ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЕКОНОМІКИ, УПРАВЛІННЯ, ПРАВА ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА МЕНЕДЖМЕНТУ ІМ. І.А. МАРКІНОЇ

Освітньо-професійна програма Менеджмент організацій
Спеціальність 073 Менеджмент
Ступінь вищої освіти Магістр

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ
Завідувач кафедри _____
Тетяна ВОРОНЬКО-НЕВІДНИЧА
18 квітня 2022 року

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **«Управління інформаційною безпекою підприємства»**
(на матеріалах «Назва підприємства» ххххххххххххххххххххх району)

виконав здобувач вищої освіти заочної форми навчання

Шабатько Євгеній Анатолійович

Керівник кваліфікаційної роботи Дмитро ДЯЧКОВ

Полтава – 2022 року

ЗМІСТ

ВСТУП

Актуальність теми. Необхідність забезпечення інформаційної безпеки держави загалом та підприємства зокрема, обумовлена сучасними умовами цифровізації ринкової економіки. Інформаційна безпека важлива як для економіки держави, так і для всіх її складових елементів та ланок, у тому числі й окремих галузей промисловості, підприємств. Особливу роль відіграє інформаційна безпека важливих підприємств, галузей народного господарства України, таких як агропродовольча. Швидкий темп зростання науково-технічного знання, широкий доступ до засобів розробки програмного забезпечення та апаратного комп'ютерного забезпечення та можливостей застосування останнього є причинами високої вразливості підприємств до загроз різного характеру. Першоджерелом такої вразливості є неточності та недоліки існуючої політики проведення заходів інформаційної безпеки підприємств Відтак, безпечність функціонування суб'єктів господарювання в умовах трансформації бізнес-середовища, захист систем управління виробничими, управлінськими, технологічними процесами, захищеність об'єктів інформаційної інфраструктури визнаються актуальними завданнями, які потребують формування теоретичного базису безпекології в сфері інформаційної захисту та практичної його реалізації.

Зв`язок роботи з науковими темами. Кваліфікаційна робота повністю відповідає плану науково-дослідних робіт Полтавського державного аграрного університету за темою «Управління національною безпекою в умовах глобалізаційних викликів: макро-, мікро-, регіональний та галузевий рівні» (державний реєстраційний номер 0118U005209).

Мета і завдання дослідження. Метою кваліфікаційної роботи є вивчення теоретичних положень та розробка рекомендацій щодо процесу управління інформаційною безпекою «Назва підприємства» ххххххххххххх району. Виконання поставленої мети допустиме при вирішенні наступних завдань:

розкриттю аспектів управління інформаційною безпекою агарних підприємств в умовах цифровізації продовольчих ринків;

аналізу управління інформаційною безпекою «Назва підприємства»;

розробці шляхів вдосконалення управління інформаційною безпекою підприємства.

Об'єктом дослідження виступає процес управління інформаційною безпекою «Назва підприємства» ххххххххххххххххххххх району.

Предметом дослідження виступають теоретичні, методичні положення та практичні рекомендації щодо управління інформаційною безпекою «Назва підприємства» ххххххххххххххххххххх району.

Методи наукових досліджень. У процесі роботи над кваліфікаційною роботою для розв'язання поставлених завдань застосовувались загальнонаукові методи: аналізу та синтезу, теоретичного узагальнення, системного та статистичного аналізу, економіко-математичні методи, графічний метод та інші.

Інформаційною базою кваліфікаційної роботи є наукові публікації, зокрема монографії, статті з відповідної тематики вітчизняних та зарубіжних авторів, матеріали наукових конференцій, власні аналітичні розрахунки та матеріали досліджень. Статистичну базу досліджень становлять дані фінансової звітності «Назва підприємства» ххххххххххххххххххххх району за 2016-2020 роки.

Елементи наукової новизни полягають в подальшому розвитку концепції управління підприємствами агросфери в умовах цифровізації, вдосконаленням напрямів та методів інформатизації виробничих та управлінських процесів на сільськогосподарських підприємствах, актуалізації підходів то етимологічного визначення сутності інформаційної безпеки та особливостей управління нею на підприємствах агропродовольчої сфери.

Практична значущість кваліфікаційної роботи полягає у визначенні стратегічних напрямів оптимізації програмної, технічної та кадрової складової системи інформаційної безпеки «Назва підприємства»та

актуалізації моделі управління інформаційною безпекою досліджуваного підприємства на основі врахування різносторонніх напрямів забезпечення захисту інформаційної інфраструктури за певними рівнями, враховуючи концепцію «глибинного захисту», та визначенні прогнозованого значення зростання рентабельності від пропонованих заходів.

Апробація результатів дослідження. Результати досліджень, викладені у кваліфікаційній роботі оприлюднені на V Всеукраїнській науково-практичній інтернет-конференції «Управління ресурсним забезпеченням господарської діяльності підприємств реального сектору економіки» (17 листопада 2021 р.) та на І Міжнародній науково-практичній конференції «Якість та безпечність продукції у внутрішній і зовнішній торгівлі й торговельне підприємництво: сучасні вектори розвитку і перспективи» (15 лютого 2022 р.)

Публікації. Результати досліджень було опубліковано в тезах:

1. Дячков Д. В., Шабатько Є.А. Стратегічні напрями актуалізації моделі системи управління інформаційною безпекою на підприємства агропродовольчої сфери.. *Матер. VI Всеукраїнської науково-практичної інтернет-конференції «Управління ресурсним забезпеченням господарської діяльності підприємств реального сектору економіки»,* (17 листопада 2021 р., м. Полтава). Полтава: РВВ ПДАУ, 2021. С. 217-219.

2. Дячков Д. В., Шабатько Є.А. Управління конкурентоспроможністю підприємств агросфери в умовах цифровізації продовольчих ринків. *Матер. І Міжнародної науково-практичної конференції (заочна форма) «Якість та безпечність продукції у внутрішній і зовнішній торгівлі й торговельне підприємництво: сучасні вектори розвитку і перспективи»,* (15 лютого 2022 р. м. Полтава). Полтава: ПДАУ, 2022. С. 77–81.

Структура та обсяг кваліфікаційної роботи. Робота складається із вступу, трьох розділів, висновків, списку використаних джерел, додатків. Загальний обсяг роботи складає 76 сторінок, містить 36 рисунків та 5 таблиць, 72 літературних джерела та 16 додатків.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ АГАРНИХ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВІЗАЦІЇ ПРОДОВОЛЬЧИХ РИНКІВ

1.1. Управління підприємствами агросфери в умовах цифровізації

Змінний характер економічної кон'юнктури все більше трансформується під впливом сучасних технологій, що висуває перший план необхідність аналізу чинників конкурентоспроможності та виявлення механізмів управління нею в умовах сучасної цифрової економіки як на рівні підприємств, так і на галузевому та загальнодержавному масштабах [**Ошибка! Источник ссылки не найден.**]. Конкурентоспроможність продукції в умовах цифрової економіці є динамічною здатністю підприємства здійснювати ефективну виробничо-господарську та торговельну діяльність на ринку [**Ошибка! Источник ссылки не найден.**]. Конкурентна перевага змушує підприємства агросфери адаптувати процес цифрової трансформації до бізнес-умов та споживчих переваг. А власне цифрова трансформація стає одним із основних механізмів забезпечення ефективності діяльності суб'єктів агропродовольчої сфери, оскільки цифрове перетворення є не тільки впровадженням нових технологій та продуктів, а й переосмислення бізнес-моделі, реінжинірингом бізнес-процесів та управлінням організаційними змінами [**Ошибка! Источник ссылки не найден.**].

Ключові зміни, які привносить цифрова трансформація в загальноекономічний простір та в агропродовольчу сферу зокрема, включають:

споживчий досвід щодо розширення традиційних методів маркетингу, наприклад: сегментація клієнтів з використанням передових інструментів та інформації, доступної в Інтернеті, знайомство з поведінкою споживачів та їх

уподобаннями через соціальні мережі, розвиток інтелектуального маркетингу, контекстної реклами, налаштувань додатків й цифрового самообслуговування;

бізнес-процеси щодо підвищення продуктивності, управління інтелектуальним капіталом, прийняття рішень на основі передової аналітики та даних;

бізнес-моделі в аспекті їх інформаційної трансформації, збільшення кількості повністю оцифрованих та цифрових бізнес-процесів виробництва й управління агропродовольчою діяльністю [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**].

Цифрова трансформація виробничих та управлінських технологій носить клієнтоорієнтований характер, тому що споживачі продукції, в даний час, стають основним драйвером цифровізації, оскільки очікують від підприємств постійного вдосконалення у частині прискорення та персоналізації взаємодії. Оптимізація бізнес-процесів підприємства в аспекті цифровізації може досягатися використанням таких інноваційних механізмів, як хмарні технології, використання великих даних, штучного інтелекту, віртуальної та доповненої реальності, а щодо ринкового позиціонування – трансформація стратегічних орієнтирів з урахуванням швидко мінливих умов середовища. Ключове стратегічне рішення щодо поведінки на ринку при трансформації цифрового бізнесу, полягає в тому, яку стратегію вибрати: наступальну або захисну, або ж поєднувати обидва напрями конкурентної боротьби [**Ошибка! Источник ссылки не найден.**].

У цифровій економіці мета та місія суб'єкту господарювання визначається на основі інноваційних елементів (рис.1.1). Щоб бути конкурентоспроможними у цифровій економіці, суб'єктам господарювання агропродовольчої сфери потрібно більше, ніж традиційні бізнес-моделі. Корпоративна стратегія має передбачати застосування цифрових технологій, а не розглядати їх як доповнення до бізнесу, що потребує окремої стратегії [**Ошибка! Источник ссылки не найден.**]. Цифровізація

технологічних, економічних та управлінських процесів на кожному окремому сільськогосподарському підприємстві поступово впливає на загальний розвиток цифрових активів сільського господарства нашої держави. Наявні цифрові активи сільськогосподарських підприємств дозволяють миттєво реагувати на нові виклики аграрного ринку та постійно розвивати к і впро значно посилює ентній боротьбі

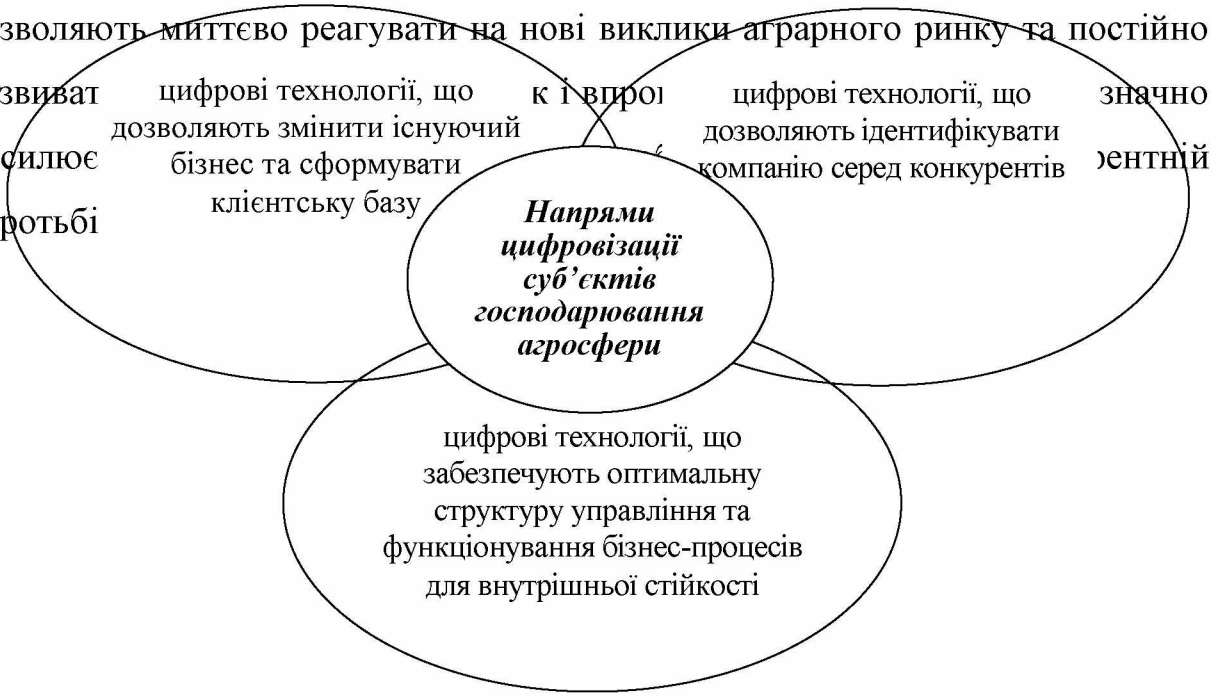

Рис. 1.1. Інноваційні напрями формування мети й місії суб'єкту господарювання агросфери в умовах цифровізації економіки [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**]

Сільськогосподарське виробництво та інша діяльність в агропродовольчій сфері загалом, мають свої специфічні особливості, які визначають застосування цифрових технологій (рис. 1.2).

Основними аргументами на підтримку цифровізації сільськогосподарського виробництва є необхідність вирішення наступних

проблемних завдань: збільшення кількості та якості врожаю, мінімізація фінансових вкладень, зниження трудомісткості та підвищення продуктивності сільськогосподарського виробництва, зменшення шкідливого впливу на довкілля, зниження залежності від людського фактору в сільському господарстві та девіації щодо врожайності, тощо [**Ошибка! Источник ссылки не найден.**].

Водночас, ключовим завданням цифрової трансформації сільського господарства є отримання релевантної інформації з великих даних про внутрішнє й зовнішнє середовище, основою для чого є хмарні платформи та рішення у галузі обробки великих даних, а також технології передиктивної аналітики та системи підтримки прийняття рішень. До кінця 2020 р. у світі налічувалося вже 75 млн сільськогосподарських пристроїв Інтернету речей, а до 2050 р. середня ферма генеруватиме 4,1 млн од. даних (data point) на день [**Ошибка! Источник ссылки не найден.**]. Здешевлення та підвищення точності сенсорного обладнання (польові датчики, датчики контролю стану виробничих приміщень, сільгоспобладнання та техніки, датчики контролю стану та здоров'я худоби та ніші прилади й технології) дозволяють значній кількості сільгосппідприємств перейти до безперервного збору та аналізу інформації, а в подальшому, інтегрувати три основні рівні моніторингу

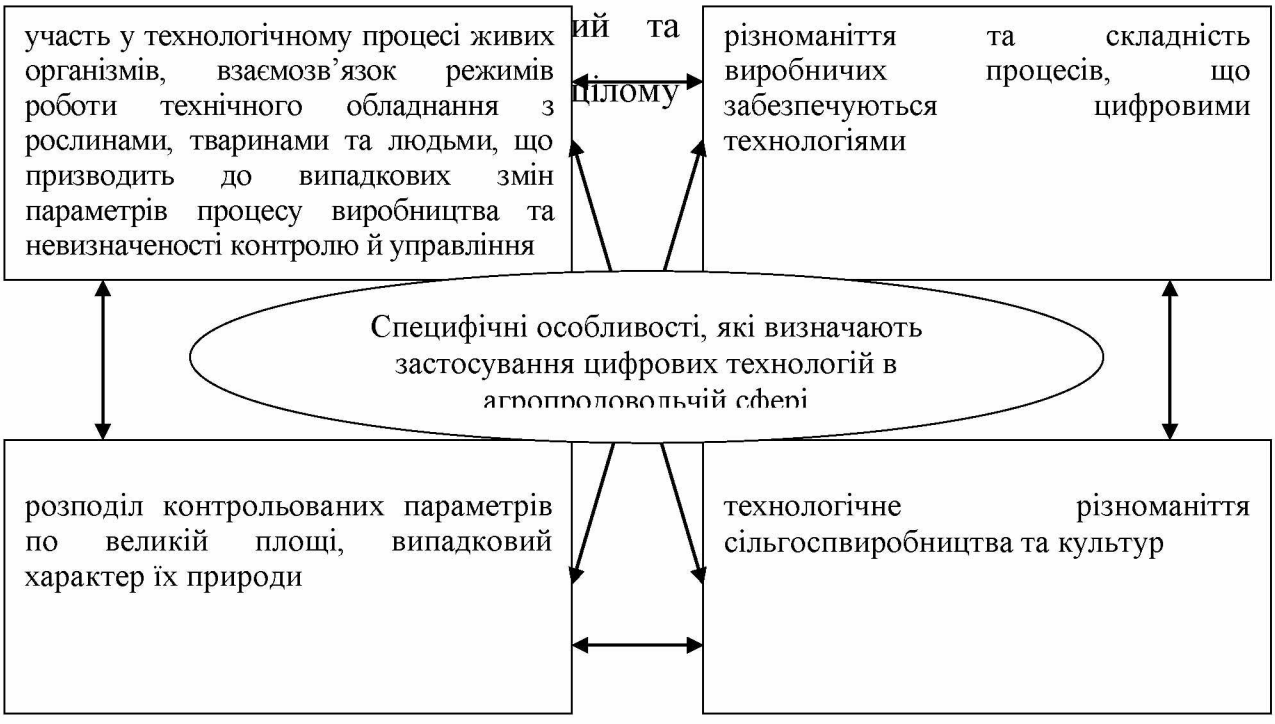

Рис. 1.2. Специфічні особливості, які визначають застосування цифрових технологій в агропродовольчій сфері [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**]

Потужними технологіями, що дозволяють здійснити перехід до цифрових систем землеробства є дистанційне зондування землі за допомогою супутникових систем для формування електронних карт полів та застосування БПЛА з мультиспектральними камерами для віддаленого моніторингу стану навколишнього середовища, ґрунту, екологічної ситуації, зростання сільськогосподарських культур, визначення вегетаційного індексу, ранньої діагностики захворювань рослин, управління іригацією тощо [**Ошибка! Источник ссылки не найден.**].

Драйвером цифровізації сільського господарства є досягнення у галузі робототехніки, які призводять до поширення автономних роботизованих систем, розумних теплиць та розумних ферм. Набирає обертів використання безпілотного транспорту при обробці та обробітку земель сільськогосподарського призначення.

Роботизовані комплекси, технології Інтернету речей, а також інтелектуальні системи на основі аналізу великих даних використовуються і в тваринництві для управління життєвим циклом тварин, безперервного моніторингу стану здоров'я, коригування відгодівлі та догляду.

Важливою тенденцією цифрової трансформації сільського господарства у світі є поширення серед малих сільгоспвиробників цифрових платформ та віртуальних помічників для управління фермерськими господарствами. Дані рішення надають фермерам рекомендації та практичні поради щодо планування робіт, вибору культур, економічної доцільності виробництва, а також щодо ведення бухгалтерського обліку та управління

фінансами.

Цифрові рішення також застосовуються і в логістиці та продажах сільськогосподарської продукції та включають системи простежуваності та контролю якості сільськогосподарської продукції, смартконтракти, а також маркетплейси для просування на ринок та збуту сільськогосподарської продукції підприємствами агропродовольчої сфери.

Цифрова трансформація сільського господарства спрямована на подолання низки глобальних викликів, таких як:

збільшення потреби у продовольстві (на 60 % до 2050 р.) внаслідок зростання чисельності населення та підвищення якості життя [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**];

виснаження продуктивних сільськогосподарських земель, зростання екологічного навантаження (70 % споживання водних ресурсів та 30 % викидів вуглекислого газу в даний час припадають на світове сільське господарство) та скорочення площ, придатних для ведення сільського господарства;

зміна агрокліматичних умов та зростання частоти природних катаклізмів, що підвищують волатильність на сільськогосподарських ринках;

трансформація споживчих переваг та розвиток моделі стійкого та екологічного споживання. Комплексне застосування технологій точного землеробства здатне забезпечити приріст урожайності на 70 % [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**].

Оперативне реагування на зміну зовнішніх умов та одночасне коригування параметрів роботи устаткування дозволяють скоротити витрати на насіннєвий матеріал, добрива й паливо, знизити тимчасові витрати на польові роботи. Технології аналітики великих даних здатні підвищити ефективність процесів селекції та розробки нових ефективних кормів та добрив, забезпечувати прогнозування врожайності та вибір оптимальної стратегії вирощування сільськогосподарських культур [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**].

Застосування безпілотної техніки суттєво знижує витрати на виконання окремих видів робіт. Наприклад, використання БПЛА для посадки насіння здатне знизити витрати на цю операцію на 85 % [**Ошибка! Источник ссылки не найден.**].

За оцінками американської асоціації фермерів, скорочення витрат унаслідок роботизації сільськогосподарських операцій досягне 40 % [**Ошибка! Источник ссылки не найден.**]. Зростає при цьому і продуктивність праці – так, одна роботизована система збирання врожаю здатна замінити 30 працівників ферми. Завдяки цифровізації у споживачів та контролюючих органів з'явиться можливість повністю простежувати походження продукції [**Ошибка! Источник ссылки не найден.**], що підвищить її безпеку та стане додатковим фактором розвитку споживчої культури.

Цифрові технології сприятимуть зниженню екологічного навантаження на сільське господарство, підвищенню ефективності використання природних ресурсів, зростанню стійкості до несприятливих агрокліматичних явищ [**Ошибка! Источник ссылки не найден.**].

Отже, цифровізація агропродовольої сфери дозволяє досягти низки непрямих та соціальних ефектів, включаючи зниження диспропорцій якості життя між містом та селом, забезпечення економічної та соціальної інтеграції дрібних сільгоспвиробників у продовольчі системи та ланцюжки поставок (у тому числі за рахунок різних маркетплейсів), надання сільським мешканцям інструментів підвищення цифрової грамотності та розширення набору компетенцій. В нашій країні потреба у цифровій трансформації галузі викликана насамперед низькою продуктивністю праці, технологічним відставанням від країн-конкурентів та необхідністю розвивати глибоку переробку сільськогосподарської продукції для нарощування та підвищення якості експорту.

Для досягнення цілей суб'єктів діяльності агропродовольчої сфери в умовах цифровізації продовольчих ринків передбачається вирішення

наступних завданнь:

створення цифрових методів, технологій, технічних засобів, які забезпечать моніторинг полів, збирання цифрових даних про рослини, тварин та корисних мікроорганізмів, цифрових методів складання та оновлення ґрунтових карт, методів актуалізації та використання селекційного та генетичного матеріалу;

впровадження цифрових інструментів для використання інформаційних ресурсів, платформ та технологій на агрооб'єктах, що підвищують ефективність сільськогосподарського виробництва;

створення технологій та технічних засобів для автоматизації, роботизації та інтелектуального сільськогосподарського виробництва;

розробка спеціалізованого програмного забезпечення для сільськогосподарських платформ та управління «розумним сільським господарством»;

забезпечення учасників сільгоспвиробництва системою управління та діагностики сільгосптехніки та засобів об'єктивного контролю, інструментами планування та управління виробництвом з елементами bigdata та штучного інтелекту;

створення технологій, що спростять процес документообігу між державними структурами, суб'єктами агропродовольчої сфери, фермерами, споживачами сільгосппродукції;

використання фінансово-регуляторних інструментів контролю сезонних спадів та інструментів управління логістикою та транспортом;

розвиток спеціалізованої аграрної освіти для цифрового сільського господарства;

підвищення конкурентоспроможності експортної сільгосппродукції, зокрема у сфері стандартизації;

впровадження технологій Інтернет-речей, блокчейн тощо для всього набору сільськогосподарської техніки, наземних, водних та повітряних, стаціонарних й нестаціонарних об'єктів;

розробка ефективної цифрової системи планування внесення добрив та хімікатів, з урахуванням актуальної ґрунтової та метеорологічної інформації;

забезпечення високошвидкісного зв'язку для сільських територій, стандартизація форматів та протоколу обміну даними між інформаційними системами управління [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**].

Тільки з урахуванням вищезгаданих аспектів цифровізація може у повному обсязі відповідати покладеним на неї очікуванням. Завдяки незалежним науковим дослідженням у цій галузі накопичені знання можуть надати сприяння оптимальній адаптації та водночас досягненню цілей.

Разом із конкурентними перевагами, які надає цифровізація сільськогосподарського виробництва та управління виробничо-господарськими процесами суб'єктами агропродовольчої сфери, вона привносить у їх діяльність і окремі ризики, які в першу чергу пов'язані з цифровою та інформаційною безпекою їх діяльності. Тому наступним питанням дослідженнях є визначення особливостей забезпечення інформаційної безпеки на підприємствах агросфери.

1.2. Особливості забезпечення інформаційної безпеки на підприємствах агропродовольчої сфери

В загальному вираженні термін «інформаційна безпека» передбачає стан захищеності даних від трьох основних ризиків: порушення конфіденційності, зміни, відсутності доступності. Проте, стосовно виробничого підприємства зазначена тріада змінюється, оскільки у виробничому процесі інформація відіграє не тільки роль активу, а й інструменту управління. Ризики за даних обставин змінюються, інформаційні потоки повинні забезпечити безперервність й безаварійність процесу виробництва, що обумовлює особливий підхід до організації системи інформаційної безпеки підприємства. Ключовими особливостями такої

системи інформаційної безпеки є:

значна кількість споживачів інформації різних типів як користувачів, так і пристроїв, при цьому вона передається по безлічі каналів та у великій кількості форматів;

крім комп'ютерів та елементів інфраструктури, об'єктами управління є напрями діяльності, ресурси, в тому числі інформаційні та цифрові, технології, бізнес-процеси, підрозділи тощо;

система інформаційної безпеки є розподіленою, оскільки її елементи можуть бути фізично важкодоступними, інформація передається по безлічі каналам зв'язку.

Значні теоретичні наопрацювання зазначеної проблематики формують багатоманітність та різносторонність трактування сутності інформаційної безпеки (рис. 1.3).

Якщо розглядати етимологію поняття інформаційної безпеки у правовому полі, то її визначено у ряді нормативно-правових актів, зокрема і у Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 рр.», який розглядає її як: «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» [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**].

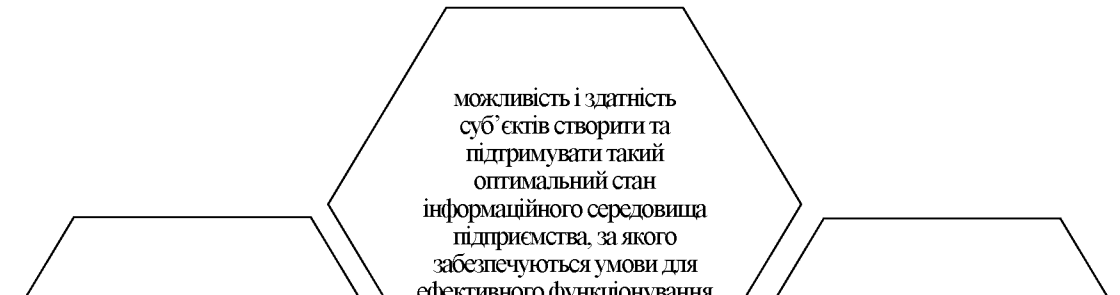

Рис. 1.3. Сутність поняття інформаційної безпеки підприємства [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**;

Ошибка! Источник ссылки не найден.]

Аналіз розглянутих підходів до трактування поняття «інформаційної безпеки» (додаток А) дозволив охарактеризувати основні її ключові положення (рис. 1.4).

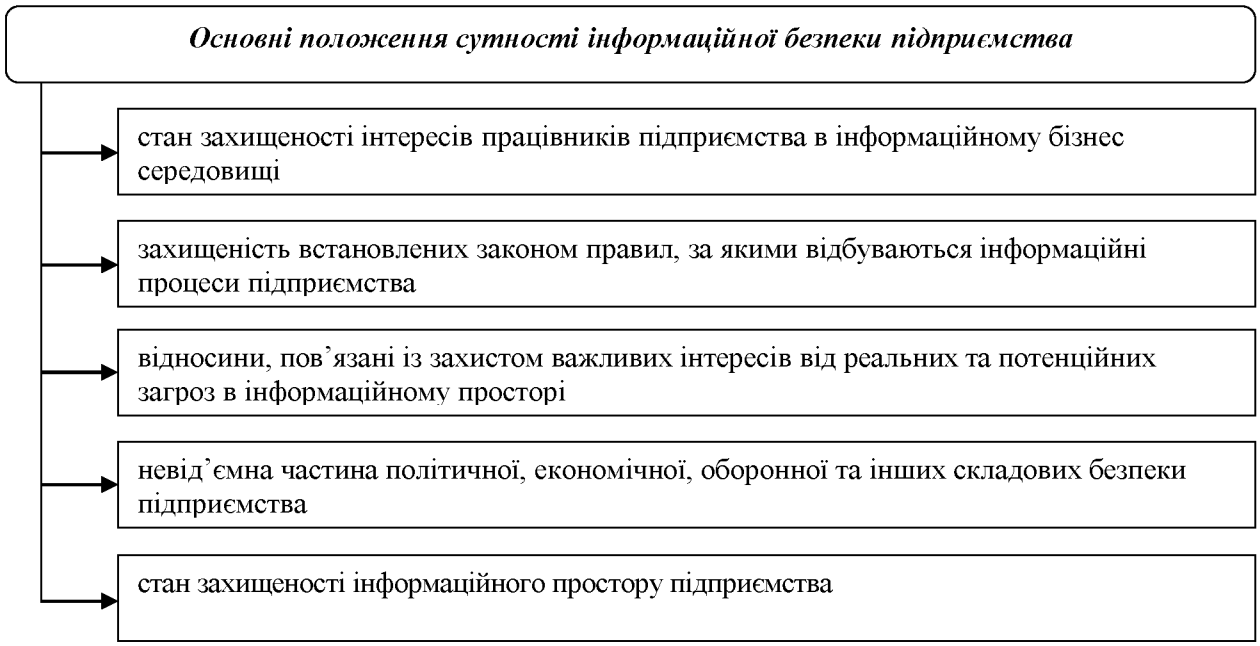

Рис. 1.4. Основні положення щодо визначення сутності інформаційної безпеки підприємства [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**]

Відтак, забезпечення інформаційної безпеки в загальній постановці проблеми може бути досягнуте лише при взаємопов'язаному розв'язку трьох складових, що представлені на рис.1.5.

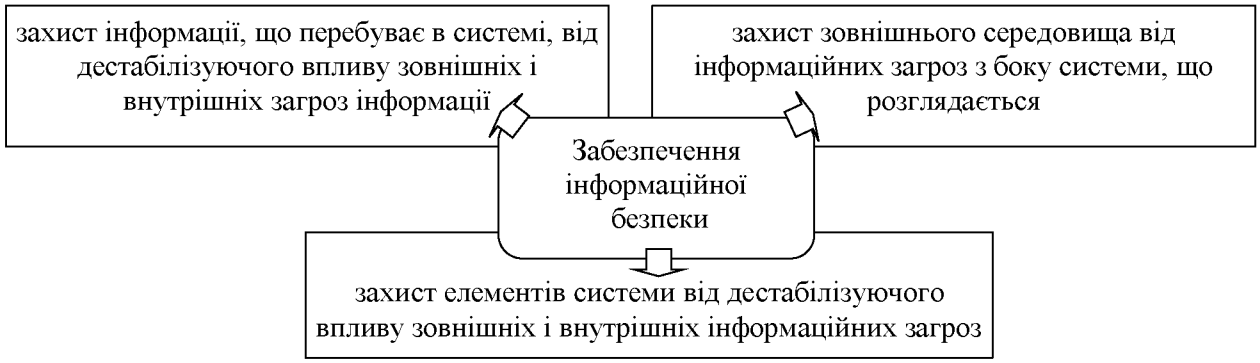

Рис. 1.5. Складові забезпечення інформаційної безпеки підприємства [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник**

ссылки не найден.; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**]

Забезпечення інформаційної безпеки на підприємствах агропродовольчої сфери переважно здійснюється за загальним сценарієм формування системи інформаційного захисту на будь-якому підприємстві, організації, установі, проте має деякі особливості. Для ефективної діяльності системи інформаційної безпеки підприємства агропродовольчої сфери безумовно необхідне визначення її основних функцій, основними з яких повинні стати: захист інформації організації, висвітлення ситуації всередині і поза межами підприємства, вчасне одержання інформації про важливі для підприємства процеси і знаходження засобів її оптимального використання. Розглядаючи зміст процесу забезпечення інформаційної складової безпеки підприємства агропродовольчої сфери, необхідно узагальнити такі основні функції інформаційної безпеки, належне виконання яких необхідне для досягнення належного рівня забезпечення інформаційної складової її економічної безпеки (рис. 1.6).

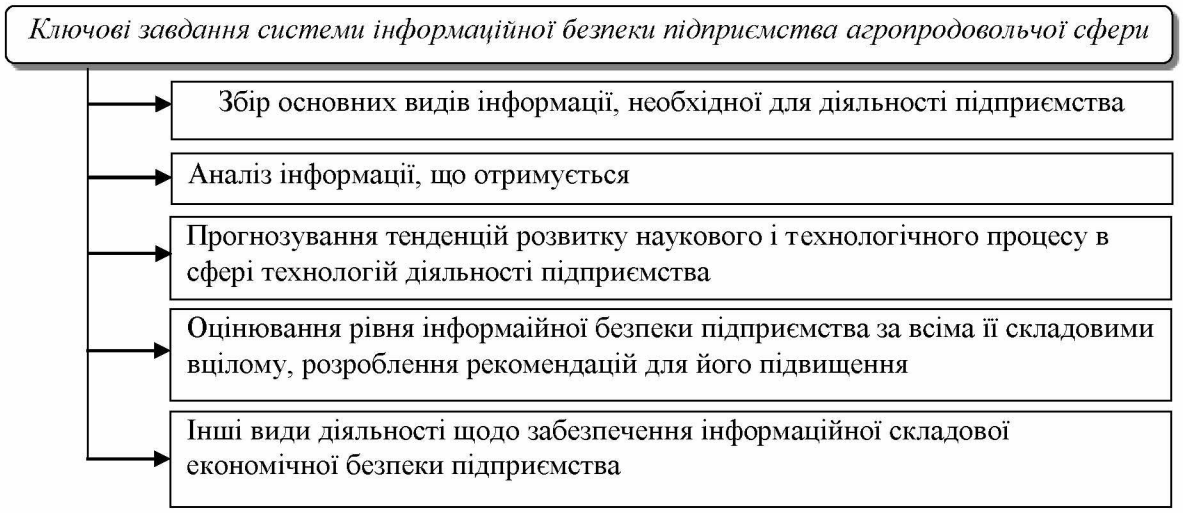

Рис. 1.6. Типові рішення системи інформаційної безпеки підприємства агропродовольчої сфери [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник**

ссылки не найден.; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**]

До об'єктів інформаційної безпеки сільськогосподарських підприємств доцільно віднести:

інформаційні ресурси, які містять відомості комерційної таємниці, конфіденційну інформацію, представлену у вигляді інформаційних баз або банків даних, цифрові об'єкти, які носять комерційну інформацію;

інфраструктуру, технології, системи інформаційної дії на підприємстві, засоби інформатизації виробничих та управлінських процесів, мережі, загальносистемне й прикладне програмне забезпечення, автоматизовані системи, системи комунікацій та передачі інформації, тощо [**Ошибка! Источник ссылки не найден.**].

Основні загрози інформаційної безпеки підприємств агропродовольчої сфери відображені на рис. 1.7.

Рис. 1.7. Основні загрози інформаційної безпеки підприємств

агропродовольчої сфери [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**]

Узагальнюючи дані, слід відмітити, що основними засобами реалізації загрози розкриття конфіденційної інформації на підприємствах агропродовольчої сфери можуть стати: розголошення конфіденційної інформації, прослуховування комунікаційних каналів або ж несанкціонований доступ до баз даних. Реалізація зазначених загроз інформаційної безпеки є наслідком однієї із зазначених дій: розголошення конфіденційної інформації, втрата конфіденційної інформації та недозволений доступ до інформації, яка підлягає захисту. У разі розголошення інформаційні або втрати інформаційних ресурсів переважно спостерігається порушення конфіденційності інформації з обмеженим доступом (рис. 1.8).

До причин та чинників, які формують передумови до втрати інформаційних ресурсів на підприємствах агропродовольчої сфери, можуть належати:

недостатнє знання працівниками правил захисту конфіденційної інформації та нерозуміння необхідності їх ретельного дотримання;

використання не атестованих технічних засобів обробки конфіденційної інформації;

слабкий контроль над дотриманням правил захисту інформації правовими організаційними та інженерно-технічними заходами [**Ошибка! Источник ссылки не найден.**].

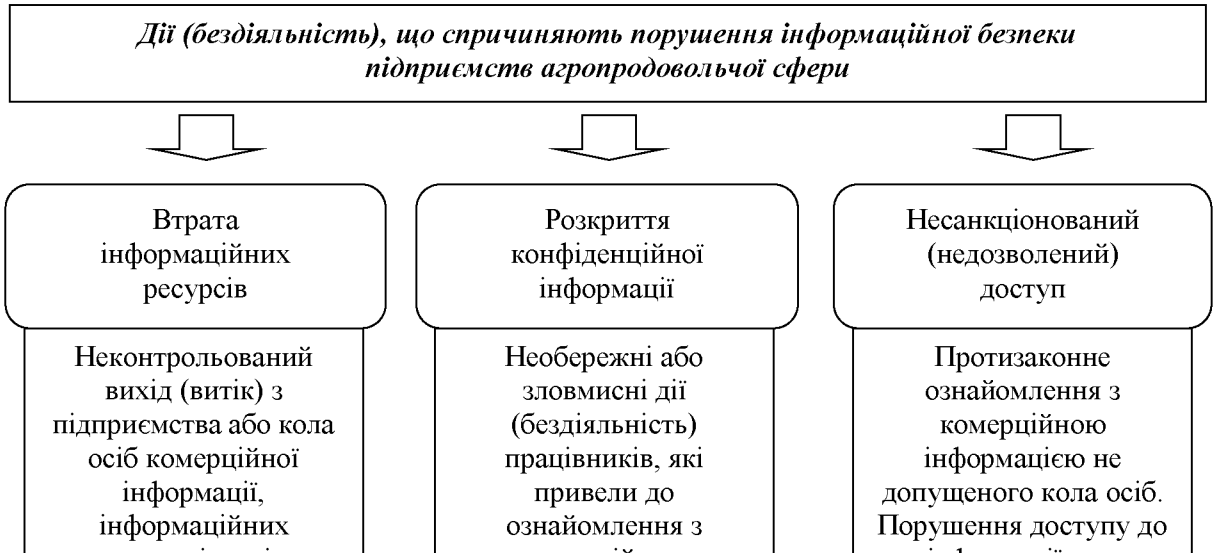

Рис. 1.8. Дії (бездіяльність), що спричиняють порушення інформаційної безпеки на підприємствах агропродовольчої сфери [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**]

Якщо розглядати відсоткове співвідношення вищезазначених причин порушення інформаційної безпеки протягом останніх років, то воно виглядатиме як відображено на рис. 1.9.

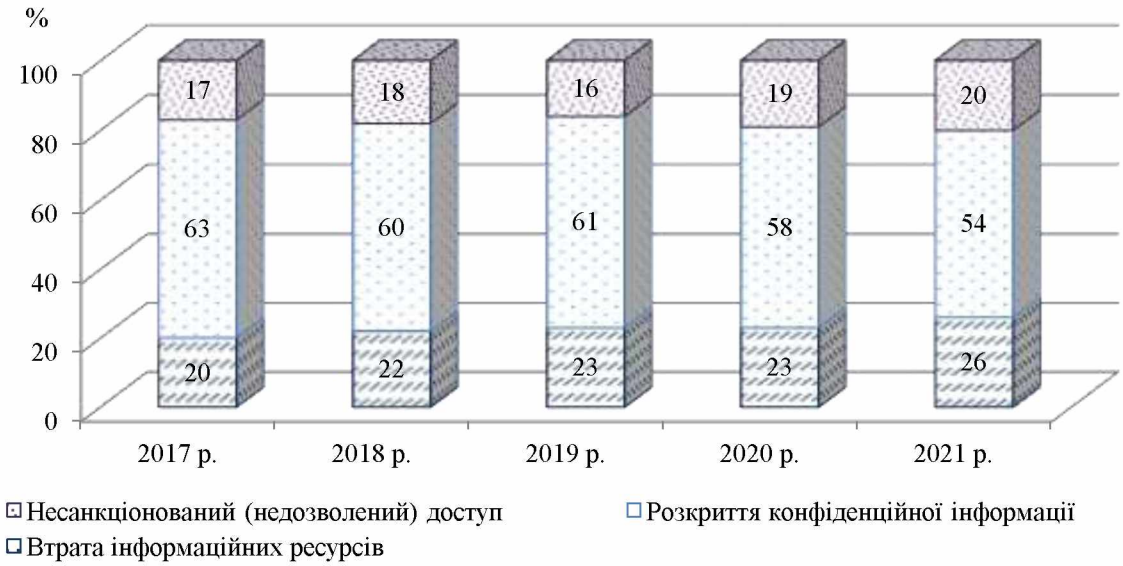

Рис. 1.9. Динаміка відсоткового вираження причин порушення інформаційної безпеки на підприємствах агропродовольчої сфери [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**]

Відтак, розголошення комерційної таємниці, або розповсюдження інформаційних ресурсів, які підлягають захисту на підприємствах

агропродовольчої сфери є головною причиною порушення інформаційного захисту – 54-63 % протягом 2017-20121 рр. Позитивною тенденцією є зменшення частки даної причини витоку інформації.

Втрата інформаційних ресурсів є другою за величиною причиною порушення інформаційної безпеки на арго підприємстві, який пов'язаний із неефективністю технічних, апаратних програмних та комунікаційних засобів системи інформаційного захисту на підприємствах агросфери.

Несанкціонований (недозволений) доступ – третій за значенням поширений вид інформаційних загроз, який полягає в отриманні користувачем доступу до об’єкта, на який у нього немає дозволу відповідно до прийнятої в організації політикою інформаційної безпеки. За характером впливу недозволений доступ є активним впливом, що використовує помилки системи.

Важливе значення для забезпечення ефективного функціонування сучасного підприємства також відіграє спосіб формування та функціонування системи інформаційної безпеки, функції, які вона виконує, методи, що застосовуються. Вищезазначене обумовлює доцільність дослідження особливостей організації інформаційної безпеки підприємства в умовах бізнес-середовища.

Висновки до розділу 1:

Здійснивши аналіз теоретичних аспектів управління інформаційною безпекою агарних підприємств в умовах цифровізації продовольчих ринків доцільно відзначити:

1. Основними аргументами на підтримку цифровізації сільськогосподарського виробництва є необхідність вирішення наступних проблемних завдань: збільшення кількості та якості врожаю, мінімізація фінансових вкладень, зниження трудомісткості та підвищення

продуктивності сільськогосподарського виробництва, зменшення шкідливого впливу на довкілля, зниження залежності від людського фактору в сільському господарстві та девіації щодо врожайності, тощо

Цифрова трансформація сільського господарства спрямована на подолання низки глобальних викликів, таких як: збільшення потреби у продовольстві, виснаження продуктивних сільськогосподарських земель, зростання екологічного навантаження, зміна агрокліматичних умов та зростання частоти природних катаклізмів, що підвищують волатильність на сільськогосподарських ринках, трансформація споживчих переваг та розвиток моделі стійкого та екологічного споживання.

2. Аналіз підходів до трактування поняття «інформаційної безпеки» дозволив охарактеризувати основні її ключові положення: стан захищеності інтересів працівників підприємства в інформаційному бізнес середовищі, захищеність встановлених законом правил, за якими відбуваються інформаційні процеси підприємства, відносини, пов'язані із захистом важливих інтересів від реальних та потенційних загроз в інформаційному просторі, невід'ємна частина політичної, економічної, оборонної та інших складових безпеки підприємства, стан захищеності інформаційного простору підприємства. Забезпечення інформаційної безпеки на підприємствах агропродовольчої сфери переважно здійснюється за загальним сценарієм формування системи інформаційного захисту на будь-якому підприємстві, організації, установі, проте має деякі особливості. Для ефективної діяльності системи інформаційної безпеки підприємства агропродовольчої сфери безумовно необхідне визначення її основних функцій, основними з яких повинні стати: захист інформації організації, висвітлення ситуації всередині і поза межами підприємства, вчасне одержання інформації про важливі для підприємства процеси і знаходження засобів її оптимального використання.

РОЗДІЛ 2
АНАЛІЗ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

«НАЗВА ПІДПРИЄМСТВА»

2.1. Організаційно-економічна характеристика «Назва підприємства»

Об'єктом дослідження, на базі якого пропонується здійснювати аналіз інформаційної безпеки є підприємство Назва підприємства», яке створене у 2007 р. та розташоване в селі ххххххххххх хххххххххххх області, хххххххххххххх районі.

Предметом діяльності підприємства є виробництво продукції рослинництва та реалізація сільськогосподарських культур

Регламентуючим документом діяльності підприємства є Статут, а саме підприємство створене і діє на підставі Законів України «Про підприємництво», «Про власність», Господарського кодексу України та інших законодавчих актів.

З метою здійснення господарської діяльності підприємство використовує власне та надане у користування або розпорядження майно. Відтак, у власності «Назва підприємства» перебуває: майно передане йому засновником та учасниками; продукція, яка вироблена в результаті здійснення виробничо-господарської діяльності; одержані доходи та прибутки від діяльності; інше майно, яке набуте на підставах, не заборонених законом.

Досліджуване підприємство самостійно вирішує питання, які стосуються ведення виробничої та управлінської діяльності, зокрема ресурсного забезпечення, кадрового забезпечення, інформаційного забезпечення, технології виробництва, маркетингу, логістики та збуту продукції, соціального розвитку, матеріального стимулювання робітників тощо.

Господарська діяльність підприємства здійснюється на основі господарського розрахунку, забезпечення самоокупності, фінансування

витрат на удосконалення виробництва, а основним видом діяльності «Назва підприємства» є вирощування зернових та бобових культур, та збут сільськогосподарської продукції. Відповідно, важливим аспектом, аналізу діяльності підприємства є характеристика динаміки структури виробництва продукції, та розрахунок коефіцієнту спеціалізації (табл. 2.1).

Таблиця 2.1

Склад та структура виробництва сільськогосподарської продукції «Назва підприємства» ххххххххххххххххххххх району, 2016-2020 рр.

Види продукції	Вартість продукції, тис. грн					Вартість за 5 роки, тис. грн	Питома вага, %	Місце за питомою вагою
	Роки							
	2016	2017	2018	2019	2020			
Пшениця озима	2008,6	1767,4	2173,4	2128,0	0	8077,4	3,2	5
Кукурудза на зерно	16543,5	25959,4	28377,3	37343,1	51836,6	160060,0	63,3	1
Ячмінь озимий	589,5	626,1	0	300,0	0	1515,6	0,6	6
Ячмінь ярий	76,8	0	0	0	0	76,8	0,0	-
Сорго	63,4	0	0	0	0	63,4	0,0	-
Інші зернові та зернобобові	98,0	0	0	0	0	98,0	0,0	-
Культури зернобобові сушені	0	1030,2	0	0	0	1030,2	0,4	7
Соняшник	2973,4	11042,3	9096,9	7516,1	14709,0	45337,7	17,9	2
Соя	627,8	5657,7	7673,1	5426,2	5907,7	25292,5	10,0	3
Ріпак озимий	3420,9	3175,5	1262,3	3576,2	0	11434,9	4,5	4
Разом по рослинництву	26401,9	49258,6	48583,0	56289,6	72453,3	252986,0	100,0	х
Всього по господарству	26401,9	49258,6	48583,0	56289,6	72453,3	252986,0	100,0	х

Коефіцієнт спеціалізації «Назва підприємства» протягом останніх п’яти років становить: Кспец=100/(63,3+17,9*3+10,0*5+4,5*7+3,2*9+0,6*11+ +0,4*13)=100/(63,3+ +53,7+50,0+31,5+28,8+6,6+5,2)=41,8.

Як і зазначалось, досліджуване підприємство спеціалізується у сфері рослинництва та не здійснює виготовлення й переробки продуктів тваринництва загалом. Спеціалізується перш за все на вирощуванні кукурудзи на зерно, яка займає провідне місце в структурі виробництва продукції – 63,3 % питомої ваги; соняшнику, який займає друге місце зі

значенням – 17,9 % питомої ваги в загальній структурі; та сої, яка займає третє місце і її питома вага в структурі становить – 10,0 %. Доцільно зазначити, що в звітному році підприємство здійснювало вирощування лише зазначених культур та відмовилось від багатьох культур, які були присутні в структурі виробництва протягом 2016-2019 рр.: пшениця озима, ячмінь озимий, ріпак озимий та інші. Рівень спеціалізації зі значенням 0,41 стверджує про достатньо поглиблений рівень спеціалізації діяльності підприємства, що і свідчить постійне звуження керівництвом асортименту продукції. Зазначені тенденції в спеціалізації означають наміри мінімізувати ринкові та підприємницькі ризики, з одночасним підвищенням рівня конкурентоспроможності підприємства.

Вирощування продукції залежить від головного ресурсу кожного сільськогосподарського підприємства – земельного фонду, його структури та ступеня використання земель в різних бізнес-процесах. Тому здійснено аналіз земельних ресурсів «Назва підприємства»за 2016-2020 рр. (рис. 2.1, додаток Б), на основі звітів про основні економічні показники роботи сільськогосподарського підприємства (додаток В).

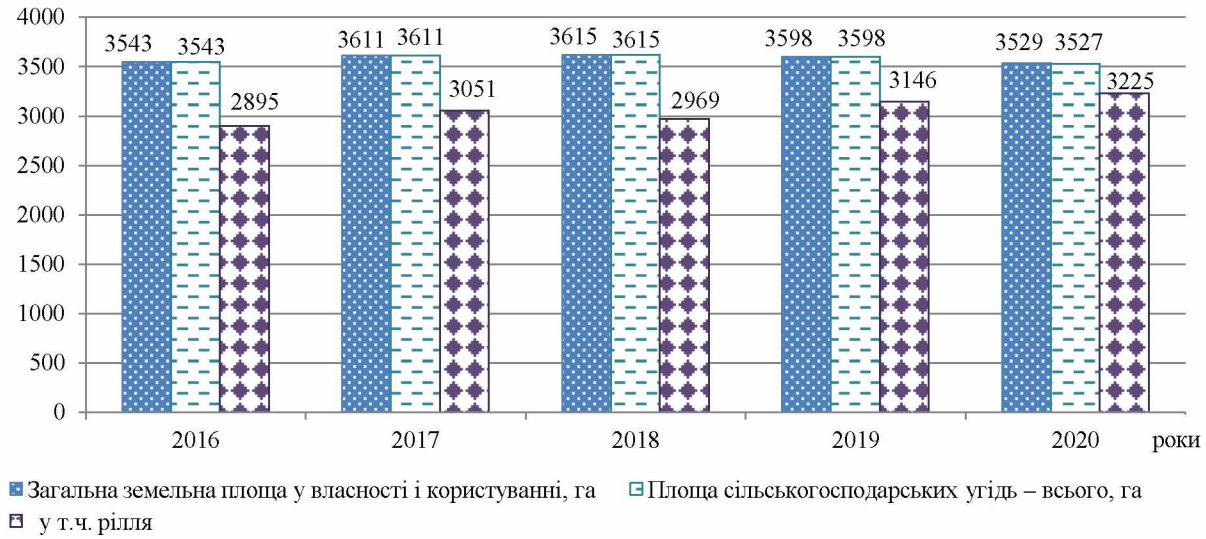

Рис. 2.1. Динаміка складу й структури земельного фонду «Назва підприємства» ххххххххххххххххххххх району, 2016-2020 рр

Відповідно до розрахованих даних, загальна земельна, власна та орендована, площа підприємства складає у звітному році 3529 га, що на 14 га

менше у порівняні з 2016 р. або ж на 0,4 %. Площа земель, які виділені під виробництво продукції підприємства становлять 3527 га у 2020 р., що складає 99,9 % питомої ваги від загальної площі підприємства. В минулі роки, цей показник становив 100,0 %. Слід відзначити, що площа земель виділених під вирощування продукції рослинництва зменшилась у звітному році відносно базового на 16 га., тобто на 0,45 %. Площа земель, які становлять рілля у звітному році складає 3225 га (91,39 % від загальної площі), що на 330 га більше ніж у 2016 р., що становить темп зростання у 11,4 %.

Наступним за значенням ресурсом для аграрного підприємства є засоби виробництва, наявність, структура та ефективність використання яких визначають результативність економічної, соціальної та продовольчої складової діяльності. Відтак, наступним етапом організаційно-економічної характеристики діяльності досліджуваного підприємства стане аналіз його структури активів за 2016-2020 рр. (рис. 2.2., додаток Г), на основі балансів підприємства за відповідний період (додаток Д).

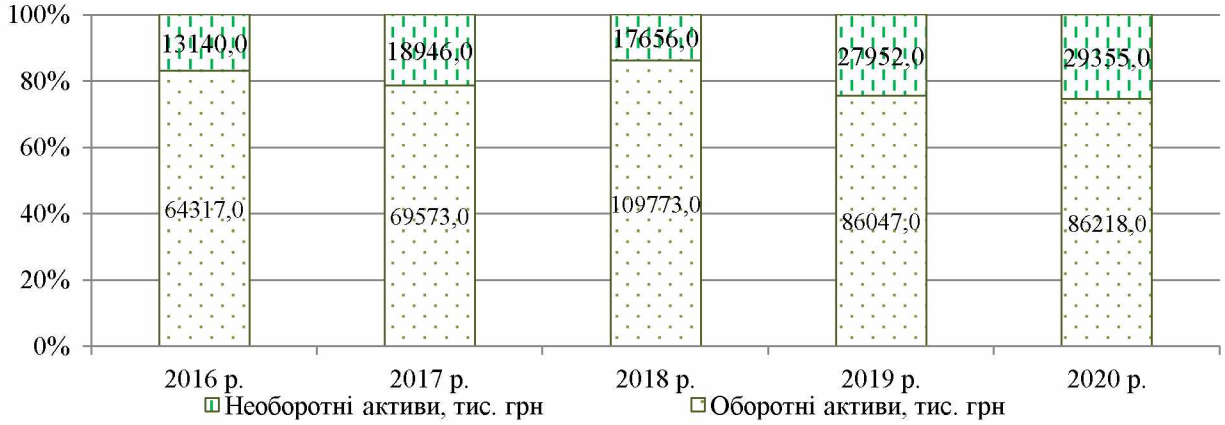

Рис. 2.2. Динаміка структури активів «Назва підприємства» ххххххххххххххххххххх району у 2016-2020 рр.

Основу активів підприємства становлять оборотні активи 2020 р. – 74,6 % в загальній структурі, що в кількісному вираженні становить 86218,0 тис. грн та на 21901,0 тис. грн більше ніж у 2016 р. Проте, слід зазначити, що питома вага цієї категорії активів у базовому році становила 83,0 %, що на 5,4 % більше. Зниження питомої ваги оборотних активів є негативною тенденцією в

діяльності підприємства. Якщо ж розглядати структуру цієї категорії активів, то її основу складають дебіторська заборгованість та запаси.

Необоротні активи становлять 17,0 % у 2016 р. та 25,4 % у 2020 р., що складає приріс у питомій вазі на 8,4 %. Загалом, для підприємства, яке здійснює виробництво та реалізацію сільськогосподарської продукції таке співвідношення активів є оптимальним.

Якщо розглядати окремо структуру необоротних активів (рис. 2.3, додаток Е), то слід відмітити зростання їх середньорічної вартості, особливо основних засобів (які є основою цієї категорії активів) у 2,1 рази протягом аналізованого періоду. Така тенденція свідчить про орієнтацію підприємства на технічну та технологічну переозброєність, що є позитивним стратегічним аспектом діяльності. Поряд спостерігається і значний рівень зносу основних засобів, який становить 22540,0 тис. грн у 2020 р. та зростає у порівняні зі значенням 2016 р. (9216,0 тис. грн) в 2,4 рази. Тобто спостерігається прискорений рівень зносу основних засобів «Назва підприємства».

Рис. 2.3. Динаміка структури необоротних активів «Назва підприємства» ххххххххххххххххххххх району у 2016-2020 рр.

Доцільно зазначити, що все ж таки основою активів «Назва підприємства» є оборотні активи, тому їх аналіз (рис. 2.4, додаток Ж) є важливіший.

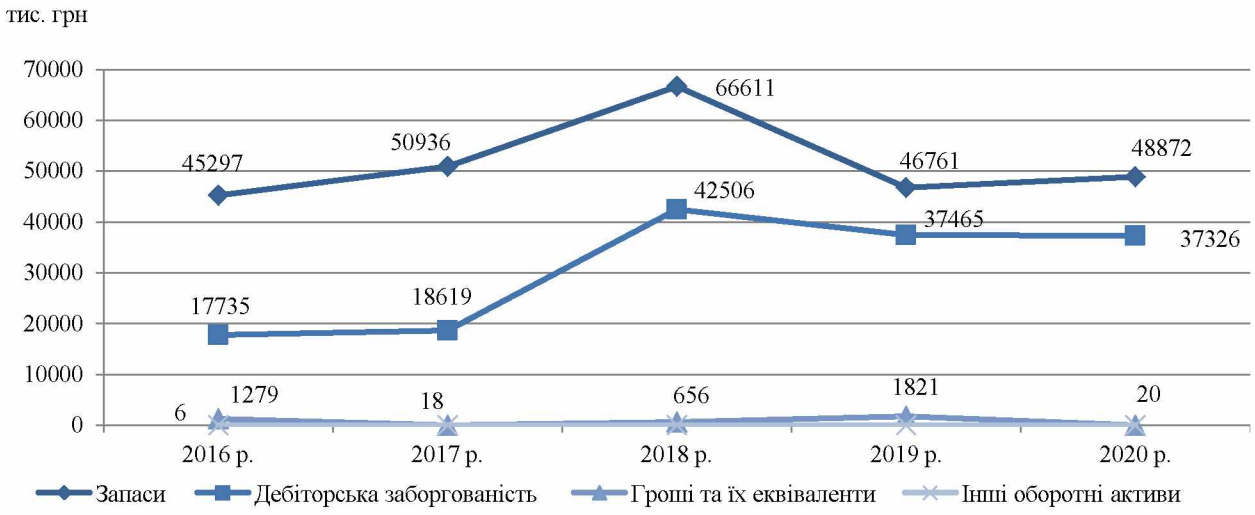

Рис. 2.4. Динаміка структури оборотних активів «Назва підприємства» ххххххххххххххххххххх району у 2016-2020 рр.

Доцільно відмітити значну питому вагу серед оборотних активів становлять:

запаси – 56,7 % у 2020 р. порівняно з 70,4 % у 2016 р., тобто їх частка зменшилась на 13,7 % протягом аналізованого періоду. Більшість запасів, а саме 24,3 % у звітному періоді це готова продукція, питома вага якої зменшується на 25,8 % порівняно з базовим роком. Водночас, значну частину запасів у 2020 р. становить незавершене виробництво – 17,2 %, що на 5,5 % більше ніж у 2016 р.;

дебіторська заборгованість, питома вага якої складає у 2020 р. – 43,3 %, що на 15,7 % більше ніж у 2016 р. (27,6 %). Звичайно це є негативною тенденцією функціональної фінансової стратегії, оскільки зростання дебіторської заборгованості призводить до зростання фінансових, а згодом і підприємницьких ризиків;

гроші та їх еквіваленти – 20 тис. грн у 2020 р., що у 64 рази менше порівняно з 2016 р. Найбільше їх значення спостерігалося у 2019 р. – 1821 тис. грн (2,1 %).

Наступним видом ресурсу агарного підприємства, який доцільно розглянути та проаналізувати є фінансовий ресурс «Назва підприємства», оскільки власне він забезпечує накопичення та підтримку функціонування

інших видів ресурсів підприємства. Аналіз наведений у додатку И, а динаміку зміни власних і позичкових фінансових ресурсів відображено на рис. 2.5.

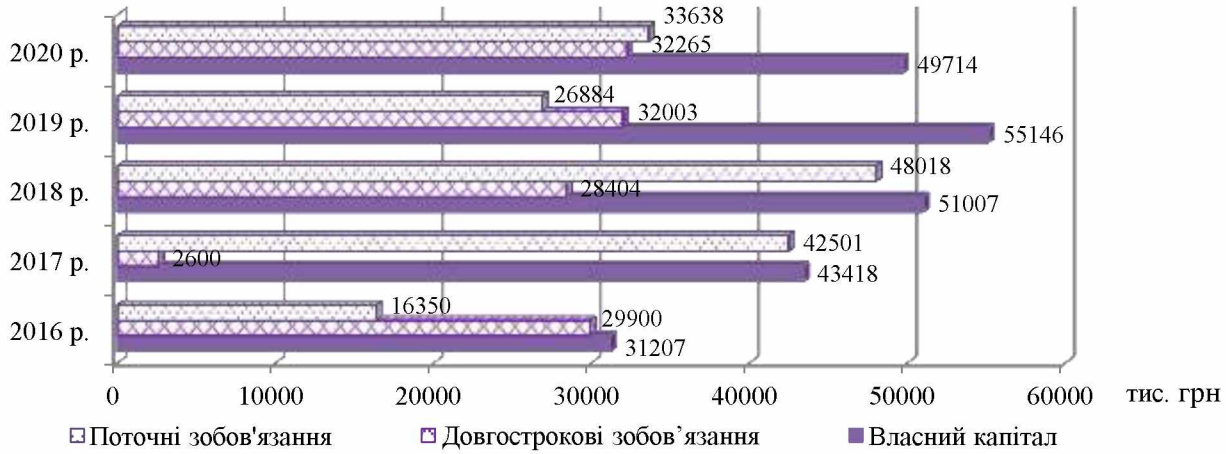

Рис. 2.5. Динаміка структури джерел формування фінансових ресурсів «Назва підприємства» ххххххххххххххххххххх району, 2016-2020 рр.

За результатами аналізу встановлено негативну тенденцію переважання у структурі джерел фінансування позичкового капіталу, значення якого становило у 2020 р. – 65903,0 тис. грн, тобто 57,0 %. Його вартість зростає на 19653,0 тис. грн по відношенню до 2016 р. (46250 тис. грн або ж 59,71 %), водночас його питома вага в загальній структурі фінансових ресурсів підприємства зменшується на 2,71 %. В зазначений категорії джерел фінансування значний обсяг поточні зобов'язання, які зростають в 2,1 рази порівняно з 2016 р. і становлять у звітному році – 33638,0 тис. грн. Проте їх питома вага в загальній структурі фінансування зростає лише на 7,98 %. Менший обсяг в даній категорії мають довгострокові зобов'язання: 32265,0 тис. грн у 2020 р. (27,91,60 %). Їх вартість зростає протягом аналізованого періоду до 32265 тис. грн у 2020 р. тобто на 2365,0 тис. грн або ж на 10,7 %. Власний капітал «Назва підприємства» становить від 31207,0 тис. грн у 2016 р. до 55146,0 тис. грн у 2019 р, а у 2020 р. цей показник становить 49714,0 тис. грн, тобто 43,00 %. Обсяг власного капіталу зріс порівняно з 2016 р. на 18507,0 тис. грн, а питома вага в структурі джерел фінансування зросла на 2,71 %. Хоча й

простежуються позитивні тенденції до збільшення власного капіталу для забезпечення діяльності підприємства, доцільно відмітити, що структура пасивів не є оптимальною і потребує зменшення зобов'язань (довгострокових і поточних).

Надалі пропонується до аналізу найважливіший ресурс будь-якого підприємства – персонал. Саме аналіз структури персоналу, ефективність його використання та мотивація визначає ефективність діяльності сільськогосподарського підприємства загалом.

Людський потенціал підприємства визначає зміну більшості показників ефективності його діяльності. Власне тому, наступним є аналіз структури персоналу «Назва підприємства»(додаток К, рис. 2.6).

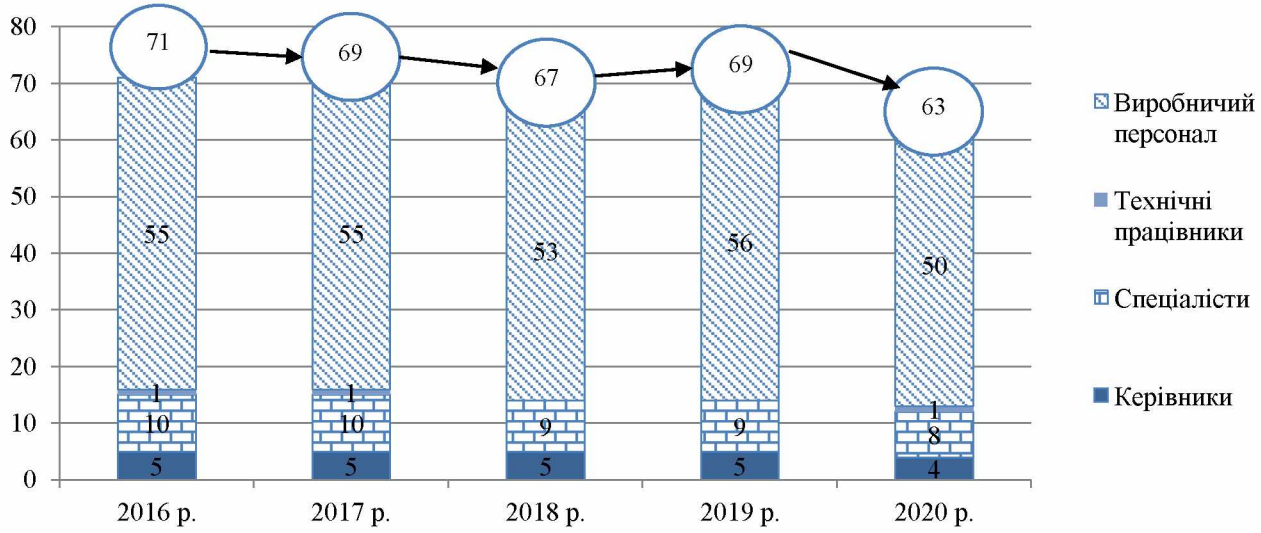

Рис. 2.6. Динаміка загальної структури персоналу «Назва підприємства» ххххххххххххххххххххх району, 2016-2020 рр.

Загальна чисельність персоналу підприємства зменшується у звітному році. Чисельність виробничого персоналу у звітному році становить 79,36 % від загальної чисельності і зменшується на 8 осіб порівняно з 2016 р. Зміни відбуваються і в структурі управлінського персоналу: зменшується чисельність керівників на 1 особу (20,0 %) та зменшується чисельність спеціалістів на 2 особи (20,0 %). Доцільно відмітити необхідність оптимізації людського потенціалу підприємства. Показники ефективності використання людського ресурсу протягом 2016-2020 рр. на «Назва підприємства» відображено у

додатку Л.

Всі працівники задіяні в сфері рослинництва. Середньооблікова чисельність працівників зменшується протягом аналізовано періоду на 8 осіб і становить у 2020 р. 63 особи, що свідчить про негативні зміни людського ресурсу.

Зі зменшенням середньооблікової чисельності працівників, зростає навантаження на одного працівника на 6,1 га на 1 особу, тобто на 12,3 %, а навантаження на одиницю виробничого персоналу зростає на 10,4 га на 1 особу, або ж на 25,5 % порівняно з показниками 2016 р.

Обсяг виробництва продукції підприємства зростає у 2,6 рази протягом 2016-2020 р. і становить у звітному році 986,9 тис. грн, проте його значення є меншим за показник попереднього періоду. Зростає і продуктивність праці одного працівника на 752,1 тис. грн, що перевищує значення 2016 р. у 2,2 рази.

Збільшується і фонд оплати праці на 3610,0 тис. грн, тобто на 90,0 %, що стверджує про інтенсивність використання людського ресурсу підприємства. Зазначене сприяє зростанню річного фонду оплати праці 1 працівника в 2,1 рази порівняно з базовим роком. Значення фондозабезпеченості було найбільшим у 2016 р. і становило 0,3 тис. грн, протягом 2017-2019 рр. – вона становила 0,2 тис. грн, а в 2020 р. –0,1 тис. грн. Зростає фондоозброєність «Назва підприємства» в 2,4 рази, що свідчить про техніко-технологічне оновлення матеріально-технічної бази підприємства. Негативною є динаміка показника фондомісткості, який збільшується на 0,1 тис. грн протягом, або ж на 47,3 %. Відповідно значення показника фондовіддачі зменшується на 32,1 тис. грн. Зазначене спричинило зменшення одержаних на 100 грн вартості основних фондів чистого доходу (виручки) від реалізації продукції (товарів, робіт, послуг) на 7,0 % та чистого прибутку на 31,9 %.

Аналізуючи персонал підприємства, доцільно й надати характеристику його системи управління. Відтак, вищим органом управління підприємством є Загальні збори учасників, а найвищою ланкою управління є директор.

Система управління підприємством включає сукупність не лише процесів, що забезпечують управлінську діяльність, але і всі підсистеми та комунікації між ними (рис. 2.7).

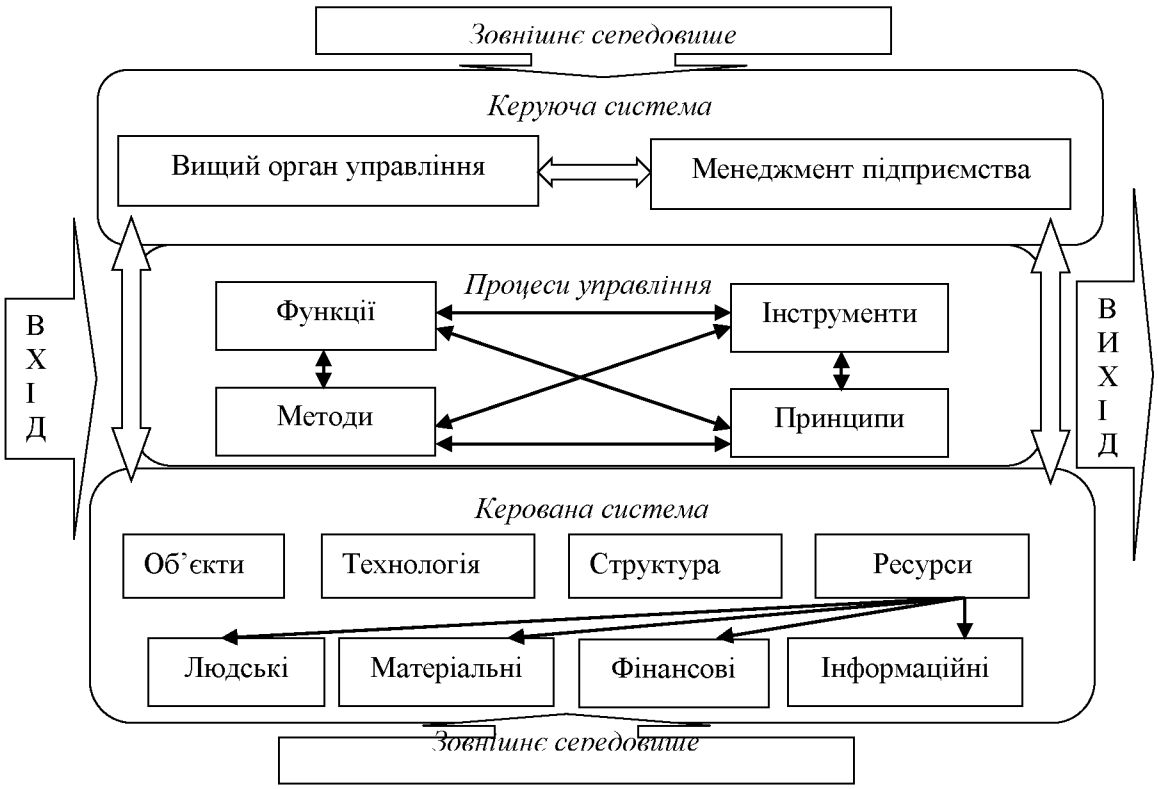

Рис. 2.7. Система управління «Назва підприємства» хххххххххх району

У підпорядкуванні директора знаходяться провідні фахівці підприємства, яким підпорядкований виробничий персонал (рис. 2.8).

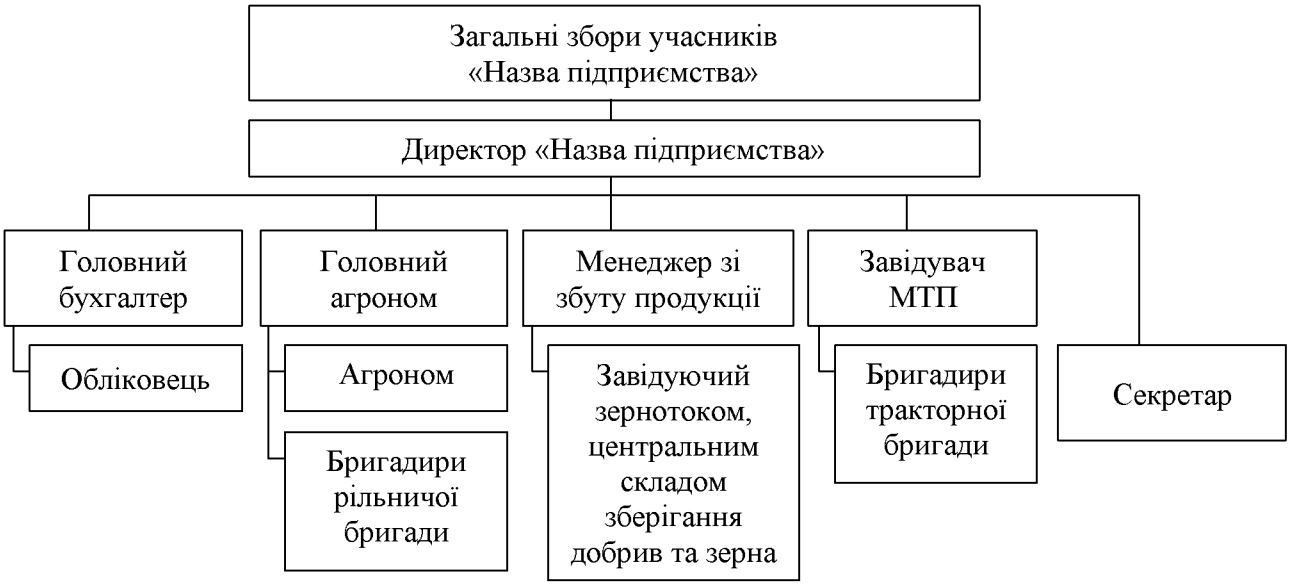

Рис. 2.8. Організаційна структура управління «Назва підприємства» хххххххххххххххххххх району

Важливим аспектом організаційно-економічної діагностики діяльності «Назва підприємства» залишається аналіз його інформаційного ресурсу, зокрема ті аспекти, які стосуються забезпечення його безпеки.

2.2. Аналіз рівня інформаційної безпеки «Назва підприємства»

Загалом, для визначення рівня інформаційної безпеки підприємства розроблено безліч методик, які можуть бути використані в залежності від особливостей діяльності підприємства, його розмірів, масштабів діяльності, спеціалізації та інших критеріїв. Водночас, аналізуючи систему інформаційної безпеки досліджуваного підприємства слід відзначити, що воно не має налагодженої системи інформаційної безпеки та не використовує конкретних методик оцінки, що ускладнює власне процес захисту інформації та визначення рівня інформаційної безпеки. Проте існує загальна та універсальна методика, відповідно до якої, кількісний розрахунок та якісний аналіз показників витрат на забезпечення інформаційного захисту, чисельність й частота загроз порушення інформаційної безпеки, їх видів, а також наслідків їх настання для підприємства дозволяють орієнтовно визначити рівень інформаційної безпеки. Власне дану методику пропонується використати для аналізу рівня інформаційної безпеки на «Назва підприємства».

Відтак, важливим аспектом оцінки рівня інформаційного забезпечення та інформаційної безпеки для підприємства є визначення основних статей витрат, спрямованих на інформатизацію діяльності та захист інформаційних ресурсів з характеристикою їх динаміки протягом 2016-2020 рр. (табл. 2.2).

Аналіз витрат на забезпечення інформаційного забезпечення підприємства дозволив визначити низький рівень інформаційної безпеки, оскільки найвищий їх обсяг спостерігався у 2020 р. і становив 31,4 тис. грн, а найменший у 2017 р. – 19,3 тис. грн, у 2016 р. цей показник становив

19,8 тис. грн. Слід відмітити позитивну тенденцію зростання обсягу витрат на вдосконалення інформаційного забезпечення та інформаційного захисту на досліджуваному підприємстві на 11,6 тис. грн або ж на 58,59 % протягом аналізованого періоду. Проте, враховуючі інфляційні процеси, хоча й обсяг витрат зростає, вартість грошей не може забезпечувати належний рівень обслуговування інформаційної інфраструктури підприємства.

Таблиця 2.2

Основні статті витрат, пов'язані з інформатизацією діяльності та забезпеченням інформаційної безпеки «Назва підприємства» xxxxxxxxxx району та забезпеченням інформаційної безпеки у 2016-2020 рр., тис. грн

Статті витрат	2016 р.	2017 р.	2018 р.	2019 р.	2020 р.	Відхилення у 2020 р. до 2016 р.	
						(+;-)	%
Консультування з питань інформатизації та захисту	-	-	1,4	2,6	3,9	3,9	100,0
Розроблення програмного забезпечення та консультування	-	-	-	-	5,2	5,2	100,0
Оброблення даних	1,6	1,9	2,1	2,2	2,4	0,8	50,0
Діяльність, пов'язана з банками даних	-	1,2	-	1,1	0,9	0,9	100,0
Ремонт та технічне обслуговування офісної та електронно-обчислювальної техніки	12,4	10,1	11,1	9,4	13,1	0,7	5,65
Інша діяльність у сфері інформатизації	5,8	6,1	6,4	6,3	5,9	0,1	1,72
Всього обсяги діяльності у сфері інформатизації	19,8	19,3	21	21,6	31,4	11,6	58,59

Доцільно відзначити, що основною статтею витрат на інформатизацію діяльності «Назва підприємства» є витрати на ремонт та технічне обслуговування офісної та електронно-обчислювальної техніки, які складають у 2020 р. – 13,1 тис. грн (41,72 % в загальній структурі витрат на інформатизацію та інформаційну безпеку), що більше порівняно з 2016 р. на 0,7 тис. грн або ж на 5,65 %, що пов'язано зі зносом та старінням апаратних засобів та збільшення. Звичайно, для потужного підприємства такий обсяг витрат не забезпечує навіть мінімальні потреби у забезпеченні інформаційної

інфраструктури та отримання необхідного рівня інформаційного захисту.

Наступною за питомою вагою є стаття витрат, яка пов'язана з різними аспектами діяльності у сфері інформатизації – 18,89 % у 2020 р. Зазначена стаття витрат зростає протягом аналізованого періоду лише на 0,1 тис. грн, тобто на 1,72 %, що безперечно негативно характеризує аспекти забезпечення інформаційної інфраструктури.

Майже аналогічною є питома вага витрат на розроблення та впровадження програмного забезпечення, яка складає 16,56 % у 2020 р. – 5,2 тис. грн. Доцільно відзначити, що протягом 2016-2019 рр. дана стаття витрат на підприємстві була відсутня.

Позитивним зрушенням є зростання питомої ваги витрат, які спрямовані на консультування з питань інформатизації, яка становить у 2020 р. 12,42 % або ж 3,9 тис. грн. Знову потрібно відмітити позитивне зрушення у сфері інформаційного забезпечення діяльності підприємства, оскільки дана стаття витрат була відсутня у 2016-2017 рр., а в 2018-2019 рр. разом становила 4,0 тис. грн.

Наступною за питомою вагою є стаття витрат, пов'язана із обробленням даних – 7,64 %, оскільки виробничі процеси спричиняють необхідність обробки великих масивів даних, через що, витрати збільшуються з 1,6 тис. грн у 2016 р. до 2,4 тис. грн у 2020 р., тобто на 0,8 тис. грн або ж на 50,0 %.

Нерегулярними є витрати, пов'язані із забезпеченням функціонування банків даних, які ще у 2016 р. та у 2018 р. біли відсутні, а у звітному році становили лише 0,9 тис. грн.

Варто зазначити, що статті витрат на інформатизацію та захист інформації на «Назва підприємства» є мінімальним та не забезпечують належний рівень цифровізації та інформаційної безпеки діяльності підприємства.

Надалі доцільним є аналіз коефіцієнтів, які характеризують рівень захисту інформації «Назва підприємства» за 2016-2020 рр. (табл. 2.3).

Таблиця 2.3

Показники рівня інформаційної безпеки на «Назва підприємства» xxxxxxxxxxxxxxxxxxxx району за 2016-2020 рр.

Статті витрат	2016 р.	2017 р.	2018 р.	2019 р.	2020 р.	Відхилення у 2020 р. до 2016 р.	
						(+;-)	%
Коефіцієнт технічного захисту інформації	0,19	0,19	0,14	0,09	0,21	0,02	10,52
Коефіцієнт програмної захищеності інформації	0,12	0,12	0,1	0,06	0,19	0,07	58,33
Коефіцієнт фінансового захисту інформації	0,08	0,1	0,11	0,09	0,07	-0,01	-12,50
Коефіцієнт правової захищеності інформації	0,07	0,06	0,09	0,1	0,11	0,04	57,14
Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства	0,21	0,18	0,18	0,18	0,16	-0,05	-23,81
Коефіцієнт підготовленості персоналу до розпізнавання загроз	0,18	0,17	0,15	0,13	0,21	0,03	16,67
Оцінка інформації, що надається особам, що приймають рішення (ОПР)	0,16	0,15	0,15	0,18	0,17	0,01	6,25
Коефіцієнт точності інформації	0,52	0,61	0,59	0,57	0,58	0,06	11,54
Коефіцієнт суперечливості інформації	0,54	0,62	0,55	0,57	0,57	0,03	5,56
Коефіцієнт своєчасності надання інформації	0,45	0,39	0,4	0,41	0,43	-0,02	-4,44
Коефіцієнт надійності інформації	0,62	0,63	0,71	0,63	0,61	-0,01	-1,61

На основі аналізу коефіцієнтів, доцільно відмітити зростання коефіцієнту технічного захисту інформації у 2020 р. порівняно з 2016 р. на 0,02 або на 10,52 %. Коефіцієнт програмної захищеності інформації таж має незначну тенденцію до зростання протягом аналізованого періоду на 0,07 або ж на 58,33 %. Проте, значення цього коефіцієнту у 2020 р. становить 0,19. За результатами аналізу зазначених коефіцієнтів доцільно відзначити їх незначний рівень, що вказує на необхідності посилення програмного та апаратного захисту.

Коефіцієнт фінансового захисту інформації зменшує значення на 0,01 або ж на 12,5 % у 2020 порівняно з 2016 р. і становить 0,07, що не

відповідає навіть мінімальному рівню захисту. Знижується на 57,14 % значення коефіцієнту правової захищеності інформації у 2020 р. і становить 0,11, що також не задовольняє умови правового захисту інформаційних ресурсів «Назва підприємства».

Позитивним є зростання коефіцієнту підготовленості персоналу до розпізнавання загроз на 16,67 % порівняно з 2016 р., проте його значення є недостатнім для забезпечення ефективного захисту інформаційної складової діяльності підприємства. Негативним є зменшення коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку на 23,81 % у 2020 р. порівняно з базовим роком. Слід відмітити й мінімальне значення даного коефіцієнту – 0,16 у звітному році. Нестабільним є значення коефіцієнту оцінки інформації, що надається особам, які приймають рішення на «Назва підприємства», тобто керівному складу підприємства. Воно коливається в межах 0,15-0,18, що є недостанім показником для забезпечення мінімального рівня захисту управлінської інформації.

Позитивною тенденцією є зростання коефіцієнту точності інформації на 0,06 (11,54 %). Проте інші коефіцієнти, які характеризують властивості інформації на підприємстві мають тенденцію до погіршення значень, зокрема: зростання рівня коефіцієнту суперечливості інформації, значення якого зростає на 5,56 % протягом аналізованого періоду і становить 0,57 у 2020 р.; зменшення коефіцієнту своєчасності надання інформації на 0,02 (4,44 %), коефіцієнту надійності інформації на 0,01 (1,61 %).

Важливим аспектом діагностики захисту інформації в системі інформаційної безпеки «Назва підприємства» є кількісна оцінка зовнішніх та внутрішніх загроз інформаційній безпеці.

У випадку з зовнішніми атаками здійснюється пошук уразливості в інформаційній структурі для доступу до основних вузлів, сховищ, персональних комп'ютерів співробітників, організаційної мережі тощо. Інструментами виступають віруси, які прийнято називати шкідливим програмним забезпеченням. Дослідження зовнішніх загроз інформаційної

безпеки підприємства, шляхом опитування управлінського персоналу дозволило отримати наступні результати (рис. 2.9, додаток М).

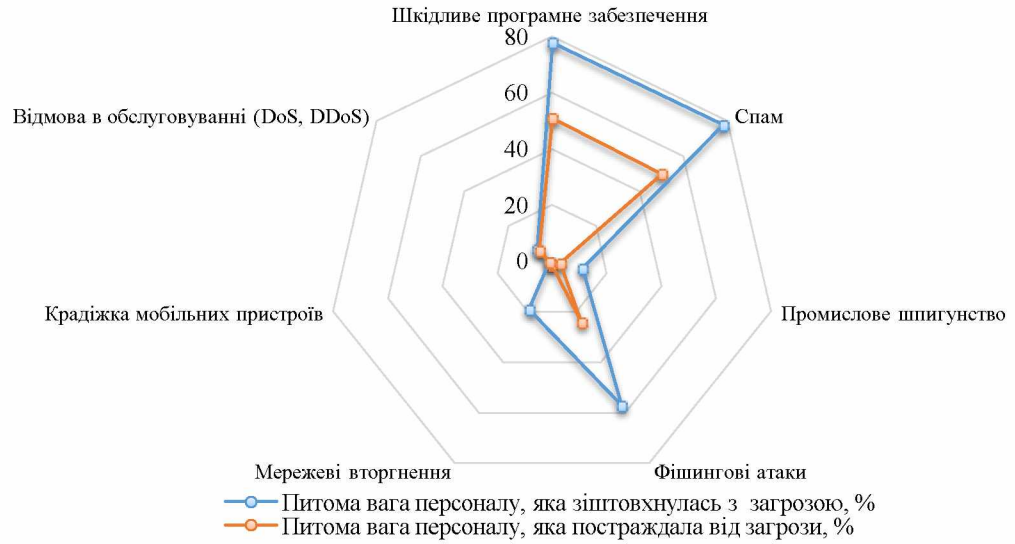

Рис. 2.9. Зовнішні загрози інформаційної безпеки «Назва підприємства» ххххххххххххххххххххх району за 2016-2020 рр.

Протягом аналізованого періоду найбільш значимими зовнішніми загрозами «Назва підприємства» визначається шкідливе програмне забезпечення та спам, який часто є носієм шкідливого програмного забезпечення. Атаки з використанням шкідливого програмного забезпечення – це найнебезпечніший інструмент, що володіє високою ефективністю. Його застосування практично в половині випадків призводить до витоку інформації. Збільшується частка працівників, які зіткнувся з фішинговими атаками. Незначними є кількість мережевих вторгнень, відмов в обслуговуванні, випадки промислового шпигунства. За всіма іншими пунктами зовнішні загрози демонструють мінімальну кількість випадків. Щодо області досліджуваного підприємства, то в цілому результат ілюструє повторення загальноукраїнських тенденцій. Основним наслідком будь-якої атаки в разі її успішного здійснення стає втрата підприємством конфіденційної інформації.

Аналогічним чином проведено аналіз внутрішніх загроз інформаційній безпеці «Назва підприємства» за 2016-2020 рр. (рис. 2.10, додаток Н).

Рис. 2.10. Зовнішні загрози інформаційної безпеки «Назва підприємства» ххххххххххххххххххххх району за 2016-2020 рр.

За даними аналізу з'ясовано, що основними внутрішніми загрозами інформаційної безпеки на досліджуваному підприємстві є наступні види: вразливість програмного забезпечення (мала місце загроза – 38 % респондентів, постраждали від загрози – 20 % респондентів), випадкові витоки від працівників (мала місце загроза – 45 % респондентів, постраждали від загрози – 29 % респондентів) та навмисні витоки інформації з вини співробітників (мала місце загроза – 14 % респондентів, постраждали від загрози – 7 % респондентів), викликані в основному незнанням затверджених на підприємстві правил. Така внутрішня загроза, як неналежний обмін інформацією через мобільні пристрої мала незначну питому вагу в структурі загроз і трапилася один раз протягом 2016-2020 рр. Втрат мобільних пристроїв співробітниками, шахрайство зі сторони співробітників та порушень безпеки зі сторони контрагента як видів внутрішніх загроз інформаційній безпеці на «Назва підприємства» протягом аналізованого періоду не спостерігалося.

Отже, групи джерел основних дестабілізуючих факторів інформаційної безпеки підприємства відображені на рис. 2.11.

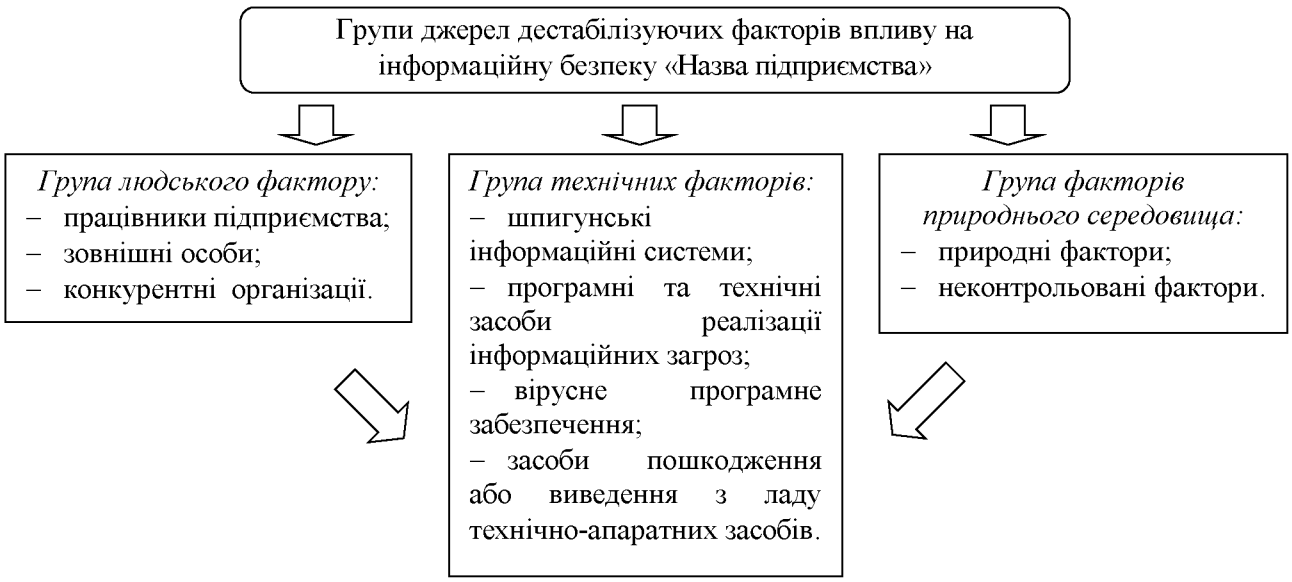

Рис. 2.11. Групи джерела основних дестабілізуючих факторів впливу на інформаційну безпеку «Назва підприємства» ххххххххххххххххххххх району за 2016-2020 рр.

Слід зазначити, що основні показники мають тенденції до скорочення. Зазначені аспекти можна пояснити активізацією процесів оновлення програмного забезпечення в зв'язку з усвідомленням небезпеки реалізації даної загрози та ознайомленням працівників та контрагентів підприємства з правилами внутрішнього розпорядку, які регулюють процеси збереження інформаційних ресурсів. Крім того, майже чверть респондентів зазначила в якості нових заходів інформаційної безпеки застосування систем для захисту від витоків даних. З одного боку, це викликано недооцінкою осіб, які приймають рішення щодо забезпечення інформаційної безпеки, з іншого боку, перелік загроз щорічно змінюється, і дуже складно встигати за ним, забезпечуючи системам інформаційного захисту максимально актуальний стан. Проте, це не завжди виправдано, тому що найчастіше наслідки реалізації інформаційних загроз для «Назва підприємства» можуть носити критичний характер. Тому на рис. 2.12. представлені наслідки реалізації інформаційних загроз для «Назва підприємства» протягом 2016-2020 рр.

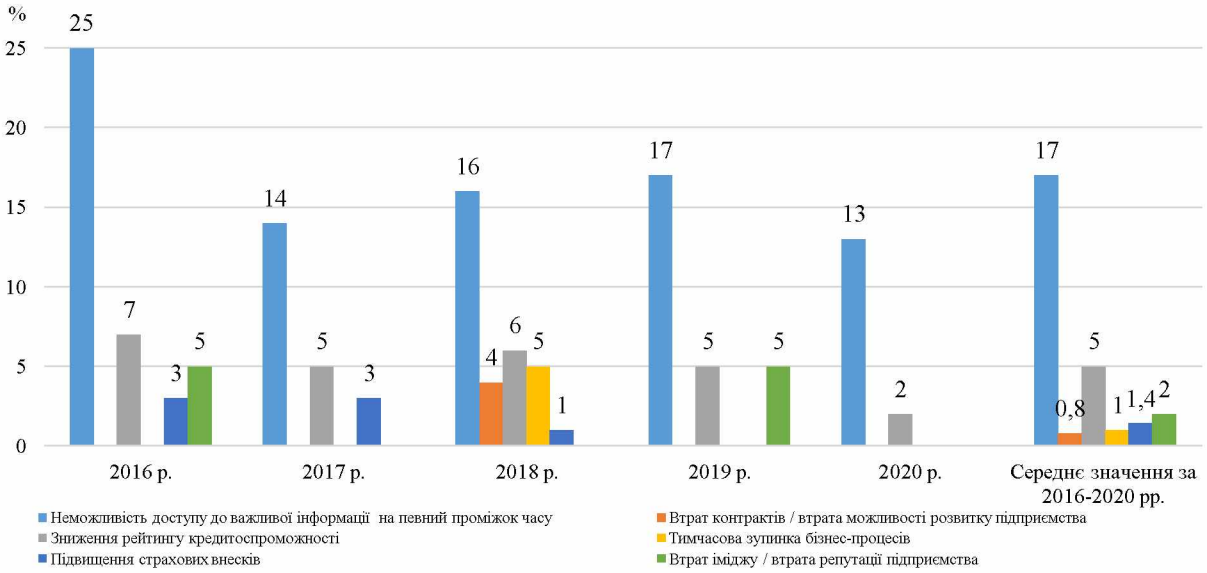

Рис. 2.12. Наслідки реалізації інформаційних загроз для «Назва підприємства» ххххххххххххххххххххх району за 2016-2020 рр., %

Відтак, основним наслідком реалізації загроз інформаційній безпеці підприємства стає неможливість (переважно тимчасова) доступу до важливої інформації. Проте значення даного наслідку зменшується протягом аналізованого періоду з 25 % у 2016 р. до 13 % 2020 р. Середнє значення даного показника протягом 2016-2020 рр. становить 17 %. Зниження рейтингу кредитоспроможності є наступним за значенням наслідком реалізації загроз інформаційній безпеці, значення якого теж зменшується з 7 % у 2016 р. до 2 % у 2020 р. Середнє значення даного показника протягом 2016-2020 рр. становить 5 %.

Поодинокі випадки втрати іміджу або ділової репутації через розкриття інформаційних ресурсів, в тому числі інформації про контрагентів, яка підлягає захисту простежувались у 2016 р. та 2019 р.

Інші види наслідків становлять незначну частину наслідків, які майже не здійснюють впливу на продовольчу, соціальну та економічну складові діяльності підприємства. Водночас, ті наслідки, які простежуються повинні бути враховані при визначенні стратегічних напрямків управління інформаційною безпекою «Назва підприємства».

На основі проведених досліджень, доцільно відмітити низький рівень інформаційного захисту підприємства, який обумовлений низьким рівнем витрат на забезпечення інформаційної діяльності на забезпечення цілісності інформаційних ресурсів, зменшення нормативних значень коефіцієнтів, які характеризують рівень інформаційної безпеки, прецедентів виникнення загроз та їх наслідків. Незважаючи на незначний рівень загроз інформаційній безпеці, за умов розвитку цифрового середовища, кожному підприємству необхідно посилювати безпеку інформаційної сфери, яка не боже дути ефективною без належного рівня управління. Тому, наступним етапом дослідження стане характеристика системи управління інформаційною безпекою «Назва підприємства».

2.3. Характеристика складових системи управління інформаційною безпекою на «Назва підприємства»

Характеризуючи систему управління інформаційною безпекою «Назва підприємства» доцільно визначити її організаційну (рис. 2.13) та функціональну побудову (рис. 2.14).

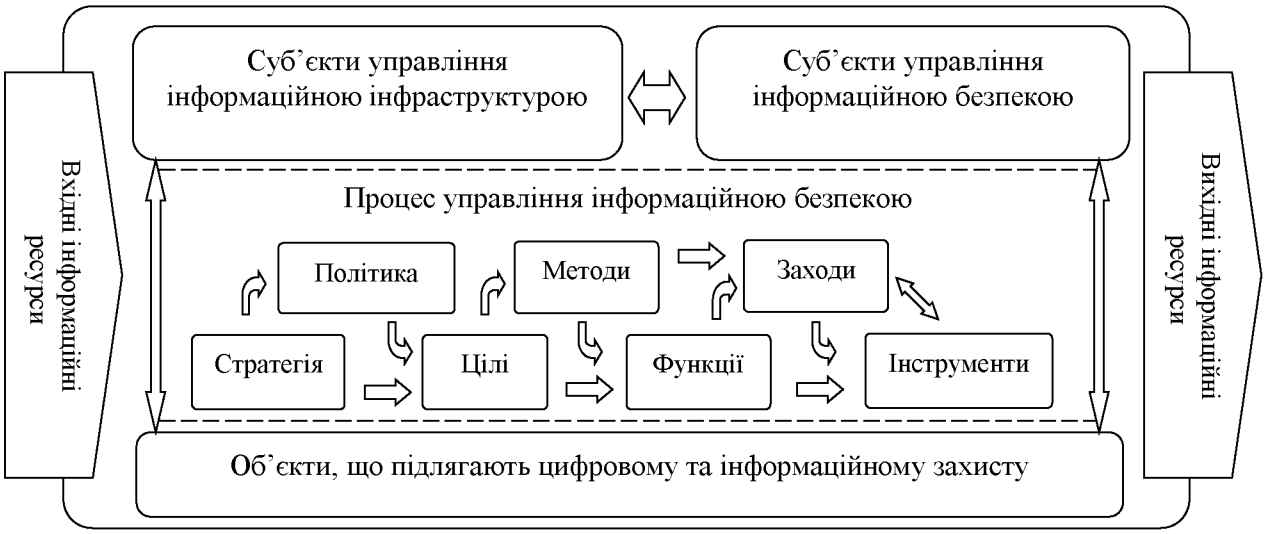

Рис. 2.13. Модель організаційної побудови системи управління інформаційною безпекою «Назва підприємства» xxxxxxxxxxxxxxxxxxxxx району, станом на 2021 р.

Організаційна побудова системи управління інформаційною безпекою «Назва підприємства» є традиційною та передбачає наявність класичних складових для забезпечення захисту інформаційної інфраструктури підприємства: суб'єктів управління інформаційною інфраструктурою та суб'єктів управління інформаційною безпекою (що переважно є одними й тими ж посадовими особами підприємства), об'єктів, що підлягають цифровому та інформаційному захисту, а також власне процесу управління, який передбачає включення стратегії, політики інформаційної безпеки (неформалізованих), цілей, методів, функцій, заходів та інструментів. Головні складові даної моделі системи управління інформаційною безпекою будуть розглядатися та аналізуватися окремо.

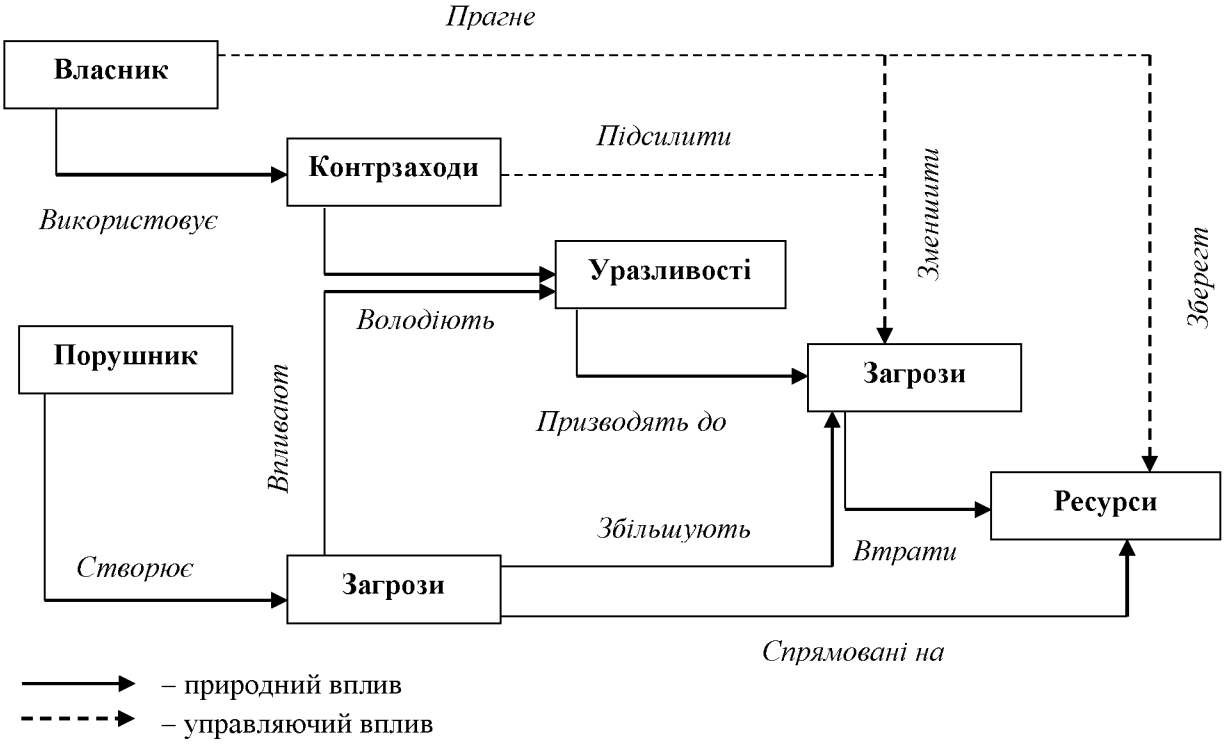

Рис. 2.14. Модель функціональної побудови системи управління інформаційною безпекою «Назва підприємства» ххххххххххххххххххххх району, станом на 2021 р. [сформовано на основі **Ошибка! Источник ссылки не найден.**]

Функціональна модель забезпечення інформаційної безпеки на «Назва підприємства» теж є класичною і передбачає реалізацію

загальноприйнятого алгоритму інформаційного захисту.

Для об'єктивного аналізу рівня інформаційної безпеки досліджуваного підприємства, перш за все, необхідно визначити органи управління, які здійснюють функції щодо забезпечення інформаційного захисту та визначити їх компетентності, ефективність діяльності. Звичайно, зважаючи на розміри підприємства, спеціального відділу або ж фахівця, який би відокремленого виконував функції управління та регулювання окремих аспектів захисту інформаційної інфраструктури підприємства та його інформаційних ресурсів відсутній.

З цією метою здійснено побудову організаційної структури системи управління інформаційної безпеки «Назва підприємства», де особливе місце належить управлінській складовій, яка передбачає взаємодію різноманітних компетентностей, навиків, необхідних керівництву підприємства з метою реалізації функцій управління не лише в системі інформаційної безпеки, а й підприємства загалом. Відтак, загальну структуру системи управління інформаційної безпеки підприємства відображено на рис. 2.15.

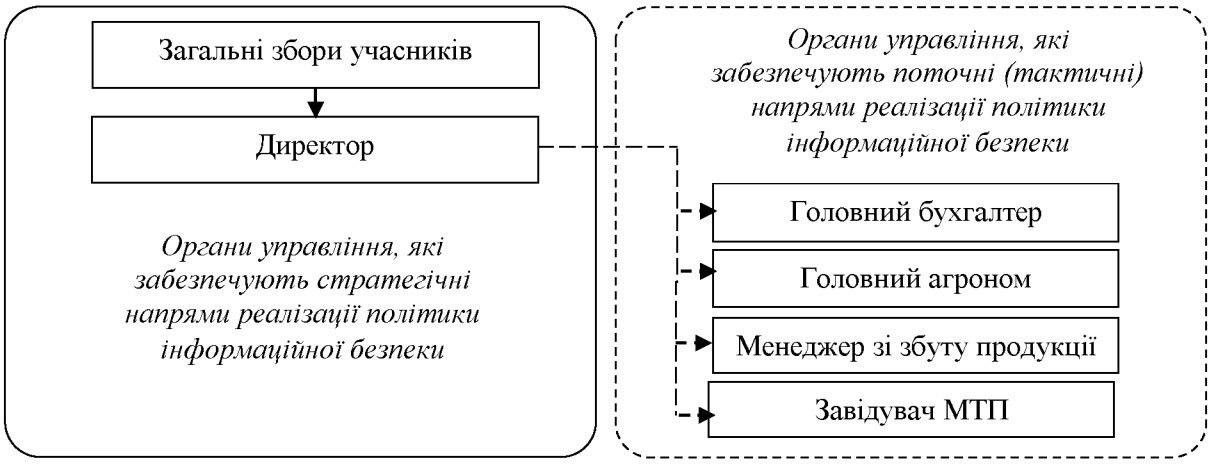

Рис. 2.15. Організаційна побудова системи інформаційної безпеки «Назва підприємства» ххххххххххххххххххххх району, станом на 2021 р.

Відповідальність за захист інформації розподілена між окремими фахівцями та підрозділами, зокрема: на стратегічному рівні – між загальними зборами учасників та директором, які визначають загальні, пріоритетні напрями розвитку системи управління інформаційною безпекою,

формують політику та модель захисту даних на підприємстві; на тактичному рівні – провідними фахівцями підприємства, які несуть відповідальність за збереження комерційної таємниці щодо окремих напрямів діяльності – між головним бухгалтером, головним агрономом, менеджером зі збуту продукції та завідувачем МТП. Кожен із провідних спеціалістів підприємства забезпечує збереження інформаційні відповідно фінансово-економічних, маркетингових, технологічних, продовольчих, технічних, кадрових та інших аспектів діяльності.

Стратегія, політика та цілі управління інформаційною безпекою не мають чіткого формалізованого окреслення і визначаються як загальноприйняті для підприємств приналежних до агропродовольчої сфери, розміру, масштабів та специфіки діяльності. Загалом стратегію управління інформаційною безпекою підприємства можна окреслити як таку, що спрямована на ліквідацію наслідків настання загроз, а також, що використовує мінімальний інструментарій інформаційного захисту.

Основні функції системи менеджменту інформаційної безпеки «Назва підприємства» відображені на рис. 2.16.

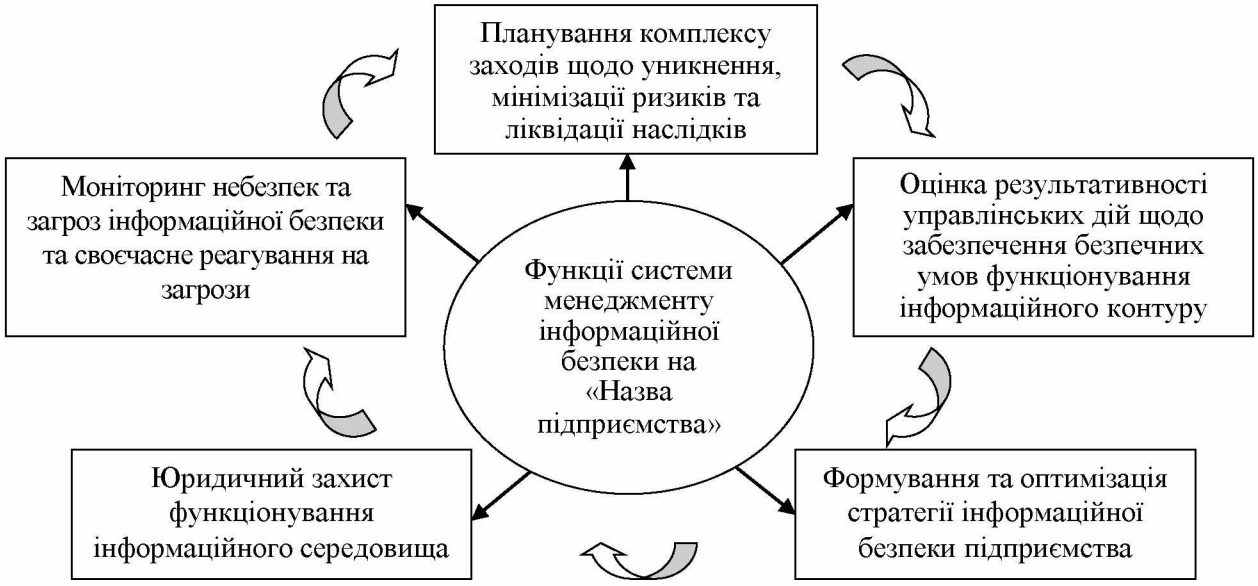

Рис. 2.16. Базові функції системи менеджменту інформаційної безпеки «Назва підприємства» ххххххххххххххххххххх району, станом на 2021 р.

Відповідно до розподілу обов'язків щодо забезпечення інформаційної

безпеки підприємства, можливо структурувати основні цілі системи управління інформаційною безпекою на «Назва підприємства» ххххххххххххххххххххх району, станом на 2021 р. (рис. 2.17).

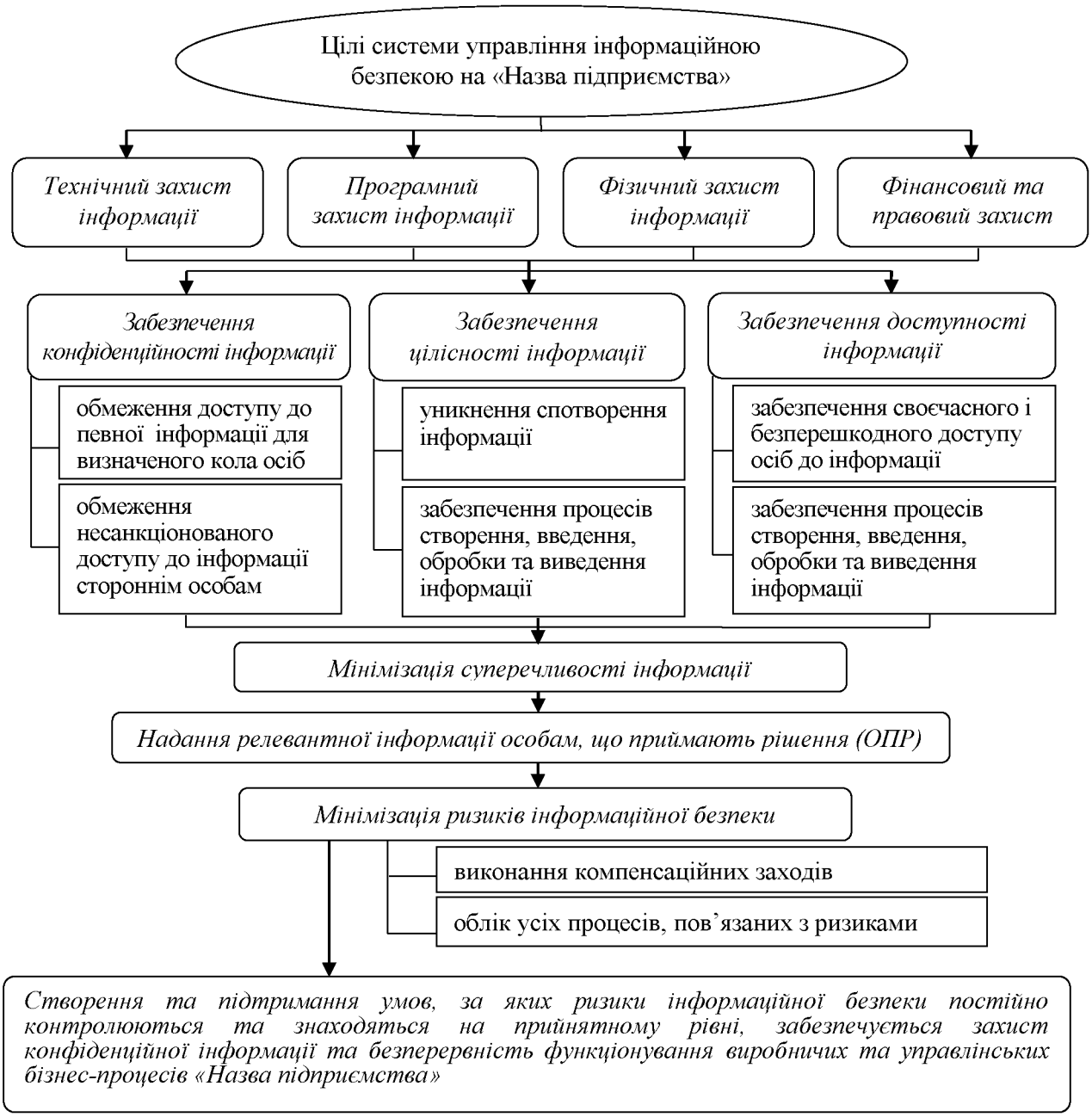

Рис. 2.17. Структура цілей системи менеджменту інформаційної безпеки «Назва підприємства» ххххххххххххххххххххх району, станом на 2021 р.

З метою більш розгорнутої діагностики системи управління інформаційною безпекою доцільно визначити склад та структуру інформаційних ресурсів «Назва підприємства», які підлягають нерозголошенню та захисту, тобто та група основних об'єктів інформаційної

інфраструктури, захист яких передбачається (додаток П).

Відтак, на «Назва підприємства» в захисті потребують переважно два типи відомостей, які підпадають під категорію службової або комерційної таємниці:

інформація, яка становить науково-технологічні відомості, пов'язані безпосередньо з технологічною документацією, відомості про сировину, а також опис методів та способів виробництва видів продукції, застосування унікального програмного продукту;

інформація, яка становить ділові відомості про діяльність підприємства: фінансова документація, перспективні плани розвитку, напрямки модернізації виробництва, аналітичні матеріали про дослідження конкурентів та ефективність роботи на ринках товарів і послуг, різні відомості про партнерів тощо;

у зв'язку з загрозами виникає необхідність забезпечення безпеки й управлінської інформації, яка виражається в управлінських рішеннях.

Водночас, визначено що значну вразливість система менеджменту інформаційної безпеки підприємства має через загрози пов'язані з автоматизованими робочими місцями виробничого та управлінського персоналу, а також загрозами порушення конфіденційності інформації (додаток Р).

Щодо діючої політики інформаційної безпеки на підприємстві, то для нейтралізації та мінімізації інформаційних загроз керівництво вживає деякі заході (рис. 2.18), ефективність яких є значною, оскільки реалізуються вони відособлено та не мають комплексності.

Відповідний вибір заходів інформаційного захисту необхідний для правильного здійснення політики інформаційного захисту. Основні сфери використання захисних заходів є: фізичне середовище; технічне середовище (апаратні засоби, програмне забезпечення та засоби комунікації); персонал; адміністрацію (керівництво підприємства). Приклади таких захисних заходів для є: мережеві системи захисту доступу; мережевий моніторинг та аналіз; кодування інформації для забезпечення конфіденційності; електронні

підписи; антивірусне програмне забезпечення; дублюючі копії інформації; резервні джерела живлення; механізми управління доступом.

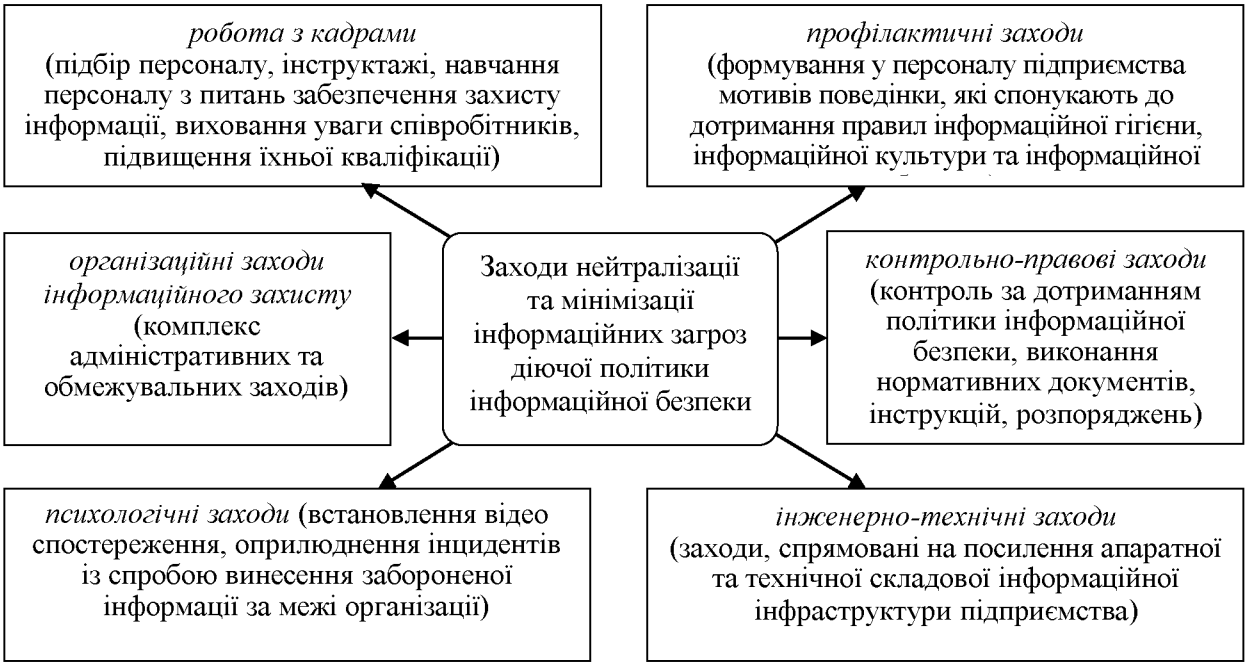

Рис. 2.18. Заходи нейтралізації та мінімізації інформаційних загроз діючої політики інформаційної безпеки «Назва підприємства» ххххххххх району, станом на 2021 р.

Для захисту інформації на «Назва підприємства» використовується корпоративна мережа, основним призначенням якої є підтримка оперативної комунікації та незначні розмежування прав доступу до визначених типів інформації підприємства. Підрозділи виконують різнорідні види робіт, проте у межах єдиного процесу, інформаційно обмінюючись документами, даними, відомостями про стан різних виробничих операцій. Користувачами корпоративної мережі підприємства є тільки його співробітники.

Отже, за сучасних умовах інформаційна безпека є невід'ємною складовою системи економічної безпеки «Назва підприємства», а надійне забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку. Щоб зберегти бізнес, розвиватися і бути конкурентоспроможним, підприємству необхідно створити ефективну систему управління інформаційною безпекою. Рекомендації щодо її вдосконалення розглянуто у наступному розділі кваліфікаційної роботи.

Висновки до розділу 2

Здійснивши аналіз управління інформаційною безпекою «Назва підприємства», доцільно відзначити:

1. Підприємство «Назва підприємства» здійснює виробництво продукції рослинництва та її реалізацію. Управління підприємством здійснюють: загальні збори учасників підприємства, директор та провідні фахівці. Отриманий результат аналізу виробничо-господарських показників діяльності вказує на поступове зниження ефективності діяльності підприємства.

2. Аналіз витрат на забезпечення інформаційної діяльності підприємства дозволив визначити низький рівень інформаційної безпеки, оскільки найвищий їх обсяг спостерігався у 2020 р. і становив 31,4 тис. грн, а найменший у 2017 р. – 19,3 тис. грн, Доцільно відзначити, що основною статтею витрат на інформатизацію діяльності є витрати на ремонт та технічне обслуговування офісної та електронно-обчислювальної техніки. Протягом аналізованого періоду найбільш значимими зовнішніми загрозами для підприємства визначено шкідливе програмне забезпечення та спам, який часто є носієм шкідливого програмного забезпечення. Основними внутрішніми загрозами інформаційної безпеки є: вразливість програмного забезпечення, випадкові витоки від працівників та навмисні витоки інформації з вини співробітників.

3. Самостійний підрозділ, який би здійснював функції із захисту інформації на підприємстві відсутній. Відповідальність за захист інформації розподілена між директором та окремими фахівцями. Організаційна та функціональна модель управління інформаційною безпекою є традиційними та передбачають наявність класичних складових для забезпечення захисту інформаційної інфраструктури. Стратегія, політика та цілі управління інформаційною безпекою не мають чіткого формалізованого окреслення і визначаються як загальноприйняті для підприємств приналежних до агропродовольчої сфери.

РОЗДІЛ 3
ШЛЯХИ ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ «НАЗВА ПІДПРИЄМСТВА»

3.1. Напрями оптимізації системи захисту інформації на «Назва підприємства»

Для визначення перспективних напрямів вдосконалення системи управління інформаційною безпекою «Назва підприємства» доцільно визначити ключові позиції, які потрібно зміцнювати для розбудови ефективності системи інформаційного захистку підприємства. Оскільки базовими аспектами будь-якої інформаційної системи сільськогосподарського підприємства є техніко-технологічне устаткування, програмне забезпечення та кадровий потенціал, який здійснює процеси управління інформаційною безпекою та який здійснює процеси її забезпечення (захисту), то пропонується розглядати напрями оптимізації системи захисту інформації на «Назва підприємства» саме в зазначених площинках.

Відтак, окреслено для вдосконалення оптимізацію трьох основних складових інформаційної інфраструктури та її захисту для «Назва підприємства»: техніко-технологічної складової, програмного забезпечення та кадрового потенціалу, який забезпечує процеси інформаційного захисту. З метою визначення доцільності підвищення ефективності зазначених складових доцільно провести кореляційно-регресійний аналіз взаємозв'язку факторів та їх вплив на результативний показник діяльності – рентабельність діяльності досліджуваного підприємства. Для формалізації та кількісного вимірювання, а також співставлення з показником рентабельності господарської діяльності підприємства встановлених складових системи інформаційної безпеки визначено їх охарактеризувати через розраховані показники: коефіцієнт технічного захисту інформації, коефіцієнт програмної

захищеності інформації, коефіцієнт підготовленості персоналу до розпізнавання загроз.

На результати дослідження та ефективність прогнозування виробничих процесів значною мірою впливає синтез або синкретика методів або використання елементів певного визначеного методу у взаємозв'язку із застосуванням іншого. Відтак, факторний аналіз доцільно підсилити регресійним аналізом, який визначатиме ступінь впливу визначених факторів.

Зважаючи, що підприємство є відкритою соціально-економічною системою, і система інформаційної безпеки теж, то їх діяльність впливає не один, а кілька факторів, між якими існують складні взаємозв'язки, а їх вплив на результативну ознаку (в даному випадку – рентабельність) є комплексним, а не сумою ізольованих впливів. Тому застосування багатофакторного кореляційно-регресійного аналізу дає надати кількісну оцінку, тобто рівень впливу на результативний показник кожного із введених у модель факторів при фіксованому положенні на середньому рівні інших факторів. Залежності зазначеного виду можуть описуються багатофакторною лінійною виробничою функцією типу:

$$\hat{Y} = a_0 + a_1X_1 + a_2X_2 + \ldots + a_nX_n. \quad (3.1)$$

А основним завданням багатофакторної виробничої регресії стає визначення ступеню впливу основних факторів забезпечення інформаційного захисту на економічний результат діяльності підприємства, тому в даному конкретному випадку на основі багатофакторної лінійної регресії досліджено вплив основних коефіцієнтів, пов'язаних з інформатизацією діяльності та забезпеченням інформаційної безпеки на рентабельність «Назва підприємства», за 2016-2020 рр. (табл. 3.1).

Для зручності, точності та об'єктивності, розрахунки проведено за допомогою електронних таблиць Microsoft Excel та вбудованих статистичних, математичних функцій та масивів (додаток С).

Таблиця 3.1

Вихідні дані для проведення кореляційно-регресійного аналізу впливу факторів забезпечення інформаційної безпеки на «Назва підприємства» ххххххххххххххххххххх району на його рентабельність, 2016-2020 рр.

Показники	Позначення	Роки				
		2016	2017	2018	2019	2020
Коефіцієнт технічного захисту інформації	x_1	0,19	0,19	0,14	0,09	0,21
Коефіцієнт програмної захищеності інформації	x_2	0,12	0,12	0,1	0,06	0,19
Коефіцієнт підготовленості персоналу до розпізнавання загроз	x_3	0,18	0,17	0,15	0,13	0,21
Рентабельність	y	12,50	12,50	10,90	4,00	9,10

Побудова багатофакторної лінійної моделі передбачає використання алгоритму методу Фаррара-Глобера з метою перевірки мультиколінеарності, яка передбачає, що в багатофакторній регресійній моделі дві або більше незалежних фактори із трьох запропонованих пов'язані між собою лінійною залежністю, тобто мають високий ступінь кореляції. Оскільки $Xi^2_{розр.}(15,06) < <Xi^2_{кр}(7,81)$ доцільно зробити висновок про мультиколінеарність матриці та факторів відображених в ній факторів.

Надалі розраховано парні коефіцієнти кореляції, які вказують на рівень впливу окремих факторів на результативний показник Y, тобто рентабельність господарської діяльності «Назва підприємства». Отримані в результаті розрахунку залежності оцінюють за рівнем показників тісноти зв'язку за шкалою вказаною на рис. 3.1.

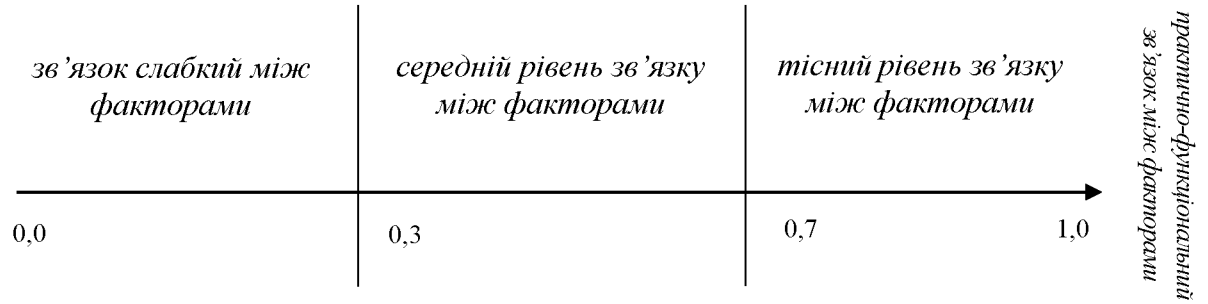

Рис. 3.1. Шкала оцінки рівня впливу окремих факторів на результативний фактор

Характеризуючи парні коефіцієнти кореляції, то можна простежити, що кожен із факторів суттєво впливає на рентабельність досліджуваного підприємства, зокрема:

у коефіцієнту технічного захисту інформації значення показника кореляції 0,74, стверджує про тісний прямий зв'язок між цим фактором та результативним показником;

у коефіцієнту програмної захищеності інформації та рентабельністю коефіцієнт кореляції 0,42 свідчить про достатній рівень зв'язку та середній рівень впливу вплив цієї складової системи інформаційної безпеки підприємства на економічний результат його діяльності;

у коефіцієнту підготовленості персоналу до розпізнавання загроз значення показника кореляції становить 0,82, що як і у випадку з коефіцієнтом технічного захисту інформації також вказує на тісний зв'язок та значний вплив цього фактору на результативний показник діяльності.

Наступним кроком є аналіз парних коефіцієнтів кореляції, які дозволяють визначити, що найменший вплив на рівень рентабельності господарської діяльності підприємства має коефіцієнт програмної захищеності, показник кореляції якого відповідає значенню 0,42, а тому, цей фактор буде виключений із подальшого економетричного аналізу багафакторної регресійної моделі. Відтак, подальший аналіз та прогнозування багатофакторної лінійної регресії рентабельності господарської діяльності підприємства буде проведений із двома факторами – елементами системи інформаційної безпеки: коефіцієнтом технічного захисту інформації та коефіцієнтом підготовленості персоналу до розпізнавання загроз.

Слід відзначити, що виключеного з багатофакторної моделі коефіцієнту програмної захищеності інформації здійснено через найменше серед інших факторів показником коефіцієнту кореляції. Проте, цей фактор, має не менш важливе значення для створення системи належного захисту інформаційної інфраструктури «Назва підприємства». Тому програмне

забезпечення разом з технічним забезпеченням визначають основу функціонування інформаційної системи будь-якого підприємства.

Побудована модель багатофакторної виробничої функції також визначає коефіцієнти кореляції, які характеризують тісноту зв'язку між окремими двома факторами. Варто зважати, що на відміну від парних, ці коефіцієнти характеризують тісноту зв'язку за умови, що інша незалежна змінна стала. Відтак, зв'язок між коефіцієнтом технічного захисту інформації та коефіцієнтом програмної захищеності інформації є значним, оскільки коефіцієнт кореляції становить 0,89. Значний зв'язок, зі значенням коефіцієнту кореляції 0,94 простежується між коефіцієнтом технічного захисту інформації та коефіцієнтом підготовленості персоналу до розпізнавання загроз. Найміцніший зв'язок простежується між коефіцієнтом програмної захищеності інформації коефіцієнтом програмної захищеності інформації, значення тісноти зв'язку – 0,98. Зазначене свідчить про необхідність оптимізації програмно, апаратної та кадрової складової системи інформаційної безпеки підприємства.

В результаті обчислень, багатофакторна виробнича лінійна регресія має вигляд:

$$Yr = -94{,}550+130{,}746X_1+3{,}67X_3 \qquad (3.1)$$

В результаті обробки даних отриманий загальний коефіцієнт детермінації 0,91. Загальний коефіцієнт детермінації говорить про тісний зв'язок між факторами (X_1, $X_{3,}$) та показником Y, тобто коефіцієнтом технічного захисту інформації, коефіцієнтом підготовленості персоналу до розпізнавання загроз та показником рентабельності «Назва підприємства», а також, що варіація рентабельності господарської діяльності підприємства на 91 % зумовлюється досліджуваними факторами, введеними в кореляційну модель. Це означає, що вибрані фактори суттєво впливають на досліджуваний показник – рентабельність діяльності підприємства.

Наступний етап – аналіз коефіцієнта еластичності, що розраховується для кожного із факторів. Коефіцієнт еластичності показує на скільки

відсотків зміниться показник, тобто рентабельність досліджуваного підприємства, якщо фактор зміниться на 1 %. Якщо коефіцієнт технічного захисту інформації зросте на 1 %, то рентабельність збільшиться на 1,65 %, а якщо коефіцієнт підготовленості персоналу до розпізнавання загроз, зросте на 1 %, то результативний показник збільшиться на 1,15 %.

Прогнозне значення чистого прибутку «Назва підприємства» на 2023 р. становить 13,44 % (рис. 3.2).

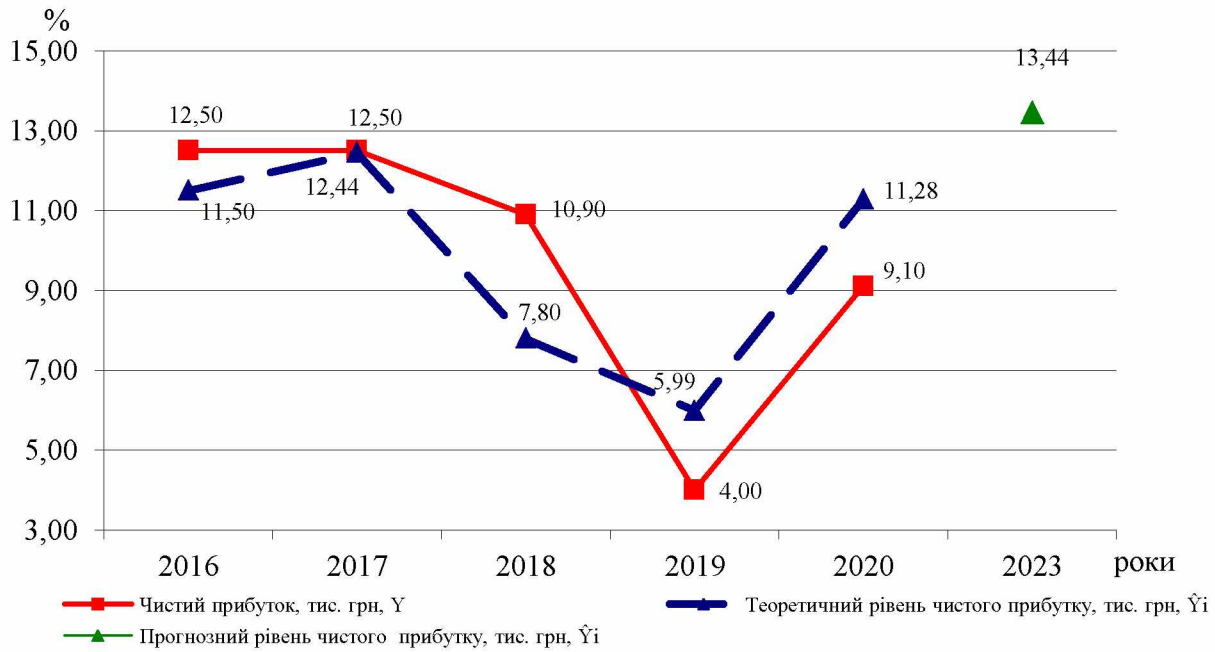

Рис. 3.2. Фактичний, теоретичний та прогнозний рівні чистого прибутку (збитку) «Назва підприємства» ххххххххххххххххххх району, 2016-2020, 2023 рр.

Отже, проаналізувавши явище мультиколінеарності, парні коефіцієнти кореляції, частинні коефіцієнти кореляції, коефіцієнт детермінації, коефіцієнти еластичності можна зробити висновок, що кожен фактор суттєво впливає на результативний показник – рентабельність «Назва підприємства».

Хоча аналізовані показники інформаційної безпеки підприємства й мають різний ступінь впливу на економічну результативність його діяльності, і з аналізу було виключено один із них, оскільки він мав високе, проте найнижче значення кореляційної залежності, їх потрібно розглядати в

єдності, оскільки між ними встановлений високий рівень взаємозв'язку, точніше між їх парами. Тому вдосконалення програмних або технічних або кадрово-організаційних аспектів управління інформаційною безпекою є недоцільним і не матиме синергічного позитивного ефекту, на відміну від їх комплексного вдосконалення, що можливо через актуалізацію моделі системи управління інформаційною безпекою досліджуваного підприємства.

Загалом, доцільно виділити ключові стратегічні напрями оптимізації системи інформаційного захисту підприємства відповідно стратегічних напрямів розвитку його діяльності (табл. 3.2).

Таблиця 3.2

Завдання та напрями інформаційного забезпечення безпеки та стратегічного розвитку «Назва підприємства»

Завдання стратегічного розвитку	Напрями інформаційного забезпечення безпеки підприємства
– підвищення економічної та фінансової міцності підприємства; – виробництво високоякісної сільськогосподарської продукції із урахуванням нових викликів та платоспроможності і вимог споживачів; – розширення інвестиційних можливостей; – нарощення експорту сільськогосподарської продукції; – впровадження стандартів виробництва та якості сільськогосподарської продукції; – модернізація матеріальної бази та виробничих потужностей; – генерування додаткових конкурентних переваг; – забезпечення економічної безпеки; – діджиталізація управління та бізнес-процесів тощо.	– автоматизація процедур накопичення, обробки, модуляції та зберігання документів; – впровадження нових інструментів інформаційно-комунікаційних технологій; – оптимізація ритмічності інформаційних потоків; – постійна верифікація стану інформаційної безпеки; – використання новітнього програмного забезпечення; – забезпечення інформаційного та кібер-захисту; – гармонізація внутрішніх та зовнішніх інформаційно-комунікаційних ланцюгів; – використання конвергенції пакетних послуг; – підвищення компетенцій працівників щодо інформаційно-комунікаційних технологій; – впровадження мережевих інструментів інформаційно-комунікаційних взаємодій; – усунення дублювання інформації; – мінімізація інформаційного шуму; – впровадження автоматизованих систем контролю; – удосконалення електронних форм внутрішньої бухгалтерської звітності; – моніторинг технологічних новинок.

Отже, інтеграція різних програмних продуктів з належним апаратно-технічним забезпеченням, а також спільна організаційна робота різних функціональних фахівців та впровадження стратегії інформатизації діяльності разом з політикою інформаційної безпеки на «Назва

підприємства»дозволить сформувати та наростити потужній інформаційний потенціал – основу сучасного конкурентоспроможного бізнесу.

3.2. Актуалізація моделі системи управління інформаційною безпекою на «Назва підприємства»

Інтеграція новітніх інформаційних технологій у виробничі та управлінські бізнес-процеси суб'єктів господарювання агросфери, розвиток потужних комп'ютерних систем, цифровізація об'єктів та соціально-економічних явищ, підвищили вимоги до рівня інформаційної безпеки та визначили необхідність розробки ефективних механізмів її захисту. Тому за сучасних умов, перевага надається не поодинокому впровадженню апаратних засобів захисту інформаційних ресурсів, програмного забезпечення оброки інформації, фізичних засобів захисту інформаційної системи, створенню комунікаційних каналів, а впровадженню системно-концептуального підходу до захисту інформації, в основу якого покладено твердження, що захист інформації є не одноразовим заходом і навіть не сукупністю заходів, а безперервним процесом, цілеспрямовано здійснюваним на всіх етапах створення та функціонування інформаційно-технологічних систем з ефективно побудованою системою менеджменту інформаційної безпеки. Відповідно, скоординовані дії, які виконуються з метою підвищення та підтримки на необхідному рівні інформаційної безпеки підприємства називаються управлінням інформаційною безпекою.

Враховуючи існуючі інформаційні, технічні, програмні засоби та, звичайно, фінансові ресурси «Назва підприємства», з метою покращення рівня інформаційного захисту, керівництву пропонується впровадити комплексну модель управління інформаційною безпекою. Впровадження зазначеної моделі передбачає поетапне проходження окремих стадій проектування, відображених на рис. 3.3.

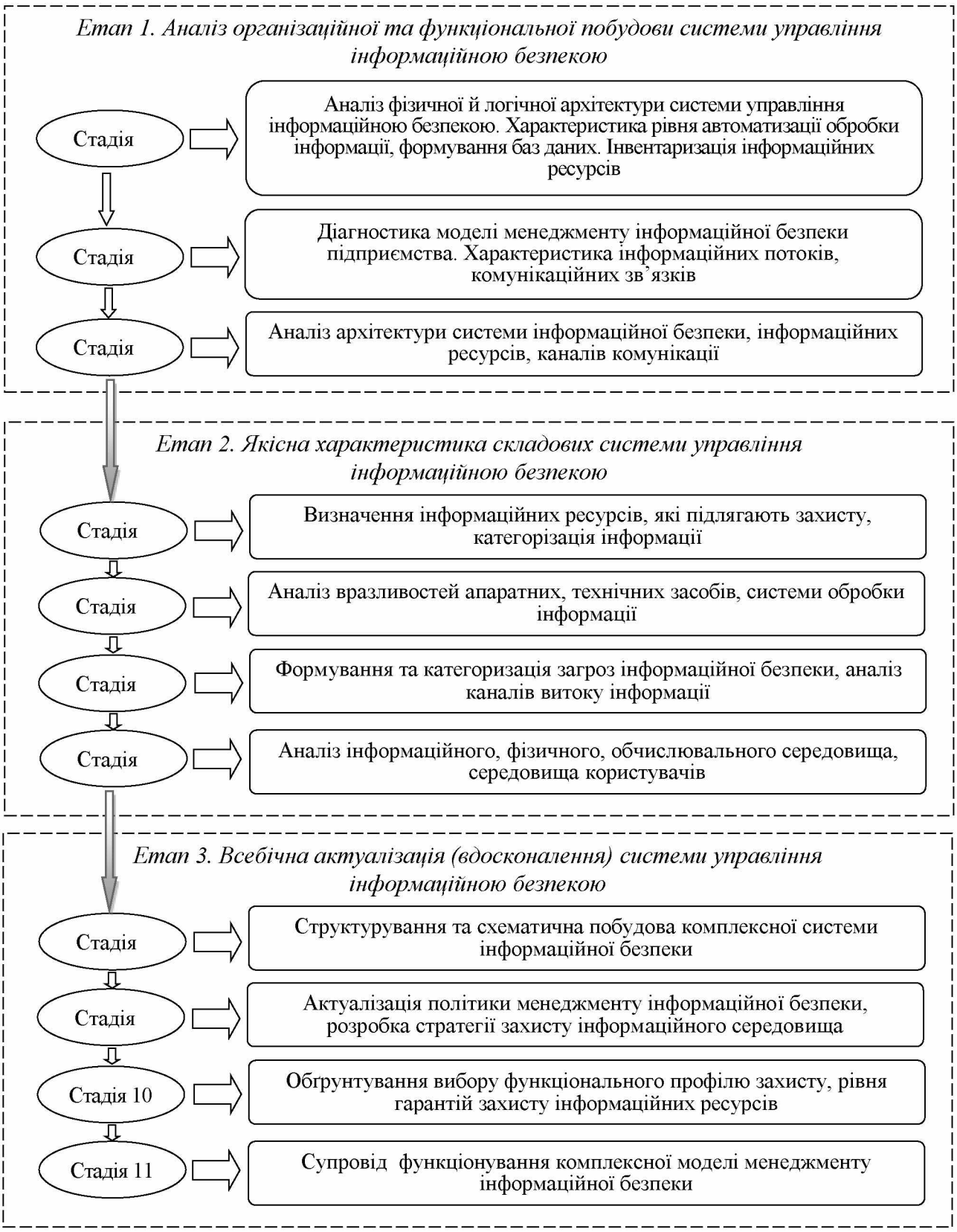

Рис. 3.3. Стадії проектування моделі управління інформаційною безпекою «Назва підприємства» xxxxxxxxxxxxxxxxxxxxx району [сформовано на основі **Ошибка! Источник ссылки не найден.**]

Пропонована модель управління інформаційною безпекою

«Назва підприємства» повинна враховувати й основні напрями забезпечення захисту інформаційної інфраструктури за певними рівнями, враховуючи концепцію «глибинного захисту» (рис. 3.4)

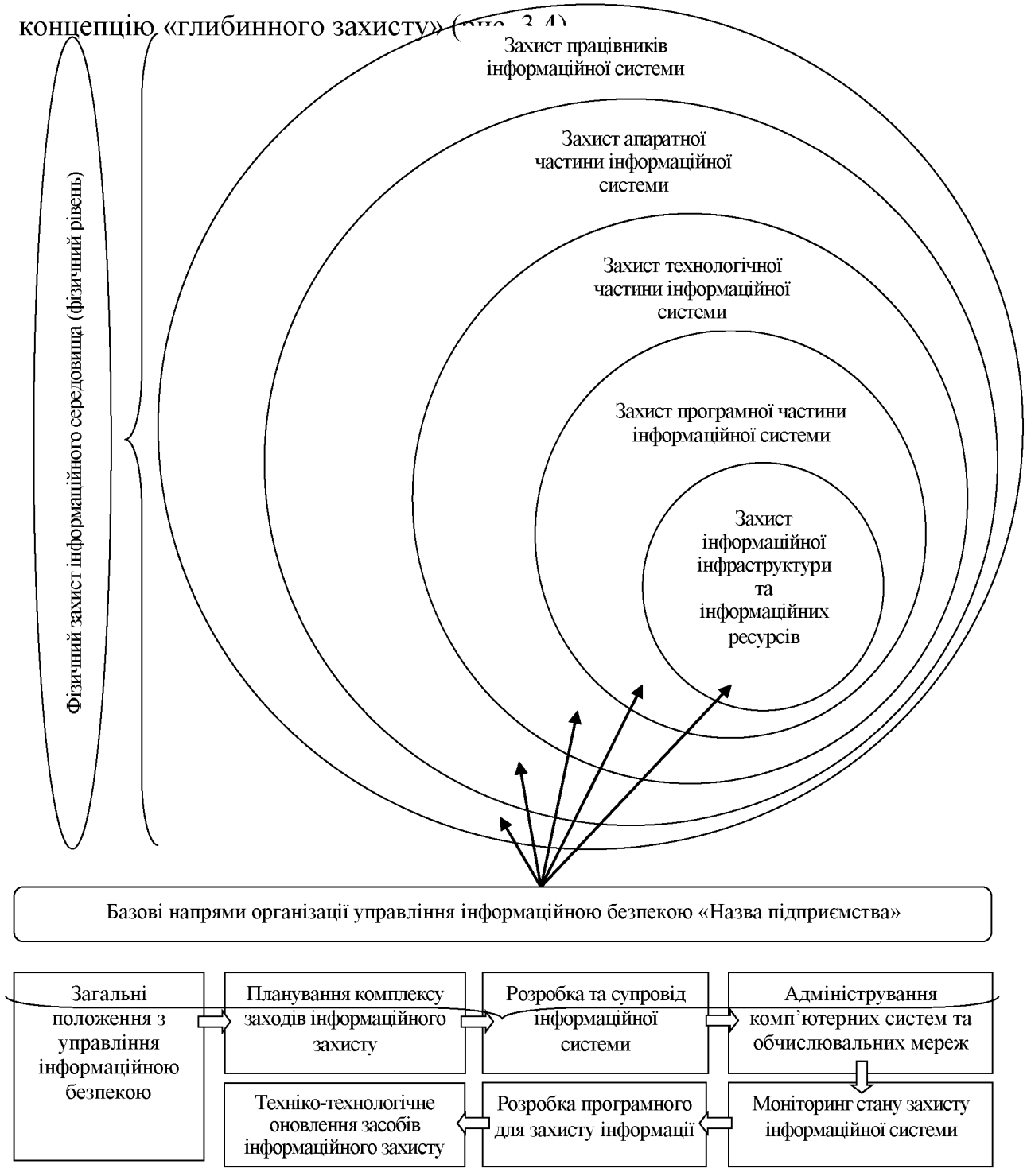

Рис. 3.4. Напрями та рівні організації управління інформаційною безпекою на основі концепції «глибинного захисту» на «Назва підприємства»

В межах пропонованої моделі, сукупність функціональних послуг захисту повинна являти собою набір елементарних функцій, виконання яких

у середовищі експлуатації дозволяє протистояти певній множині загроз для інформації. Враховуючи зазначене, зазначена модель повинна створюватися з використанням пакетного інформаційного забезпечення на програмно-керованих технічних засобах загального користування. Також вона повинна бути оснащена штатними і, при необхідності, додатковими позаштатними засобами технічного захисту інформації (рис. 3.5), які при спільному використанні формують комплекс засобів та механізмів захисту, що забезпечують потрібний рівень захищеності інформаційних ресурсів підприємства, тобто спроможності системи інформаційної безпеки протистояти впливам загроз. Також до штатних функціональних послуг пропонованої моделі системи управління інформаційною безпекою доцільно включити заходи ліквідації настання наслідків від реалізованих загроз та систему управління техніко-технологічного захисту інформації на пі

Рис. 3.5. Штатні та додаткові засоби технічного захисту інформації для «Назва підприємства» ххххххххххххххххххххх району

Водночас, реалізацію основних напрямів управління інформаційною

безпекою за різними рівнями та базовими напрямами доцільно забезпечити нормативно-організаційними та методичними засобами, серед яких особливе місце повинні політика, стратегія, модель поведінки працівника, навчання п

Рис. 3.6. Пропонована структурно-логічна схема реалізації нормативно-організаційних та методичних заходів актуалізації моделі системи управління інформаційною безпекою «Назва підприємства»

Реалізація напрямів управління інформаційною безпекою в інформаційній інфраструктурі підприємства не повинна перешкоджати реалізації виробничо-господарської діяльності. Тому в процесі управління інформаційною безпекою повинна бути здійснена оцінка ризиків порушення безпеки (рис. 3.7).

Рис. 3.7. Напрями оцінки ризиків порушення інформаційної безпеки «Назва підприємства» xxxxxxxxxxxxxxxxxxxxx району

На основі узагальнення зазначених пропозицій, модель функціональної побудови системи управління інформаційною «Назва підприємства» потрібно модифікувати відповідно до вигляду відображеного на рис. 3.8.

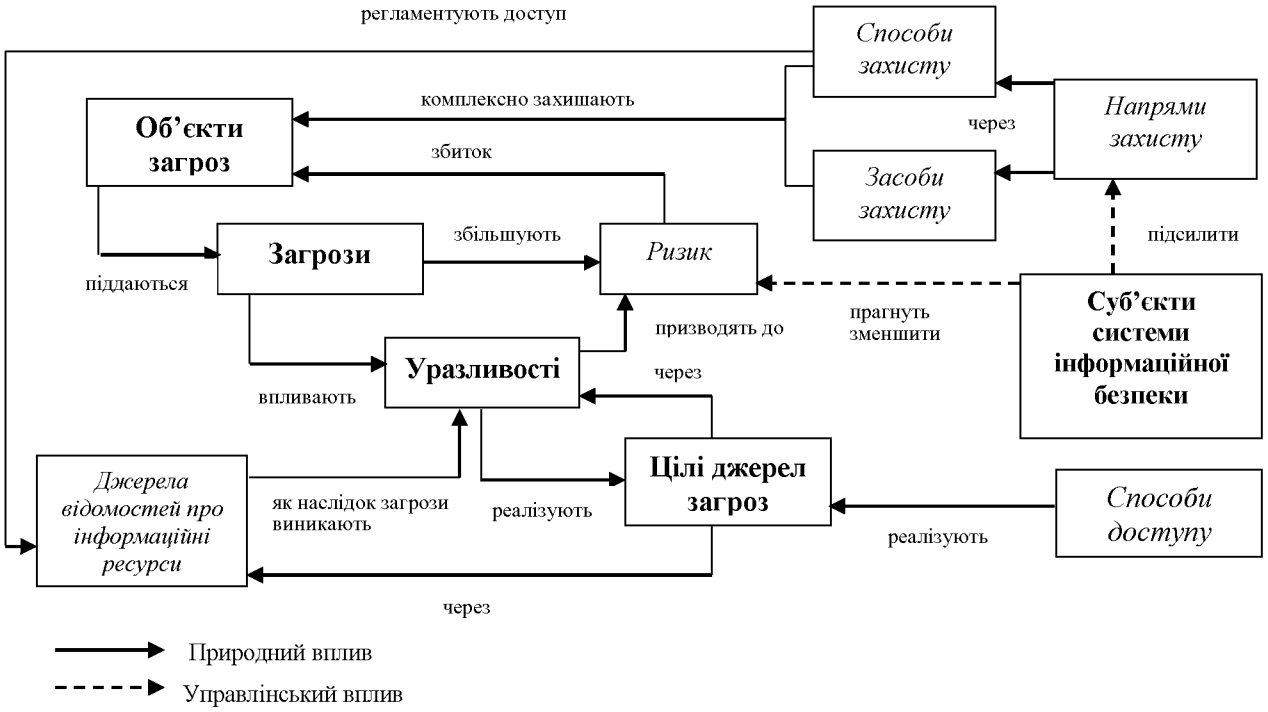

Рис. 3.8. Пропонована функціональна модель управління інформаційною безпекою на «Назва підприємства» xxxxxxxxxxxxxxxxxxxxx району [сформовано на основі **Ошибка! Источник ссылки не найден.**]

Зазначена модель, на відміну від існуючої на підприємстві, має більш широкий функціонал та спрямована на одночасне застосування декількох

напрямів забезпечення інформаційної безпеки та одному або декількох рівнях, що за незмінних програмних, апаратних та техніко-технологічних засобах матиме значно вищу ефективність захисту інформаційної інфраструктури «Назва підприємства».

Враховуючи вимоги до моделі менеджменту інформаційної безпеки підприємства, окреслено основні принципи заходів інформаційного захисту, серед яких: обґрунтованість доступу, глибина контролю доступу, розмежування потоків інформації, чистота повторно використовуваних ресурсів, персональна відповідальність, цілісність засобів захисту. Реалізація зазначених принципів здійснюється через застосування «монітору звернень», який передбачає контроль запитів до даних або програмного забезпечення зі сторони користувача або його програмного забезпечення. Схематична формалізація пропонованого механізму такого «монітору звернень» відображена на рис. 3.9.

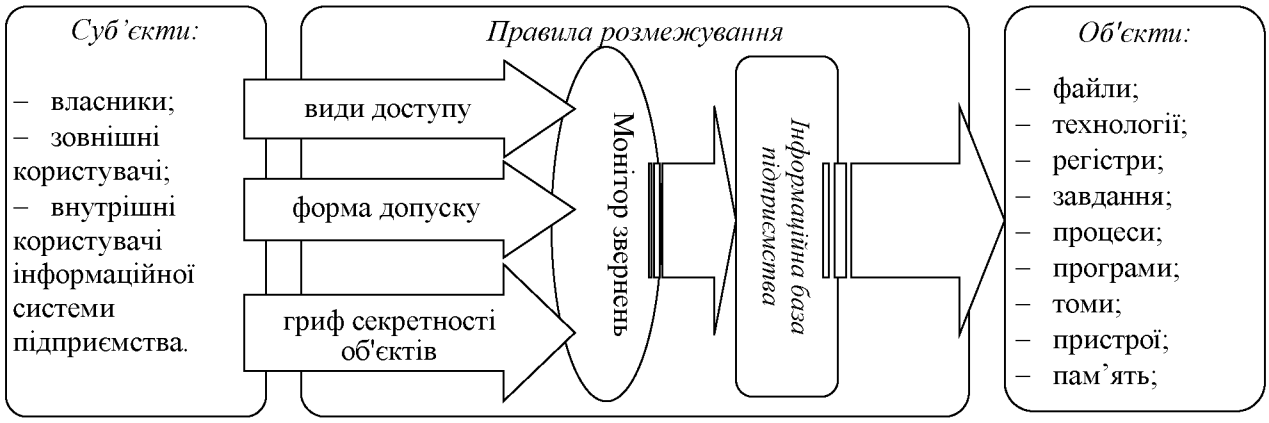

Рис. 3.9. Формалізація «монітору звернень» користувачів інформаційних ресурсів «Назва підприємства» ххххххххххххххххххххх району

Практичне застосування монітора звернень передбачає розробку та дотримання особливих правил розмежування доступу, що забезпечує захист інформаційних ресурсів. Доцільно пам'ятати, що при актуалізації системи управління інформаційною безпекою слід зважати на принцип: витрати на систему захисту інформації та систему менеджменту інформаційної безпеки повинні відповідати цінності (вартості) інформаційних ресурсів, які підлягають захисту, а також взаємоспівставними зі збитками, які може

отримати підприємство при порушенні системи інформаційного захисту.

Висновки до розділу 3

За результатами рекомендаційного розділу дослідження слід зазначити:

1. Встановлено, що базовими аспектами будь-якої інформаційної системи сільськогосподарського підприємства є техніко-технологічне устаткування, програмне забезпечення та кадровий потенціал, який здійснює процеси управління інформаційним захистом. Запропоновано розглядати напрями оптимізації системи захисту інформації на «Назва підприємства» саме в зазначених площинках шляхом формування багатофакторної виробничої регресії. Характеризуючи коефіцієнти кореляції, то можна простежити, що кожен із факторів (коефіцієнт технічного захисту інформації, коефіцієнт програмної захищеності інформації та коефіцієнт підготовленості персоналу до розпізнавання загроз) суттєво впливає на рентабельність діяльності. Вдосконалення даних напрямів дозволить отримати прогнозне значення рентабельності – 13,44 %.

2. Враховуючи існуючі інформаційні, технічні, програмні засоби та, звичайно, фінансові ресурси «Назва підприємства», з метою покращення рівня інформаційного захисту, керівництву пропонується впровадити комплексну модель управління інформаційною безпекою. Пропонована модель повинна враховувати й основні напрями забезпечення захисту інформаційної інфраструктури за певними рівнями, враховуючи концепцію «глибинного захисту». Зважаючи на зазначене, модель повинна створюватися з використанням пакетного інформаційного забезпечення на програмно-керованих технічних засобах загального користування. Також вона повинна бути оснащена штатними і, при необхідності, додатковими позаштатними засобами технічного захисту інформації. Водночас, реалізацію основних напрямів управління інформаційною безпекою за різними рівнями та базовими напрямами доцільно забезпечити нормативно-організаційними

та методичними засобами, серед яких особливе місце повинні політика, стратегія, модель поведінки працівника, навчання персоналу та інші.

ВИСНОВКИ

Здійснивши дослідження на тему «Управління інформаційною безпекою підприємства (на матеріалах «Назва підприємства» ххххххххххххххххххх району)» доцільно зробити наступні висновки:

1. Впровадження цифрових технологій у сільськогосподарське виробництво в умовах сьогодення, виступає одним із найважливіших елементів стратегічного розвитку агропродовольчої сфери. З урахуванням поточного стану функціонування вітчизняного сільського господарства та прискорення процесів зміни зовнішнього та внутрішнього середовища, цифрова трансформація сільськогосподарського виробництва особливо актуальна, оскільки є значним джерелом для забезпечення суттєвого економічного зростання, оскільки спрямована на збільшення кількості та якості врожаю, мінімізація фінансових вкладень, зниження трудомісткості та підвищення продуктивності виробництва, зменшення шкідливого впливу на довкілля, зниження залежності від людського фактору та девіації щодо врожайності, тощо.

2. Етимологічні аспекти трактування поняття «інформаційної безпеки» визначають дане поняття як: стан захищеності інтересів працівників підприємства в інформаційному бізнес середовищі; захищеність встановлених законом правил, за якими відбуваються інформаційні процеси підприємства; відносини, пов’язані із захистом важливих інтересів від реальних та потенційних загроз в інформаційному просторі; невід’ємну частину політичної, економічної, оборонної та інших складових безпеки підприємства, стан захищеності інформаційного простору підприємства. Забезпечення інформаційної безпеки на підприємствах агропродовольчої сфери переважно здійснюється за загальним сценарієм формування системи інформаційного захисту на будь-якому підприємстві, проте має деякі особливості.

3. Підприємство «Назва підприємства» здійснює виробництво продукції

рослинництва та її реалізацію. Управління підприємством здійснюють: загальні збори учасників підприємства, директор та провідні фахівці. Отриманий результат аналізу виробничо-господарських показників діяльності вказує на поступове зниження ефективності діяльності підприємства, про що свідчить: зниження питомої ваги оборотних активів, переважну частину яких становлять запаси (56,7 % у 2020 р. порівняно з 70,4 % у 2016 р.) та дебіторська заборгованість (43,3 % у 2020 р. порівняно з 27,6 % у 2016 р.); переважання у структурі джерел фінансування позичкового капіталу, значення якого становило у 2020 р. – 65903,0 тис. грн, тобто 57,0 %; зменшення загальної чисельності персоналу на 8 осіб порівняно з 2016 р.; зменшення загальної земельної, власної та орендованої площі підприємства, яка складає у звітному році 3529 га, що на 14 га менше у порівняні з 2016 р. або ж на 0,4 %.

4. Простежується низький рівень витрат на формування інформаційного забезпечення підприємства, що обумовлює і низький рівень інформаційної безпеки. Найвищий їх обсяг спостерігався у 2020 р. і становив 31,4 тис. грн, а найменший у 2017 р. – 19,3 тис. грн. Основною статтею витрат на інформатизацію діяльності є витрати на ремонт та технічне обслуговування офісної та електронно-обчислювальної техніки. Протягом аналізованого періоду найбільш значимими зовнішніми загрозами визначено шкідливе програмне забезпечення та спам, який часто є його носієм. Основними внутрішніми загрозами інформаційної безпеки є: вразливість програмного забезпечення, випадкові витоки від працівників та навмисні витоки інформації з вини співробітників.

5. Організаційна та функціональна модель управління інформаційною безпекою є традиційними та передбачають наявність класичних складових для забезпечення захисту інформаційної інфраструктури. Самостійний підрозділ із захисту інформації на підприємстві відсутній. Відповідальність за захист інформації розподілена між директором та окремими фахівцями. Стратегія, політика та цілі управління інформаційною безпекою не мають чіткого формалізованого окреслення і визначаються як загальноприйняті для

підприємств приналежних до агропродовольчої сфери.

6. Базовими аспектами інформаційної системи та системи захисту інформації «Назва підприємства» окреслено техніко-технологічне устаткування, програмне забезпечення та кадровий потенціал, що забезпечує реалізацію процесів управління інформаційною безпекою. Запропоновано розглядати напрями оптимізації системи захисту інформації саме в зазначених площинках, шляхом формування багатофакторної виробничої регресії. Характеризуючи коефіцієнти кореляції, то можна простежити, що кожен із факторів (коефіцієнт технічного захисту інформації, коефіцієнт програмної захищеності інформації та коефіцієнт підготовленості персоналу до розпізнавання загроз) суттєво впливає на рентабельність діяльності підприємства, а синкретична оптимізація цих напрямів дозволить отримати прогнозне значення рентабельності – 13,44 % у 2023 р.

7. Враховуючи існуючі інформаційні, технічні, програмні засоби та, звичайно, фінансові ресурси «Назва підприємства», з метою покращення рівня інформаційного захисту, керівництву пропонується впровадити комплексну модель управління інформаційною безпекою. Пропонована модель повинна враховувати й основні напрями забезпечення захисту інформаційної інфраструктури за певними рівнями, враховуючи концепцію «глибинного захисту». Зважаючи на зазначене, модель повинна створюватися з використанням пакетного інформаційного забезпечення на програмно-керованих технічних засобах загального користування. Також вона повинна бути оснащена штатними і, при необхідності, додатковими позаштатними засобами технічного захисту інформації. Враховуючи вимоги до моделі менеджменту інформаційної безпеки підприємства, окреслено основні принципи заходів інформаційного захисту, реалізація яких здійснюється через застосування «монітору звернень», що передбачає контроль запитів до даних або програмного забезпечення зі сторони користувача або його програмного забезпечення. Водночас, реалізацію основних напрямів управління інформаційною безпекою за різними рівнями та базовими напрямами доцільно забезпечити нормативно-організаційними та

методичними засобами, серед яких особливе місце повинні політика, стратегія, модель поведінки працівника, навчання персоналу та інші.