральної оцінки інформаційної безпеки підприємств агропродовольчої сфери України

Рис. 5.11. Рівняння залежності результативних показників діяльності досліджуваних підприємств від показника інтегральної оцінки інформаційної безпеки підприємств агропродовольчої сфери України [побудовано автором]

Отже, рівняння регресії (5.10) залежності показника обсягу продукції від показника інтегральної оцінки інформаційної безпеки підприємств агропродовольчої сфери України матиме вигляд:

$$P_1 = p_{11}W + p_{10}. \quad (5.10)$$

А рівняння регресії (5.11) залежності показника продуктивності праці від показника інтегральної оцінки інформаційної безпеки підприємств агропродовольчої сфери України матиме вигляд:

$$P_2 = p_{21}W + p_{20}. \quad (5.11)$$

Через W_1 позначено відому інтегральну оцінку інформаційної безпеки досліджуваних підприємств агропродовольчої сфери конкретної області в останній рік ретроспективного періоду, а через W_2 – прогнозовану інтегральну оцінку на визначений рік. Через $\Delta W = W_2 - W_1$ позначено очікуваний приріст інтегральної оцінки за період від закінчення ретроспективного періоду до року, на який здійснюється прогноз. Очікуваний приріст за цей період показників обсягу продукції та продуктивності праці досліджуваних підприємств агропродовольчої сфери конкретної області позначено, відповідно, через ΔP_1 та ΔP_2 . Для показників P_1 та P_2 одержано рівності (5.12 та 5.13):

$$\Delta P_1 = (p_{11}W_2 + p_{10}) - (p_{11}W_1 + p_{10}) = p_{11}(W_2 - W_1) = p_{11}\Delta W, \quad (5.12)$$

$$\Delta P_2 = (p_{21}W_2 + p_{20}) - (p_{21}W_1 + p_{20}) = p_{21}(W_2 - W_1) = p_{21}\Delta W, \quad (5.13)$$

де $\Delta W = W_2 - W_1$ – очікуваний приріст інтегральної оцінки за період від закінчення ретроспективного періоду до року, на який робиться прогноз;

ΔP_1 та ΔP_2 – очікуваний приріст показників обсягу продукції та продуктивності праці на підприємствах агропродовольчої сфери кожної досліджуваної області.

Прогнозоване значення показників P_1 та P_2 обчислено шляхом додавання одержаних очікуваних приростів указаних показників до їх значень в останній рік ретроспективного періоду. Результати обчислень наведено в табл. 5.19.

За прогнозованими даними, у 2020 р. досліджувані підприємства агропродовольчої сфери Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей матимуть приріст показника інтегральної оцінки інформаційної безпеки. Найбільший приріст матимуть підприємства Сумщини (0,03181) та Полтавщини (0,03166), найменший – Луганщини (0,02047) та Харківщини (0,01093). Відповідним чином відбувався і приріст обсягу випущеної продукції підприємств за досліджуваними областями: найбільше у Сумській області – 319,883 млн грн, у Полтавській – 318,374 млн грн, менше у Кіровоградській – 289,513 млн грн, найменше у Луганській – 205,847 млн грн і Харківській – 109,913 млн грн.

Зберігаються тенденції за областями і в прирості показника продуктивності праці: на досліджуваних підприємствах агропродовольчої сфери Сумської області приріст становив 6863,33 грн, Полтавської – 6830,97 грн, Кіровоградської – 6211,74 грн, Луганської – 4416,61 грн і Харківської – 2358,26 грн.

Таблиця 5.19

Прогноз зміни результативних показників від зміни інтегрального показника рівня інформаційної безпеки підприємств агропродовольчої сфери України на 2020 р. [побудовано автором]

Показник Область	Інтегральна оцінка інформаційної безпеки			Обсяг продукції, млн грн			Продуктивність праці, грн		
	2018 р.	Прогноз на 2020 р.	Приріст	2018 р.	Прогноз на 2020 р.	Приріст	2018 р.	Прогноз на 2020 р.	Приріст
Полтавська	0,9327	0,96436	0,03166	11748,8	12067,2	318,374	297167	303998	6830,97
Кіровоградська	0,6577	0,68649	0,02879	7546,8	7836,31	289,513	271948	278160	6211,74
Сумська	0,8498	0,88161	0,03181	7993,8	8313,68	319,883	410001	416864	6863,33
Харківська	0,6609	0,67183	0,01093	8397,9	8507,81	109,913	304406	306764	2358,26
Луганська	0,39239	0,41286	0,02047	2937,7	3143,55	205,847	253180	257597	4416,61

Отже, за прогнозними даними, зростання рівня інформаційної безпеки забезпечить значний приріст продуктивності праці на досліджуваних підприємствах агропродовольчої сфери України та призведе до зростання обсягу виробництва продукції, що вплине на продовольчу та економічну безпеку України.

Список використаних джерел до розділу 5

1. Про рішення Ради національної безпеки і оборони України «Про Доктрину інформаційної безпеки України» : Указ Президента України від 29 грудня 2016 року. URL: <https://zakon.rada.gov.ua/laws/show/47/2017>.
2. Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України від 24 червня 2016 р. № 440-р. URL: <http://zakon2.rada.gov.ua/laws/show/440-2016-%D1%80>.
3. ISO 17799. Code of Practice for Information Security Management. URL: http://www.iso.org/iso/catalogue_detail?csnumber=39612.
4. ISO / IEC Standard 15408. Information technology. Security techniques – Evaluation criteria for IT security. URL: <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-1540>.
5. Критерії безпеки комп'ютерних систем (Trusted Computer System Evaluation Criteria). URL: <https://www.cs.clemson.edu/course/cpsc420/material/Evaluation/TCSEC.pdf>.
6. Абакумов В. М. Інформаційна безпека підприємництва як об'єкт адміністративної правової охорони. *Форум права*. 2012. № 4. С. 10–16.

7. Аверченкова Е. Э., Гончаров Д. И., Лысов Д. А. Модель информационной безопасности информационной советующей системы. *Вестник Брянского государственного технического университета*. 2016. № 4 (52). С. 251–261.

8. Алиева М. Ф. Информационная безопасность как элемент информационной культуры. *Вестник Адыгейского государственного университета*. URL: http://vestnik.adygnet.ru/files/2013.1/2320/aliyeva2013_1.pdf.

9. Апетик А. Інформаційна безпека now: яких елементів не вистачає? *Громадський Простір*. 2019. URL: <https://www.prostir.ua/?library=informatsijna-bezpeka-now-yakyh-elementiv-ne-vystachaje>.

10. Аранчій В. І., Зоря О. П., Різніченко О. А. Формування стратегії розвитку аграрних підприємств на основі сильних і слабких сторін сільського господарства України. *Український журнал прикладної економіки*. 2018. Т. 3. № 4. С. 251–257.

11. Астахова Л. В. Сущность понятия «Культура информационной безопасности» и ее формирование у студентов ВУЗА. *Экономика. Информатика. Безопасность. Сборник научных трудов Международной научно-практической конференции*. Челябинск : Изд-во ЮУрГУ, 2007. С. 93–99.

12. Астахова Л. В., Лушникова С. С. Культура информационной безопасности предприятия : сравнительный анализ зарубежных и российских исследований. *Вестник УрФО*. 2019. № 1 (31). С. 37–47.

13. Ахрамович В. М. Адміністративний рівень інформаційної безпеки. *Сучасний захист інформації*. 2017. № 1. С. 10–14.

14. Бирюков В. А., Лихарев Н. С. Стратегия информационной безопасности медиаорганизации. *Вестник МГУП*. 2015. № 3. URL: <https://cyberleninka.ru/article/n/strategiya-informatsionnoy-bezopasnosti-mediaorganizatsii>.

15. Божкова В. В., Білан А. О. Сутність державної інформаційної політики в умовах розвитку інформаційного суспільства в Україні. *Інвестиції : практика та досвід*. 2019. № 11. С. 106–110.

16. Бородакий Ю. В. Интеллектуальные системы обеспечения информационной безопасности. *Известия Южного федерального университета. Технические науки*. 2005. № 48 (4). С. 65–69.

17. Власова Л. А. Защита информации. Хабаровск : РИЦ ХГАЭП, 2007. 84 с.

18. Голубенко О. Л., Хорошко В. О., Петров О. С., Головань С. М., Яремчук Ю. Є. Політика інформаційної безпеки. Луганськ : Вид. СНУ ім. В. Даля, 2009. 300 с.

19. Гужов В. В., Калюжная И. А., Тюнина Н. О. Федорова Т. Н. Разработка политики информационной безопасности в организациях инновационной сферы экономики : монографія. URL: <https://docplayer.ru/55719555-Guzhov-v-v-kalyuzhnaya-i-a-tyunina-n-o-fedorova-t-n.html/>.

20. Дзьобань О. П., Пилипчук В. Г., Інформаційне насильство та безпека : світоглядно-правові аспекти : монографія. Харків : Майдан, 2011. 244 с.

21. Дячков Д. В. Алгоритм формування інформаційних технологій забезпечення інформаційної безпеки. *Управління ресурсним забезпеченням господарської діяльності підприємств реального сектору економіки* : матер. II Всеукр. наук.-практ. Інтернет-конф., 31 жовтня 2018 р. Полтава : РВВ ПДАА, 2018. С. 253–254.

22. Дячков Д. В. Стратегічні напрями управління інформаційною безпекою підприємств агропродовольчої сфери. *Український журнал прикладної економіки*. 2019. Том 4. № 4. С. 70–78.

23. Дячков Д. В., Вибиванець А. Б. Особливості вибору інноваційної стратегії підприємства. *Управління ресурсним забезпеченням господарської діяльності підприємств реального сектору економіки* : матер. III Всеукр. наук.-практ. інтернет-конф., 31 жовтня 2018 р. Полтава : РВВ ПДАА, 2018. С. 66–67.

24. Дячков Д. В., Вибиванець А. Б. Особливості розробки інноваційної стратегії підприємства. *Актуальні проблеми маркетингового менеджменту в умовах інноваційного розвитку економіки* : тези VI Міжнар. наук.-практ. конф. студентів та молодих науковців, 29 березня 2019 р. Луцьк : ІВВ Луцького ЛНУ, 2019. С. 79–80.

25. Дячков Д. В., Кисіль І. Г., Крепко К. В. Онтологічні засади визначення сутності конкурентоспроможності підприємства як засобу протидії підприємницьким ризикам. *Економічний форум*. Луцьк : РВВ Луцького НТУ, 2018. № 4. С. 162–169.

26. Дячков Д. В., Сьомич М. І. Взаємоінтеграція інформаційної безпеки та інформаційної культури. *Наукові розробки, передові технології, інновації* : зб. наук. праць та тез доповідей IV Міжн. наук.-практ. конф., 06-08 травня 2017 р. К. : НДІСР, 2017. С. 502–506.

27. Євсєєв С. П. Дисертація методологія побудови системи безпеки банківських інформаційних ресурсів : дис. ... ступеня д-ра тех. наук : 21.05.01 / Національний авіаційний університет. Київ, 2018. 471 с.

28. Жабинець О. Й. Політика інформаційної безпеки страхових компаній : українські реалії та досвід США. *Проблеми економіки*. 2014. № 4. С. 22–27.

29. Захаренко К. Категорія інформаційної безпеки у вітчизняному філософсько-політологічному дискурсі. *Вища освіта України*. 2018. № 1. С. 48–54.

30. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Вісник Національного університету «Львівська політехніка». Політичні науки.* № 1. Вип. 2. 2016. С. 27–32.

31. Кавун С. В. Информационная безопасность в бизнесе. Харьков : Изд. ХНЭУ, 2007. 408 с.

32. Каминский А. Формирование политики безопасности информационных систем. *Securitatea informațională : Conferința Internațională.* (20-21 Mai 2009, Moldova), ediția a VI-a, 2009. P. 90–93.

33. Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві. URL: <http://dspace.nbuv.gov.ua/handle/123456789/24811>.

34. Левков Я. Разработка стратегии и архитектуры информационной безопасности предприятия. 2011. URL: <https://profit.kz/articles/1700>.

35. Маркіна І. А., Дячков Д. В. Інформаційна безпека як аспект економічної стабільності на різних рівнях господарювання. *Управління системою економічної безпеки: від теорії до практики* : зб. тез доп. учасників Всеукр. наук.-практ. конф., 19 квітня 2019 р. / упорядник І. О. Ревак. Львів : ЛьвДУВС, 2019. С. 102–105.

36. Маркіна І. А., Дячков Д. В., Мандалина Н. А. Фінансова безпека як важливий чинник забезпечення економічної безпеки підприємства. *Економічний форум.* Луцьк : РВВ Луцького НТУ, 2018. № 4. С. 192–198.

37. Мезенцева Н. Б. До питання наукового обґрунтування політики і методології державної системи інформаційної безпеки. *Економіка та держава.* 2013. № 3. С. 142–144.

38. Нижегородцев Р. М. Пискун Е. И. Кудревич В. В. Прогнозирование показателей социально-экономического развития региона. *Экономика региона.* 2017. Вып. 1. Т. 13. С. 38–48.

39. Осадченко О. Политика информационной безопасности предприятия. URL: <http://security.ase.md/publ/ru/pubru101/15.pdf>.

40. Петренко С., Курбатов В. Разработка политики информационной безопасности предприятия. URL: <http://dspace.nbuv.gov.ua/handle/123456789/24811><http://www.nestor.minsk.by/sr/2005/08/sr50803.html>.

41. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні : автореф. дис. на здобуття наук. ступеня к-та юрид. наук : 12.00.07. Львів, 2019. 23 с.

42. Почепцов Г. Г., Чукут А. С. Інформаційна політика: навч. посіб. Вид. 2-е, стер. Київ : Знання, 2008. 663 с.

43. Прудникова О. В. Інформаційна культура : концептуальні засади та світоглядний сенс : монографія. Х. : Право, 2015. 352 с.

44. Скриньковський Р. М., Костюк Н. Р., Семчук Ж. В. Діагностика політики керівництва у сферах якості, соціальної відповідальності, інформаційної безпеки й охорони праці та механізм забезпечення гідної праці на підприємстві. *Бізнес Інформ*. 2016. № 3. С. 131–137.

45. Твердохліб О. С. Європейський підхід до розроблення інформаційної політики держави. *Актуальні проблеми економіки*. 2016. № 3. С. 429–435.

46. Твердохліб О. С. Теоретико-прикладні засади дослідження державної інформаційної політики у вітчизняному науковому дискурсі. *Держава та регіони. Серія: Державне управління*. 2016. № 1. С. 26–30.

47. Тубеева Ф. К. Проблемы формирования информационной культуры специалистов в сфере образования на примере логопедов. *Научный интернет-журнал «Мир науки»*. 2014. Вып. 2. С. 4–12.

48. Турчак А. В. Основні засади державної політики забезпечення інформаційної безпеки в Україні. *Інвестиції: практика та досвід*. 2019. № 11. С. 123–127.

49. Хохлачова Ю. Політика інформаційної безпеки об'єкта. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Вип. 2 (24). 2012. С. 23–29.

50. Чаплыгин Р. Стратегия информационной безопасности. URL: <https://docplayer.ru/43503819-Strategiya-informacionnoy-bezopasnosti.html>.

51. Чередниченко А. О. Організаційно-економічне забезпечення управління інформаційною безпекою підприємств будівельної галузі : автореф. дис. на здобуття наук. ступеня к-та екон. наук : 21.04.02. Харків, 2016. 24 с.

52. Чередниченко А. Проактивна стратегія інформаційної безпеки підприємств будівельної галузі. *Вісник економіки транспорту і промисловості*. 2015. Вип. 49. С. 150–155.

53. Чуруброва С. М. Політика інформаційної безпеки в системах інформаційно-аналітичного забезпечення підтримки прийняття організаційних рішень. *Проблеми програмування*. 2016. № 4. С. 97–103.

54. Якубівська Ю. Є. Інформаційна безпека суспільства: концептуальний аналіз. URL: http://dspace.tneu.edu.ua/bitstream/316497/19378/1/Муравська%20Якубівська%29_Стаття.pdf.

55. Anderson E. E., Choobineha J. Enterprise information security strategies. *Computers & Security*. 2018. № 8. Р. 22–29.

56. Atif A., Maynard S. B., Park S. Information security strategies: towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*. 2014. 25 (2). URL: <https://www.researchgate.net/publication/257580942>.

57. Chen H., Li W. Understanding organization employee's information security omission behavior : an integrated model of social norm and deterrence

2014. *PACIS 2014 Proceedings*. URL: <http://aisel.aisnet.org/pacis2014/280>.

58. D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information systems research*. 2009. № 20 (1). P. 79–98.

59. Diachkov D. Formation of the information security policy of an enterprise. *Theory and practice of social, economic and technological changes : collective monograph*. Nemoros. Prague, 2018. P. 277–284.

60. Hone K. Eloff, J. Information security policy – what do international information security standards say? *Computers & Security*. 2002. № 21 (5). P. 402–409.

61. Tapiador J. E., Clark J. A. Masquerade mimicry attack detection: a randomised approach. *Computers and Security*. 2011. № 30 (5). P. 297–310.

62. Williamson M. M. Resilient Infrastructure for Network Security. *Complexity*. 2004. № 9 (2). P. 34–40.

63. Адаптивные стратегии информационной безопасности. *Экономика и жизнь*. 2018. URL: <https://www.eg-online.ru/article/365352/>.

64. Кореляційний аналіз. *Вікіпедія* : веб-сайт. URL: https://uk.wikipedia.org/wiki/Кореляційний_аналіз.

65. Політика інформаційної безпеки. *Вікіпедія* : веб-сайт. URL: https://uk.wikipedia.org/wiki/Політика_інформаційної_безпеки.

66. Построения системы информационной безопасности. Основные аспекты построения системы информационной безопасности URL: <https://www.intuit.ru/studies/courses/13845/1242/lecture/27501>.

67. Политика информационной безопасности организации. URL: <http://er76.ru/content/files/Политика%20ИБ%20МО.pdf>.

68. Сільське, лісове та рибне господарство. *Державна служба статистики України*: веб-сайт. http://www.ukrstat.gov.ua/druk/publicat/Arhiv_u/07/Arch_sg_zb.htm

69. Стандарты информационной безопасности: государственные и международные. URL: <http://tvoi.biz/biznes/informatsionnaya-bezopasnost/prakticheskaya-polza-standartov-info.html>.

70. Стратегии защиты информации. URL: <https://studfiles.net/preview/1770970/page:15/>.

71. Стратегия информационной безопасности. URL: <http://docplayer.ru/43503819-Strategiya-informacionnoy-bezopasnosti.html>.

72. Security Policy: Enforcement and Compliance. URL: https://www.cybersecurity.my/data/content_files/11/27.pdf.

73. Т-критерий Стьюдента. *Вікіпедія*. URL: https://ru.wikipedia.org/wiki/Т-критерий_Стьюдента.

ВИСНОВКИ

У монографії отримано нове вирішення складного для економіки України наукового завдання розроблення та обґрунтування теоретико-методологічних засад та розробки науково-практичних положень щодо управління інформаційною безпекою. Це дозволило сформулювати висновки, які повною мірою відображають теоретико-методологічний та прикладний характер дослідження:

Означено, що становлення цифрової економіки є важливим етапом розвитку суспільства, що дає змогу розширити інформаційний простір, використовувати інтелектуальний потенціал і знання людини, створюючи фактори стабільного безпечного соціального середовища в майбутньому. Узагальнення наукових парадигм розвитку цифрової економіки та цифрового менеджменту дозволило визначити та охарактеризувати основні етапи трансформації інформаційної економіки, зумовлені розвитком ІТ-сфери, формуванням цифрової інфраструктури, появою штучного інтелекту, віртуалізацією міжнародних ринків і, як наслідок, зміною інформаційної культури соціально-економічних відносин у суспільстві, що дало змогу виокремити головні елементи та напрями цифровізації традиційної економіки та актуалізувати необхідність переходу від традиційної концепції управління до концепції цифрового менеджменту як сучасного наукового напрямку сфери управління для формування новітньої – цифрової парадигми управління, яка інтегруватиме інформаційну, віртуальну, цифрову сфери, штучний інтелект і людські знання.

Систематизовано основні терміни, які характеризують поняття «інформаційна безпека» та об'єднані в чотири групи, а саме ті, що визначають наукову основу інформаційної безпеки, предметну область інформаційної безпеки, основу діяльності щодо забезпечення інформаційної безпеки, основу ризику інформаційної безпеки. Здійснено етимологічний аналіз поняття «інформаційна безпека» на основі ключових слів і їх змісту залежно від контексту застосування та предметної області, враховуючи об'єкт і предмет спрямування. Запропоновано розглядати інформаційну безпеку як стан захищеності інформаційного середовища, який забезпечується діями компетентних осіб шляхом використання сучасних інформаційних і цифрових технологій проти випадкових або навмисних природних чи штучних впливів, які можуть завдати неприйнятних збитків суб'єктам інформаційних відносин і суперечити їхнім інтересам. З методологічного погляду такий підхід до проблем інформаційної безпеки

починається з визначення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних із використанням інформаційних систем.

Розроблено організаційно-функціональну модель управління інформаційною безпекою підприємства. Структура моделі передбачає наявність суб'єктів управління інформаційною безпекою підприємства, які можна умовно поділити на три основні групи: група I – вище керівництво, провідні спеціалісти підприємства; група II – спеціалізовані органи управління інформаційною безпекою підприємства; група III – персонал підприємства, який опосередковано бере участь у створенні належних умов забезпечення інформаційної безпеки, збереження комерційної таємниці. Наступним елементом організаційно-функціональної моделі управління інформаційною безпекою підприємства є власне процес управління інформаційною безпекою підприємства, що передбачає наявність таких складових, як види захисту, способи захисту, загальні функції, спеціальні функції, методи, принципи. Об'єктами захисту є інформаційні ресурси, інформаційний потенціал, технічні засоби, програмні продукти, засоби комунікації, засоби фізичного захисту, бази даних, бази моделей. В окрему групу об'єктів захисту зараховано персонал, оскільки він причетний до управління іншими об'єктами, що підлягають захисту, і водночас є основною загрозою порушення інформаційної безпеки. А знання визначено як особливий об'єкт – результат симбіозу інформаційних ресурсів і персоналу. Управління інформаційною безпекою підприємства визначено як можливість і здатність суб'єктів управління інформаційною безпекою підприємства створити та підтримувати такий оптимальний стан інформаційного середовища підприємства, за якого забезпечуються умови для ефективного функціонування об'єктів захисту та мінімізація випадкових або навмисних природних чи штучних впливів, які можуть завдати збитків суб'єктам інформаційних відносин.

Проведено аналіз стану та визначено позитивні й негативні тенденції розвитку агропродовольчої сфери України. Серед негативних тенденцій трансформації агропродовольчої сфери України відзначено: зменшення кількості сільських населених пунктів, зменшення індексів фізичного обсягу продукції, зростання навантаження на зайнятих у сільському господарстві та відсутність трудового резерву, збільшення питомої ваги матеріальних витрат, витрат на оплату послуг та амортизацію і одночасне зменшення питомої ваги витрат на оплату праці. Серед позитивних тенденцій – зростання обсягу реалізованої продукції, зростання вартості необоротних і оборотних активів, значне підвищення продуктивності праці, зростання обсягів капітальних інвестицій, розвиток діджиталізації, зростання показників рентабельності.

Аналіз оцінки загроз системі управління інформаційною безпекою аграрних підприємств показав, що особливе значення серед них набувають неосвіченість і поведінка працівників, технологічний прогрес, відсутність стратегії інформаційної безпеки та політики інформаційної безпеки, недостатній рівень програмного забезпечення. Найбільш розповсюдженими наслідками порушення інформаційної безпеки підприємств агропродовольчої сфери є такі: перерва в господарській діяльності підприємства або працівника, спричинена неможливістю виконання певних управлінських або виробничих процесів, знищення / пошкодження програмного забезпечення та апаратних засобів, пошкодження елементів інформаційної системи підприємства, недоступність ІКТ-послуг через зовнішні атаки (електронна пошта, Інтернет, віддалений доступ, хмарна технологія, вебсайт тощо). Зазначене дозволило сформувати карту ризиків порушення інформаційної безпеки суб'єктів аграрного бізнесу, що в подальшому дає можливість оцінювати ці ризики та сприяє розробці напрямів зниження їх рівня.

Здійснено аналіз рівня інформаційної безпеки підприємств агропродовольчої сфери на основі розробленої системи показників-коефіцієнтів оцінки, об'єднаних у п'ять груп, які характеризують стан програмно-технічної захищеності інформаційної системи, рівень фінансування інформаційної безпеки, інформаційну надійність персоналу, властивості управлінської інформації та систему інформаційної безпеки. Встановлено потужний потенціал системи інформаційної безпеки підприємств Полтавської та Сумської областей, середній рівень захисту інформаційного середовища на аграрних підприємствах Кіровоградської та Харківської областей і суттєві вразливості системи інформаційної безпеки на аграрних підприємствах Луганщини.

Узагальнення напрямів, методичних підходів, методик і метрик оцінки та діагностики рівня інформаційної безпеки аграрного підприємства, використання переваг кожної з них дозволило запропонувати концепцію методології оцінювання та діагностики інформаційної безпеки підприємств агропродовольчої сфери, яка передбачає послідовне проходження шести етапів: перші чотири з яких – це основні етапи проведення оцінки та прогнозування рівня інформаційної безпеки підприємств агропродовольчої сфери (діагностування системи інформаційної безпеки підприємства, оцінка системи інформаційної безпеки підприємства, інтегральне оцінювання рівня інформаційної безпеки підприємства та прогнозування інтегрального показника рівня інформаційної безпеки підприємства), два інші – додаткові, які передбачають розробку напрямів оптимізації системи управління інформаційною безпекою підприємства агропродовольчої сфери та

визначення впливу рівня інформаційної безпеки підприємства на результативні показники його діяльності.

Обґрунтовано методологічні підходи до оцінювання (через нормалізацію одиничних коефіцієнтів, які характеризують різні аспекти інформаційної безпеки методом аналізу ієрархій і методом модифікованої головної компоненти) та прогнозування (через прогнозування зміни одиничних коефіцієнтів методом найменших квадратів і методом експоненціального прогнозування) інтегрального показника рівня інформаційної безпеки підприємств шляхом визначення інтегральних показників підсистем програмно-технічного, фінансового, кадрового, інформаційного, організаційного забезпечення системи інформаційної безпеки, що дозволило визначити поточні та спрогнозувати інтегральні значення показників підсистем і системи інформаційної безпеки досліджуваних підприємств агропродовольчої сфери України.

Формалізовано організаційні основи створення віртуальної платформи «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу, окреслено суб'єктів-учасників платформи на основі ідентифікації системи їх ролей за допомогою матричної моделі, сформовано архітектуру зазначеної платформи, визначено напрями та основні результати співпраці в межах віртуальної платформи. Віртуальна платформа «забезпечення інформаційної безпеки підприємств агропродовольчої сфери» на засадах інтелектуального краудсорсингу є масштабним інструментом, що формує та регулює процеси забезпечення інформаційної безпеки агропродовольчого ринку, робить прозорими відносини між діючими суб'єктами зазначеного ринку за рахунок технологій безпечної участі, репутаційних оцінок і зрозумілого механізму співпраці, зокрема в межах захисту інформації. Використання запропонованої віртуальної платформи є своєрідним драйвером інноватизації та цифровізації діяльності підприємств агропродовольчої сфери, з одного боку, та дозволить створити надійну систему захисту інформаційних активів та ефективну систему управління інформаційною безпекою – з іншого.

Створено модель системи менеджменту інформаційної безпеки підприємства агропродовольчої сфери України з урахуванням визначених драйверів її створення. Розроблено логіко-структурну схему формування системи менеджменту інформаційної безпеки підприємства агропродовольчої сфери, яка базується на послідовному проходженні дванадцяти основних етапів, кожен із яких відповідає окремій послідовності циклу Демінга. Запропоновано технологію гнучкого реінжинірингу системи менеджменту інформаційної безпеки підприємства, яка полягає у

варіативності процедур реінжинірингу системи по горизонтально-вертикальних схемах, що забезпечують можливість реалізації вимог на різних рівнях перепроєктування агропродовольчої сфери.

Запропоновано до застосування адаптовану модель захисту інформації, яка базується на поєднанні концепції «глибинного захисту», що інтегрує ключові переваги вищерозглянутих моделей (Diamond, MITRE ATT & CK, PICERL, Cyber Kill Chain, Pyramid of Pain, PICERL, CVSS3, Bell-LaPadula, Biba, Харрісона – Руззо – Ульмана та інших) та концепції «mind map», яка як «карта розуму» дозволяє визначити наповнення кожного «шару» моделі «глибинного захисту» компонентами, які відповідатимуть необхідності формування ефективної системи інформаційної безпеки підприємства. Пропонована модель захисту інформації, окрім модифікованих класичних шарів захисту, включає інші компоненти, які посилюють рівні захисту, зокрема технологію інформаційної безпеки, персонал, безпеку ділових комунікацій, безпеку бездротового зв'язку, управління ризиками інформаційною безпекою, показники інформаційної безпеки – як ключові компоненти забезпечення інформаційного захисту, два з яких – технологію інформаційної безпеки та персонал – запропоновано визначити як окремі самостійні рівні. В умовах автоматизації виробничих бізнес-процесів у сільському господарстві рівень моделі «безпеки мережних систем» пропонується посилити такими двома складовими: безпека ділових комунікацій і безпека бездротового зв'язку. З метою оцінки рівня моделі рекомендовано включити до складу модулі показників інформаційної безпеки та управління ризиками інформаційної безпеки, які мають передбачати захист на чотирьох основних рівнях: адміністративному, програмному, технічному та фізичному. Зазначена модель захисту інформації має ряд переваг – диверсифікацію, практичну апробацію, масштабованість і прийнятність, комплексність та інтегрованість.

Розроблено стратегії управління інформаційною безпекою підприємств агропродовольчої сфери України на основі матричного методу, який дозволив визначати стратегію для кожного підприємства на основі показника існуючого рівня інформаційної безпеки та показника рівня рентабельності, який свідчить одночасно про ефективність діючої інформаційної стратегії та наявність необхідного ресурсного забезпечення для реалізації визначеної або запропонованої до реалізації стратегії інформаційної безпеки. Для підприємств із низьким рівнем інформаційної безпеки, який у межах матриці визначений як «недостатній», запропоновано реалізувати одну із захисних стратегій інформаційної безпеки, із помірним рівнем – наступальні стратегії, з високим рівнем – превентивні стратегії. Акцентовано увагу на тому, що стратегія

інформаційної безпеки не має бути статичною і в міру зменшення фактора невизначеності з плином часу її необхідно переглядати і в разі необхідності коригувати, задаючи нові пріоритети прийняття тактичних рішень. Розроблено систему критеріїв на основі темпів зміни показника рентабельності та рівня інформаційної безпеки, яка дозволить спрогнозувати майбутні варіанти зміни стратегії (розвиток / регрес) і типи зміни стратегії (еволюційний тип / революційні типи).

Сформовано політику інформаційної безпеки на основі концепції інформаційної культури, що визначає її не тільки з позиції формалізації – розробки документів, планів інформаційної безпеки, встановлення правил, методів, але й з позиції формування інформаційних взаємовідносин і запровадження моделі поведінки користувачів інформаційної системи підприємства агропродовольчої сфери України. На основі зазначеного запропоновано функціональну модель формування політики інформаційної безпеки підприємства, засновану на адаптації загальних стандартів ISO 15408 та ISO 17799 з урахуванням запровадження інформаційної культури підприємства. В межах моделі формування політики інформаційної безпеки запропоновано проведення регулярних перевірок ефективності систем захисту (управління надійністю) та заходи щодо впровадження інформаційної культури підприємства на основі визначення моделі поведінки працівника з інформаційними ресурсами.

Спрогнозовано зміни результативних показників діяльності підприємств агропродовольчої сфери України, з-поміж яких обрано продуктивність праці та обсяг виробництва продукції, залежно від зміни інтегрального показника рівня інформаційної безпеки, визначено тісноту зв'язку між коефіцієнтами в межах підмножин і між інтегральними значеннями підмножин шляхом проведення кореляційно-регресійного аналізу. Розраховано очікуваний приріст показників обсягу продукції та продуктивності праці досліджуваних підприємств агропродовольчої сфери Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей на основі прогнозних значень інтегрального значення показника рівня інформаційної безпеки підприємств. Визначено, що, за прогнозними даними, зростання рівня інформаційної безпеки забезпечить значний приріст продуктивності праці на досліджуваних підприємствах агропродовольчої сфери та призведе до зростання обсягу виробництва продукції, що вплине на продовольчу та економічну безпеку України.

ДОДАТКИ

Додаток А

Таблиця А.1

Трансформація сутності поняття «Інформаційна економіка» [згруповано на основі 21; 41; 45; 90; 100; 116; 123; 193; 203]

Автор	Зміст визначення	Рік
Ф. Махлуп [193]	Інформаційна економіка – це такий тип економіки, де переважна частка валового внутрішнього продукту забезпечується діяльністю з виробництва, обробки, зберігання та передачі інформації і знань.	1966
М. Порат [203]	Інформаційна економіка – це кластер галузей, що виробляють сучасні бази даних та засоби, що забезпечують їх функціонування і застосування.	1978
С. Мочерний [116]	Інформаційна економіка – характеристика сучасної економіки з погляду речового змісту, в якій відбувається поширення інформаційної технології у сфері матеріального і нематеріального виробництва, перетворення інформації на один із важливих факторів соціально-економічного прогресу суспільства та окремої особи. В інформаційній економіці переважатиме виробництво та споживання не матеріальних благ, а інформаційних та духовних цінностей, а її інтегруючим показником буде рівень інформатизації.	2000
Ю. Бажал [21]	Інформаційна економіка – це така фаза розвитку суспільства, в якій головними продуктами виробництва є інформація та знання, а відмінними рисами є збільшення ролі інформації та знань у житті суспільства, зростання частки інформаційних комунікацій, продуктів і послуг у ВВП, створення глобального інформаційного простору, де відбувається ефективна інформаційна взаємодія людей, зокрема й завдяки їх доступу до світових інформаційних ресурсів.	2004
А. Колодюк [90]	Інформаційна економіка – це особливий тип економіки, в якому інформація є визначальним виробничим ресурсом, базується на інформаційному виробництві та інформаційних технологіях.	2004
В. Плєскач, Т. Затонацька [123]	Інформаційна економіка – це електронна економічна діяльність, де переважає господарська діяльність у сфері інформаційних послуг, їх виробництва та обміну, де основними ресурсами є інформація та знання.	2007
В. Гєсць, А. Мазаракі [41]	Інформаційна економіка – це перша, початкова стадія нової економіки постіндустріального суспільства, яка в процесі розвитку перетвориться на економіку знань.	2008
П. Лемещенко, Є. Шумських [100]	Інформаційна економіка – це економіка, заснована на передумові, що інформація має не тільки соціально-економічну цінність, але і вимагає інформаційного ринку, на якому можливий інформаційний обмін. Йдеться про дохід, який можуть отримати учасники цього ринку. Інформаційна економіка кожної конкретної країни формується індивідуально.	2014
І. Гусєєва [45]	Інформаційної економіки самої по собі не існує, а існує як і раніше економіка в її класичному визначенні як сукупність відносин, що виникають в процесі виробництва, розподілу, обміну та споживання товарів (робіт, послуг), різні сфери якої в тій чи іншій мірі пронизані цифровими інформаційно-комунікаційними технологіями.	2018

Таблиця А.2

Трансформація сутності поняття «Цифрова економіка» [згруповано на основі 15; 33; 34; 51; 72, 73; 83; 84; 86; 137; 160; 200; 201; 206; 207; 208]

Автор	Зміст визначення	Рік
1	2	3
Д. Тапскотт [206]	Цифрова економіка – економіка, що базується на цифрових комп’ютерних технологіях, яку іноді називають інтернет-економікою, новою економікою або веб-економікою. Під цифровою економікою розуміють виробництво, продаж і постачання продуктів за допомогою комп’ютерних мереж.	1995
Н. Негропonte [201]	Цифрова економіка – перехід від обробки атомів до обробки бітів	2001
Т. Месенбург [200]	Цифрова економіка це поєднання: 1) підтримуючої інфраструктури (апаратне забезпечення, програмне забезпечення, телекомунікації, мережі); 2) електронного бізнесу (будь-які процеси, які організація проводить через комп’ютерні мережі); 3) електронної комерції (передача товарів онлайн). Цифрова економіка базується на інформаційно-комунікаційних та цифрових технологіях, стрімкий розвиток та поширення яких сьогодні впливає на традиційну економіку. Внаслідок цього вона трансформується від такої, що споживає ресурси до економіки, що створює ресурси. Економіку, що активно абсорбує і застосовує цифрові технології.	2001
О. Тугуї [207]	Цифрова економіка – створення мережі господарюючих суб’єктів, шляхом потоку і процесу «оцифровки» об’єктів і шляхом створення та обміну цифровими активами (віртуальними активами) на тлі фізичного розширення і розвитку Інтернету.	2009
Л. З. Кіт [86]	Цифрова економіка – трансформація всіх сфер економіки завдяки перенесенню інформаційних ресурсів та знань на комп’ютерну платформу з ціллю їх подальшого використання (включаючи там, де це можливо) на цій платформі.	2014
В. Апалькова [15, с. 13]	Цифрова економіка є найважливішим двигуном інновацій, конкурентоспроможності і економічного розвитку.	2015
О. Тугуї [208]	Цифрова економіка – конкретна економічна форма прояву виробництва товарів і послуг, в якій домінують цифрові технології, де інформаційні потоки функціонально залежать від ІКТ (інформаційно-комунікаційних технологій)	2015
М. Войнареко, Л. Скоробогата [34]	Цифрова економіка передбачає, що всі економічні процеси (за винятком виробництва товару) протікають незалежно від реального світу. Товари та послуги не мають фізичного носія та є «електронними».	2015
А. Добринін [51, с. 12]	Цифрова економіка – економіка, що заснована на домінуючому застосуванні цифрових технологій.	2016

1	2	3
С. Веретюк [33, с. 52]	Цифрова економіка є складовою частиною економіки, в якій домінують знання суб'єктів та нематеріальне виробництво – основний показник під час визначення інформаційного суспільства. Поняття «цифрова економіка», «економіка знань», «інформаційне суспільство» формують нову економічну систему, яка замінює індустріальну парадигму. Ця економічна модель надає можливість реалізації висококонкурентної продукції з високою доданою вартістю, створення робочих місць нової якості, пошук ефективних рішень соціальних, культурних та екологічних завдань.	2016
В. Фіщук [160]	Цифровою економікою називають економіку, яка застосовує цифрові технології та сервіси. Сферу, котра створює цифрові технології та сервіси, впроваджує та обслуговує їх називають цифровою індустрією (в українських реаліях цю сферу називають «ІТ-сектор»).	2017
Д. Євтянова, М. Тіранова [72]	Цифрова економіка – автоматизоване управління господарством на основі передових інформаційних технологій; уклад, заснований на ефективному інформаційному управлінні системою виробництва	2017
А. Кешелава, В. Буданов, В. Румянцев [84]	Цифрова (електронна) економіка – це економіка, характерною особливістю якої є максимальне задоволення потреб усіх її учасників за рахунок використання інформації, в тому числі персональної. Це стає можливим завдяки розвитку інформаційно-комунікаційних і фінансових технологій, а також доступності інфраструктури, що разом забезпечують можливість повноцінної взаємодії в гібридному світі всіх учасників економічної діяльності – суб'єктів і об'єктів процесу створення, розподілу, обміну та споживання товарів і послуг.	2017
К. Семячков [137, с. 14]	Цифрова економіка – сучасний тип господарювання, який характеризується переважаючою роллю даних і методів управління ними як визначального ресурсу у сфері виробництва, розподілу, обміну і споживання.	2017
Г. Карчева [83, с. 14]	Цифрова економіка – це інноваційна динамічна економіка, що базується на активному впровадженні інновацій та інформаційно-комунікаційних технологій в усі види економічної діяльності та сфери життєдіяльності суспільства, що дозволяє підвищити ефективність та конкурентоспроможність окремих компаній, економіки та рівень життя населення.	2017
В. Єфімушкін, Т. Ледовских, О. Щербакова [73]	Цифрова економіка – система економічних, соціальних і культурних відносин, заснованих на використанні цифрових інформаційно-комунікаційних технологій.	2017
Н. Деева, В. Делейчук [47, с. 654]	Цифрова економіка – це економічна діяльність, яка виникає через мільярди повсякденних онлайн-зв'язків.	2018

Додаток Б

Таблиця Б.1

Природний приріст населення України в сільській місцевості, 1991, 2009–2018 рр. [сформовано на основі 106]

Роки	Кількість живо народжень, осіб	Кількість смертей, осіб	Природний приріст, скорочення, осіб (–)	На 1000 осіб наявного населення		
				кількість живо народжень, осіб	кількість смертей, осіб	природний приріст, скорочення, осіб (–)
1991	211608	288972	-77364	12,6	17,2	-4,6
2009	173028	274445	-101417	11,9	18,9	-7,0
2010	171102	267105	-96003	11,9	18,6	-6,7
2011	173661	253563	-79902	12,1	17,7	-5,6
2012	179106	251352	-72246	12,6	17,7	-5,1
2013	173373	249815	-76442	12,3	17,7	-5,4
2014*	161692	240557	-78865	12,2	18,1	-5,9
2015*	145699	236047	-90348	11,3	18,0	-6,7
2016*	138349	228997	-90648	10,8	17,6	-6,8
2017*	126113	223574	-97461	9,9	17,3	-7,4
2018*	115772	223933	-108161	9,2	17,5	-8,3

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток В

Таблиця В.1

**Міграційний рух в Україні у сільській місцевості у 2009–2018 рр.
[сформовано на основі 106]**

Роки	Усі потоки міграції, осіб			У т. ч. міждержавна міграція, осіб		
	кількість прибулих	кількість вибулих	міграційний приріст, скорочення (–)	кількість прибулих	кількість вибулих	міграційний приріст, скорочення (–)
2009	187497	203982	-16485	8177	3835	4342
2010	204032	209281	-5249	7637	2739	4898
2011	200674	204894	-4220	7799	2394	5405
2012	199531	203159	-3628	8413	2167	6246
2013	184708	192799	-8091	7758	2314	5444
2014*	155157	152158	2999	6493	2370	4123
2015*	172849	160910	11939	5084	2728	2356
2016*	94068	75408	18660	2385	1261	1124
2017*	135528	127612	7916	3768	2067	1701
2018*	198356	209098	-10742	4903	3609	1294

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток Г

Таблиця Г.1

Кількість підприємств, зайнятих та найманих працівників на підприємствах за видами економічної діяльності в Україні у 2010–2018 рр. [складено за матеріалами 112]

Галузь	Роки	Кількість підприємств, од	Кількість зайнятих працівників, осіб	З них кількість найманих працівників, осіб
Усього	2010	378810	7958252	7836443
	2011	375695	7793106	7712429
	2012	364935	7679667	7577595
	2013	393327	7406494	7285562
	2014*	341001	6298491	6192987
	2015*	343440	5889701	5778120
	2016*	306369	5801140	5713871
	2017*	338256	5812922	5714585
	2018*	355877	5959474	5870601
сільське господарство	2010	49060	690503	647277
	2011	39951	636980	633736
	2012	45923	637577	623867
	2013	47826	616708	582237
	2014*	44180	563281	530948
	2015*	44897	530401	502696
	2016*	43359	545400	514969
	2017*	48311	525195	490926
	2018*	48653	516102	481398

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток Д

Таблиця Д.1

Капітальні інвестиції підприємств за видами економічної діяльності в Україні у 2010–2018 рр. [сформовано на основі 106; 112]

Галузі	Роки	Капітальні інвестиції – усього, млрд грн	У тому числі					
			капітальні інвестиції у матеріальні активи, млрд грн	з них, млрд грн				капітальні інвестиції у нематеріальні активи, млрд грн
				у землю	в існуючі будівлі та споруди	у будівництво та перебудову будівель	у машини та обладнання	
Усього	2010	130,76	124,97	1,12	3,95	62,36	57,39	5,79
	2011	193,02	185,26	2,02	6,94	93,07	81,87	7,76
	2012	229,49	222,27	1,69	5,24	103,16	104,04	7,22
	2013	216,99	207,62	1,08	4,57	100,76	91,95	9,37
	2014*	178,38	172,19	0,92	2,70	85,97	75,85	6,20
	2015*	213,48	196,40	1,15	4,96	85,73	96,25	17,08
	2016*	281,67	271,80	1,58	7,96	105,56	145,25	9,87
	2017*	359,16	344,85	1,89	6,20	120,79	200,89	14,31
	2018*	471,12	437,43	1,63	10,42	166,16	241,16	33,69
сільське господарство	2010	10,26	10,21	0,04	0,40	2,26	6,07	0,05
	2011	16,20	16,08	0,04	0,54	3,57	10,42	0,12
	2012	18,90	18,84	0,05	0,40	4,75	11,66	0,06
	2013	18,51	18,18	0,02	0,35	3,85	11,54	0,33
	2014*	18,18	18,11	0,09	0,33	4,01	11,67	0,07
	2015*	28,98	28,81	0,05	0,99	5,56	19,32	0,17
	2016*	49,50	49,23	0,10	0,57	7,45	37,68	0,27
	2017*	63,26	62,66	0,15	0,40	9,65	48,43	0,60
	2018*	65,56	64,25	0,19	2,16	12,15	44,84	1,31

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток Е

Таблиця АА.1

Індекси фізичного обсягу продукції сільського господарства, реалізованої господарствами населення (у % до попереднього року) в Україні, 2009–2019 рр. [сформовано на основі 117]

Роки	Продукція сільського господарства – всього	У тому числі	
		продукція рослинництва	продукція тваринництва
2009	96,1	109,2	89,8
2010	99,6	100,2	99,2
2011	111,3	130,5	99,3
2012	95,1	92,9	96,7
2013	108,9	123,2	98,8
2014*	98,6	99,4	97,9
2015*	99,6	109,9	90,1
2016*	96,7	100,0	91,8
2017*	101,2	102,1	99,7
2018*	103,4	106,0	98,8
2019*	107,3	114,6	94,4

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток Ж

Таблиця Ж.1

Обсяг виробництва (валовий збір) сільськогосподарських культур в Україні у всіх категоріях господарств у 1991, 2009–2019 рр., тис. т [сформовано на основі 116]

Роки	культури зернові та зернобобові ¹	буряк цукровий фабричний	соняшник ¹	картопля	культури овочеві	культури плодові та ягідні ²
1991	38674	36168	2311	14550	5932	1537
2009	46028	10068	6364	19666	8341	1618
2010	39271	13749	6772	18705	8122	1747
2011	56747	18740	8671	24248	9833	1896
2012	46216	18439	8387	23250	10017	2009
2013	63051	10789	11051	22259	9873	2295
2014 ³	63859	15734	10134	23693	9638	1999
2015 ³	60126	10331	11181	20839	9214	2153
2016 ³	66088	14011	13627	21750	9415	2007
2017 ³	61917	14882	12236	22208	9286	2048
2018 ³	70057	13968	14165	22504	9440	2571
2019 ³	75143	10205	15254	20269	9688	2119

¹ У масі після доробки;

² Із загальної площі насаджень;

³ Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях.

Додаток И

Таблиця И.1

Внесення мінеральних та органічних добрив в Україні у всіх категоріях господарств у 1990, 2009–2018 рр. [сформовано на основі 117]

Показник	1990	2009	2010	2011	2012	2013	2014*	2015*	2016*	2017*	2018 *
Площа сільськогосподарських угідь, млн га	42,0	41,6	41,6	41,6	41,6	41,5	41,5	41,5	41,5	41,5	41,5
Внесення азотних добрив на одиницю площі сільськогосподарських угідь, кг / га	44,2	15,3	18,7	21,6	22,4	25,1	24,6	23,7	28,9	32,9	36,9
Внесення фосфорних добрив на одиницю площі сільськогосподарських угідь, кг / га	31,4	3,2	3,8	4,7	5,3	5,7	5,8	5,4	6,9	8,8	10,8
Внесення калійних добрив на одиницю площі сільськогосподарських угідь, кг / га	29,5	2,9	3,1	4,1	4,7	5,2	5,0	5,0	5,9	7,2	8,8
Обсяг внесених мінеральних добрив на одиницю площі сільськогосподарських угідь, кг / га	105,1	21,4	25,6	30,5	32,4	36,0	35,5	34,1	41,7	48,9	56,5
Частка площ, оброблених мінеральними добривами, до загальної площі сільськогосподарських угідь, %	62,9	27,6	30,5	34,1	35,1	37,1	35,7	34,9	37,8	39,8	38,8
Внесення органічних добрив на одиницю площі сільськогосподарських угідь, кг / га	6207,8	252,7	239,5	239,3	232,8	232,6	238,5	232,8	220,8	223,5	280,7
Частка площ, оброблених органічними добривами, до загальної площі сільськогосподарських угідь, %	13,1	1,2	1,0	1,0	1,0	1,0	1,0	1,0	1,2	1,2	1,9

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток К

Таблиця К.1

Групування підприємств за розмірами зібраної площі основних сільськогосподарських культур в Україні у 2018 р.* [сформовано на основі 117]

Розмір зібраної площі	Кількість підприємств		Обсяг виробництва		Урожайність, ц з 1 га
	одиниць	у % до загальної кількості	тис. т	у % до загального обсягу виробництва	
Зернові та зернобобові культури					
Підприємства	34859	100,0	56096,2	100,0	52,2
з них з площею, га					
до 100,00	21788	62,5	2227,5	4,0	33,2
100,01–200,00	3429	9,8	2050,8	3,6	41,2
200,01–500,00	4087	11,7	6052,8	10,8	45,7
500,01–1000,00	2648	7,6	9066,3	16,2	47,9
1000,01–2000,00	1887	5,4	13682,8	24,4	52,1
2000,01–3000,00	554	1,6	7359,4	13,1	54,9
більше 3000,00	466	1,4	15656,6	27,9	65,6
Соняшник					
Підприємства	22821	100,0	12193,6	100,0	24,1
з них з площею, га					
до 100,00	13972	61,2	952,2	7,8	19,4
100,01–200,00	2882	12,6	990,5	8,1	23,5
200,01–500,00	3304	14,5	2609,3	21,4	24,5
500,01–1000,00	1597	7,0	2722,8	22,3	24,5
1000,01–2000,00	792	3,5	2688,5	22,1	24,9
2000,01–3000,00	170	0,7	1033,5	8,5	25,1
більше 3000,00	104	0,5	1196,8	9,8	24,4
Соя					
Підприємства	10136	100,0	4102,1	100,0	26,4
з них з площею, га					
до 100,00	7084	69,9	506,1	12,3	21,9
100,01–200,00	1262	12,5	449,9	11,0	24,7
200,01–500,00	1156	11,4	935,8	22,8	26,3
500,01–1000,00	381	3,8	715,9	17,5	27,4
1000,01–2000,00	167	1,6	651,8	15,9	28,8
більше 2000,00	86	0,8	842,6	20,5	28,4

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток Л

Таблиця Л.1

Групування підприємств за кількістю сільськогосподарських тварин в Україні на 1 січня 2019 р.* [сформовано на основі 117]

Групи підприємств	Кількість підприємств		Кількість тварин	
	одиниць	у % до загальної кількості	тис. голів	у % до загальної кількості
Велика рогата худоба				
Підприємства – усього	2296	100,0	1138,1	100,0
з них мали, голів				
до 50	633	27,6	12,3	1,1
50 – 99	210	9,1	15,0	1,3
100 – 499	741	32,3	202,9	17,8
500 – 999	394	17,1	274,7	24,1
1000 – 1499	144	6,3	177,0	15,6
більше 1500	174	7,6	456,2	40,1
Корови				
Підприємства – усього	2130	100,0	467,8	100,0
з них мали, голів				
до 50	752	35,3	11,9	2,5
50 – 99	244	11,5	17,8	3,8
100 – 499	877	41,2	206,6	44,2
500 – 999	188	8,8	123,1	26,3
більше 1000	69	3,2	108,4	23,2
Свині				
Підприємства – усього	1729	100,0	3395,6	100,0
з них мали, голів				
до 100	382	22,1	8,6	0,3
100 – 199	206	11,9	14,9	0,4
200 – 499	539	31,2	134,0	3,9
500 – 999	195	11,3	141,8	4,2
1000 – 4999	283	16,3	640,8	18,9
5000 – 9999	50	2,9	348,6	10,3
більше 10000	74	4,3	2106,9	62,0
Птиця свійська				
Підприємства – усього	449	100,0	118812,9	100,0
з них мали, голів				
до 4999	187	41,6	186,6	0,2
5000 – 49999	113	25,2	2378,9	2,0
50000 – 99999	25	5,6	1800,7	1,5
100000 – 499999	87	19,4	21150,1	17,8
більше 500000	37	8,2	93296,6	78,5

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток М

Таблиця М.1

Кількість сільськогосподарських тварин в Україні у всіх категоріях господарств на 1 січня у 1990–1991, 2009–2019 рр., тис. голів [сформовано на основі 119]

Роки	велика рогата худоба, тис. голів		свині, тис. голів	вівці та кози тис. голів	птиця, млн голів
	усього	у т. ч. корови			
1990	25194,8	8527,6	19946,7	9003,1	255,1
1991	24623,4	8378,2	19426,9	8418,7	246,1
2009	5079,0	2856,3	6526,0	1726,9	177,6
2010	4826,7	2736,5	7576,6	1832,5	191,4
2011	4494,4	2631,2	7960,4	1731,7	203,8
2012	4425,8	2582,2	7373,2	1739,4	200,8
2013	4645,9	2554,3	7576,7	1738,2	214,1
2014*	4534,0	2508,8	7922,2	1735,2	230,3
2015*	3884,0	2262,7	7350,7	1371,1	213,3
2016*	3750,3	2166,6	7079,0	1325,3	204,0
2017*	3682,3	2108,9	6669,1	1314,8	201,7
2018*	3530,8	2017,8	6109,9	1309,3	204,8
2019*	3332,9	1919,4	6025,3	1268,6	211,7

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток Н

Таблиця Н.1

Виробництво основних видів продукції тваринництва в Україні у всіх категоріях господарств у 1990–1991, 2009–2018 рр. [сформовано на основі 119]

Роки	м'ясо (у забійній масі), тис. т	молоко, тис. т	яйця від птиці, млн шт	вовна, т
1990	4357,8	24508,3	16286,7	29804
1991	4029,1	22408,6	15187,8	26646
2009	1917,4	11609,6	15907,5	4111
2010	2059,0	11248,5	17052,3	4192
2011	2143,8	11086,0	18689,8	3877
2012	2209,6	11377,6	19110,5	3724
2013	2389,4	11488,2	19614,8	3520
2014 [*]	2359,6	11132,8	19587,3	2602
2015 [*]	2322,6	10615,4	16782,9	2270
2016 [*]	2323,6	10381,5	15100,4	2072
2017 [*]	2318,2	10280,5	15505,8	1967
2018 [*]	2354,9	10064,0	16132,0	1908

^{*} Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток П

Таблиця П.1

Середній річний удій молока від однієї корови в Україні, 1990, 2000, 2014–2018 рр., кг [сформовано на основі 119]

Види господарств	1990	2000	2014*	2015*	2016*	2017*	2018*
Господарства усіх категорій	2863	2359	4508	4644	4735	4820	4922
Підприємства	2941	1588	5027	5352	5643	6025	6190
Господарства населення	2637	2960	4363	4437	4473	4480	4559

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток Р

Таблиця Р.1

Витрати кормів усіх видів на виробництво одиниці продукції тваринництва та у розрахунку на одну умовну голову великої худоби в Україні в господарствах усіх категорій (на один центнер) в 1990, 2000, 2014–2018 рр., ц корм. од. [сформовано на основі 119]

Показник	1990	2000	2014*	2015*	2016*	2017*	2018*
приросту великої рогатої худоби	11,73	8,88	11,93	10,03	9,89	10,39	9,26
приросту свиней	7,92	9,05	6,28	5,99	5,79	5,35	5,64
виробництва молока	1,41	1,33	0,97	0,96	0,96	0,94	0,91

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях.

Додаток С

Таблиця С.1

Наявність бджолосімей у господарствах усіх категорій в Україні (на 1 січня) в 1991, 2001, 2011, 2015, 2017–2019 рр., тис. од [сформовано на основі 119]

Регіони	1991	2001	2011	2015*	2017*	2018*	2019*
Україна	3515,1	2849,3	2921,5	2699,6	2487,1	2642,2	2601,0
Автономна Республіка Крим	113,9	94,6	116,0	...	...	...	...
області							
Волинська	43,6	16,2	26,3	27,4	23,4	24,3	24,1
Рівненська	49,1	32,7	51,6	49,4	44,1	45,3	44,8
Херсонська	94,5	20,2	55,8	46,6	45,3	52,8	45,1
Луганська	238,7	111,6	67,1	57,6	43,6	47,0	48,4
Київська	132,0	80,9	51,8	49,5	49,4	49,9	50,5
Чернігівська	104,1	64,8	55,1	55,8	52,1	51,9	53,2
Тернопільська	93,3	75,8	59,3	58,0	55,7	53,9	53,6
Львівська	47,3	34,7	65,1	65,0	65,6	62,9	63,8
Закарпатська	125,0	103,6	67,3	79,1	68,5	68,5	70,0
Чернівецька	125,0	97,4	83,0	81,9	84,2	81,0	84,2
Одеська	121,4	111,4	119,5	110,5	103,2	105,4	104,9
Черкаська	203,1	180,3	136,8	124,9	107,2	105,2	105,8
Запорізька	163,7	160,6	114,7	114,6	113,5	112,6	110,1
Харківська	167,0	105,2	128,8	130,6	124,4	123,2	113,5
Кіровоградська	155,2	130,0	120,9	120,7	114,0	113,0	117,4
Дніпропетровська	167,7	169,5	142,5	146,0	128,0	129,8	122,6
Сумська	112,0	186,4	121,0	123,7	115,5	112,3	122,9
Донецька	338,3	218,4	263,7	185,5	145,4	141,7	141,6
Івано-Франківська	142,6	141,6	147,2	147,0	144,0	143,1	143,0
Полтавська	165,5	116,2	161,5	148,4	143,8	141,6	146,4
Миколаївська	71,8	156,8	153,4	168,0	167,4	165,3	163,3
Вінницька	340,2	210,0	193,2	191,9	183,7	176,3	170,8
Житомирська	84,4	88,5	156,0	193,4	195,6	195,9	196,6
Хмельницька	115,7	141,9	262,1	224,1	169,5	339,3	304,4

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток Т

Таблиця Т.1

Середні ціни продукції сільського господарства, реалізованої підприємствами в Україні за 2009–2019 рр., грн за т [сформовано на основі 117; 118]

Роки	Культури зернові та зернобобові	Насіння культур олійних	Буряк цукровий фабричний	Картопля	Культури овочеві	Культури плодові та ягідні	Сільськогосподарські тварини (у живій масі)	Молоко	Яйця, за тис.шт
2009	799,0	2086,2	409,9	1298,6	1790,0	1892,4	10362,9	1888,8	403,9
2010	1120,9	2942,6	478,5	2131,0	2551,6	2419,8	10797,1	2938,7	470,6
2011	1374,2	3312,0	516,0	2032,8	2139,1	3175,9	11967,2	3041,6	521,5
2012	1547,1	3584,0	426,8	1139,6	1956,6	2707,1	13456,9	2662,2	627,0
2013	1299,8	3087,5	397,8	1860,9	2354,0	3010,8	12901,3	3364,0	656,7
2014 ²	1801,4	4062,8	494,2	2173,6	2514,3	2429,1	15736,9	3588,4	782,4
2015 ²	2912,1	7531,5	788,6	2436,3	3903,4	5894,5	21966,2	4347,3	1333,2
2016 ²	3414,0	8656,1	848,6	2631,8	3924,2	5863,8	22468,0	5461,8	1108,7
2017 ²	3771,6	9132,0	825,3	3296,3	4136,1	8766,6	31838,4	7234,0	1145,9
2018 ²	4315,0	9318,3	749,0	3746,0	4448,0	5054,0	33331,2	7602,4	1600,3
2019 ²	3867,5	8321,2	753,7	5474,7	4497,0	6494,4	32679,8	8198,2	1206,1

¹ Без ПДВ, дотацій, транспортних, експедиційних та накладних витрат; за 1996-2011 рр. – з урахуванням дотацій;

² Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях.

Таблиця Т.2

Індекси цін реалізованої продукції сільського господарства сільськогосподарськими підприємствами в Україні у 2009–2019 рр., % до попереднього року [сформовано на основі 117; 118]

Роки	Продукція сільського господарства	У тому числі	
		продукція рослинництва	продукція тваринництва
2009	106,4	109,1	101,4
2010	130,0	139,8	114,3
2011	113,6	115,7	109,2
2012	106,8	105,6	108,0
2013	97,1	91,8	102,4
2014*	124,3	129,2	119,1
2015*	154,5	167,2	141,3
2016*	109,0	116,3	101,7
2017*	111,5	107,3	130,7
2018*	109,3	109,8	108,6
2019*	92,4	91,2	96,8

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток У

Таблиця У.1

Фінансові результати до оподаткування підприємств за видами економічної діяльності в Україні, 2010–2018 рр.* [сформовано на основі 112]

Галузь	Роки	Усього				
		фінансовий результат (сальдо) до оподаткування, млрд. грн	підприємства, які одержали прибуток		підприємства, які одержали збиток	
			у % до загальної кількості підприємств	фінансовий результат, млрд. грн	у % до загальної кількості підприємств	фінансовий результат, млрд. грн
Всього по економіці	2010	54,41	59,00	189,64	41,00	135,24
	2011	118,61	65,10	255,55	34,90	136,94
	2012	75,67	64,50	248,04	35,50	172,37
	2013	11,34	65,90	209,86	34,10	198,53
	2014*	-564,38	66,30	233,62	33,70	798,00
	2015*	-348,47	73,70	387,65	26,30	736,12
	2016*	69,89	73,40	443,01	26,60	373,12
	2017*	236,95	72,80	593,17	27,20	356,22
	2018*	369,21	74,30	668,89	25,70	299,68
Сільське господарство	2010	17,31	69,30	22,15	30,70	4,85
	2011	25,35	83,40	30,27	16,60	4,92
	2012	26,84	78,50	33,67	21,50	6,83
	2013	15,00	80,10	26,26	19,90	11,26
	2014*	21,47	84,50	51,75	15,50	30,28
	2015*	101,98	88,70	127,62	11,30	25,64
	2016*	90,10	88,20	102,79	11,80	12,70
	2017*	68,57	86,50	89,00	13,50	20,43
	2018*	70,73	86,50	93,56	13,50	22,83
Рослинництво	2010	13,34	72,90	16,48	27,10	3,14
	2011	20,61	86,20	23,25	13,80	2,63
	2012	18,57	80,10	23,87	19,90	5,30
	2013	7,60	81,80	16,45	18,20	8,85
	2014*	16,14	86,50	39,78	13,50	23,65
	2015*	88,34	90,70	108,24	9,30	19,90
	2016*	81,95	90,40	91,55	9,60	9,60
	2017*	58,92	88,40	76,59	11,60	17,66
	2018*	62,97	88,50	81,59	11,50	18,62
Тваринництво	2010	4,04	63,00	5,01	37,00	0,97
	2011	4,30	69,00	6,15	31,00	1,84
	2012	6,84	71,20	7,78	28,80	0,94
	2013	6,28	70,80	7,43	29,20	1,15
	2014*	6,93	74,70	8,92	25,40	1,99
	2015*	13,75	78,00	16,24	22,00	2,49
	2016*	7,10	72,80	9,01	27,20	1,91
	2017*	8,33	76,00	9,87	24,00	1,54
	2018*	7,41	76,40	9,61	23,60	2,20
Виробництво харчових продуктів	2010	1,71	61,30	6,47	38,70	4,76
	2011	1,15	60,70	7,44	39,30	6,30
	2012	5,82	62,80	10,43	37,30	4,61
	2013	5,10	63,80	9,36	36,20	4,25
	2014*	-12,99	63,50	10,11	36,50	23,10
	2015*	-11,64	72,90	16,02	27,10	27,66
	2016*	-2,45	71,50	15,55	28,50	18,00
	2017*	9,29	70,10	22,91	29,90	13,63
	2018*	12,20	70,80	18,75	29,20	6,55

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток Ф

Таблиця Ф.1

Фінансовий результат (сальдо) до оподаткування за розмірами підприємств в Україні у 2010–2018 рр., млрд грн [сформовано на основі 111; 112]

Галузі	Роки	Усього	У тому числі			
			великі підприємства	середні підприємства	малі підприємства	з них мікропідприємства
Всього по економіці						
	2010	54,41	28,47	41,58	-15,65	-13,90
	2011	118,61	92,57	31,09	-5,06	-8,71
	2012	75,67	37,18	47,74	-9,25	-12,83
	2013	11,34	28,00	8,39	-25,06	-25,04
	2014*	-564,38	-189,93	-199,18	-175,26	-100,97
	2015*	-348,47	-145,40	-91,16	-111,91	-57,96
	2016*	69,89	61,22	32,82	-24,15	-34,64
	2017*	236,95	156,91	90,77	-10,72	-25,29
	2018*	369,21	175,18	147,17	46,87	-1,16
Сільське господарство						
	2010	17,31	2,61	12,36	2,33	0,17
	2011	25,35	...	...	7,54	2,06
	2012	26,84	5,30	13,66	7,88	1,91
	2013	15,00	3,84	6,90	4,26	1,09
	2014*	21,47	5,22	9,19	7,06	1,48
	2015*	101,98	24,79	43,14	34,05	9,36
	2016*	90,10	12,08	42,37	35,64	10,15
	2017*	68,57	8,06	35,09	25,42	4,11
	2018*	70,73	11,19	38,14	21,40	4,99

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток X

Таблиця X.1

Рентабельність операційної та всієї діяльності підприємств за видами економічної діяльності в Україні за 2010-2018 рр. з розподілом на великі, середні, малі та мікропідприємства [сформовано на основі 111; 112]

Галузь	Роки	Рівень рентабельності (збитковості) операційної діяльності, %					Рівень рентабельності (збитковості) всієї діяльності, %				
		усього	у тому числі підприємства				усього	у тому числі підприємства			
			великі	середні	малі	з них мікропідприємства		великі	середні	малі	з них мікропідприємства
1	2	3	4	5	6	7	8	9	10	11	12
Всього по економіці	2010	4,0	3,9	5,0	1,8	-3,5	0,5	0,2	2,3	-5,7	-13,9
	2011	5,9	6,2	6,0	4,2	0,8	1,8	3,3	1,2	-2,5	-8,0
	2012	5,0	5,2	5,0	4,1	-0,1	1,0	0,9	2,2	-3,3	-10,2
	2013	3,9	5,0	3,2	2,2	-2,3	-0,7	0,6	-0,1	-6,2	-16,1
	2014 ¹	-4,1	0,7	-3,6	-17,9	-30,1	-14,2	-11,1	-12,5	-26,5	-40,2
	2015 ¹	1,0	4,0	0,0	-4,2	-8,2	-7,3	-7,0	-5,0	-13,6	-20,4
	2016 ¹	7,4	8,8	6,9	5,2	-0,4	0,6	2,4	0,7	-3,6	-11,7
	2017 ¹	8,8	11,2	7,3	6,5	2,4	3,0	5,2	3,1	-2,0	-8,0
	2018 ¹	8,1	9,1	7,0	8,3	4,7	4,5	5,2	4,6	2,7	-1,8
Сільське господарство	2010	24,4	29,8	25,1	18,7	11,2	17,4	22,0	18,2	12,0	3,7
	2011	24,7	...	...	26,5	24,2	19,3	...	...	22,4	20,0
	2012	22,8	29,7	21,0	23,1	19,8	16,3	24,6	14,0	17,1	13,9
	2013	11,7	20,0	8,9	13,1	13,3	8,3	15,3	6,6	8,3	7,3
	2014 ¹	21,4	23,8	22,0	19,0	15,1	9,2	14,9	7,2	10,1	7,2
	2015 ¹	43,0	54,3	39,9	41,9	37,1	30,4	45,4	24,4	32,8	31,6
	2016 ¹	33,6	29,3	32,3	37,6	33,5	25,6	24,7	22,8	30,3	26,9
	2017 ¹	23,2	24,6	22,0	24,4	24,5	16,5	20,5	16,3	15,8	7,8
	2018 ¹	18,9	22,9	18,2	18,8	16,5	14,2	21,2	15,2	11,0	7,9

Продовж. табл. X.1

1	2	3	4	5	6	7	8	9	10	11	12
Рослинництво	2010	27,8	...	...	...	...	20,1	...	...	...	...
	2011	26,3	33,2	23,1	30,6	27,9	21,5	26,2	18,4	26,6	24,6
	2012	21,7	24,3	19,1	25,2	22,3	14,9	19,1	11,8	18,9	16,5
	2013	8,8	16,3	4,2	14,4	15,2	5,6	9,9	2,8	9,6	9,6
	2014 ¹	23,0	26,5	22,1	23,0	19,6	9,1	16,6	4,6	14,0	13,6
	2015 ¹	47,2	59,7	44,2	46,3	41,4	33,4	51,3	26,3	37,4	37,0
	2016 ¹	38,4	35,8	36,8	41,4	37,0	29,2	29,9	25,9	33,7	30,2
	2017 ¹	24,6	22,8	23,5	26,4	26,8	17,3	20,0	17,1	17,1	8,7
	2018 ¹	20,6	23,7	20,3	20,2	18,5	15,5	22,1	17,2	12,1	10,7
Тваринництво	2010	19,9	...	...	...	...	15,1	...	...	...	...
	2011	22,1	30,1	22,8	3,9	0,7	14,9	27,2	14,0	1,1	-6,8
	2012	27,6	...	...	8,7	-0,9	22,7	...	...	6,0	-4,9
	2013	23,1	50,6	18,3	3,6	-4,5	19,9	48,1	15,1	0,7	-9,5
	2014 ¹	23,8	...	...	4,4	-6,8	17,5	...	...	0,8	-10,6
	2015 ¹	33,1	44,2	28,4	21,5	5,7	25,4	34,6	21,0	17,0	-1,7
	2016 ¹	16,0	18,1	16,1	10,5	-0,9	12,2	15,6	11,4	7,9	-4,1
	2017 ¹	20,0	29,7	19,2	12,3	0,6	15,8	22,2	15,9	8,9	-2,6
	2018 ¹	13,8	20,9	11,7	10,3	1,0	11,3	18,9	9,7	5,4	-11,7

* Дані наведено без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток Ц

АНКЕТА

визначення внутрішніх та зовнішніх факторів впливу на виникнення загроз інформаційній безпеці підприємства

(назва підприємства)

(ПІБ, посада респондента)

Здійсніть балову оцінку факторів, які спричиняють виникнення загроз інформаційній безпеці підприємства (поставте позначку).

Оцінка від 1 до 5 по висхідній: 1 – найменший ступінь вплив фактора на формування загрози інформаційній безпеці підприємства; 2 – нижче середнього ступінь вплив фактора на формування загрози інформаційній безпеці підприємства; 3 – середній ступінь вплив фактора на формування загрози інформаційній безпеці підприємства; 4 – вище середнього ступінь вплив фактора на формування загрози інформаційній безпеці підприємства; 5 – найбільший ступінь вплив фактора на формування загрози інформаційній безпеці підприємства.

1. Неосвідченість працівника

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

2. Поведінка працівника

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

3. Дії зловмисників

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

4. Відсутність відділу управління інформаційною системою

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

5. Відсутність підтримки вищого керівництва

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

6. Застаріле технічне обладнання

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

7. Помилки технології

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

8. Недостатній рівень програмного забезпечення

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

9. Відсутність внутрішніх інструкцій та стандартів

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

10. Відсутність або низький рівень фінансування ресурсів інформаційних систем та систем захисту інформації

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

11. Відсутність стратегії інформаційної безпеки та політики інформаційної безпеки

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

12. Сертифікація

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

13. Законодавство

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

14. Державна підтримка інформаційної безпеки

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

15. Технологічний прогрес

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

16. Ризик стихійного лиха

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

17. Помилка надання послуг сторонніми організаціями (аутсорсинг)

☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

Здійсніть балову оцінку факторів, які спричиняють виникнення загроз інформаційній безпеці підприємства (поставте позначку).

Оцінка від 0 до 5 по висхідній: 0 – подія в наслідок настання загроз інформаційній безпеці не наступала; 1 – подія в наслідок настання загроз інформаційній безпеці наступала рідше ніж 1 раз на рік; 2 – подія в наслідок настання загроз інформаційній безпеці наступала не рідше ніж 1 раз на рік; 3 – подія в наслідок настання загроз інформаційній безпеці наступала не рідше ніж 1 раз на квартал; 4 – подія в наслідок настання загроз інформаційній безпеці наступала не рідше ніж 1 раз на місяць; 5 – подія в наслідок настання загроз інформаційній безпеці має певну періодичність (не рідше ніж 1 раз на тиждень).

1. Знищення/пошкодження апаратних засобів

☐ — 0 балів ☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

2. Знищення/пошкодження програмного забезпечення

☐ — 0 балів ☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

3. Проникнення в інформаційну систему підприємства

☐ — 0 балів ☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

4. Пошкодження елементів інформаційної системи підприємства

☐ — 0 балів ☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

5. Несанкціонований доступ до інформаційних активів та інформаційних ресурсів

☐ — 0 балів ☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

6. Знищення даних

☐ — 0 балів ☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

7. Втрата конфіденційних даних

☐ — 0 балів ☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

8. Несанкціонована модифікація інформації

☐ — 0 балів ☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

9. Розкриття/викрадення фінансової інформації

☐ — 0 балів ☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

10. Недоступність ІКТ-послуг через зовнішні атаки (електронна пошта, Інтернет, віддалений доступ, хмарна технологія, веб-сайт тощо)

☐ — 0 балів ☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

11. Перерва в господарській діяльності підприємства/працівника

☐ — 0 балів ☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

12. Заподіяння шкоди діловій репутації/бренду підприємства

☐ — 0 балів ☐ — 1 бал ☐ — 2 бали ☐ — 3 бали ☐ — 4 бали ☐ — 5 балів

Додаток III

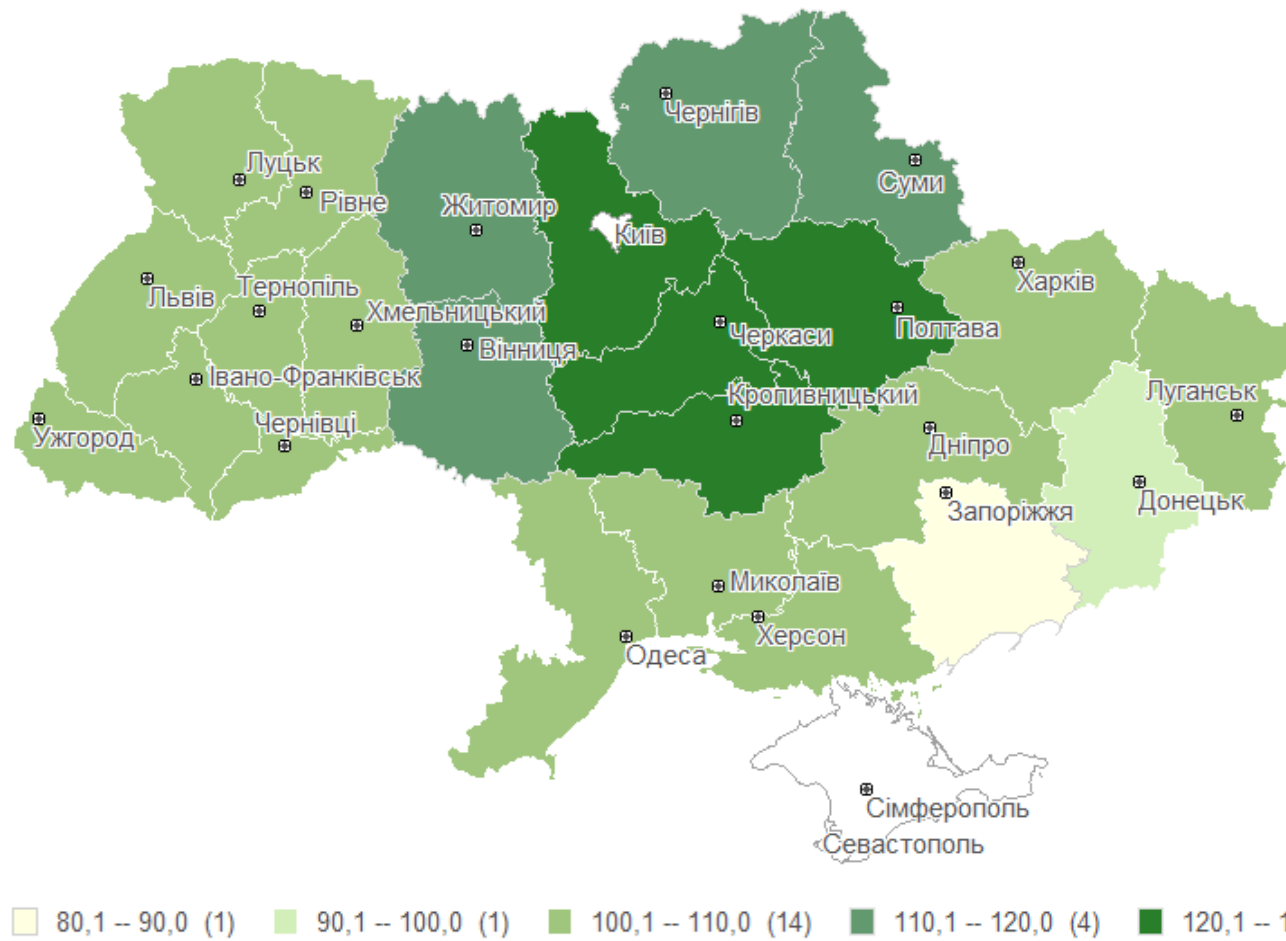
Таблиця III.1

Динаміка приросту виробництва сільськогосподарської продукції підприємств областей України за 2013–2018 рр.[сформовано на основі 107; 118]

Область	Приріст виробництва сільськогосподарської продукції, %					
	2014 р. до 2013 р.	2015 р. до 2014 р.	2016 р. до 2015 р.	2017 р. до 2016 р.	2018 р. до 2017 р.	Усереднене значення за 5 років
Вінницька	111,0	91,8	117,0	95,8	110,8	105,3
Волинська	106,3	95,4	101,9	104,8	103,1	102,3
Дніпропетровська	94,1	106,3	100,3	100,5	102,2	100,7
Донецька	93,0	64,9	108,3	102,2	90,3	91,7
Житомирська	105,1	91,2	116,7	105,8	110,8	105,9
Закарпатська	99,9	95,1	96,8	101,4	106,5	99,9
Запорізька	96,6	109,3	98,7	96,7	85,6	97,4
Івано-Франківська	106,3	95,5	101,7	104,0	101,1	101,7
Київська	105,8	89,2	109,8	95,7	120,7	104,2
Кіровоградська	98,2	97,7	109,4	86,1	120,4	102,4
Луганська	79,8	77,8	119,3	94,0	103,5	94,9
Львівська	105,5	97,1	102,6	106,1	104,7	103,2
Миколаївська	93,3	102,1	108,5	90,9	105,9	100,1
Одеська	97,4	96,2	111,6	99,4	100,5	101,0
Полтавська	96,9	107,3	103,3	83,2	123,7	102,9
Рівненська	105,2	92,8	104,9	105,0	101,9	102,0
Сумська	109,7	95,4	103,5	100,0	111,7	104,1
Тернопільська	113,9	88,8	104,6	111,1	103,9	104,5
Харківська	103,1	97,2	106,6	90,1	106,0	100,6
Херсонська	105,1	105	103,7	99,6	100,3	102,7
Хмельницька	115,4	87,3	108,2	112,0	102,8	105,1
Черкаська	98,4	99,4	102,5	88,5	119,7	101,7
Чернівецька	104,2	91,1	100,0	105,3	103,7	100,9
Чернігівська	107,5	98,1	104,5	105,3	109,2	104,9

Дані наведено без урахування тимчасово окупованої території АРК, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Додаток Щ



Дані наведено без урахування тимчасово окупованої території АРК, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях

Рис. Щ.1. Кластеризація областей України за індексом сільськогосподарської продукції за 2018 р. [113]

Додаток Ю

АНКЕТА

оцінки рівня інформаційної безпеки підприємств агропродовольчої сфери

(назва підприємства)

(ПІБ, посада респондента)

З метою визначення рівня інформаційної безпеки Вашого підприємства, надайте відповіді на запитання. В разі, якщо Ви не володієте інформацією для надання об'єктивної відповіді, прохання не відповідати на питання.

1. Зазначте загальну кількість інформаційних атак протягом року, од.:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

2. Вкажіть кількість відвернутих інформаційних атак протягом року, од.:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

3. Зазначте час безперебійного функціонування інформаційної системи протягом року, люд.-год:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

4. Зазначте нормативний час функціонування інформаційної системи протягом року, люд.-год:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

5. Зазначте загальну кількість процесів спрямованих на програмно-технічний захист інформації, од.:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

6. Вкажіть кількість автоматизованих процесів спрямованих на програмно-технічний захист інформації в конкретному році, од.:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

7. Вкажіть загальну кількість програмно-технічних засобів захисту інформаційної системи в конкретному році, од.:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

8. Зазначте кількість новітніх (які, перебувають на ринку менше року) програмно-технічних засобів захисту інформаційної системи в конкретному році, од.:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

9. Вкажіть суму загальних витрат підприємства в конкретному році, тис. грн:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

10. Вкажіть суму витрат на забезпечення інформаційної безпеки підприємства в конкретному році, тис. грн:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

11. Вкажіть суму витрат на утримання інформаційної служби (фахівця з інформаційної безпеки) в конкретному році, тис. грн:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

12. Зазначте суму витрат на програмно-технічний захист інформаційних ресурсів в конкретному році, тис. грн:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

13. Вкажіть суму витрат на забезпечення інформаційної безпеки, яка спрямована на захист фінансової підсистеми в конкретному році, тис. грн:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

14. Вкажіть суму витрат на забезпечення інформаційної безпеки, спрямована на захист виробничої підсистеми підприємства в конкретному році, тис. грн:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

15. Зазначте суму витрат на забезпечення інформаційної безпеки, спрямована на захист виробничої підсистеми підприємства в конкретному році, тис. грн:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

16. Вкажіть суму витрат на витрат на забезпечення інформаційної безпеки, спрямована на захист комерційної, інноваційної та продовольчої підсистем підприємства в конкретному році, тис. грн:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

17. Вкажіть вартість програмного забезпечення, яке застосовується для створення інформаційного захисту в конкретному році, тис. грн:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

18. Вкажіть вартість технічного забезпечення, яке застосовується для створення інформаційного захисту в конкретному році, тис. грн:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

19. Вкажіть суму витрат на забезпечення інформаційної безпеки, яка спрямована на захист фізичних об'єктів підприємства в конкретному році, тис. грн:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

20. Зазначте суму витрат на забезпечення інформаційної безпеки, яка спрямована на захист персоналу підприємства в конкретному році, тис. грн:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

21. Вкажіть суму витрат на забезпечення інформаційної безпеки, яка спрямована на захист персоналу підприємства в конкретному році, тис. грн:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

22. Вкажіть загальну чисельність персоналу підприємства в конкретному році, осіб:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

23. Вкажіть чисельність працівників, які ознайомлені з політикою інформаційної підприємства в конкретному році, осіб:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

24. Вкажіть чисельність працівників, які мають доступ до комерційної таємниці (баз даних, банків даних тощо) в конкретному році, осіб:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

25. Зазначте чисельність працівників, які мають доступ до комерційної таємниці (баз даних, банків даних тощо), що працюють на підприємстві більше одного року в конкретному році, осіб:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

26. Вкажіть загальну чисельність звільнених працівників підприємства в конкретному році, осіб:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

27. Вкажіть загальну чисельність звільнених працівників за причиною витоку інформації підприємства в конкретному році, осіб:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

28. Вкажіть загальну чисельність працівників підприємства, що мають доступ до закритої інформації в конкретному році, осіб:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

29. Вкажіть чисельність працівників підприємства, що мають доступ до закритої інформації, ненавмисні дії яких призвели до витоку інформації через низький в конкретному році, осіб:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

30. Вкажіть загальну чисельність працівників системи управління інформаційною безпекою підприємства в конкретному році, осіб:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

31. Зазначте чисельність працівників системи управління інформаційною безпекою підприємства, які мають відповідну спеціальність та кваліфікацію в конкретному році, осіб:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

32. Вкажіть обсяг юридично захищеної інформації, у % до загального обсягу інформації в конкретному році:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

33. Вкажіть обсяг інформації, розголошення якої може спричинити негативні наслідки для підприємства, у % до загального обсягу інформації в конкретному році:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

34. Вкажіть чисельність інформаційних загроз (інформаційних атак), які відвернуті через дії персоналу, який забезпечує інформаційну безпеку в конкретному році, од.:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

35. Зазначте чисельність інформаційних загроз (інформаційних атак), які відвернуті через дії персоналу, який забезпечує інформаційну безпеку в конкретному році, од.:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

36. Зазначте обсяг інформації, що є в розпорядженні ОПР для прийняття рішення в конкретному році, %

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

37. Зазначте обсяг необхідної інформації, що є в розпорядженні ОПР для прийняття рішення в конкретному році, %

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

38. Зазначте обсяг релевантної інформації, що є в розпорядженні ОПР для прийняття рішення в конкретному році, %

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

39. Зазначте обсяг релевантної інформації, що є в розпорядженні ОПР для прийняття рішення в конкретному році, %

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

40. Вкажіть кількість незалежних свідчень на користь ухвалення рішення до загальної кількості незалежних свідчень у сумарному обсязі релевантної інформації

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

41. Зазначте обсяг своєчасно наданої ОПР інформації для прийняття рішення, в конкретному році, %

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

42. Зазначте обсяг інформації, наданої ОПР з перевірених джерел, в конкретному році, %

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

43. Вкажіть обсяг інформації, наданої ОПР у коректній та зручній формі для ефективного та швидкого прийняття рішення, в конкретному році, %

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

44. Зазначте загальні компетентності, якими повинен володіти керівний персонал системи інформаційної безпеки

їх кількість у конкретному році

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

45. Вкажіть компетентності, якими володіє керівний персонал системи інформаційної безпеки

їх кількість у конкретному році

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

46. Вкажіть кількість загального програмного забезпечення, яке використовується для захисту інформаційної системи в конкретному році, од.:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

47. Зазначте кількість програмного забезпечення, розробленого працівниками підприємства, яке задіяне для забезпечення інформаційної безпеки підприємства в конкретному році, од.:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

48. Вкажіть кількість технічних засобів, які використовуються для захисту інформаційної системи в конкретному році, од.:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

49. Вкажіть кількість технічних засобів, розроблених працівниками підприємства, що задіяні для забезпечення інформаційної безпеки підприємства в конкретному році, од.:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

50. Вкажіть суму загальних втрат від порушення безпеки на підприємстві в конкретному році, тис. грн:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

51. Зазначте суму втрат спричинених пошкодженням інформаційної цілісності в конкретному році, тис. грн:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

52. Визначте здатність системи управління інформаційною безпекою підприємства швидко адаптувати організаційну побудову до зовнішніх та внутрішніх потреб за шкалою: від 0 до 1, де 0 – неможливість системи інформаційної безпеки підприємства до адаптації; 1 – можливість системи інформаційної безпеки підприємства до швидкої реструктуризації, адаптації:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

53. Зазначте наявність та актуальність нормативно-правового забезпечення системи інформаційної безпеки підприємства за шкалою: від 0 до 1, де 0 – нормативно-правове забезпечення системи інформаційної безпеки підприємства відсутнє; 0,33 – наявне застаріле та неактуальне, частково формалізоване нормативно-правове забезпечення системи інформаційної безпеки; 0,66 – наявне неактуальне повністю формалізоване нормативно-правове забезпечення системи інформаційної безпеки; 1 – наявне актуальне повністю формалізоване нормативно-правове забезпечення системи інформаційної безпеки:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

54. Визначте наявність на підприємстві політики інформаційної безпеки за шкалою: від 0 до 1, де 0 – політика інформаційної безпеки відсутня; 0,5 – політика інформаційної безпеки наявна, але не формалізована; 1 – наявна дієва та ефективна політика інформаційної безпеки на підприємстві:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

55. Визначте наявність на підприємстві стратегії інформаційної безпеки за шкалою: від 0 до 1, де 0 – стратегія інформаційної безпеки відсутня; 0,33 – стратегія інформаційної безпеки наявна, але не формалізована; 0,67 – визначена стратегія інформаційної безпеки підприємства; 1 – визначена стратегія інформаційної безпеки підприємства, яка інтегрована у загальну стратегію розвитку підприємства:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

56. Визначте наявність на підприємстві підрозділу управління інформаційною безпекою за шкалою: від 0 до 1, де 0 – підрозділ управління інформаційною безпекою на підприємстві відсутній; 0,5 – є окремі фахівці, які забезпечують захист інформаційної безпеки; 1 – сформований та організаційно закріплений підрозділ управління інформаційною безпекою підприємства:

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

Система показників для оцінки інформаційної безпеки підприємства агропродовольчої сфери [39]

№ п/п	Показники інформаційної безпеки	Характеристика	Можливе порогове значення / нормативне значення
1	2	3	4
Група показників оцінки програмно-технічної захищеності інформаційної системи			
1	Коефіцієнт технічного захисту інформаційної системи	Співвідношення кількості відвернутих інформаційних атак до загальної кількості інформаційних атак за певний проміжок часу	Прямує до зростання (до 1)
2	Коефіцієнт програмної захищеності інформаційної системи	Співвідношення часу безперебійного функціонування інформаційної системи до нормативного часу функціонування інформаційної системи	Прямує до зростання (до 1)
3	Коефіцієнт автоматизації програмно-технічної захищеності інформаційної системи	Співвідношення автоматизованих процесів спрямованих на програмно-технічний захист інформації до загальної кількості процесів спрямованих на програмно-технічний захист інформації	Прямує до зростання (до 1)
4.	Коефіцієнт інноваційності (новітності) програмно-технічної захищеності інформаційної системи	Співвідношення використання новітніх (які, перебувають на ринку менше року) програмно-технічних засобів захисту інформаційної системи до загальної кількості програмно-технічних засобів захисту	Прямує до зростання (нормативне 0,15)
Група показників оцінки фінансування (витрат) забезпечення інформаційної безпеки підприємства			
1	Коефіцієнт фінансування інформаційної безпеки	Співвідношення витрат на забезпечення інформаційної безпеки підприємства до загальних витрат підприємства	(прямує до зростання, нормативне значення 0,07–0,10)
2	Коефіцієнт фінансування інформаційних служб підприємства	Співвідношення витрат утримання інформаційної служби підприємства до загальних витрат підприємства	(нормативне значення 0,03–0,04)

1	2	3	4
3	Коефіцієнт фінансування програмно-технічної захищеності інформації	Співвідношення витрат на програмно-технічний захист інформаційних ресурсів до загальних витрат підприємства	(нормативне значення 0,03–0,04)
4	Коефіцієнт фінансування інформаційної безпеки фінансової підсистеми підприємства	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист фінансової підсистеми підприємства до загальних витрат на інформаційну безпеку	(нормативне значення 0,40–0,45)
5	Коефіцієнт фінансування інформаційної безпеки виробничої підсистеми підприємства	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист виробничої підсистеми підприємства до загальних витрат на інформаційну безпеку	(нормативне значення 0,30–0,35)
6	Коефіцієнт фінансування інформаційної безпеки комерційної, інноваційної та продовольчої підсистем підприємства	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист комерційної, інноваційної та продовольчої підсистем до загальних витрат на інформаційну безпеку	(нормативне значення 0,20–0,30)
7	Коефіцієнт фінансування програмної захищеності інформації	Співвідношення вартості програмного забезпечення, яке застосовується для створення інформаційного захисту до загальних витрат на інформаційну безпеку	(нормативне значення 0,20–0,25)
8	Коефіцієнт фінансування технічної захищеності інформації	Співвідношення вартості технічного забезпечення, яке застосовується для створення інформаційного захисту до загальних витрат на інформаційну безпеку	(нормативне значення 0,30–0,35)
9	Коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист фізичних об'єктів підприємства до загальних витрат на інформаційну безпеку	(нормативне значення 0,10–0,15)

1	2	3	4
10	Коефіцієнт фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист персоналу підприємства до загальних витрат на інформаційну безпеку	(нормативне значення 0,25–0,40)
Група показників оцінки інформаційної надійності персоналу			
1	Коефіцієнт обізнаності працівників підприємства з політикою інформаційної безпеки	Співвідношення чисельності працівників, які ознайомлені з політикою інформаційної підприємства до загальної чисельності працівників підприємства	Прямує до зростання (до 1)
2	Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства	Співвідношення чисельності працівників, маючих доступ до комерційної таємниці (баз даних, банків даних тощо), що працюють на підприємстві більше одного року до загальної чисельності працівників, що мають доступ до комерційної таємниці (баз даних, банків даних тощо)	Прямує до зростання (до 1)
3	Коефіцієнт ненадійності персоналу, що забезпечує інформаційну безпеку підприємства	Співвідношення чисельності працівників, звільнених за причиною витоку інформації до загальної чисельності звільнених працівників	Прямує до зменшення (до 0)
4	Коефіцієнт невідповідності персоналу до розпізнавання загроз інформаційній безпеці	Співвідношення чисельності працівників, ненавмисні дії яких призвели до витоку інформації через низький рівень компетентності персоналу та невміння розпізнавання загроз інформаційній безпеці до загальної чисельності працівників, що мають доступ до закритої інформації	Прямує до зменшення (до 0)
5	Коефіцієнт освіченості персоналу системи управління інформаційною	Співвідношення чисельності працівників системи управління інформаційною безпекою, які мають відповідну спеціальність та кваліфікацію, до загальної	Прямує до зростання (до 1)

1	2	3	4
	безпекою	чисельності працівників системи управління інформаційною безпекою підприємства	
6	Коефіцієнт правової незахищеності інформації	Співвідношення обсягу інформації, розголошення якої може спричинити негативні наслідки для підприємства до загального обсягу юридично захищеної інформації	Прямує до зменшення (до 0)
7	Коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку	Співвідношення інформаційних загроз (інформаційних атак), які відвернуті через дії персоналу, який забезпечує інформаційну безпеку до загальної кількості інформаційних атак за певний проміжок часу	Прямує до зростання (до 1)
Група показників оцінки інформації, що надається особам, які приймають рішення, системою інформаційного забезпечення (системою інформаційного захисту)			
1	Коефіцієнт повноти інформації	Співвідношення обсягу інформації, що є в розпорядженні ОПР до обсягу інформації, необхідної для ухвалення обґрунтованого рішення	Прямує до зростання (до 1)
2	Коефіцієнт точності інформації	Співвідношення обсягу релевантної інформації до загального обсягу наявної в розпорядженні ОПР інформації	Прямує до зростання (до 1)
3	Коефіцієнт суперечливості інформації	Співвідношення кількості незалежних свідчень на користь ухвалення рішення до загальної кількості незалежних свідчень у сумарному обсязі релевантної інформації	Прямує до зростання (до 1)
4	Коефіцієнт своєчасності надання інформації	Співвідношення обсягу своєчасно наданої ОПР інформації до обсягу інформації, необхідної для ухвалення обґрунтованого рішення	Прямує до зростання (до 1)
5	Коефіцієнт надійності інформації	Співвідношення обсягу інформації, наданої ОПР з перевірених джерел до загального обсягу наданої ОПР інформації	Прямує до зростання (до 1)

1	2	3	4
6	Коефіцієнт коректності форми подання інформації	Співвідношення обсягу інформації, наданої ОНР у коректній та зручній формі для ефективного та швидкого прийняття рішення до загального обсягу наданої ОНР інформації	Прямує до зростання (до 1)
Група показників оцінки системи інформаційної безпеки підприємства			
1	Коефіцієнт керованості системи інформаційної безпеки підприємства	Співвідношення компетентностей, якими володіє керівний персонал системи інформаційної безпеки до загальних компетентностей, якими повинен володіти керівник відповідного рівня.	1, зростання
2	Коефіцієнт власного програмного забезпечення	Співвідношення програмного забезпечення, розробленого працівниками підприємства, яке задіяне для забезпечення інформаційної безпеки підприємства до загального програмного забезпечення, яке використовується для захисту інформаційної системи	1, зростання
3	Коефіцієнт власних технічних засобів	Співвідношення технічних засобів, розроблених працівниками підприємства, що задіяні для забезпечення інформаційної безпеки підприємства до загальної чисельності технічних засобів, які використовуються для захисту інформаційної системи	0,25, зростання
4	Ступінь інформаційного ризику	відсоток втрат (у грошову вираженні) спричинених пошкодженням інформаційної цілісності підприємства до загальних втрат від порушення безпеки	Прямує до зменшення (до 0)
5	Гнучкість системи інформаційної безпеки підприємства	Здатність системи управління інформаційною безпекою швидко адаптувати організаційну побудову до зовнішніх та внутрішніх потреб	(від 0 до 1, де 0 – неможливість системи інформаційної безпеки підприємства до адаптації; 1 – можливість системи інформаційної безпеки підприємства до швидкої реструктуризації, адаптації;

1	2	3	4
6	Наявність та актуальність нормативно-правового забезпечення системи інформаційної безпеки підприємства	(від 0 до 1, де 0 – нормативно-правове забезпечення системи інформаційної безпеки підприємства відсутнє; 0,33 – наявне застаріле та неактуальне, частково формалізоване нормативно-правове забезпечення системи інформаційної безпеки; 0,66 – наявне неактуальне повністю формалізоване нормативно-правове забезпечення системи інформаційної безпеки; 1 – наявне актуальне повністю формалізоване нормативно-правове забезпечення системи інформаційної безпеки)	
7	Наявність на підприємстві політики інформаційної безпеки	(від 0 до 1, де 0 – політика інформаційної безпеки відсутня; 0,5 – політика інформаційної безпеки наявна, але не формалізована; 1 – наявна дієва та ефективна політика інформаційної безпеки на підприємстві)	
8	Наявність на підприємстві стратегії інформаційної безпеки	(від 0 до 1, де 0 – стратегія інформаційної безпеки відсутня; 0,33 – стратегія інформаційної безпеки наявна, але не формалізована; 0,67 – визначена стратегія інформаційної безпеки підприємства; 1 – визначена стратегія інформаційної безпеки підприємства, яка інтегрована у загальну стратегію розвитку підприємства)	
9	Наявність на підприємстві підрозділу управління інформаційною безпекою	(від 0 до 1, де 0 – підрозділ управління інформаційною безпекою на підприємстві відсутній; 0,5 – політика інформаційної безпеки наявна, але не формалізована; 1 – сформований та організаційно закріплений підрозділ управління інформаційною безпекою підприємства)	

Додаток АА

Таблиця АА.1

Оцінка програмно-технічної захищеності інформаційної системи підприємств Полтавської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт технічного захисту інформаційної системи	0,65	0,73	0,69	0,74	0,79	0,85	0,79	0,84	0,83	0,86	0,777
Коефіцієнт програмної захищеності інформаційної системи	0,78	0,81	0,79	0,75	0,84	0,89	0,91	0,89	0,92	0,87	0,845
Коефіцієнт автоматизації програмно-технічної захищеності інформаційної системи	0,11	0,13	0,15	0,19	0,17	0,21	0,25	0,35	0,39	0,42	0,237
Коефіцієнт інноваційності (новітності) програмно-технічної захищеності інформаційної системи	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,06	0,07	0,06	0,019

Таблиця АА.2

**Оцінка фінансування забезпечення інформаційної безпеки підприємств Полтавської області за 2009-2018 рр.
[побудовано автором]**

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт фінансування інформаційної безпеки	0,01	0,01	0,01	0,03	0,03	0,03	0,07	0,08	0,07	0,08	0,042
Коефіцієнт фінансування інформаційних служб підприємства	0,00	0,00	0,00	0,00	0,02	0,00	0,02	0,03	0,03	0,03	0,013
Коефіцієнт фінансування програмно-технічної захищеності інформації	0,01	0,01	0,01	0,03	0,01	0,03	0,05	0,05	0,04	0,05	0,029
Коефіцієнт фінансування інформаційної безпеки фінансової підсистеми підприємства	0,15	0,15	0,19	0,24	0,25	0,31	0,32	0,34	0,37	0,39	0,271
Коефіцієнт фінансування інформаційної безпеки виробничої підсистеми підприємства	0,21	0,24	0,27	0,25	0,28	0,34	0,33	0,35	0,34	0,35	0,296
Коефіцієнт фінансування інформаційної безпеки комерційної, інноваційної та продовольчої підсистем підприємства	0,11	0,10	0,10	0,11	0,12	0,08	0,10	0,13	0,12	0,14	0,111
Коефіцієнт фінансування програмної захищеності інформації	0,11	0,14	0,21	0,15	0,22	0,21	0,19	0,18	0,22	0,23	0,186
Коефіцієнт фінансування технічної захищеності інформації	0,19	0,21	0,22	0,23	0,19	0,21	0,19	0,24	0,26	0,27	0,221
Коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства	0,04	0,05	0,09	0,04	0,04	0,05	0,09	0,07	0,08	0,05	0,06
Коефіцієнт фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства	0,23	0,19	0,21	0,19	0,25	0,24	0,28	0,29	0,3	0,32	0,25

Таблиця АА.3

Оцінка інформаційної надійності персоналу підприємств Полтавської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт обізнаності працівників підприємства з політикою інформаційної безпеки	0,45	0,35	0,45	0,55	0,61	0,58	0,64	0,65	0,65	0,73	0,566
Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства	0,65	0,63	0,59	0,64	0,71	0,73	0,75	0,76	0,80	0,80	0,706
Коефіцієнт ненадійності персоналу, що забезпечує інформаційну безпеку підприємства	0,04	0,00	0,00	0,05	0,00	0,00	0,00	0,00	0,00	0,00	0,009
Коефіцієнт невідповідності персоналу до розпізнавання загроз інформаційній безпеці	0,15	0,12	0,10	0,08	0,06	0,06	0,05	0,05	0,04	0,03	0,074
Коефіцієнт освіченості персоналу системи управління інформаційною безпекою	0,20	0,20	0,25	0,45	0,40	0,35	0,55	0,65	0,60	0,70	0,435
Коефіцієнт правової незахищеності інформації	0,09	0,08	0,08	0,07	0,06	0,05	0,04	0,05	0,06	0,05	0,063
Коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку	0,58	0,63	0,59	0,68	0,69	0,75	0,78	0,81	0,85	0,81	0,717

Таблиця АА.4

Оцінка інформації, що надається особам, які приймають рішення, системою інформаційного забезпечення (системою інформаційного захисту) на підприємствах Полтавської області за 2009-2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт повноти інформації	0,35	0,35	0,40	0,45	0,40	0,35	0,35	0,35	0,30	0,30	0,360
Коефіцієнт точності інформації	0,40	0,45	0,45	0,45	0,50	0,55	0,60	0,65	0,65	0,70	0,540
Коефіцієнт суперечливості інформації	0,50	0,55	0,60	0,60	0,70	0,70	0,80	0,70	0,65	0,70	0,650
Коефіцієнт своєчасності надання інформації	0,60	0,65	0,65	0,65	0,70	0,75	0,80	0,75	0,85	0,80	0,720
Коефіцієнт надійності інформації	0,75	0,75	0,75	0,80	0,85	0,85	0,85	0,80	0,90	0,85	0,815
Коефіцієнт коректності форми подання інформації	0,65	0,70	0,65	0,65	0,70	0,70	0,70	0,65	0,70	0,70	0,680

Таблиця АА.5

Оцінка системи інформаційної безпеки підприємств Полтавської області за 2009-2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт керованості системи інформаційної безпеки підприємства	0,60	0,70	0,70	0,65	0,70	0,75	0,70	0,65	0,70	0,70	0,685
Коефіцієнт власного програмного забезпечення	0,05	0,05	0,05	0,05	0,10	0,05	0,10	0,10	0,15	0,12	0,082
Коефіцієнт власних технічних засобів	0,10	0,08	0,09	0,08	0,09	0,10	0,10	0,10	0,15	0,15	0,104
Ступінь інформаційного ризику	0,15	0,12	0,12	0,12	0,10	0,10	0,07	0,12	0,10	0,09	0,109
Гнучкість системи інформаційної безпеки підприємства	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00	1,00	1,00	0,300
Наявність та актуальність нормативно-правового забезпечення системи інформаційної безпеки підприємства	0,33	0,33	0,33	0,33	0,33	0,67	0,67	0,67	0,67	0,67	0,500
Наявність на підприємстві політики інформаційної безпеки	0,00	0,00	0,00	0,50	0,50	0,50	0,50	0,50	0,50	1,00	0,400
Наявність на підприємстві стратегії інформаційної безпеки	0,33	0,33	0,33	0,33	0,33	0,67	0,67	0,67	0,60	0,67	0,493
Наявність на підприємстві підрозділу управління інформаційною безпекою	0,00	0,00	0,00	0,00	0,00	0,00	0,50	0,50	0,50	0,50	0,200

Таблиця АА.6

Оцінка програмно-технічної захищеності інформаційної системи підприємств Сумської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт технічного захисту інформаційної системи	0,73	0,69	0,78	0,74	0,81	0,79	0,84	0,81	0,81	0,77	0,777
Коефіцієнт програмної захищеності інформаційної системи	0,69	0,71	0,73	0,75	0,78	0,74	0,81	0,82	0,87	0,81	0,771
Коефіцієнт автоматизації програмно-технічної захищеності інформаційної системи	0,09	0,08	0,05	0,11	0,19	0,15	0,17	0,23	0,25	0,29	0,161
Коефіцієнт інноваційності (новітності) програмно-технічної захищеності інформаційної системи	0,00	0,00	0,00	0,00	0,00	0,01	0,02	0,06	0,05	0,06	0,020

Таблиця АА.7

**Оцінка фінансування забезпечення інформаційної безпеки підприємств Сумської області за 2009-2018 рр.
[побудовано автором]**

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт фінансування інформаційної безпеки	0,01	0,01	0,01	0,02	0,03	0,05	0,05	0,07	0,07	0,06	0,038
Коефіцієнт фінансування інформаційних служб підприємства	0,00	0,00	0,00	0,00	0,01	0,01	0,02	0,03	0,03	0,02	0,012
Коефіцієнт фінансування програмно-технічної захищеності інформації	0,01	0,01	0,01	0,02	0,02	0,04	0,03	0,04	0,04	0,04	0,026
Коефіцієнт фінансування інформаційної безпеки фінансової підсистеми підприємства	0,22	0,23	0,25	0,26	0,19	0,29	0,25	0,28	0,33	0,31	0,261
Коефіцієнт фінансування інформаційної безпеки виробничої підсистеми підприємства	0,25	0,19	0,31	0,27	0,29	0,22	0,24	0,31	0,32	0,37	0,277
Коефіцієнт фінансування інформаційної безпеки комерційної, інноваційної та продовольчої підсистем підприємства	0,09	0,08	0,07	0,11	0,11	0,10	0,12	0,11	0,10	0,11	0,100
Коефіцієнт фінансування програмної захищеності інформації	0,09	0,12	0,13	0,15	0,16	0,17	0,14	0,19	0,20	0,19	0,154
Коефіцієнт фінансування технічної захищеності інформації	0,18	0,19	0,16	0,19	0,18	0,17	0,19	0,22	0,25	0,23	0,196
Коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства	0,06	0,05	0,05	0,05	0,05	0,07	0,08	0,07	0,05	0,07	0,060
Коефіцієнт фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства	0,20	0,20	0,23	0,24	0,26	0,27	0,21	0,29	0,22	0,25	0,237

Таблиця АА.8

Оцінка інформаційної надійності персоналу підприємств Сумської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт обізнаності працівників підприємства з політикою інформаційної безпеки	0,33	0,41	0,38	0,37	0,56	0,59	0,65	0,67	0,60	0,70	0,526
Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства	0,65	0,65	0,60	0,64	0,70	0,70	0,75	0,75	0,85	0,80	0,709
Коефіцієнт ненадійності персоналу, що забезпечує інформаційну безпеку підприємства	0,00	0,00	0,00	0,00	0,05	0,04	0,04	0,00	0,00	0,00	0,013
Коефіцієнт невідповідності персоналу до розпізнавання загроз інформаційній безпеці	0,10	0,10	0,15	0,10	0,08	0,08	0,08	0,09	0,05	0,05	0,088
Коефіцієнт освіченості персоналу системи управління інформаційною безпекою	0,25	0,20	0,20	0,25	0,35	0,35	0,50	0,50	0,70	0,70	0,40
Коефіцієнт правової захищеності інформації	0,09	0,08	0,08	0,07	0,07	0,06	0,08	0,05	0,04	0,05	0,067
Коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку	0,54	0,58	0,62	0,61	0,57	0,69	0,73	0,8	0,82	0,76	0,672

Таблиця АА.9

Оцінка інформації, що надається особам, які приймають рішення, системою інформаційного забезпечення (системою інформаційного захисту) на підприємствах Сумської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт повноти інформації	0,40	0,40	0,35	0,35	0,40	0,40	0,35	0,30	0,35	0,35	0,365
Коефіцієнт точності інформації	0,40	0,45	0,45	0,40	0,55	0,55	0,55	0,65	0,65	0,70	0,535
Коефіцієнт суперечливості інформації	0,65	0,60	0,60	0,55	0,60	0,65	0,70	0,70	0,65	0,70	0,640
Коефіцієнт своєчасності надання інформації	0,65	0,60	0,70	0,65	0,65	0,65	0,80	0,75	0,75	0,80	0,700
Коефіцієнт надійності інформації	0,65	0,75	0,75	0,70	0,75	0,80	0,85	0,85	0,90	0,85	0,785
Коефіцієнт коректності форми подання інформації	0,75	0,75	0,75	0,75	0,70	0,70	0,70	0,70	0,75	0,75	0,730

Таблиця АА.10

Оцінка системи інформаційної безпеки підприємств Сумської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт керованості системи інформаційної безпеки підприємства	0,6	0,65	0,65	0,65	0,65	0,70	0,70	0,70	0,75	0,75	0,680
Коефіцієнт власного програмного забезпечення	0,05	0,08	0,08	0,10	0,08	0,07	0,09	0,09	0,09	0,10	0,083
Коефіцієнт власних технічних засобів	0,07	0,08	0,09	0,09	0,09	0,08	0,09	0,10	0,10	0,11	0,090
Ступінь інформаційного ризику	0,14	0,18	0,17	0,1	0,09	0,1	0,08	0,10	0,10	0,09	0,115
Гнучкість системи інформаційної безпеки підприємства	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00	1,00	1,00	0,300
Наявність та актуальність нормативно-правового забезпечення системи інформаційної безпеки підприємства	0,33	0,33	0,33	0,33	0,33	0,33	0,67	0,67	0,67	0,67	0,466
Наявність на підприємстві політики інформаційної безпеки	0,00	0,00	0,00	0,00	0,00	0,50	0,50	0,50	0,50	0,50	0,250
Наявність на підприємстві стратегії інформаційної безпеки	0,33	0,33	0,33	0,33	0,33	0,33	0,67	0,67	0,67	0,67	0,466
Наявність на підприємстві підрозділу управління інформаційною безпекою	0,00	0,00	0,00	0,00	0,00	0,00	0,50	0,50	0,50	0,50	0,200

Таблиця АА.11

Оцінка програмно-технічної захищеності інформаційної системи підприємств Кіровоградської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт технічного захисту інформаційної системи	0,66	0,67	0,72	0,73	0,69	0,74	0,71	0,77	0,68	0,69	0,706
Коефіцієнт програмної захищеності інформаційної системи	0,70	0,65	0,69	0,71	0,73	0,65	0,62	0,61	0,65	0,68	0,669
Коефіцієнт автоматизації програмно-технічної захищеності інформаційної системи	0,10	0,08	0,07	0,10	0,20	0,17	0,12	0,14	0,15	0,20	0,133
Коефіцієнт інноваційності (новітності) програмно-технічної захищеності інформаційної системи	0,00	0,00	0,00	0,00	0,00	0,00	0,03	0,02	0,02	0,03	0,010

**Оцінка фінансування забезпечення інформаційної безпеки підприємств Кіровоградської області за 2009–2018 рр.
[побудовано автором]**

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт фінансування інформаційної безпеки	0,01	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,04	0,04	0,023
Коефіцієнт фінансування інформаційних служб підприємства	0,00	0,00	0,00	0,01	0,01	0,01	0,00	0,01	0,01	0,01	0,006
Коефіцієнт фінансування програмно-технічної захищеності інформації	0,01	0,02	0,02	0,01	0,01	0,01	0,02	0,01	0,03	0,03	0,017
Коефіцієнт фінансування інформаційної безпеки фінансової підсистеми підприємства	0,12	0,12	0,15	0,13	0,16	0,22	0,20	0,21	0,23	0,23	0,177
Коефіцієнт фінансування інформаційної безпеки виробничої підсистеми підприємства	0,17	0,16	0,17	0,19	0,23	0,22	0,25	0,2	0,31	0,27	0,217
Коефіцієнт фінансування інформаційної безпеки комерційної, інноваційної та продовольчої підсистем підприємства	0,07	0,08	0,06	0,06	0,05	0,06	0,08	0,06	0,05	0,08	0,065
Коефіцієнт фінансування програмної захищеності інформації	0,06	0,06	0,07	0,09	0,10	0,07	0,07	0,07	0,07	0,06	0,072
Коефіцієнт фінансування технічної захищеності інформації	0,10	0,09	0,08	0,09	0,10	0,11	0,12	0,09	0,08	0,12	0,098
Коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства	0,01	0,06	0,05	0,05	0,05	0,05	0,06	0,07	0,06	0,07	0,053
Коефіцієнт фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства	0,14	0,15	0,15	0,16	0,18	0,15	0,17	0,17	0,17	0,17	0,161

**Оцінка інформаційної надійності персоналу підприємств Кіровоградської області за 2009–2018 рр.
[побудовано автором]**

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт обізнаності працівників підприємства з політикою інформаційної безпеки	0,33	0,33	0,33	0,35	0,39	0,42	0,45	0,62	0,55	0,60	0,437
Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства	0,43	0,48	0,42	0,51	0,56	0,57	0,58	0,60	0,60	0,61	0,536
Коефіцієнт ненадійності персоналу, що забезпечує інформаційну безпеку підприємства	0,00	0,00	0,00	0,05	0,04	0,00	0,06	0,05	0,00	0,00	0,020
Коефіцієнт невідповідності персоналу до розпізнавання загроз інформаційній безпеці	0,19	0,21	0,16	0,15	0,14	0,19	0,15	0,14	0,12	0,11	0,156
Коефіцієнт освіченості персоналу системи управління інформаційною безпекою	0,15	0,15	0,15	0,20	0,20	0,20	0,20	0,30	0,40	0,40	0,235
Коефіцієнт правової захищеності інформації	0,10	0,09	0,08	0,11	0,10	0,11	0,11	0,10	0,10	0,10	0,100
Коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку	0,43	0,48	0,54	0,51	0,62	0,54	0,61	0,68	0,72	0,65	0,578

Таблиця АА.14

Оцінка інформації, що надається особам, які приймають рішення, системою інформаційного забезпечення (системою інформаційного захисту) на підприємствах Кіровоградської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт повноти інформації	0,45	0,45	0,45	0,40	0,40	0,40	0,35	0,40	0,45	0,40	0,415
Коефіцієнт точності інформації	0,40	0,40	0,40	0,45	0,45	0,45	0,40	0,40	0,50	0,50	0,435
Коефіцієнт суперечливості інформації	0,50	0,50	0,45	0,55	0,45	0,60	0,65	0,60	0,55	0,65	0,550
Коефіцієнт своєчасності надання інформації	0,50	0,55	0,55	0,65	0,65	0,65	0,60	0,65	0,65	0,65	0,610
Коефіцієнт надійності інформації	0,65	0,65	0,70	0,70	0,65	0,65	0,70	0,65	0,70	0,70	0,675
Коефіцієнт коректності форми подання інформації	0,55	0,55	0,55	0,55	0,60	0,60	0,60	0,60	0,60	0,65	0,585

Таблиця АА.15

Оцінка системи інформаційної безпеки підприємств Кіровоградської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт керованості системи інформаційної безпеки підприємства	0,60	0,65	0,60	0,60	0,60	0,65	0,65	0,70	0,70	0,70	0,645
Коефіцієнт власного програмного забезпечення	0,04	0,04	0,05	0,05	0,05	0,05	0,06	0,07	0,08	0,09	0,058
Коефіцієнт власних технічних засобів	0,00	0,07	0,08	0,08	0,09	0,09	0,08	0,09	0,09	0,10	0,077
Ступінь інформаційного ризику	0,17	0,17	0,17	0,15	0,14	0,12	0,10	0,10	0,10	0,06	0,128
Гнучкість системи інформаційної безпеки підприємства	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00	0,100
Наявність та актуальність нормативно-правового забезпечення системи інформаційної безпеки підприємства	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,67	0,364
Наявність на підприємстві політики інформаційної безпеки	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,50	0,50	0,50	0,150
Наявність на підприємстві стратегії інформаційної безпеки	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,67	0,364
Наявність на підприємстві підрозділу управління інформаційною безпекою	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,50	0,50	0,50	0,150

Таблиця АА. 16

Оцінка програмно-технічної захищеності інформаційної системи підприємств Харківської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт технічного захисту інформаційної системи	0,56	0,61	0,63	0,58	0,59	0,55	0,64	0,69	0,71	0,63	0,619
Коефіцієнт програмної захищеності інформаційної системи	0,60	0,60	0,61	0,64	0,70	0,61	0,63	0,62	0,62	0,64	0,627
Коефіцієнт автоматизації програмно-технічної захищеності інформаційної системи	0,11	0,12	0,12	0,14	0,12	0,15	0,12	0,14	0,19	0,22	0,143
Коефіцієнт інноваційності (новітності) програмно-технічної захищеності інформаційної системи	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,05	0,05	0,07	0,017

**Оцінка фінансування забезпечення інформаційної безпеки підприємств Харківської області за 2009–2018 рр.
[побудовано автором]**

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт фінансування інформаційної безпеки	0,01	0,01	0,01	0,01	0,01	0,02	0,03	0,04	0,05	0,05	0,024
Коефіцієнт фінансування інформаційних служб підприємства	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,02	0,02	0,02	0,008
Коефіцієнт фінансування програмно-технічної захищеності інформації	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,02	0,03	0,03	0,016
Коефіцієнт фінансування інформаційної безпеки фінансової підсистеми підприємства	0,14	0,15	0,17	0,16	0,18	0,18	0,19	0,18	0,18	0,20	0,173
Коефіцієнт фінансування інформаційної безпеки виробничої підсистеми підприємства	0,21	0,20	0,18	0,19	0,18	0,19	0,15	0,21	0,25	0,24	0,200
Коефіцієнт фінансування інформаційної безпеки комерційної, інноваційної та продовольчої підсистем підприємства	0,09	0,05	0,04	0,03	0,04	0,07	0,08	0,07	0,08	0,07	0,062
Коефіцієнт фінансування програмної захищеності інформації	0,07	0,07	0,08	0,08	0,08	0,06	0,06	0,06	0,05	0,06	0,067
Коефіцієнт фінансування технічної захищеності інформації	0,11	0,10	0,12	0,09	0,08	0,13	0,12	0,10	0,09	0,10	0,104
Коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства	0,06	0,06	0,06	0,06	0,06	0,06	0,04	0,05	0,05	0,06	0,056
Коефіцієнт фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства	0,15	0,16	0,18	0,17	0,18	0,17	0,15	0,13	0,14	0,17	0,160

Таблиця АА.18

Оцінка інформаційної надійності персоналу підприємств Харківської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт обізнаності працівників підприємства з політикою інформаційної безпеки	0,25	0,33	0,35	0,42	0,47	0,55	0,59	0,63	0,64	0,64	0,487
Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства	0,41	0,43	0,47	0,51	0,51	0,56	0,63	0,65	0,60	0,67	0,544
Коефіцієнт ненадійності персоналу, що забезпечує інформаційну безпеку підприємства	0,00	0,00	0,05	0,06	0,00	0,06	0,05	0,00	0,00	0,00	0,022
Коефіцієнт невідповідності персоналу до розпізнавання загроз інформаційній безпеці	0,25	0,19	0,18	0,19	0,17	0,15	0,15	0,14	0,15	0,09	0,166
Коефіцієнт освіченості персоналу системи управління інформаційною безпекою	0,20	0,20	0,25	0,25	0,35	0,35	0,40	0,40	0,35	0,45	0,320
Коефіцієнт правової захищеності інформації	0,11	0,12	0,09	0,08	0,09	0,12	0,07	0,12	0,14	0,15	0,109
Коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку	0,45	0,54	0,48	0,54	0,53	0,55	0,59	0,61	0,59	0,62	0,550

Таблиця АА.19

Оцінка інформації, що надається особам, які приймають рішення, системою інформаційного забезпечення (системою інформаційного захисту) на підприємствах Харківської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт повноти інформації	0,50	0,50	0,45	0,45	0,4	0,45	0,35	0,45	0,35	0,40	0,430
Коефіцієнт точності інформації	0,45	0,40	0,50	0,45	0,50	0,45	0,45	0,45	0,40	0,50	0,455
Коефіцієнт суперечливості інформації	0,45	0,45	0,45	0,45	0,55	0,50	0,50	0,45	0,55	0,60	0,495
Коефіцієнт своєчасності надання інформації	0,55	0,55	0,60	0,60	0,65	0,60	0,65	0,60	0,65	0,65	0,610
Коефіцієнт надійності інформації	0,50	0,65	0,65	0,70	0,65	0,75	0,65	0,70	0,65	0,70	0,660
Коефіцієнт коректності форми подання інформації	0,55	0,50	0,55	0,55	0,60	0,65	0,60	0,55	0,60	0,60	0,575

Оцінка системи інформаційної безпеки підприємств Харківської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	
Коефіцієнт керованості системи інформаційної безпеки підприємства	0,60	0,60	0,60	0,60	0,60	0,60	0,65	0,65	0,65	0,65	0,620
Коефіцієнт власного програмного забезпечення	0,05	0,04	0,05	0,05	0,05	0,09	0,08	0,08	0,09	0,10	0,068
Коефіцієнт власних технічних засобів	0,05	0,06	0,04	0,05	0,09	0,08	0,09	0,10	0,09	0,10	0,075
Ступінь інформаційного ризику	0,15	0,15	0,14	0,16	0,15	0,13	0,12	0,13	0,12	0,11	0,136
Гнучкість системи інформаційної безпеки підприємства	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00	1,00	0,200
Наявність та актуальність нормативно-правового забезпечення системи інформаційної безпеки підприємства	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,67	0,364
Наявність на підприємстві політики інформаційної безпеки	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,50	0,50	0,50	0,150
Наявність на підприємстві стратегії інформаційної безпеки	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,67	0,67	0,398
Наявність на підприємстві підрозділу управління інформаційною безпекою	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,50	0,50	0,50	0,150

Таблиця АА. 21

Оцінка програмно-технічної захищеності інформаційної системи підприємств Луганської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014*	2015*	2016*	2017*	2018*	
Коефіцієнт технічного захисту інформаційної системи	0,56	0,59	0,61	0,66	0,61	0,61	0,62	0,63	0,69	0,64	0,622
Коефіцієнт програмної захищеності інформаційної системи	0,54	0,61	0,62	0,62	0,6	0,59	0,58	0,65	0,69	0,67	0,617
Коефіцієнт автоматизації програмно-технічної захищеності інформаційної системи	0,10	0,09	0,11	0,12	0,12	0,13	0,11	0,10	0,13	0,14	0,115
Коефіцієнт інноваційності (новітності) програмно-технічної захищеності інформаційної системи	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,04	0,04	0,008

* Дані наведено без урахування частини тимчасово окупованих територій у Луганській області

**Оцінка фінансування забезпечення інформаційної безпеки підприємств Луганської області за 2009–2018 рр.
[побудовано автором]**

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014*	2015*	2016*	2017*	2018*	
Коефіцієнт фінансування інформаційної безпеки	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,03	0,03	0,03	0,017
Коефіцієнт фінансування інформаційних служб підприємства	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,01	0,01	0,01	0,005
Коефіцієнт фінансування програмно-технічної захищеності інформації	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,02	0,02	0,013
Коефіцієнт фінансування інформаційної безпеки фінансової підсистеми підприємства	0,09	0,08	0,1	0,11	0,14	0,15	0,14	0,12	0,19	0,19	0,131
Коефіцієнт фінансування інформаційної безпеки виробничої підсистеми підприємства	0,15	0,14	0,19	0,18	0,17	0,15	0,14	0,14	0,15	0,18	0,159
Коефіцієнт фінансування інформаційної безпеки комерційної, інноваційної та продовольчої підсистем підприємства	0,05	0,05	0,04	0,03	0,04	0,03	0,03	0,04	0,04	0,04	0,039
Коефіцієнт фінансування програмної захищеності інформації	0,04	0,05	0,04	0,05	0,05	0,05	0,04	0,04	0,03	0,05	0,044
Коефіцієнт фінансування технічної захищеності інформації	0,05	0,06	0,06	0,05	0,04	0,05	0,06	0,07	0,05	0,06	0,055
Коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства	0,03	0,03	0,04	0,05	0,03	0,03	0,04	0,03	0,03	0,04	0,035
Коефіцієнт фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства	0,11	0,12	0,15	0,14	0,10	0,09	0,10	0,13	0,09	0,08	0,111

* Дані наведено без урахування частини тимчасово окупованих територій у Луганській області

Таблиця АА.23

Оцінка інформаційної надійності персоналу підприємств Луганської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014*	2015*	2016*	2017*	2018*	
Коефіцієнт обізнаності працівників підприємства з політикою інформаційної безпеки	0,23	0,25	0,27	0,27	0,29	0,35	0,34	0,35	0,36	0,34	0,305
Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства	0,31	0,35	0,33	0,29	0,27	0,35	0,40	0,34	0,35	0,38	0,337
Коефіцієнт ненадійності персоналу, що забезпечує інформаційну безпеку підприємства	0,00	0,05	0,05	0,06	0,07	0,06	0,05	0,00	0,00	0,00	0,034
Коефіцієнт невідповідності персоналу до розпізнавання загроз інформаційній безпеці	0,18	0,17	0,16	0,11	0,14	0,18	0,17	0,19	0,18	0,09	0,157
Коефіцієнт освіченості персоналу системи управління інформаційною безпекою	0,40	0,15	0,15	0,20	0,25	0,30	0,30	0,29	0,40	0,35	0,279
Коефіцієнт правової захищеності інформації	0,09	0,08	0,08	0,10	0,10	0,15	0,14	0,12	0,14	0,14	0,114
Коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку	0,25	0,29	0,28	0,24	0,24	0,26	0,31	0,28	0,31	0,29	0,275

* Дані наведено без урахування частини тимчасово окупованих територій у Луганській області

Таблиця АА.24

Оцінка інформації, що надається особам, які приймають рішення, системою інформаційного забезпечення (системою інформаційного захисту) на підприємствах Луганської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014*	2015*	2016*	2017*	2018*	
Коефіцієнт повноти інформації	0,45	0,50	0,45	0,50	0,45	0,45	0,45	0,40	0,40	0,40	0,445
Коефіцієнт точності інформації	0,35	0,45	0,50	0,35	0,30	0,30	0,35	0,35	0,35	0,30	0,360
Коефіцієнт суперечливості інформації	0,40	0,35	0,35	0,40	0,45	0,40	0,35	0,40	0,40	0,35	0,385
Коефіцієнт своєчасності надання інформації	0,55	0,50	0,45	0,50	0,45	0,45	0,40	0,35	0,40	0,45	0,450
Коефіцієнт надійності інформації	0,45	0,45	0,40	0,50	0,45	0,45	0,35	0,40	0,40	0,40	0,425
Коефіцієнт коректності форми подання інформації	0,55	0,55	0,65	0,65	0,65	0,55	0,50	0,50	0,55	0,50	0,565

*Дані наведено без урахування частини тимчасово окупованих територій у Луганській області

Таблиця АА.25

Оцінка системи інформаційної безпеки підприємств Луганської області за 2009–2018 рр. [побудовано автором]

Показник	Роки										Усереднене значення за 2009–2018 рр.
	2009	2010	2011	2012	2013	2014*	2015*	2016*	2017*	2018*	
Коефіцієнт керованості системи інформаційної безпеки підприємства	0,40	0,40	0,45	0,40	0,35	0,40	0,45	0,35	0,40	0,40	0,40
Коефіцієнт власного програмного забезпечення	0,03	0,03	0,02	0,03	0,02	0,03	0,02	0,04	0,03	0,03	0,028
Коефіцієнт власних технічних засобів	0,04	0,04	0,03	0,04	0,05	0,03	0,04	0,05	0,03	0,04	0,039
Ступінь інформаційного ризику	0,21	0,20	0,19	0,18	0,20	0,16	0,17	0,16	0,17	0,15	0,179
Гнучкість системи інформаційної безпеки підприємства	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,00	0,00	0,100
Наявність та актуальність нормативно-правового забезпечення системи інформаційної безпеки підприємства	0,00	0,00	0,00	0,33	0,33	0,33	0,33	0,33	0,33	0,67	0,265
Наявність на підприємстві політики інформаційної безпеки	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,50	0,050
Наявність на підприємстві стратегії інформаційної безпеки	0,00	0,00	0,00	0,00	0,33	0,33	0,33	0,33	0,67	0,67	0,266
Наявність на підприємстві підрозділу управління інформаційною безпекою	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,50	0,50	0,100

Дані наведено без урахування частини тимчасово окупованих територій у Луганській області

**Рівень інформаційної безпеки підприємств агропродовольчої сфери,
2014-2018 рр. [побудовано автором]**

Досліджувані підприємства	Роки					Середнє значення за 2014-2018 рр.
	2014	2015	2016	2017	2018	
ПрАТ «ПОЕЗ Кернел-груп»	0,74	0,74	0,77	0,71	0,8	0,75
ФГ «Батьківщина»	0,13	0,16	0,18	0,17	0,21	0,17
СК «Іскра»	0,21	0,14	0,19	0,11	0,18	0,17
СТОВ «Мусіївське»	0,34	0,41	0,34	0,27	0,31	0,33
ПрАТ «Агротон»	0,44	0,57	0,63	0,58	0,61	0,57
ТОВ «РОСТ АГРО»	0,42	0,35	0,37	0,29	0,39	0,36
ПСП «Солоницьке»	0,21	0,23	0,19	0,18	0,21	0,20
СТОВ «Агрофірма «Оржицька»	0,16	0,14	0,11	0,18	0,14	0,15
ТОВ «Агрофірма ім. Довженка»	0,66	0,69	0,71	0,73	0,7	0,70
СТОВ «Агрофірма «Дружба»	0,24	0,26	0,28	0,3	0,24	0,26
ПП «Альтаір»	0,09	0,08	0,06	0,11	0,11	0,09
ФГ «Товсте»	0,09	0,15	0,18	0,22	0,24	0,18
ПП «Надь»	0,19	0,24	0,2	0,24	0,3	0,23
СФГ «Зеніт»	0,35	0,38	0,36	0,4	0,39	0,38
ТОВ «АПК Докучаєвські чорноземи»	0,55	0,63	0,59	0,7	0,68	0,63

Динаміка зміни рівня інформаційної безпеки підприємств агропродовольчої сфери, 2014-2018 рр. [побудовано автором]

Досліджувані підприємства	Значення темпу зміни				Усереднене значення темпу зміни
	2014/2015 рр.	2015/2016 рр.	2016/2017 рр.	2017/2018 рр.	
ПрАТ «ПОЕЗ Кернел-груп»	0,00	4,05	-7,79	12,68	2,23
ФГ «Батьківщина»	23,08	12,50	-5,56	23,53	13,39
СК «Іскра»	-33,33	35,71	-42,11	63,64	5,98
СТОВ «Мусіївське»	20,59	-17,07	-20,59	14,81	-0,56
ПрАТ «Агротон»	29,55	10,53	-7,94	5,17	9,33
ТОВ «РОСТ АГРО»	-16,67	5,71	-21,62	34,48	0,48
ПСП «Солоницьке»	9,52	-17,39	-5,26	16,67	0,88
СТОВ «Агрофірма «Оржицька»	-12,50	-21,43	63,64	-22,22	1,87
ТОВ «Агрофірма ім. Довженка»	4,55	2,90	2,82	-4,11	1,54
СТОВ «Агрофірма «Дружба»	8,33	7,69	7,14	-20,00	0,79
ПП «Альтаір»	-11,11	-25,00	83,33	0,00	11,81
ФГ «Говсте»	66,67	20,00	22,22	9,09	29,49
ПП «Надь»	26,32	-16,67	20,00	25,00	13,66
СФГ «Зеніт»	8,57	-5,26	11,11	-2,50	2,98
ТОВ «АПК Докучаєвські чорноземи»	14,55	-6,35	18,64	-2,86	6,00

**Рівень рентабельності підприємств агропродовольчої сфери,
2014-2018 рр. [побудовано автором]**

Досліджувані підприємства	Роки					Середнє значення за 2014-2018 рр.
	2014	2015	2016	2017	2018	
ПрАТ «ПОЕЗ Кернел-груп»	-49,94	-30,51	54,47	5,69	-1,15	-4,29
ФГ «Батьківщина»	24,81	19,62	13,14	18,29	17,26	18,62
СК «Іскра»	2,86	51,74	21,82	11,92	7,85	19,24
СТОВ «Мусіївське»	12,86	4,98	10,19	7,87	9,44	9,07
ПрАТ «Агротон»	-36,12	24,11	-15,68	13,87	21,64	1,56
ТОВ «РОСТ АГРО»	14,61	-6,36	-9,18	15,18	11,35	5,12
ПСП «Солоницьке»	15,60	94,20	115,10	7,90	-25,80	41,40
СТОВ«Агрофірма «Оржицька»	18,24	8,83	7,06	9,01	6,63	9,95
ТОВ «Агрофірма ім. Довженка»	29,55	10,51	38,96	37,42	36,12	30,51
СТОВ «Агрофірма «Дружба»	4,70	19,53	27,59	10,66	15,77	15,65
ПП «Альтаір»	18,60	18,70	9,40	5,00	25,90	15,52
ФГ «Товсте»	23,16	19,85	29,33	31,45	32,49	27,26
ПП «Надь»	37,02	-6,06	-3,17	24,09	32,15	16,81
СФГ «Зеніт»	3,93	1,72	1,76	21,54	7,03	7,20
ТОВ «АПК Докучаєвські чорноземи»	18,08	12,55	18,98	17,42	16,51	16,71

Таблиця АВ.2

Динаміка зміни рівня рентабельності підприємств агропродовольчої сфери, 2014-2018 рр. [побудовано автором]

Досліджувані підприємства	Значення темпу зміни				Усереднене значення темпу зміни
	2014/2015 рр.	2015/2016 рр.	2016/2017 рр.	2017/2018 рр.	
ПрАТ «ПОЕЗ Кернел-груп»	38,91	278,53	-89,55	-120,21	26,92
ФГ «Батьківщина»	-20,92	-33,03	39,19	-5,63	-5,10
СК «Іскра»	1709,09	-57,83	-45,37	-34,14	392,94
СТОВ «Мусіївське»	-61,28	104,62	-22,77	19,95	10,13
ПрАТ «Агротон»	166,75	-165,04	188,46	56,02	61,55
ТОВ «РОСТ АГРО»	-143,53	-44,34	265,36	-25,23	13,06
ПСП «Солоницьке»	503,85	22,19	-93,14	-426,58	1,58
СТОВ «Агрофірма «Оржицька»	-51,59	-20,05	27,62	-26,42	-17,61
ТОВ «Агрофірма ім. Довженка»	-64,43	270,69	-3,95	-3,47	49,71
СТОВ «Агрофірма «Дружба»	315,53	41,27	-61,36	47,94	85,84
ПП «Альтаір»	0,54	-49,73	-46,81	418,00	80,50
ФГ «Говсте»	-14,29	47,76	7,23	3,31	11,00
ПП «Надь»	116,37	47,09	859,49	33,46	264,10
СФГ «Зеніт»	-56,23	2,33	1123,86	-67,36	250,65
ТОВ «АПК Докучаєвські чорноземи»	-30,59	51,24	-8,22	-5,22	1,80

Додаток АГ

Таблиця АГ.1

Продукція сільського господарства підприємств Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей (у постійних цінах 2010 року; мільйонів гривень), у 2009-2018 рр. [сформовано за матеріалами 68]

Підприємства	Роки										Усереднене значення за 2009-2018 рр.
	2009	2010	2011	2012	2013	2014*	2015*	2016*	2017*	2018*	
Полтавської області	3094,2	6564,4	9493,3	8265,6	10500,0	9765,9	10753,8	11438,8	8970,4	11748,8	9059,5
Сумської області	1390,2	2785,0	4630,1	4997,3	6128,9	6770,6	6596,3	6849,1	6849,4	7993,8	5499,1
Кіровоградської області	1843,7	4840,2	6693,0	5400,0	7485,7	7076,0	6727,8	7434,2	5936,1	7546,8	6098,4
Харківської області	2331,6	4586,5	7293,5	6325,1	8132,2	8702,4	8110,0	8864,7	7653,4	8397,9	7039,7
Луганської області	1305,6	2568,9	3526,6	3522,2	3643,3	2999,7	2208,6	2966,7	2800,5	2937,7	2848,0

*Дані наведено без урахування частини тимчасово окупованих територій у Луганській області.

Додаток АД

Таблиця АД. 1

Продуктивність праці в сільськогосподарських підприємствах Полтавської, Сумської, Кіровоградської, Харківської та Луганської областей(на 1 зайнятого в сільськогосподарському виробництві, у постійних цінах 2010 року; гривень), у 2009-2018 рр. [сформовано за матеріалами 68]

Підприємства	Роки										Усереднене значення за 2009-2018 рр.
	2009	2010	2011	2012	2013	2014*	2015*	2016*	2017*	2018*	
Полтавської області	154778,4	128845,1	173216,3	147841,0	199110,4	185060,9	209793,1	261458,7	212582,2	297167,4	196985,4
Сумської області	138163,1	118515,7	196904,8	220357,8	280628,8	309758,5	298872,2	307619,4	322260,8	410001,1	260308,2
Кіровоградської області	150355,3	154421,9	196034,5	161424,7	237075,6	223871,4	215629,5	259322,9	207121,8	271948,1	207720,6
Харківської області	146863,7	132592,3	198138,1	179150,7	234115,3	258113,7	249008,2	318897,3	272121,1	304405,9	229340,6
Луганської області	123333,2	120205,0	158294,0	159530,3	168447,2	205526,4	160442,9	245361,8	232967,0	253180,2	182728,8

*Дані наведено без урахування частини тимчасово окупованих територій у Луганській області.

Наукове видання

Дячков Дмитро Володимирович

Управлінські аспекти інформаційної безпеки: теорія, методологія, практика

Підписано до друку 02.12.2019 р.

Формат 60х84/16. Папір офсетний. Гарнітура Times.

Друк різнографічний. Умовн. друк. арк. 19,92

Наклад 500 прим. **Замовлення 2019-79.**

Видавництво «Інтр-М»

69014 м. Запоріжжя, вул. Колерова, 5

тел.: (061) 228-17-87, (061) 228-17-86, (067) 618-81-70

E-mail: marketing@inter-m.com.ua, веб-сайт: inter-m.bitrix24site.ua

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру
видавців, виготовників і розповсюджувачів видавничої продукції

Серія 33№26 від 23червня 2008р.

Друк ПП «Астроя»

36014, м. Полтава, вул. Шведська, 20, кв. 4

Тел.: +38 (0532) 509-167, 611-694

**Дата державної реєстрації та номер запису в ЄДР
14.12.1999 р. № 1 588 120 0000 010089**