ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут економіки, управління, права та інформаційних технологій

Кафедра менеджменту ім. І.А. Маркіної

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти «Магістр»

на тему «Управління інформаційною безпекою підприємства в сучасному бізнес-середовищі»

Виконав: здобувач вищої освіти
за освітньою програмою
Бізнес-адміністрування
спеціальності 073 Менеджмент
ступеня вищої освіти магістр
групи 1
заочної форми здобуття освіти
Боголюбський Олег Євгенович

Керівник:
Дячков Дмитро Володимирович
Рецензент:
Клочан В'ячеслав Васильович

Полтава 2025 року

ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
Навчально-науковий інститут економіки, управління, права та інформаційних технологій
Кафедра менеджменту ім. І. А. Маркіної

Освітня програма Бізнес-адміністрування
Спеціальність 073 Менеджмент
Рівень вищої освіти магістерський

ЗАТВЕРДЖУЮ
Завідувач кафедри _____
Тетяна ВОРОНЬКО-НЕВІДНИЧА
19 травня 2025 року

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Боголюбський Олег Євгенович

1. Тема роботи «Управління інформаційною безпекою підприємства в сучасному бізнес-середовищі (на матеріалах «ПІДПРИЄМСТВА»)», керівник роботи доктор економічних наук, професор, професор кафедри менеджменту ім. І.А. Маркіної Дячков Д. В.

Затверджено засіданням кафедри протокол № 32 від «19» травня 2025 р.

2. Строк подання здобувачем вищої освіти роботи «24» листопада 2025 р.

3. Вихідні дані до роботи:
- звітність організації за 2020-2024 рр.
- інші інформаційні дані:
– нормативно-довідкова література,
– літературні джерела,
– Інтернет-джерела,
– власні спостереження автора

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

Розділ 1. Теоретичні аспекти системи управління інформаційною безпекою підприємства в сучасному бізнес-середовищі

Розділ 2. Аналіз діяльності та системи управління інформаційною безпекою досліджуваного підприємства

Розділ 3. Шляхи впровадження заходів інформаційної безпеки виробництва

5. Перелік графічного матеріалу: схеми, рисунки, графіки, діаграми за темою та об’єктом дослідження.

6. Консультант із застосування прикладних комп’ютерних програм

Прізвище, ініціали та посада консультанта	Підпис, дата	
	завдання видала	завдання отримала
Копішинська Олена Петрівна, кандидат фізико-математичних наук, доцент, професор кафедри інформаційних систем та технологій	01.09.2025	30.09.2025

7. Дата видачі завдання: «19» травня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів роботи	Строк виконання етапів кваліфікаційної роботи	Примітка
1	Вибір і затвердження теми роботи	12.05.25-20.05.25	виконано
2	Складання та погодження розгорнутого плану та завдання на кваліфікаційну роботу	12.05.25-20.05.25	виконано
3	Опрацювання джерел інформації	21.05.25-02.06.25	виконано
4	Збір, вивчення і обробка інформації, необхідної для виконання роботи	03.06.25-20.07.25	виконано
5	Виконання теоретико-методологічного розділу роботи	21.07.25-22.08.25	виконано
6	Виконання дослідницько-аналітичного розділу роботи	25.08.25-17.10.25	виконано
7	Виконання проектно-рекомендаційного розділу роботи	20.10.25-20.11.25	виконано
8	Оформлення тексту роботи та перевірка на наявність текстових запозичень	19.11.25-24.11.25	виконано
9	Попередній захист роботи на кафедрі	24.11.25	виконано
10	Доопрацювання роботи з урахуванням зауважень і пропозицій	25.11.25-27.11.25	виконано
11	Нормоконтроль	24.11.25-28.11.25	виконано
12	Захист кваліфікаційної роботи	04.12-05.12.25	

Здобувач вищої освіти Олег БОГОЛЮБСЬКИЙ

Керівник роботи Дмитро ДЯЧКОВ

АНОТАЦІЯ

Боголюбський О.Є. Управління інформаційною безпекою підприємства в сучасному бізнес-середовищі (на прикладі ПрАТ «Фірма «Полтавпиво»). – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття ступеня вищої освіти магістр за освітньо-професійною програмою Бізнес-адміністрування, спеціальністю 073 Менеджмент. – Полтавський державний аграрний університет, Полтава, 2025.

Досліджено теоретичні, методичні та прикладні аспекти управління інформаційною безпекою підприємства в ринкових умовах господарювання, загальні тенденції та досвід з управління інформаційною безпекою в Україні.

Проведено загальний аналіз організаційно-економічної діяльності товариства, здійснено аналіз системи управління інформаційною безпекою, зокрема, узагальнені потенційні загрози інформації, що обробляється в АС досліджуваного підприємства, розроблена модель загроз для інформації та сформована модель порушника для об'єкта інформаційної діяльності підприємства.

Розроблено шляхи вдосконалення управління інформаційною безпекою, зокрема, план управління ризиками, який передбачає визначення переліку потенційних ризиків, імовірності виникнення цих ризиків та їхнього негативного впливу, шляхів запобігання або їх пом'якшення, розгляд непередбачуваних ситуацій та встановлення точок запуску для активізації заходів у разі настання непередбачуваної ситуації та розроблена матриця ризиків ПрАТ «Фірма «Полтавпиво» з визначенням превентивні заходи по їх недопущенню. Розроблена ієрархічна структура робіт (WBS), календарний план-графік робіт по проекту з модернізації виробництва, визначені всі учасники проєкту із зазначенням строків їх зайнятості по проекту та відсотка завантаженості, визначений план управління командою проекту та створена матриця відповідальності (RACI Matrix) учасників проекту.

Ключові слова: підприємство, інформація, інформаційна безпека, «бізнес-довідка», стратегія, політика захисту інформації, управління, ризики, загрози.

ЗМІСТ

ВСТУП

Актуальність теми. В сучасних умовах інформаційної епохи XXI століття, інформаційна безпека стає надзвичайно важливою, а проблеми її гарантування набувають особливої гостроти. Швидке поширення інформаційних та комп'ютерних технологій у всіх галузях життя суспільства та зростання економіки роблять особливо актуальним пошук обґрунтованих та дієвих способів забезпечення інформаційної безпеки. В умовах сьогодення, коли методи управління в організаціях постійно розвиваються, питання інформаційної безпеки стає все більш очевидним як ключовий інструмент для ефективної роботи компанії. Інформаційна безпека впливає на всі сфери діяльності організації та тісно пов'язана з її економічною безпекою. Економічна безпека підприємства є широким поняттям, що включає фінансову, фізичну, техніко-технологічну, кадрову, правову та інформаційну безпеку. У сучасному бізнес-середовищі інформаційна безпека є одним з найважливіших факторів, що забезпечують його існування та подальший розвиток.

Вивчення комплексу проблем, пов’язаних з інформаційною безпекою підприємства розроблено у дослідженнях зарубіжних та українських вчених-економістів, зокрема: Азаров А. М., Барановський О. М., Захарченко В. А., Береза А. В., Величко Р. С., Гуменюк О. О., Дячков Д. В., Задорожна Н. О., Кириленко С. В., Ковальчук О. П., Кузьменко О. П., Нікітін Л. М., Нестеренко О. Г., Полозова Т. В., Сазонова Т.О., Скрипник А. І., Харченко О. М., Шевченко А. А., Федорова Л. В. Є. та ін.

Мета і завдання дослідження. Метою кваліфікаційної роботи є обґрунтування теоретичних аспектів та розробка рекомендацій щодо удосконалення управління інформаційною безпекою підприємства.

Завданнями кваліфікаційної роботи є:

визначити сутність, роль та значення системи управління інформаційною безпекою підприємства в ринкових умовах господарювання;

дослідити загальні тенденції та досвід з управління інформаційною безпекою в Україні;

проаналізувати об’єкт і суб’єкт системи управління підприємством;

проаналізувати техніко-економічні показники діяльності підприємства;

проаналізувати систему управління інформаційною безпекою підприємства;

розробити моделі загроз для інформації та моделі порушника для об’єкта інформаційної діяльності;

розробити шляхи впровадження заходів інформаційної безпеки для модернізація виробництва підприємства.

Об’єктом дослідження кваліфікаційної роботи є процес управління інформаційною безпекою підприємства в сучасному бізнес-середовищі.

Предметом дослідження є система управління інформаційною безпекою підприємства.

Методи наукових досліджень. У процесі виконання кваліфікаційної роботи було застосовано комплекс наукових методів. Зокрема, використано методи теоретичного пізнання (абстрагування, аналіз і синтез, ідеалізація, індукція та дедукція, уявне моделювання, перехід від абстрактного до конкретного) та методи емпіричного дослідження (спостереження, порівняння, вимірювання). Зазначені методи взаємодоповнювали один одного та забезпечили всебічне розв’язання поставлених завдань.

Інформаційною базою роботи виступають наступні джерела: наукова література та розробки вітчизняних і зарубіжних авторів з управління інформаційною безпекою на підприємствах, статистична та бухгалтерська звітність підприємства за 2020-2024 роки.

Елементи наукової новизни полягають у формуванні основних принципів інформаційної безпеки, методів запобігання та ліквідації загроз інформаційній безпеці, визначенні класів загроз інформаційної безпеки організації в сучасних умовах господарювання.

Практична значущість одержаних результатів для підприємства полягає в розробці моделі загроз для інформації та моделі порушника для об’єкта інформаційної діяльності підприємства, розробці плану управління ризиками, який передбачає визначення переліку потенційних ризиків, імовірності їх виникнення та негативного впливу, а також шляхів запобігання чи їх пом’якшення. Результатом цього стала розробка матриці ризиків підприємства та визначено превентивні заходи по їх недопущенню.

Апробація результатів дослідження. Результати проведеного дослідження були апробовані на Міжнародній науково-практичній конференції [9, 42].

Публікації. Результати досліджень було опубліковано в:

1. Сазонова Т.О., Боголюбський О.Є. Стратегічне управління інформаційною безпекою підприємства. *Менеджмент XXI століття: глобалізаційні виклики*: матеріали IX Міжнародної науково-практичної конференції. 15 травня 2025 р. Полтава: ПДАУ. 2025. 677 с.

2. Боголюбський О.Є. Сучасні проблеми управління інформаційною безпекою підприємства. *Менеджмент XXI століття: глобалізаційні виклики:* матеріали IX Міжнародної науково-практичної конференції. 15 травня 2025р. Полтава: ПДАУ. 2025. 677 с.

Структура та обсяг кваліфікаційної роботи. Кваліфікаційна робота складається із вступу, трьох розділів, висновків, списку використаних джерел та додатків. Основний зміст кваліфікаційної роботи викладено на 72 сторінках машинописного тексту. Робота містить 5 таблиць, 10 рисунків, 18 додатків та список використаних літературних джерел, що налічує 55 найменувань.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

1.1. Сутність, роль та значення системи управління інформаційною безпекою підприємства в ринкових умовах господарювання

Під інформаційною безпекою розуміють захист інформації та відповідної інфраструктури від ненавмисних або навмисних дій природного чи техногенного характеру, що можуть завдати шкоди власникам інформаційних ресурсів або користувачам інформації та підтримуючої інфраструктури [16, с.15].

Для створення ефективної системи інформаційної безпеки підприємства першочергово необхідно визначити учасників інформаційних відносин та їхні потреби, пов'язані з використанням інформаційних систем. Вимоги до інформаційної безпеки можуть значно відрізнятися залежно від категорії цих суб'єктів. Інформаційна безпека є всебічною, складною і актуальною проблемою. Для побудови захищеної системи потрібний комплексний підхід, що опрацьовує аспекти інформаційної безпеки на адміністративному, процедурному і програмно-технічному рівнях [5, с.42].

Термін «інформаційна безпека» з'явився одночасно з розвитком засобів інформаційних комунікацій та усвідомленням людських інтересів, яким може бути завдано шкоди через вплив на ці засоби. Якщо інформаційна безпека означає захищеність інформаційного простору, то захист інформації є комплексом заходів, спрямованих на запобігання витоку інформації, що підлягає охороні, а також на протидію несанкціонованим або випадковим діям, спрямованим на цю інформацію. Інакше кажучи, інформаційна безпека (безпека даних) характеризується відсутністю неприйнятного рівня ризику, пов'язаного з витоком інформації через технічні канали, а також з несанкціонованими або випадковими діями, спрямованими на цю інформацію

або інші ресурси, що використовуються в автоматизованій інформаційній системі.

Захист інформації в інформаційній системі підприємства має здійснюватись на рівні апаратного та програмного забезпечення, а також забезпечення зв'язку (комунікації). При цьому механізми захисту розділяються на фізичний і організаційний рівні. Основоположними принципами інформаційної безпеки є [34, с.52]: гарантування цілісності та збереження даних, що передбачає їх надійне зберігання без пошкоджень; забезпечення конфіденційності інформації, тобто її недоступність для неавторизованих осіб; надання доступу до інформації всім авторизованим користувачам з одночасним контролем за процесами її використання; забезпечення безперебійного доступу до інформації в будь-який час, коли вона може знадобитися підприємству. Ці принципи можна реалізувати лише в інтегрованій системі інформаційної безпеки, що передбачає наступні функції [37, с.131]: розробка стратегії та політики інформаційної безпеки; оцінка ризиків, що включає аналіз ситуацій, які можуть призвести до порушення функціонування інформаційної системи, а також до втрати або розкриття даних; розробка плану заходів для забезпечення інформаційної безпеки; підготовка плану дій на випадок надзвичайних ситуацій; вибір технічних інструментів для гарантування інформаційної безпеки.

В умовах посиленої конкуренції підприємства все частіше стикаються з загрозами безпеці від суперників, які експлуатують залежність бізнесу від інформаційних технологій з метою промислового шпигунства та здобуття переваг на ринку. У жорсткому конкурентному середовищі здатність підприємства ефективно використовувати свої інформаційні ресурси безпосередньо впливає на його конкурентоздатність та загальний успіх діяльності [8, с.46].

Сучасні підприємства для попередження та усунення загроз інформаційній безпеці застосовують правові, програмно-технічні та організаційно-економічні підходи [43, с.227].

Правові методи включають розробку та впровадження системи законодавчих актів і положень, які регулюють інформаційні відносини в суспільстві, а також керівних і нормативно-методичних документів, спрямованих на забезпечення інформаційної безпеки [50, с. 36].

Програмно-технічні методи це сукупність методів, основна захисна функція яких реалізується комплексом програмно-технічних засобів. Їх розрізняють за такими критеріями: за метою дій: попередження, виявлення, знаходження, ліквідація наслідків; за активністю: пасивні, напівактивні, активні; за рівнем забезпечення захисту: системи слабкого захисту, системи сильного захисту, системи дуже сильного захисту, системи особливого захисту [9, с.118].

Програмно-технічні методи спрямовані на запобігання витоку інформації, унеможливлення несанкціонованого доступу до неї, відвернення впливів, що можуть призвести до знищення, пошкодження, спотворення інформації або до збоїв у роботі засобів інформатизації. Ці методи також включають виявлення прихованих пристроїв, унеможливлення перехоплення інформації технічними засобами та використання криптографічних інструментів для захисту інформації під час її передачі каналами зв'язку.

Організаційно-економічні методи включають створення та підтримку працездатності систем захисту секретної та конфіденційної інформації, їх сертифікацію згідно з вимогами інформаційної безпеки, ліцензування діяльності у цій сфері, стандартизацію способів і засобів захисту інформації, а також контроль за діями персоналу в захищених інформаційних системах. Серед організаційно-економічних методів інформаційної безпеки важливе місце займають: методи оцінки важливості інформації, що потребує захисту, та інформаційних ризиків підприємства; методи оцінки вразливості інформації та системи, в якій вона функціонує; методи, що використовуються для економічного обґрунтування затрат на інформаційну безпеку [13, с.114].

Інформаційна безпека відображає рівень захищеності інформаційного середовища та ефективність інформаційного забезпечення управлінських процесів на підприємстві. Забезпечення інформаційної безпеки підприємства

можна розглядати як взаємодію трьох основних компонентів [48, с.171]: підсистеми інформаційного забезпечення управління підприємством; підсистеми захисту інформаційного середовища підприємства; та підсистеми оцінки рівня інформаційної безпеки. Основними завданнями підсистеми інформаційного забезпечення управління є: збір необхідних даних; їх обробка та систематизація; оцінка й аналіз отриманої інформації; прогнозування різних аспектів діяльності підприємства; а також надання потрібної інформації особам, які приймають управлінські рішення [11, с.215]. Для ефективної роботи цієї підсистеми необхідне безперервне виконання всіх зазначених завдань.

Забезпечення захисту інформаційного середовища підприємства охоплює протидію як зловмисним діям конкурентів і власних співробітників, так і нейтралізацію ненавмисних внутрішніх негативних впливів. Для ефективного захисту інформаційного середовища підприємства необхідно послідовно виконувати такі етапи: аналіз ризиків для інформаційної безпеки; планування та розробка заходів щодо її забезпечення; оперативне впровадження запланованих дій [14, с.89].

Основні ключові напрямки за якими необхідно проводити діагностику рівня інформаційної безпеки підприємства наступні: оцінка програмно-технічної захищеності інформації; оцінка інформаційної надійності персоналу; оцінка інформації, що надається особам, що приймають рішення, інформаційною службою підприємства [15, с.173].

Для забезпечення інформаційної безпеки підприємства необхідно вирішити наступні ключові задачі [37, с.3]: забезпечення програмно-технічного захисту від несанкціонованого доступу до закритої інформації; забезпечення захисту від промислового шпигунства; забезпечення безпеки підтримки зв’язків з контрагентами; організація збору, оцінки, обробки, систематизації та аналізу інформації, необхідної для забезпечення ефективного процесу управління підприємством.

Ризики для інформаційної безпеки являють собою можливі джерела небажаних подій, які можуть завдати шкоди інформаційним ресурсам системи.

Будь-які загрози, спрямовані на програмне та апаратне забезпечення інформаційної системи, в кінцевому підсумку позначаються на безпеці інформаційних ресурсів, порушуючи основні принципи їхнього зберігання та оброблення. Зазвичай загрози інформаційній безпеці класифікують за способом їхньої реалізації. Виходячи з цього критерію, можна виокремити основні категорії загроз безпеки, спрямованих проти інформаційних ресурсів (рис. 1.1).

Рис. 1.1. Класи загроз інформаційної безпеки організації [33, с.95]

Загрози з використанням програмних засобів. Найпоширеніша категорія ризиків для конфіденційності, цілісності та доступності інформаційних ресурсів виникає через отримання внутрішніми та зовнішніми зловмисниками логічного доступу до інформації. Вони використовують можливості, які надає загальносистемне та прикладне програмне забезпечення. Наслідком таких загроз є неправомірний доступ до даних, інформації, що зберігається на комп'ютері системного адміністратора, конфігураційних даних технічних засобів, а також до відомостей, які передаються каналами зв'язку. До цього класу належать такі основні загрози: використання працівниками чужих

облікових даних; використання чужих облікових даних постачальниками послуг; використання чужих облікових даних сторонніми особами; неправомірний доступ до програмного забезпечення; розповсюдження шкідливого програмного забезпечення; зловживання системними ресурсами; заперечення авторства переданої інформації; помилки в маршрутизації; використання телекомунікацій для несанкціонованого доступу працівниками організації, постачальниками послуг, сторонніми особами; несправність засобів керування мережею, контролерів або мережевих серверів; збої системного та мережевого програмного забезпечення; збої прикладного програмного забезпечення.

Загрози технічним засобам. Ризики для доступності та цілісності інформації (незалежно від того, чи вона зберігається, обробляється, чи передається мережами) виникають через фізичні пошкодження та збої в роботі технічних засобів системи та допоміжних комунікацій. Наслідком цих загроз може стати повне або часткове знищення інформації, відмова в наданні послуг користувачам та обробці їхніх запитів, а також неможливість отримати або передати інформацію. До цього класу належать такі основні загрози: пожежа, затоплення, стихійні лиха, а також несправності мережевого сервера, пристроїв зберігання даних, друкувального обладнання, мережевих комутаторів, мережевих шлюзів, мережевих інтерфейсів, систем електроживлення та кондиціонування повітря.

Загрози, обумовлені людським чинником. Ці ризики виникають через навмисні або ненавмисні дії персоналу чи сторонніх осіб, що призводять до порушень у роботі або непередбачуваних ситуацій з програмним чи апаратним забезпеченням інформаційної системи. До основних загроз цієї категорії належать: помилки операторів (адміністраторів при конфігурації системи); помилки користувачів під час експлуатації системи; помилки при роботі з програмним забезпеченням (адміністраторів під час технічного обслуговування); помилки при роботі з обладнанням (фахівців технічної підтримки під час профілактичних заходів); а також крадіжки, вчинені співробітниками.

Загрози що виникають при перехопленні електромагнітних випромінювань зображення монітора поширений спосіб розкрадання інформації. Це стає можливим через його побічне випромінювання, яке можна перехопити на відстані до 50 метрів. Щодо джерел загроз, вони можуть бути як зовнішніми, так і внутрішніми. Зовнішні джерела можуть бути випадковими або навмисними і мати різний рівень підготовки. До них належать: хакери, недобросовісні партнери, конкуренти, технічний персонал постачальників послуг. Внутрішні суб'єкти (джерела), як правило, є висококваліфікованими фахівцями у сфері розробки та експлуатації програмного забезпечення й технічних засобів, обізнаними зі специфікою виконуваних завдань, структурою, основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, і мають можливість використовувати штатне обладнання та технічні засоби мережі. До них належать: основний персонал (користувачі, програмісти, розробники), представники служби захисту інформації, допоміжний персонал (прибиральники, охорона), технічний персонал (життєзабезпечення, експлуатація).

Наявність політики інформаційної безпеки є ознакою зрілості та компетентності підприємства в питаннях захисту інформації [28, с.117]. Під політикою інформаційної безпеки розуміють сукупність вимог, правил, обмежень, рекомендацій, систему заходів, розподіл відповідальності між співробітниками та контрольні механізми, що регулюють порядок інформаційної діяльності в організації та спрямовані на досягнення й підтримку належного рівня інформаційної безпеки. Ефективна політика інформаційної безпеки визначає необхідний і достатній обсяг вимог безпеки, мінімально впливає на продуктивність праці, враховує специфіку бізнес-процесів підприємства, підтримується керівництвом, позитивно сприймається та виконується працівниками [17, с. 125]. Відсутність такої політики, навпаки, негативно відображається на оцінці діяльності підприємства та його позиціях у ринкових рейтингах.

1.2. Загальні тенденції та досвід з управління інформаційною безпекою в Україні

Сучасний розвиток суспільства визначається зростанням значення інформаційної сфери, яка охоплює сукупність інформаційних ресурсів, інфраструктури, учасників, що займаються збиранням, створенням, розповсюдженням і використанням інформації, а також систему норм і механізмів регулювання взаємовідносин у цій сфері.

За останні роки було впроваджено низку заходів, спрямованих на підвищення рівня інформаційної безпеки держави. У різних органах влади, на підприємствах, в установах і організаціях незалежно від форми власності здійснюються кроки щодо захисту інформації.

Однак проведений аналіз стану інформаційної безпеки в Україні свідчить, що її поточний рівень все ще недостатньо відповідає потребам держави та суспільства. На сучасному етапі політичного й соціально-економічного розвитку країни спостерігається загострення суперечностей між потребою суспільства у вільному доступі й обміні інформацією та необхідністю збереження визначених обмежень щодо її поширення.

Інтенсивне впровадження іноземних інформаційних технологій у різні сфери діяльності особистості, суспільства та держави, а також широке використання відкритих інформаційно-телекомунікаційних систем та інтеграція українських інформаційних ресурсів у міжнародні системи спричинили зростання ризиків застосування так званої «інформаційної зброї» проти критичної інформаційної інфраструктури. Заходи з комплексної та ефективної протидії таким загрозам реалізуються без достатньої координації та за умов обмеженого фінансування з боку підприємств. Крім того, розвитку систем інформаційної розвідки та інформаційної протидії приділяється недостатньо уваги.

Проведений аналіз дозволяє визначити більш раціональний шлях подолання цих суперечностей – впровадження системи забезпечення безпеки

в державних і комерційних структурах на основі міжнародних стандартів ISO. Такий підхід передбачає застосування сучасних рішень і комплексу вимог та правил, спрямованих на ефективне управління безпекою інформаційних мереж.

В Україні забезпечення інформаційної безпеки здійснюється шляхом захисту інформації у випадках, коли така необхідність прямо визначена законодавством у сфері захисту даних. Для реалізації цих вимог на підприємствах створюють комплексну систему захисту інформації (КСЗІ). Якщо ж суб'єкт інформаційної безпеки прагне самостійно розробити та впровадити політику інформаційної безпеки без порушення чинних норм законодавства, він може використовувати альтернативні підходи:

міжнародні стандарти ISO, зокрема ISO/IEC 17799:2005, ISO/IEC 27001:2005 та інші, що дозволяють підтримувати рішення на базі ITIL та COBIT, а також виконувати вимоги Sarbanes-Oxley Act (закону Сербейна-Окслі щодо відповідальності акціонерів за обізнаність про стан своїх активів). У такому разі на підприємстві формується система управління інформаційною безпекою (СУІБ), яка має відповідати всім вимогам міжнародних стандартів;

власні внутрішні методики та рішення.

Підприємство повинно обирати і застосовувати заходи управління таким чином, щоб забезпечувати достатній рівень впевненості у зниженні інформаційних ризиків. Ці заходи можуть бути взяті зі стандартів, інших нормативних документів, спеціальних рекомендацій для певних класів систем або ж розроблені самостійно – відповідно до політики безпеки, яку обрала компанія [43, с. 274].

Вибір заходів управління повинен ґрунтуватися на співвідношенні витрат на впровадження засобів безпеки та очікуваного зниження ризиків і можливих збитків у разі інциденту. При цьому важливо враховувати не тільки фінансові чинники, але й нематеріальні – зокрема репутаційні втрати чи соціальні наслідки, адже вони суттєво впливають на конкурентоспроможність підприємства.

Певні заходи управління, описані в стандартах та нормативних документах, можуть використовуватися як універсальні рекомендації з організації інформаційної безпеки та підходять для більшості компаній. З огляду на це, доцільно розглянути такі законодавчо обумовлені напрями управління: захист персональних даних та конфіденційної інформації; охорона інформаційних ресурсів підприємства; дотримання прав інтелектуальної власності.

Сьогодні стандартною та загальновживаною практикою в сфері інформаційної безпеки є впровадження таких груп заходів управління (додаток А, рис. А.1):

нормативні документи, що регламентують політику інформаційної безпеки;

чіткий розподіл обов'язків, пов'язаних із забезпеченням безпеки;

структура підрозділів та навчання персоналу з питань інформаційної безпеки;

процеси повідомлення та реагування на інциденти безпеки;

заходи, спрямовані на підтримання безперервності бізнесу.

Ці засоби управління є доречними для більшості організацій і більшості операційних середовищ. Варто підкреслити, що хоча всі зазначені заходи мають важливе значення, їх доцільність у конкретному випадку повинна визначатися на основі оцінки ризиків, властивих конкретній компанії. Таким чином, зазначений підхід може слугувати базовою точкою відліку у формуванні системи безпеки, але він не замінює індивідуального підбору заходів, що базуються на аналізі ризиків.

До ключових чинників, що визначають успішність упровадження інформаційної безпеки в організації, належать:

наявність чітко сформованої політики безпеки, стратегічних цілей і дій, які відображають завдання бізнесу;

підхід до організації безпеки, що відповідає корпоративній культурі та етичним нормам підприємства;

активна підтримка та зобов’язання керівництва щодо реалізації вимог інформаційної безпеки;

коректне розуміння потреб у захисті інформації, проведення оцінювання ризиків та ефективне управління ними;

результативна внутрішня комунікація та «маркетинг» безпеки, орієнтований на адміністраторів і всіх працівників;

чітке визначення та розподіл відповідальності за реалізацію політики й стандартів інформаційної безпеки між персоналом і підрядниками;

забезпечення належного навчання та підвищення кваліфікації працівників;

використання збалансованої системи показників для оцінювання ефективності заходів інформаційної безпеки та формування пропозицій щодо її вдосконалення;

аналіз можливих загроз інформації, вразливостей інформаційних ресурсів і ймовірності реалізації цих загроз;

процес ідентифікації ризиків, управління ними та мінімізація або повне усунення ризиків для інформаційних систем при прийнятному рівні витрат.

Одним із головних елементів забезпечення інформаційної безпеки в ІКСМ має бути чітко сформована система правил керування доступом. Права кожного користувача чи групи користувачів необхідно однозначно визначити та закріпити в політиці доступу.

Система вимог і правил щодо управління безпекою сучасних інформаційно-комунікаційних систем має включати такі основні елементи (додаток А, рис. А.2):

визначення вимог до захисту кожного бізнес-додатку;

ідентифікація всіх видів інформації, що пов’язані з цими додатками;

формування політик розповсюдження та авторизації інформації, що передбачають розуміння принципів, рівнів захисту та класифікації даних, які обробляються в системі;

узгодження політик керування доступом із системою класифікації інформації в різних інформаційних системах і мережах, що взаємодіють між собою;

дотримання чинного законодавства та виконання договірних зобов'язань, які стосуються захисту даних і доступу до послуг системи;

встановлення стандартних профілів доступу для типових категорій працівників;

організація управління правами доступу в розподіленому або об'єднаному мережевому середовищі з урахуванням усіх доступних каналів взаємодії.

На основі аналізу заходів із забезпечення та управління безпекою ІКСМ сформовано систему вимог і правил, що відповідає міжнародним стандартам, зокрема ISO. Під час розроблення нових ІКСМ або вдосконалення наявних систем вимоги щодо безпеки мають бути чітко визначені відповідно до засобів захисту та прийнятої системи керування безпекою. Ці вимоги повинні відображати комерційну цінність інформаційних ресурсів і спрямовуватися на мінімізацію можливих збитків бізнесу, які можуть виникнути в разі відмови або відсутності належних засобів захисту.

Сучасні виклики у сфері інформаційної безпеки зумовлюють активне застосування таких інструментів, як конкурентна розвідка та промислове шпигунство, які фактично відображають дві протилежні сторони однієї проблеми – легальну (позитивну) та нелегальну (негативну).

Термін «розвідка» у широкому розумінні означає процес отримання важливої та значущої інформації для певних користувачів. У наукових і публіцистичних джерелах зустрічаються різні її види: «економічна розвідка», «ділова розвідка», «корпоративна розвідка», «бізнес-розвідка», «конкурентна розвідка» тощо. Аналіз відкритих джерел інформації, які відображають ключові тенденції у сфері бізнесу та наміри конкурентів, а також оцінка ризиків свідчать, що у західній практиці найбільш усталеним є термін «конкурентна розвідка» (competitive intelligence). В українському

інформаційному середовищі частіше застосовують поняття «ділова розвідка» та «бізнес-розвідка», які часто вживаються як синоніми до «інформаційно-аналітичної діяльності» або «моніторингу» [41, с. 12].

Конкурентна розвідка (competitive intelligence) є спеціалізованим напрямом економічної розвідки, метою якого є формування ефективної системи взаємодії з конкурентами. Вона передбачає організацію комплексу заходів зі збору та аналізу інформації про ресурси та можливості конкурентів - майнові, фінансові, управлінські, а також їхню уразливість та стратегічні й оперативні плани.

По суті, конкурентна розвідка – це безперервний процес збору, накопичення, систематизації та аналізу даних про внутрішнє та зовнішнє середовище організації, а також передача цих даних керівництву для прийняття обґрунтованих управлінських рішень. Основною метою є зниження ризиків, підвищення конкурентоспроможності продукції, оптимізація виробничих процесів і збільшення прибутковості. Важливо підкреслити, що конкурентна розвідка використовує виключно легальні методи отримання інформації та є невід'ємним елементом корпоративної культури сучасних компаній.

Для забезпечення належного рівня інформаційної безпеки на підприємстві в межах загальної системи безпеки створюються спеціалізовані підрозділи: конкурентної (ділової) розвідки, контррозвідки та інформаційно-аналітичної служби. Кожен із них виконує визначені функції, що в сукупності забезпечують формування та захист інформаційної складової економічної безпеки підприємства. До основних напрямів їх діяльності належать:

збирання різних видів інформації, що стосується діяльності певного суб'єкта господарювання;

аналіз отриманих даних із суворим дотриманням загальноприйнятих принципів (систематичність, безперервність надходження, комплексність аналітичних процедур) та відповідних методів (специфічних і загальнокорпоративних);

прогнозування тенденцій розвитку науково-технологічних, економічних і політичних процесів як на рівні підприємства, так і на національному та глобальному рівнях для відповідної галузі бізнесу, а також визначення цільових показників, яких має досягти підприємство;

оцінювання рівня економічної безпеки за кожним елементом окремо і в цілому, а також формування рекомендацій щодо його підвищення;

інші види діяльності, пов'язані зі створенням і підтримкою інформаційної компоненти економічної безпеки, включаючи роботу з громадськістю, формування позитивного іміджу компанії, захист конфіденційних даних тощо.

У сучасних умовах особливо важливою стає якісна організація збору інформації, без якої діяльність конкурентної розвідки є неможливою. Конкурентна розвідка виконує дві ключові функції:

пасивну – передбачає постійне спостереження за діями конкурентів;

активну – пов'язана з цілеспрямованим збором і глибокою обробкою інформації для оперативного управління конкурентними ситуаціями та швидкого прийняття управлінських рішень на основі актуальних даних.

Збір відкритої (доступної) інформації спрямований на забезпечення високого рівня обізнаності щодо питань, які є загальновідомими або можуть бути легко отримані конкурентами. Учасники ринку прагнуть не відставати від динамічних потоків інформації, тому постійно здійснюють збір первинних даних.

Первинні дані отримують тоді, коли вторинної інформації недостатньо або вона має форму, непридатну для вирішення конкретної проблеми.

Вторинні дані не є результатом спеціальних досліджень – вони збираються у процесі кабінетного аналізу і не завжди безпосередньо пов'язані з цілями маркетингових досліджень.

У комплексі первинна та вторинна інформація формують так звану «бізнес-довідку». Узагальнені переваги та недоліки обох типів інформації подані на рис. 1.2.

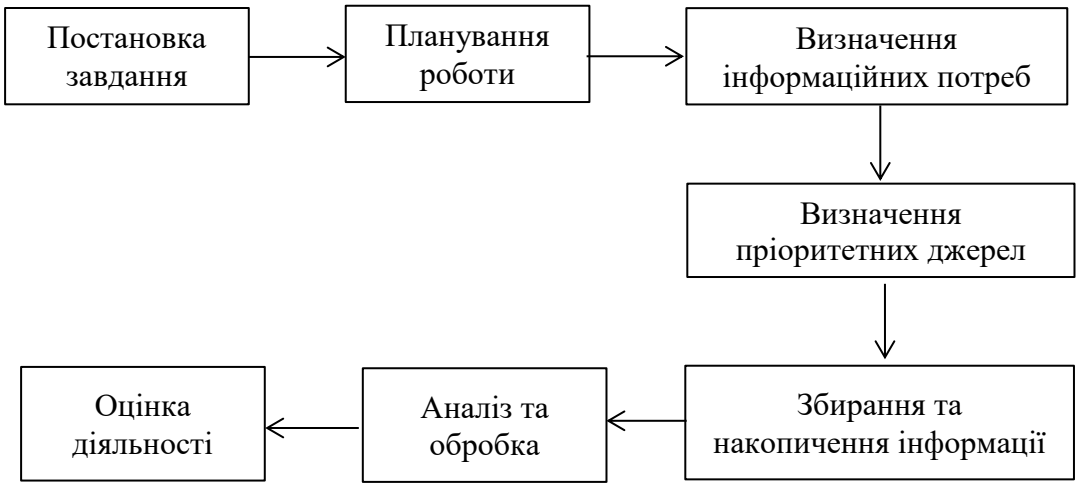

Рис. 1.2. Схема діяльності конкурентної розвідки підприємства [41, с.15]

Повноцінне управлінське рішення може бути ухвалене лише за умови комплексного використання первинної та вторинної інформації, що міститься у бізнес-довідці. Підприємство постійно отримує різноманітні потоки даних, які відрізняються між собою за джерелами походження. За способом отримання інформацію умовно поділяють на такі категорії:

відкрита офіційна інформація;

достовірні, не конфіденційні відомості, отримані завдяки неформальним контактам працівників підприємства з іншими особами;

конфіденційна інформація, здобута шляхом несанкціонованого доступу.

В Україні пошук інформації не є протизаконним, а тому будь-який суб'єкт господарювання чи громадянин має право збирати дані, за умови що не застосовуються заборонені методи, які порушують конституційні права і свободи людини. За оцінками фахівців, про діяльність бізнес-структур можна отримати 90-95% необхідних і достовірних відомостей з легальних джерел - з Інтернету, друкованих ЗМІ, під час професійних семінарів, конференцій, виставок тощо.

Законодавством чітко визначено перелік інформації, що підлягає обмеженню: до неї належать державна, комерційна і банківська таємниця. Хоча поняття службової таємниці також має нормативне визначення, зміст

цього виду інформації та правові критерії її віднесення до категорії обмеженого доступу залишаються недостатньо деталізованими.

Інформація підприємства вважається службовою або комерційною таємницею, якщо вона:

має реальну або потенційну комерційну цінність у зв'язку з тим, що невідома третім особам;

недоступна на законних підставах необмеженому колу осіб;

охороняється власником шляхом упровадження спеціальних заходів для збереження її конфіденційності.

Конфіденційною вважається будь-яка інформація, яка, навіть не будучи безпосередньо пов'язаною з господарською діяльністю підприємства, може впливати на його фінансово-економічні процеси або на взаємовідносини з контрагентами та іншими зовнішніми суб'єктами.

Відповідно до статті 505 Цивільного кодексу України, комерційна таємниця – це інформація, яка є секретною в тому сенсі, що повністю або частково, у певній формі чи у поєднанні складових, вона залишається невідомою та важкодоступною для осіб, які за характером своєї діяльності зазвичай мають справу з інформацією такого типу [3]. Саме її недоступність забезпечує їй комерційну цінність. Водночас така інформація повинна бути захищена шляхом застосування відповідних заходів безпеки особою, яка законно контролює її зміст. Комерційною таємницею можуть виступати дані технічного, виробничого, організаційного, комерційного та іншого характеру, за винятком інформації, яка згідно із законом не може бути віднесена до такої категорії.

Господарський кодекс України також розглядає комерційну таємницю та відносить її до об'єктів прав інтелектуальної власності. Крім того, ГКУ визначає права суб'єктів господарювання щодо контролю та захисту такої інформації. Зокрема, підкреслюється, що суб'єкт господарювання, який володіє технічною, організаційною чи іншою інформацією комерційного

характеру, має право вимагати її захисту від незаконного використання третіми особами за умови, що:

ця інформація має комерційну цінність у зв'язку з її невідомістю третім особам;

доступ до неї не є вільним на законних підставах;

власник вживає необхідних заходів для підтримання її конфіденційності [1].

На відміну від промислового шпигунства, конкурентна розвідка здійснюється виключно в межах правового поля та з дотриманням етичних норм. Уся діяльність конкурентної розвідки ґрунтується на суворому дотриманні чинного законодавства. Сучасні інформаційні технології – такі як мережа Internet, спеціалізовані професійні бази даних, системи пошуку та обробки інформації – разом із доступністю інформаційних ресурсів забезпечують аналітикам можливість формувати високоякісні аналітичні матеріали для прийняття управлінських рішень керівниками компаній. При цьому використовується виключно відкрита інформація.

Подібні методи аналізу відкритих джерел активно застосовуються й спецслужбами різних держав. Однак для конкурентної розвідки принципово важливим є суворе дотримання етичних принципів та здійснення діяльності лише в рамках законодавчих норм [41, с.124].

Узагальнено роботу підрозділу конкурентної розвідки будь-якої організації можна представити у вигляді типової схеми (додаток Б, рис. Б.1).

Усі зазначені дії є типовими для будь-якого завдання, поставленого перед підрозділом корпоративної розвідки. Проте їхній зміст та обсяг можуть змінюватися залежно від установлених строків виконання. Іноді виникають ситуації, коли керівництво компанії має ухвалити критично важливе рішення у стислі терміни – рішення, від якого може залежати подальший розвиток або навіть існування підприємства. У таких випадках підрозділ корпоративної розвідки отримує конкретне доручення: оперативно зібрати необхідні відомості у максимально короткий час.

Сьогодні конкурентна розвідка є невід'ємною складовою корпоративної культури сучасного бізнесу. В умовах загострення конкуренції особливо важливими стають своєчасне з'ясування намірів конкурентів, аналіз тенденцій ринку, оцінка потенційних ризиків, а також виявлення можливих каналів витоку інформації. Саме ці елементи значною мірою визначають здатність підприємства адаптуватися та ефективно функціонувати в конкурентному середовищі.

Висновки до розділу 1

Отже, у першому розділі кваліфікаційної роботи було:

1. Детально розглянуто сутність, роль та значення системи управління інформаційною безпекою підприємства в сучасних ринкових умовах господарювання. Висвітлено теоретичні основи побудови комплексної системи інформаційної безпеки, визначено її ключові функції та стратегічну важливість для стабільної діяльності підприємств. Проаналізовано базові принципи забезпечення інформаційної безпеки, зокрема конфіденційність, цілісність і доступність інформації, а також принципи безперервності бізнес-процесів, відповідальності персоналу та правомірності використання інформаційних ресурсів. Досліджено методи запобігання, виявлення та ліквідації загроз інформаційній безпеці, включаючи організаційні, технічні та правові заходи. Систематизовано класи загроз інформаційної безпеки організації, серед яких внутрішні, зовнішні, техногенні, випадкові та навмисні ризики, що дозволило створити цілісне уявлення про можливі вектори атак та шляхи їх нейтралізації.

2. Проведено огляд сучасних тенденцій та вивчено досвід управління інформаційною безпекою в Україні. Проаналізовано нормативно-правове забезпечення сфери інформаційної безпеки, включаючи чинні закони, стандарти, регламенти та рекомендації міжнародного рівня. Розкрито

актуальні проблеми та виклики, що стоять перед українськими підприємствами у процесі забезпечення інформаційного захисту, зокрема недостатність фінансування, потребу у кваліфікованих кадрах, високий рівень кіберзагроз та необхідність адаптації до міжнародних стандартів ISO/IEC серії 27000. Оцінено позитивний досвід впровадження систем управління інформаційною безпекою на провідних підприємствах України та окреслено перспективи їх подальшого розвитку.

3. Розкрито й детально охарактеризовано спеціально орієнтовану методику прийняття управлінських рішень на основі технологій інформаційного менеджменту «Бізнес-довідка» («конкурентна розвідка»). Показано, що конкурентна розвідка є важливою складовою сучасної системи економічної та інформаційної безпеки підприємства, адже забезпечує керівництво актуальними та структурованими даними щодо ринку, конкурентного середовища, можливих ризиків та перспектив розвитку. Описано етапи формування бізнес-довідки, джерела отримання первинної та вторинної інформації, принципи аналітичної обробки даних та способи їх використання при обґрунтуванні стратегічних управлінських рішень. Визначено її практичне значення для прогнозування тенденцій, запобігання кризовим ситуаціям, оптимізації бізнес-процесів і підвищення конкурентоспроможності підприємства.

РОЗДІЛ 2
АНАЛІЗ ДІЯЛЬНОСТІ ТА СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

2.1. Загальна характеристика діяльності підприємства

Об’єктом дослідження є підприємство, яке працює у харчовій промисловості. Приватне акціонерне товариство є правонаступником Полтавського пивзаводу, має виробничі потужності, які дозволяють виготовляти до 2,5 млн. декалітрів пива на рік. Асортимент підприємства налічує 12 сортів пива та 6 видів безалкогольних напоїв, серед яких популярний квас «Губернський». Найвідоміші торгові марки компанії «Ячмінний колос», «Гелон», «Полтавське», «Ай-Нікола», «Диканські вечори», «Гоголівське», «Мгарське», «Старий Млин», «Жигулівське» та інші, кожна з яких має власний унікальний смак і аромат.

Підприємство було створене на базі Полтавського пивзаводу, збудованого у 1965 році. Вже з моменту заснування головним принципом його діяльності стало виробництво не просто якісної, а найкращої продукції. Початкова річна потужність становила 1 млн. декалітрів. До 1985 року завод випускав лише безтарне та пляшкове пиво. У радянський період він входив до складу Полтавського пивоб’єднання Укрхарчопрому.

Засновником підприємства виступив Фонд комунального майна Полтавської обласної ради депутатів. Товариство є правонаступником усіх прав і зобов’язань колективної виробничо-торговельної фірми «Полтавпиво».

Сьогодні на підприємстві виготовляють пиво під брендом «Полтава». Його рецептура базується на природному способі бродіння та використанні високоякісних натуральних інгредієнтів, що надає напою насиченого, повного смаку. Особливої гармонії пиву надає м’яка артезіанська вода, яку видобувають із власних свердловин глибиною до 750 метрів.

Підприємство є юридичною особою, створеною відповідно до чинного законодавства України. У 1993 р. Фондом комунального майна було ухвалено рішення про приватизацію державного майна орендного Полтавського пивзаводу. Цього ж року наказом Фонду затверджено план приватизації та акт оцінки майнового комплексу підприємства.

Організація орендарів заводу придбала цілісний майновий комплекс Полтавського орендного пивзаводу. Після передачі державного майна підприємство було перереєстровано у колективну виробничо-торговельну фірму «Полтавпиво», а згодом – у закрите акціонерне товариство «Фірма «Полтавпиво».

Починаючи з 1998 р., підприємство розпочало співпрацю з німецькими технологами компанії «Kaltenberg», що стало важливим етапом у модернізації виробничих процесів.

У кінці 1990-х рр. на підприємстві було запущено автоматизовану лінію розливу пива в КЕГ-тару продуктивністю 50 КЕГ на годину. Вже у 1999 р. на полтавському пивзаводі було встановлено перші в Україні чотири циліндро-конічні комбі-танки, що дозволило істотно підвищити якість і стабільність виробничих процесів.

Подальший розвиток підприємства продовжився у 2001 р., коли було введено в експлуатацію оновлену лінію розливу пива в КЕГ-тару потужністю 120 КЕГ на годину. У тому ж році відкрито новий виробничий цех, у якому впроваджено сучасну технологію розливу пива, що відповідала міжнародним стандартам.

Невдовзі на заводі було встановлено ще одну автоматизовану лінію розливу в ПЕТ-пляшки та бочки (барильця), які згодом стали фірмовою ознакою полтавського пива. Потужність нової лінії становила 36 тисяч пляшок на годину. Завдяки впровадженню цих та інших технологічних інновацій підприємство досягло виробничої потужності 2,5 мільйона декалітрів продукції на рік, що закріпило його позиції серед провідних виробників пива в Україні.

На підприємстві функціонує сучасне технологічне обладнання, зокрема установка для пропагації дріжджів та автоматизована станція CIP, призначена для очищення виробничих систем.

Автоматична лінія розливу пива в КЕГ-тару досягла виробничої потужності 120 КЕГ на годину, що дало змогу істотно підвищити ефективність виробничих процесів.

У 2003 р. завершено будівництво та введено в експлуатацію варильний цех компанії «Huppmann AG», оснащений системою повної комп'ютеризації процесу варіння сусла, що забезпечило високий рівень автоматизації та стабільну якість продукції.

У червні 2010 р. підприємство вперше в Україні здійснило розлив пива в одноразову ПЕТ-КЕГ (key keg), що стало важливим кроком у розвитку інноваційної упаковки та розширенні ринкових можливостей компанії.

У 2011 році на підприємстві проведено повну реорганізацію організаційної структури, здійснено модернізацію виробництва, а також впроваджено нові методи управління та сучасні стратегії розвитку підприємства.

Наступного, 2012 р., було запущено оновлений варильний цех із системою повної комп'ютеризації процесу варіння сусла, що дозволило вдосконалити контроль якості та стабільність технологічного процесу.

У 2011 р., у зв'язку з приведенням діяльності до вимог Закону України «Про акціонерні товариства», підприємство отримало статус публічного акціонерного товариства, а рішенням загальних зборів акціонерів від 20 квітня 2017 р. його тип змінено на приватне акціонерне товариство.

Відповідно до Статуту (нова редакція, протоколи №33 від 20.04.2017 р. та №34 від 19.04.2018 р.), основними напрямами діяльності підприємства є: виробництво пива, виробництво сидру та інших плодово-ягідних вин, виробництво безалкогольних напоїв, мінеральних вод та вод у пляшках, інші спеціалізовані будівельні роботи, оптова торгівля напоями, роздрібна торгівля напоями у спеціалізованих магазинах.

У сучасних умовах стратегія товарної політики підприємства спрямована на об’єднання всіх сортів пива та безалкогольних напоїв під брендом «Полтава». Компанія реалізувала рестайлінг продуктової лінійки, розпочала випуск безалкогольних соковмісних напоїв та квасу, а також представила оновлену фірмову пляшку.

Рецептура пива, що виробляється на підприємстві, базується на природному способі бродіння та використанні високоякісних натуральних інгредієнтів. Особливу м’якість і гармонійність смаку напою забезпечує артезіанська вода з власних свердловин підприємства. Продукція підприємства неодноразово відзначалася золотими медалями на професійних конкурсах в Україні та за кордоном, що підтверджує її високу якість та конкурентоспроможність.

Асортимент продукції підприємства постійно розширюється. Наразі підприємство виробляє 37 найменувань пива, 17 видів безалкогольних напоїв (БАН) та 4 різновиди квасу. Кожен продукт має власний, неповторний і збалансований смаковий профіль, що формує унікальну лінійку торгової марки «Полтава».

Діяльність підприємства значною мірою залежить від сезонних коливань попиту. У літній період виробництво пива та безалкогольних напоїв зростає в декілька разів у порівнянні з зимовими місяцями. Квас випускається виключно в теплу пору року, коли споживчий попит на нього є найвищим.

Основними ринками збуту є центральний, східний та південний регіони України. Продукція реалізується в 22 областях країни та частково постачається на експорт. Система збуту побудована через дистриб’юторські компанії, які забезпечують поставки до національних і локальних торговельних мереж. Фасована продукція реалізується у гіпермаркетах, мінімаркетах, павільйонах, кіосках та лотках, а пиво у КЕГ-тарі – через кафе, бари та ресторани.

До ключових ризиків діяльності товариства належать:

зміни у податковому та акцизному законодавстві;

нестабільна політична ситуація в Україні;

зниження купівельної спроможності населення;

перенасичення ринку пивоварної продукції.

З метою мінімізації ризиків і підвищення стабільності роботи, підприємство реалізує комплекс заходів, серед яких:

збільшення термінів придатності та реалізації напоїв;

розроблення нових видів продукції;

розширення ринків збуту як в середині країни, так і за її межами.

В останні роки пивоварна галузь України характеризується високою конкуренцією та тенденцією до зниження обсягів виробництва. Водночас локальні виробники поступово посилюють свої позиції на регіональних ринках, тоді як лідери галузі втрачають частку ринку.

Основними конкурентами підприємства є: «АБІНБЕВ ЕФЕС УКРАЇНА»; «Carlsberg Ukraine»; «Оболонь»; «Перша Приватна Броварня».

Високий рівень конкуренції стимулює підприємство до пошуку нових ринкових сегментів, впровадження сучасних технологій виробництва та розширення продуктової лінійки.

Перспективна стратегія підприємства передбачає:

розширення ринків збуту в Україні та за кордоном;

створення нових видів продукції, орієнтованих на різні цінові сегменти;

посилення маркетингової політики та розвиток бренду «Полтава»;

збільшення обсягів виробництва та укладання нових партнерських угод;

досягнення стабільних фінансових результатів шляхом підвищення конкурентоспроможності продукції.

Вищим органом управління підприємства є загальні збори акціонерів. Станом на кінець звітного періоду підприємство не має філій, представництв чи структурних підрозділів.

Для аналізу організаційно-господарської діяльності товариства необхідно врахувати його організаційну структуру управління. Скориставшись Статутом товариства, штатним розкладом, посадовими

інструкціями працівників апарату управління та Положеннями про структурні підрозділи, проведемо аналіз системи та організації управління.

Організаційна структура управління підприємства (додаток В, рис. В.1) складається з трьох рівнів управління. До першого рівня організаційної структури управління відносяться: Загальні збори, Генеральний директор, Ревізійна комісія та Наглядова рада. До другого рівня організаційної структури управління відносяться: головний інженер, помічник директора по технічному розвитку та загальним питанням, заступник директора, директор по продажам, головний бухгалтер, головний технолог, менеджер з управління персоналом. До третього рівня організаційної структури управління відносяться: відділи головного механіка та головного енергетика, відділ по загальних питаннях та МТС, відділ безпеки та інформаційних технологій, планово-економічний відділ та логістики, маркетингу та продаж, бухгалтерія, виробництва пива та б/а напоїв, юридичний відділ. До виробничих підрозділів підприємства відносяться цехи, служби, ділянки, господарства, склади та лабораторії.

Підприємство використовує лінійно-функціональну організаційну структуру. До переваг лінійно-функціональної структури управління можна віднести: чіткість і простоту взаємодії між підрозділами підприємства; надійний контроль та дисципліну; оперативність прийняття та виконання управлінських рішень; економічність, так як товариство великих розмірів; спеціалізацію функціональних керівників; інформаційну оперативність; розвантаження вищого керівництва.

Така структура є формально визначеною та логічно побудованою, проте характеризується меншою гнучкістю. Директор підприємства виконує стратегічне управління, координує діяльність усіх відділів і функціональних служб, визначає напрями розвитку, формує цінову політику, забезпечує підбір кваліфікованих кадрів і контролює виконання планів та програм розвитку підприємства.

Функціональні підрозділи підприємства доводять свої рішення до виконавців як через керівника підприємства, так і безпосередньо – у межах наданих їм повноважень. Загалом, функціональні служби не мають права самостійно віддавати розпорядження виробничим дільницям. Їхня роль полягає у підготовці управлінських рішень для лінійних керівників, які здійснюють прямий адміністративний вплив на виконавців.

До основних завдань функціональних служб належать:

технічна підготовка виробництва;

розроблення варіантів рішень щодо управління виробничими процесами;

підготовка планових і фінансових розрахунків;

зниження навантаження на лінійних керівників у питаннях планування та аналітики.

Загальна структура підприємства охоплює всі виробничі, невиробничі та управлінські підрозділи, які функціонують на засадах узгодженої взаємодії для досягнення спільних стратегічних результатів.

До складу функціональних відділів підприємства входять: бухгалтерія, юридичний відділ, відділ управління персоналом, маркетинг, логістика, продажі, виробництво пива та безалкогольних напоїв, планово-економічний відділ, відділ головного механіка, відділ головного енергетика, відділ із загальних питань, відділ матеріально-технічного забезпечення, відділ інформаційних технологій, служба безпеки.

Серед основних переваг системи управління на підприємстві варто відзначити простоту організаційної структури. Виробництво поділене на окремі відділи, кожен із яких відповідає за певну стадію технологічного процесу. Крім основних виробничих підрозділів, на підприємстві діють допоміжні дільниці, що забезпечують ремонт обладнання, виготовлення запчастин, технічне обслуговування, а також лабораторія, яка здійснює контроль якості продукції та вирощування дріжджів - ключового компоненту у пивоварінні.

Директор з продажів підпорядковується безпосередньо генеральному директору та координує роботу відділів логістики, маркетингу і збуту. Він несе відповідальність за:

формування та реалізацію цінової політики підприємства;

аналіз і систематизацію клієнтської бази;

контроль дебіторської та кредиторської заборгованості;

підбір персоналу у підпорядковані відділи;

аналіз ринкових тенденцій і впровадження нових технологій;

розроблення товарної політики;

дотримання трудової дисципліни та належного стану робочих місць.

Основною стратегічною метою підприємства є збільшення обсягів продажів та розширення частки ринку. Діяльність підприємства зосереджена на оптимізації виручки і підвищенні ефективності реалізації продукції. На даному етапі стратегія компанії полягає у поглибленому проникненні на внутрішній ринок України з використанням уже відомих брендів пивоваріння.

Система управління виробництвом підприємства (принципова схема) показана в додатку Г рис. Г.1.

Як система управління, підприємство складається із суб’єкта та об’єкта управління. Об’єкт управління – це керовані ресурси та процеси, зокрема: трудові ресурси, енергетичні та матеріальні (основні засоби, оборотні активи), фінансові ресурси (власні та залучені кошти), а також виробничі й збутові процеси.

Суб’єкт управління – керівна підсистема, яка поділяється на громадський і професійний рівні. До громадського суб’єкта управління належать: Загальні збори акціонерів, Наглядова рада та Ревізійна комісія. До професійного суб’єкта управління входить управлінський апарат підприємства, у складі якого працюють: директор, заступник директора, директор з продажів, головний бухгалтер, головний технолог, головний інженер, помічник директора з технічного розвитку, менеджер з управління персоналом. Для ефективної роботи системи управління на підприємстві

створено налагоджений двосторонній канал зв’язку та обміну інформацією між усіма рівнями – від виконавців до керівництва. Це забезпечує безперервну взаємодію між управлінською та виробничою підсистемами, сприяє оперативному прийняттю рішень та підвищенню ефективності виробництва.

Система охорони праці на підприємстві охоплює такі основні складові: правові та організаційні засади; фізіологію, гігієну праці та виробничу санітарію; виробничу безпеку; пожежну безпеку.

Правові та організаційні основи охоплюють комплекс взаємопов’язаних законодавчих і нормативно-правових актів, соціально-економічних і організаційних заходів, спрямованих на безпечну організацію трудового процесу. Основна мета – створення умов, що забезпечують працівників засобами індивідуального захисту, гарантують компенсації за роботу у шкідливих або важких умовах, а також навчання персоналу правилам безпечного ведення робіт. Сюди ж належить регламентування відповідальності та порядок відшкодування шкоди у випадку травмування чи погіршення здоров’я працівників.

Фізіологія, гігієна праці та виробнича санітарія включає організаційні, гігієнічні та санітарно-технічні заходи, спрямовані на попередження або мінімізацію впливу шкідливих виробничих факторів на працівників. Йдеться про забезпечення належного мікроклімату, чистоти, освітлення, вентиляції, а також про дотримання санітарно-гігієнічних норм у робочому середовищі.

Виробнича безпека на підприємстві полягає у запобіганні нещасним випадкам, аваріям і мінімізації їх наслідків. Її забезпечують шляхом технічного обслуговування обладнання, проведення інструктажів, контролю за дотриманням технологічної дисципліни та використанням засобів захисту.

Пожежна безпека на виробництві – це система заходів, спрямованих на запобігання займанням, пожежам і вибухам, а також на зменшення шкоди у разі їх виникнення. Вона передбачає навчання працівників правилам поведінки при пожежі, обладнання приміщень засобами пожежогасіння,

дотримання норм зберігання легкозаймистих матеріалів і систематичні перевірки протипожежного стану.

Служба управління персоналом є окремим структурним підрозділом підприємства і підпорядковується безпосередньо директору підприємства. У своїй діяльності відділ керується чинним законодавством України, нормативно-правовими актами уряду, наказами директора підприємства, Статутом товариства, правилами внутрішнього трудового розпорядку, а також Положенням про службу управління персоналом, затвердженим на підприємстві.

Основні завдання, функції та повноваження кадрової служби визначені у Положенні про службу управління персоналом. Метою діяльності відділу є організація ефективної кадрової роботи, забезпечення підприємства компетентними працівниками та ведення повного обліку персоналу відповідно до чинного законодавства. До основних завдань відділу кадрів належать:

підготовка та оформлення розпорядчих документів з особового складу (наказів, розпоряджень тощо);

організація документообігу, що забезпечує оперативний контроль за рухом персоналу та виконанням доручень керівництва;

здійснення контролю за виконанням наказів і розпоряджень товариства;

ведення обліку особового складу під час прийняття, переведення та звільнення працівників;

контроль за станом підготовки, перепідготовки та атестації персоналу;

оформлення, ведення та зберігання трудових книжок, довідок і документів, пов’язаних із трудовими відносинами;

забезпечення передачі документів до архіву та організація їх тривалого зберігання.

До складу персоналу підприємства входять усі наймані працівники, а також власники і співвласники підприємства, які беруть участь у його діяльності. Проведемо аналіз структури персоналу по категоріях зайнятих

(додаток Д, табл. Д.1). Аналіз персоналу дозволяє зазначити, що абсолютна чисельність управлінського персоналу за останні 5 років дещо зменшилася. Так, у 2024 р. в порівнянні з 2020 р. кількість управлінського персоналу зменшилася на 4 особи, тенденція до незначного, але постійного скорочення спостерігалася протягом всього досліджуваного періоду, тому ми можемо зробити висновок, що серед цієї категорії персоналу відбувається деяке скорочення чисельності. Що стосується виробничого персоналу, то тут чисельність також знизилася, так у 2024 р. вона знизилася на 14 осіб відносно 2020 р., і подібна тенденція до поступового скорочення чисельності виробничого персоналу простежується протягом всього досліджуваного періоду. Дані зміни відобразилися й на середньооблікові чисельності персоналу підприємства, яка склала у 2020 р. 291 особу, а у 2024 р. вже 273 особи, скорочення чисельності персоналу склало більше 6% відносно досліджуваного періоду (додаток К, рис. К.1).

Для більш повної характеристики персоналу підприємства варто проаналізувати його і за рівнем загальної освіти (додаток Е, табл. Е.1). Доцільно зробити висновок, що на підприємстві, в основному, працюють працівники з неповною або повною вищою освітою, працівників без вищої освіти налічується трохи більше 30% і даний показник є сталим. Протягом досліджуваного періоду підприємство проводило перекваліфікацію своїх працівників, за цей період частка працівників, що її проходили щоправда зменшувалася з 5,15% у 2020 р. до 1,1% у 2024 р., здебільшого вона стосувалася працівників, що не мають вищої освіти. Таким чином, можна зробити висновок, що кадрова політика товариства повністю забезпечує виробництво висококваліфікованими кадрами, необхідними для наукомісткої праці й виготовлення відповідної продукції.

Наступним кроком аналізу системи управління персоналом підприємства є розрахунок показників, які характеризують рух персоналу за допомогою звітів про використання робочого часу. Результати розрахунку цих показників розглянуто в наступній таблиці, що дасть змогу охарактеризувати

плинність персоналу (додаток Л, табл. Л.1). Показники даної таблиці дають можливість проаналізувати рух персоналу підприємства, який свідчить, що за даними розрахунків за досліджуваний період звільнено було близько 6% працівників, простежується тенденція незначного звільнення працівників майже щороку. Ми можемо зробити висновок, що попри незначну кількість звільнених працівників з року в рік, середньооблікова чисельність працівників змінювалася з нижчим темпами щорічно, що не пов'язане зі змінами в технологічному укладі підприємства, а більше до циклічного природного руху персоналу чи нечисленних випадків порушення трудової дисципліни.

2.2. Аналіз техніко-економічних показників діяльності підприємства

Для проведення аналізу діяльності підприємства, визначення ефективності його господарської діяльності використаємо для розрахунку документи бухгалтерської звітності – баланс за 2020-2024 рр., звіт про фінансові результати за 2020-2024 рр. (додаток Щ). Почнемо з характеристики основних показників діяльності підприємства (додаток Л, табл. Л.2). Підприємство кожного року збільшує обсяг чистого доходу від реалізації продукції, товарів, робіт послуг, так він зріс у 2022 р. порівняно з 2020 р. майже вдвічі, що безумовно є позитивною динамікою, але це пов'язано з падінням курсу гривні в результаті повномасштабної агресії росії проти України, ніж з покращенням діяльності підприємства, оскільки й собівартість випущеної продукції зросла більш, ніж удвічі. Якщо розглядати уже воєнні роки діяльності, то тут теж простежується ріст, але вже поступовий. Слід відмітити, що підприємство протягом усього досліджуваного періоду залишається прибутковим, незважаючи на те, що і в довоєнні роки він мав тенденцію до падіння, але після росту в період початку повномасштабної

агресії, пов’язаного все з тими ж інфляційними процесами, теж знизився за 2024 р. (рис. 2.1).

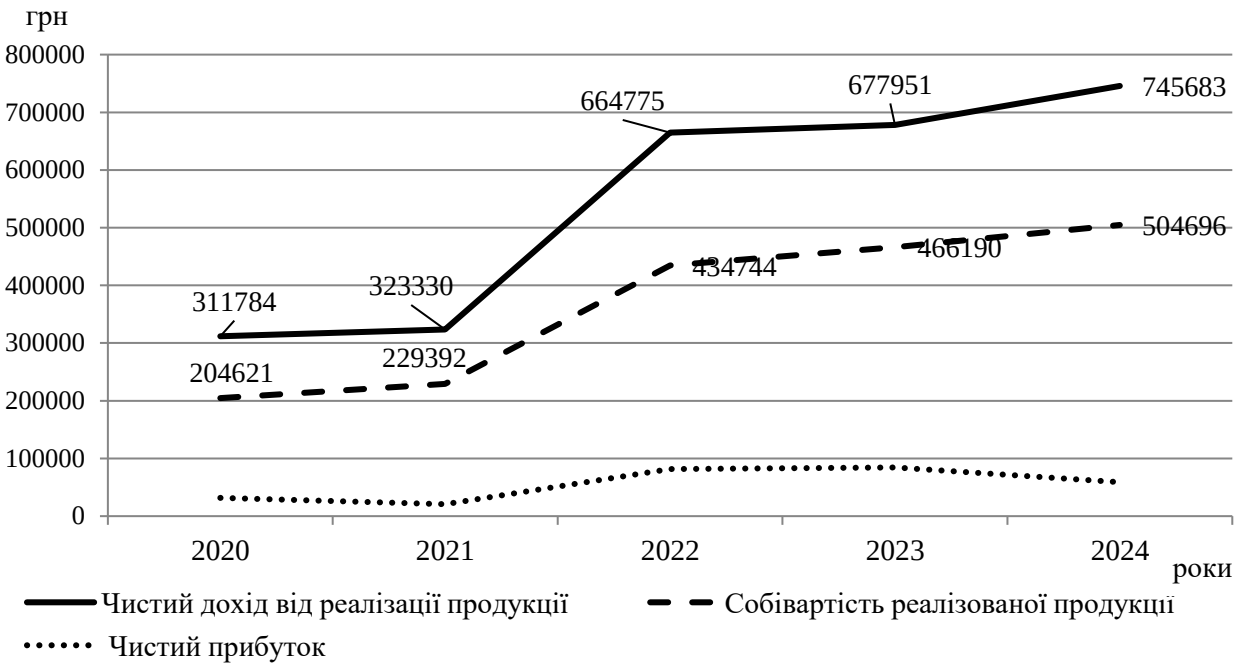

Рис. 2.1. Динаміка основних показників діяльності підприємства, за 2020-2024 рр.

В цілому, товариство має достатній рівень запасів для здійснення своєї господарської діяльності протягом досліджуваного періоду.

Наступним етапом дослідження стане аналіз показників ефективності використання основних фондів підприємства (додаток М, табл. М.1). Позитивною тенденцією для підприємства є зростання показника фондовіддачі, що ми можемо відзначити з розрахунків з 1,42 грн у 2020 р. до 2,63 грн у 2024 р., відзначаємо тенденцію росту, проте знову зауважуємо, що стрімкий тем більше пов’язаний з інфляційним ростом та падінням курсу гривні. Показник фондоємності, що зменшується теж є позитивною тенденцією. Так у 2020 р. 0,71 грн, а вже у 2024 р. 0,38 грн. Це свідчить про незначне прискорення темпів ділової активності підприємства. Відзначимо ріст продуктивності праці з 1071,42 грн на 1 особу у 2020 р. до 2731,44 грн на 1 особу у 2024 р. Аналіз показників рентабельності за 2020-2024 рр.(додаток

М, табл. М.2) дає можливість зробити висновок, що підприємство на кінець 2024 р. залишається рентабельним (рис. 2.2), оскільки всі показники рентабельності є позитивними на 2024 р., щоправда хоча й мають тенденцію до зниження за останній рік.

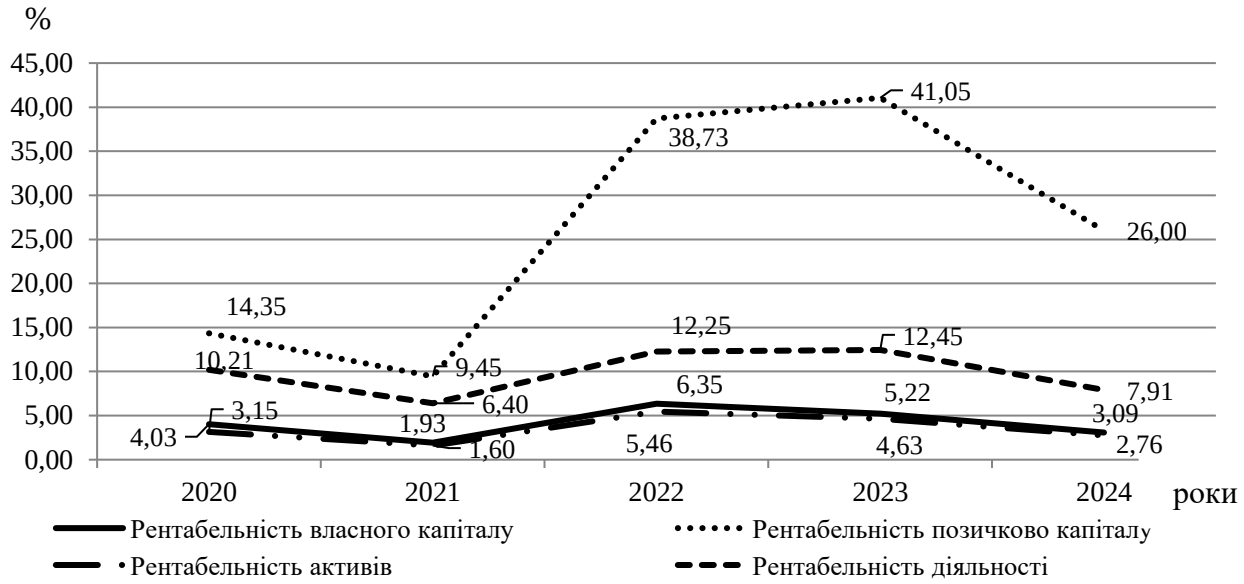

Рис. 2.2. Показники рентабельності підприємства, за 2020-2024 рр.

Далі необхідно проаналізувати динаміку структури операційних витрат (додаток Р, табл. Р.1), при аналіз даних слід звернути увагу на тенденції що відображають процеси до вторгнення росії до України, так і після. Тому звертаємо увагу саме на частки до зростання (зменшення) питомої ваги окремих статей витрат підприємства. Аналізуючи отримані результати, можемо зробити висновок, що всі статті витрат протягом аналізованого періоду зростають, це пов’язано як з нарощуванням обсягів виробництва, так і з перерахунком вартості у зв’язку із знеціненням гривні в період початку війни. У структурі витрат найбільшими статтями є матеріальні витрати, що складають майже дві третини від усієї сукупності операційних витрат і цей показник має тенденцію до зростання протягом досліджуваного періоду та витрати на оплату праці (додаток Н, рис. Н.1).

Далі здійснимо аналіз ефективності складу і розміщення активів підприємства (додаток П, табл. П.1). Для даної таблиці важливо проаналізувати

структуру активів товариства. Оптимальною вважається: 60% необоротні активи, 40% оборотні активи. Дані даної таблиці засвідчують структуру і склад активів товариства, так зокрема, в довоєнний період зазначена умова пропорцій часток дотримувалася, але у воєнні роки, частки змінилися обернено пропорційно. Так у 2020 р. 58,12% складають необоротні активи та 41,86% оборотні активи, на 2024 р. вже 37,16% складають необоротні активи та 62,82% оборотні активи, що свідчить, в цілому, про високу ліквідність, що є характерним для оптової та роздрібної торгівлі, дистрибуції, але існують ризики неефективного використання капіталу (наприклад, надлишкові запаси чи готівка, бачимо їх ріст за досліджуваний період). На основі аналізу подальших показників відзначаємо, що керівництву підприємства необхідно звернути увагу на ефективне управління оборотним капіталом (рис. 2.3).

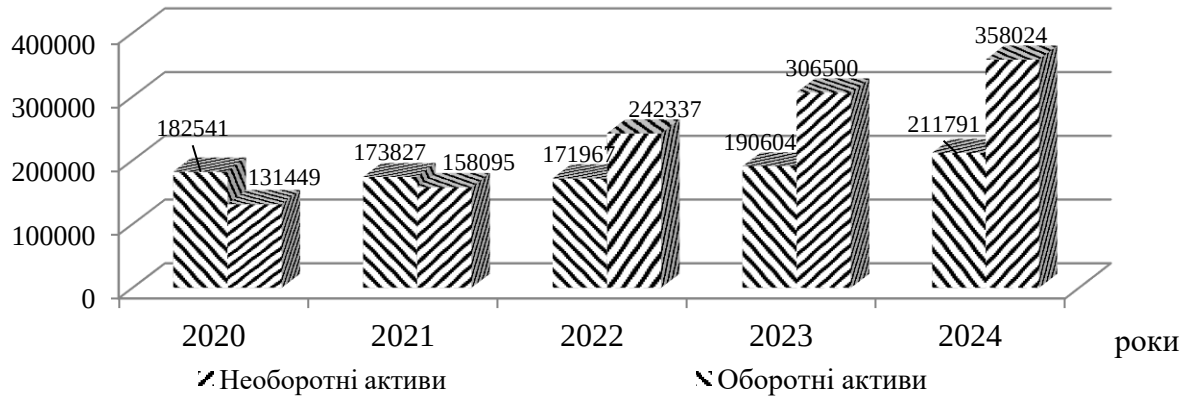

Рис. 2.3. Динаміка зміни складу і розміщення активів підприємства, за 2020-2024 рр.

Ліквідність характеризує здатність підприємства швидко перетворити активи на гроші. Аналіз складу і структури оборотних активів підприємства за 2020-2024 рр. був проаналізований в додатку П, табл. П.2. На основі аналізу, спостерігаємо, що в розрахунках основну частку оборотних активів складають грошові кошти 41,46% на кінець 2020 р. і 62,59% на кінець 2024 р. Слід відмітити позитивну тенденцію, що чітко намітилася за цей період – це стрімке скорочення майже втричі дебіторської заборгованості, у 2020 р. її частка складала майже 31%, а вже в 2024 р. майже 11%. Дебіторська заборгованість відноситься до середньоліквідних активів, тобто на їх перетворення потрібен час. Скорочення

даної статті є позитивом для підприємства, отже, товариство посилило роботу з дебіторами. Швидколіквідними активами є грошові кошти та поточні фінансові інвестиції. І зростання цієї статті є позитивним для товариства, але слід зазначити, про вже зроблений висновок, що слід звернути увагу на ефективність управління оборотним капіталом на підприємстві (рис. 2.4).

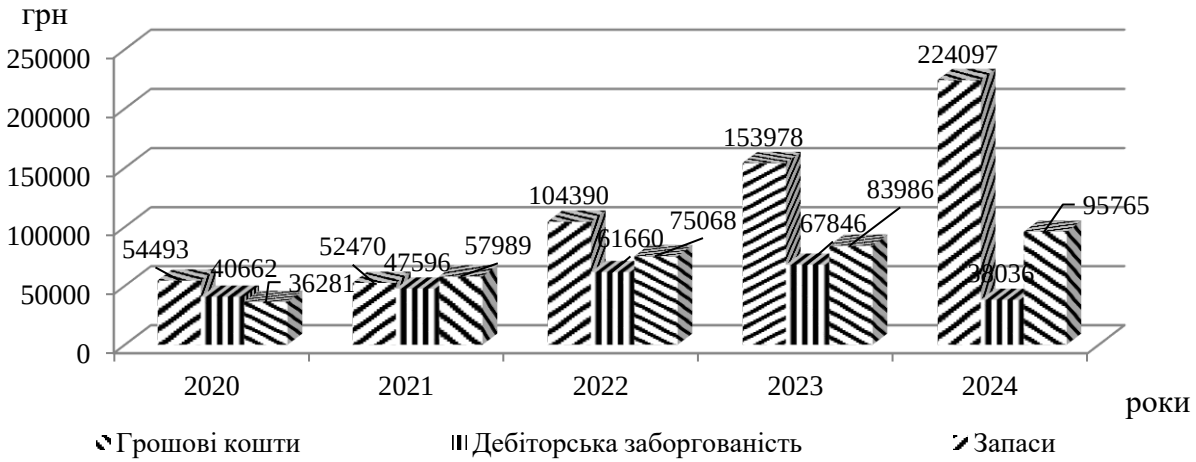

Рис. 2.4. Динаміка зміни складу і структури оборотних активів підприємства, за 2020-2024 рр.

Наступним етапом буде аналіз динаміки показників платоспроможності підприємства за 2020-2024 рр. (додаток Р, табл. Р.2). Дані таблиці свідчать, що товариство в аналізованому періоді є платоспроможним, про що говорять розраховані коефіцієнти. Так всі розраховані коефіцієнти суттєво перевищують порогові нормативні значення, з одного боку це добре, але перевищення в такій мірі, говорить про вже зроблені раніше висновки про не досить високу ефективність управління оборотним капіталом на підприємстві (рис. 2.5).

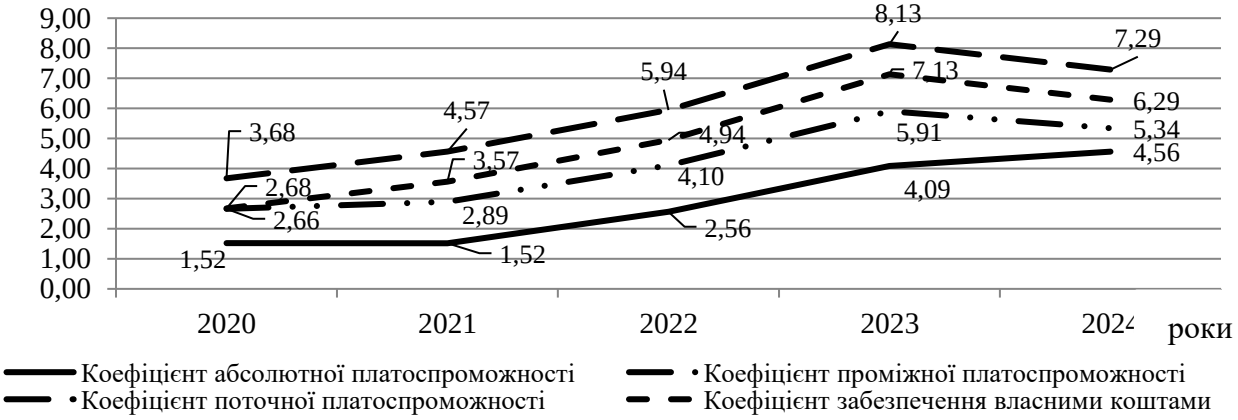

Рис. 2.5. Динаміка зміни показників платоспроможності підприємства, за 2020-2024 рр.

Ступінь захищеності інтересів кредиторів та інвесторів, що мають довгострокові, вкладення в підприємство, характеризують показники фінансової стійкості.

Можемо їх проаналізувати за допомогою додатку Р, табл. Р.3. Як видно з таблиці товариство має досить гарну фінансову стійкість за досліджуваний період, про що говорять розраховані коефіцієнти та підтверджує попередньо зроблені висновки про можливі загрози для товариства через не досить високу ефективність управління оборотним капіталом на підприємстві (рис. 2.6).

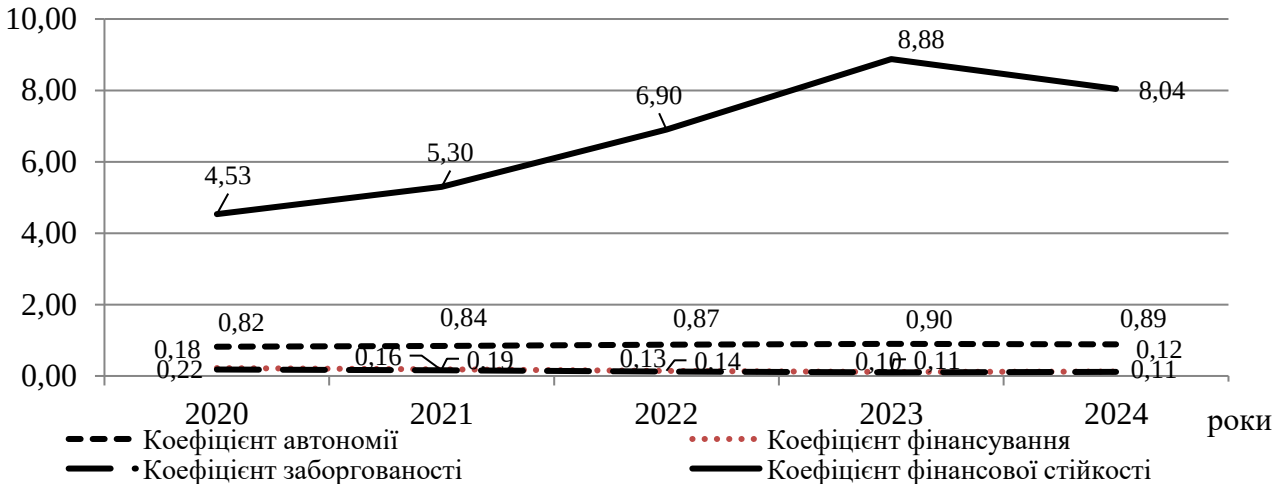

Рис. 2.6. Динаміка зміни показників фінансової стійкості підприємства, за 2020-2024 рр.

Таким чином, підводячи підсумки, можемо зробити висновок, що загалом підприємство за 2020-2024 роки діяльності, незважаючи на початок повномасштабного вторгнення росії в Україну має досить потужне та міцне фінансове становище, як показують нам проведені розрахунки. Проте у таких високих та позитивних показниках є й зворотна сторона медалі, це надмірна величина не використовуваних належним чином вільних грошових коштів, що може свідчити про не досить високу ефективність управління оборотним капіталом на підприємстві.

2.3. Аналіз системи управління інформаційною безпекою підприємства

Розглянемо і проаналізуємо інформаційну безпеку підприємства. За світовою статистикою, втрата лише 20% інформації призводить до банкрутства 65% фірм і компаній. Докладніше розглянемо які можливі наслідки втрати інформації для підприємства:

розголошення комерційної інформації може спричинити значні фінансові втрати для підприємства;

повідомлення про викрадення великого обсягу даних суттєво шкодить репутації компанії, що, у свою чергу, знижує обсяги торгівлі4

конкуренти можуть скористатися несанкціонованим доступом до інформації, якщо факт витоку залишився непоміченим, для підриву фінансової стабільності фірми, нав’язуючи їй збиткові або фіктивні контракти;

модифікація даних як під час їх передачі, так і зберігання в межах організації, може стати причиною серйозних фінансових втрат;

повторні успішні кібератаки на компанію знижують рівень довіри з боку клієнтів і, відповідно, негативно впливають на дохідність бізнесу.

Основними цілями системи захисту інформації на підприємстві є:

недопущення витоку, викрадення, спотворення, втрати чи фальсифікації інформації;

усунення загроз безпеці особи, підприємства, суспільства та держави;

запобігання несанкціонованому доступу з метою знищення, зміни, спотворення, копіювання або блокування інформації;

протидія будь-яким незаконним спробам втручання в інформаційні системи та ресурси, а також забезпечення правового захисту документованої інформації як об’єкта власності;

забезпечення збереження й конфіденційності документованої інформації згідно з чинним законодавством.

Для досягнення цілей системи інформаційної безпеки підприємства

вирішуються такі основні завдання:

встановлення переліку цінної інформації підприємства та оцінка ступеня її важливості;

передбачення потенційних загроз інформаційній безпеці, своєчасне їх виявлення, а також аналіз факторів, що можуть призвести до фінансових, матеріальних або репутаційних втрат;

забезпечення таких умов роботи, за яких імовірність реалізації загроз інформаційним ресурсам є мінімальною;

розробка ефективного механізму швидкого реагування на загрози інформаційної безпеки, а також прояви негативних процесів, із залученням правових, організаційних та технічних інструментів захисту;

створення умов для максимально ефективного відновлення та компенсації збитків, завданих неправомірними діями, зниження негативного впливу порушень інформаційної безпеки на досягнення стратегічних завдань підприємства.

Система захисту інформації підприємства виконує такі функції:

підтримка цілісності програмного забезпечення (як прикладного, так і системного) та достовірності оброблюваної інформації;

захист конфіденційних даних, зокрема комерційної таємниці, із застосуванням сертифікованих засобів криптографічного захисту;

впровадження захищеного електронного документообігу на базі сертифікованих криптографічних засобів і використання електронного цифрового підпису;

централізоване управління системою інформаційної безпеки, що здійснюється з робочого місця адміністратора;

забезпечення захищеного доступу до корпоративної мережі для мобільних користувачів шляхом використання технологій VPN;

контроль за доступом до інформаційних ресурсів;

реалізація ефективного антивірусного захисту з метою запобігання загрозам зловмисного програмного забезпечення.

На підприємстві фізичний рівень захисту спрямований на зниження ризику несанкціонованого доступу як з боку сторонніх осіб, так і з боку персоналу, а також на мінімізацію впливу техногенних загроз. На мережевому рівні забезпечено безпечний обмін даними між автоматизованими робочими місцями, включно з віддаленими та мобільними, і створено захищене зовнішнє середовище по периметру всієї інформаційної системи. На рівні користувача доступ до інформаційної системи надається виключно авторизованим особам, реалізовано захисні механізми навколо її складових, а також впроваджено індивідуальне робоче середовище для кожного користувача.

Для побудови надійної системи захисту необхідно попереднього проаналізувати можливі загрози безпеки системи на підприємстві. Цей аналіз включає в себе:

виявлення можливих загроз, особливо небезпечних (наприклад, несанкціонований перегляд або зміна даних);

оцінка витрат часу та грошей, що можуть знадобитися зловмисникам для її зламу;

визначення важливості інформації, що зберігається;

моделювання потенційного зловмисника (вирішити, від кого саме потрібен захист: зовнішні особи, користувачі, адміністратори тощо);

визначення, скільки часу, ресурсів та коштів можна витратити на захист системи.

На підприємстві користувачі працюють з операційною системою Windows 11 Enterprise. Цей вибір зумовлений тим, що зазначена версія Windows 11 спеціально призначена для підприємств і має розширені функції безпеки та системи захисту. На серверах компанії використовується операційна система Windows Server 2022 Standard Edition.

Задля безпеки персональних комп'ютерів від несанкціонованого втручання та використання, на всіх комп'ютерах підприємства, окрім тих, що належать директору та адміністраторам безпеки, відключено оптичні приводи та USB-порти. Контроль доступу до персональних комп'ютерів реалізовано за

допомогою інтегрованих механізмів безпеки операційної системи Windows 11 Enterprise. Для кожного структурного підрозділу підприємства створено окрему робочу групу (домен) з відповідними обліковими записами користувачів, які мають змогу працювати виключно в межах своєї призначеної робочої групи з попередньо визначеними правами доступу. Аутентифікація користувачів однієї робочої групи в іншій є неможливою. Після успішної авторизації в системі на персональний комп'ютер користувача завантажуються його персональні дані з файлового сервера та сервера баз даних.

При розробці плану організації робочих місць на підприємстві було враховано наступні принципи:

орієнтація екранів комп'ютерів таким чином, щоб уникнути їхнього розташування навпроти вікон або дверей;

розміщення робочих станцій для мінімізації можливості візуального контролю за роботою одних користувачів іншими.

На підприємстві циркуляція та обробка інформація відбувається в АС «2» класу. В складі АС підприємства функціонують такі засоби захисту: сенсори розбитого скла; пожежна сигналізація; металеві решітки; відеоспостереження; охоронна система; джерела безперебійного живлення; кабельне обладнання. Для забезпечення безпеки території компанії та запобігання викраденню інформації вжито низку заходів: цілодобове чергування, постійне відеоспостереження зовнішньої та внутрішньої зон, а також функціонування системи електронних пропусків, що ефективно протидіє проникненню сторонніх осіб з метою отримання несанкціонованого доступу до інформації.

В АС підприємства обробляється відкрита та конфіденційна інформація (додаток С, табл. С.1). Інформація в компанії класифікується на конфіденційну, до якої належать дані про клієнтів, їхні операції, технологічні розробки та ключові відомості, та відкриту, яка є загальнодоступною. Серед персоналу товариства та користувачів АС виділяються технічний та обслуговуючий персонал, системні адміністратори, адміністратор відділу безпеки, співробітники охорони, бухгалтерія, відділ маркетингу, канцелярія, відділ продаж, керівний склад відділів та директор.

Найнижчим рівнем доступу до інформації, що обробляється в АС, володіють технічний та обслуговуючий персонал, а також співробітники служби охорони. Значно ширші права доступу мають працівники маркетингового відділу, відділу інформаційних технологій та дирекція. Найвищі повноваження щодо адміністрування комплексної системи захисту інформації (КСЗІ) належать адміністратору безпеки, дещо нижчий пріоритет мають співробітники служби безпеки та системні адміністратори. Доступ до серверних приміщень, приміщень для зберігання документації, звітів про діяльність компанії, зареєстрованих носіїв інформації, даних відеоспостереження, журналів відвідувань тощо надається виключно дирекції та особам, які мають відповідний допуск до цих матеріалів.

Визначимо яка інформація для підприємства потребує захисту:

технологічні відомості: методи виробництва, технологічні процеси та обладнання, удосконалення існуючих технологій;

управлінська інформація: дані про управління підприємством та його стратегічні плани;

фінансові дані: відомості про систему оплати праці, показники фінансового планування, майновий стан, запаси товарів, баланс підприємства, стан банківських рахунків та рівень доходів;

плани діяльності: плани закупівель, збуту та інвестицій;

комерційна політика: цінова та збутова стратегії, собівартість продукції;

аналіз ринку: порівняльні характеристики власної продукції та продукції конкурентів (якість, дизайн, упаковка тощо);

виробничі плани: плани щодо розширення або скорочення виробництва;

комерційні переговори: факти проведення переговорів щодо купівлі-продажу;

кадрова інформація: дані про персонал підприємства;

інформація про контрагентів: відомості про постачальників, продавців та покупців;

логістична інформація: відомості про способи придбання та реалізації продукції;

договірна інформація: зміст та умови укладених договорів і контрактів;

інформація про безпеку: відомості щодо встановлення охоронної сигналізації та її розташування.

На підприємстві для здійснення контролю та управління доступом використовується система SDK-Z2USB MF. Зазначена система управління доступом відповідає ключовим вимогам політики інформаційної безпеки підприємства. Передбачається можливість її подальшої модифікації та вдосконалення.

Система відеоспостереження, що використовується на підприємстві, відповідає ключовим вимогам політики інформаційної безпеки, встановленим для даного об'єкту. Засоби відеоспостереження формують систему замкнутого відеоконтролю, в якій передача відеосигналів від камер до моніторів здійснюється в межах контрольованої (охоронюваної) зони, переважно за допомогою кабельних з'єднань. Функціональність системи відеоконтролю розширена процедурою автоматичного детектування руху, що значно підвищує ефективність виявлення подій під час спостереження.

На підприємстві використовується інтегрована система охоронно-пожежної сигналізації, що об'єднує функції виявлення пожежі та несанкціонованого доступу. Управління системою здійснюється централізовано, проте охоронна та пожежна підсистеми мають незалежні пости керування та функціонують автономно. Охоронна підсистема своєчасно інформує службу безпеки про будь-які спроби або факти незаконного проникнення в будівлі або окремі зони, реєструючи час, місце та дату порушення. Пожежна підсистема оперативно виявляє осередок пожежі та передає сигнали керування системам оповіщення про займання та автоматичного пожежогасіння.

На підприємстві використовується охоронна сигналізація, розроблена відомою польською компанією Satel. Система Satel CA-10 LS призначена для превентивних заходів та фіксації фактів несанкціонованого проникнення в приміщення. Вона являє собою комплекс технічних засобів, ключовими елементами якого є сповіщувачі (датчики виявлення) та центральний пульт

управління. Дана сучасна сигналізація здійснює контроль та інформування про спроби руйнування скляних поверхонь, перекриттів, стін, розбиття вікон, а також про рух осіб всередині контрольованих зон.

Система пожежної сигналізації призначена для виявлення осередків загоряння та передачі сигналу тривоги черговому персоналу, а також на централізований пульт спостереження з метою оперативного реагування та локалізації пожежі. Виявлення місця займання супроводжується передачею відповідного сигналу на пульт управління сповіщувачів. На підприємстві використовуються комбіновані пожежні сповіщувачі моделі DX-60 Plus.

Система охоронно-пожежної сигналізації відповідає основним вимогам політики інформаційної безпеки для підприємства та сертифікована на території України.

Системи пожежогасіння призначені для превентивних заходів щодо пожежі, обмеження її розповсюдження, безпосереднього гасіння, а також забезпечення захисту життя людей та збереження матеріальних цінностей. Одним із найбільш ефективних засобів для досягнення цих цілей є системи автоматичного пожежогасіння. На відміну від систем ручного керування та систем, що приводяться в дію оператором, автоматичні системи активуються пожежною автоматикою на основі об'єктивних показників та забезпечують оперативне усунення вогнища займання без втручання людини.

На підприємстві функціонує станція пожежогасіння WILO HWJ 202 EM 20L. Дана установка являє собою автоматизовану систему водопостачання, що базується на самовсмоктуючому, одноступінчастому горизонтальному насосі, який може працювати як на всмоктування, так і на подачу води. Станція пожежогасіння WILO HWJ 202 EM 20L повністю відповідає чинним нормативним вимогам у сфері пожежної безпеки.

Висновки до розділу 2

Таким чином, у другому розділі кваліфікаційної роботи були отримані наступні результати:

1. Зокрема, були розглянуті коротка історія становлення та трансформації підприємства, загальні відомості про підприємство, напрямки його діяльності, проаналізована організаційна структура управління, яка є лінійно-функціональною, проаналізований об’єкт та суб’єкт управління, виконаний аналіз управління персоналом, результатом якого є встановлення скорочення чисельності персоналу більше 6% відносно досліджуваного періоду.

2. Проведений комплексний аналіз техніко-економічних показників діяльності підприємства. Так, зокрема, був зроблений висновок про те, що підприємство за 2020-2024 рр. діяльності має досить потужне та міцне фінансове становище. Зокрема, чистий прибуток зріс із 31819 тис. грн у 2020 р. до 58953 тис. грн у 2024 р. Проте недоліком в роботі підприємства є надмірна величина не використовуваних належним чином вільних грошових коштів, що може свідчити про не досить високу ефективність управління оборотним капіталом на підприємстві. Так, їхня частка у складі структури оборотних активів підприємства складає 62,59%, що є досить великим показником.

3. Виконаний аналіз системи управління інформаційною безпекою підприємства, який дозволяє зробити висновок, що товариство в цілому захищене достатньо добре, проте не позбавлено деяких недоліків. має базовий рівень організації інформаційної безпеки, який відповідає мінімальним вимогам для виробничого підприємства середнього розміру. До основних досягнень можна віднести: наявність правової бази та функціональний захист, а також свідомість персоналу. Впроваджено необхідні локальні нормативні документи, що регламентують доступ до інформації, використання корпоративних ресурсів та політику конфіденційності, що відповідає вимогам

законодавства України. Забезпечено базовий захист мережевої інфраструктури (міжмережеві екрани, антивірусне програмне забезпечення) та резервне копіювання критично важливих даних (бухгалтерський облік, виробничі рецептури). Зафіксовано відносно високий рівень обізнаності ключових співробітників відділу ІТ та бухгалтерії щодо основних загроз (фішинг, шкідливе ПЗ).

РОЗДІЛ 3
ШЛЯХИ ВПРОВАДЖЕННЯ ЗАХОДІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВИРОБНИЦТВА НА ПІДПРИЄМСТВІ

3.1. Розробка моделі загроз для інформації та моделі порушника для об’єкта інформаційної діяльності

У сучасному діловому середовищі практично кожна комерційна організація в розвинених країнах має у своїй структурі підрозділи, що здійснюють інформаційну діяльність. Залежно від компанії, ці функції можуть бути зосереджені в інформаційно-аналітичному відділі, відділі маркетингу (на який, окрім іншого, покладаються інформаційно-аналітичні завдання), або ж у відділі комерційної розвідки. Структура та функціональне навантаження часто визначаються рівнем усвідомлення керівництвом компанії значущості інформаційно-аналітичної роботи для забезпечення безпеки всіх аспектів діяльності будь-якої комерційної структури.

Загрози інформаційній безпеці автоматизованої системи визначаються низкою факторів, включаючи характеристики операційної системи, фізичне оточення, людський фактор, технології обробки даних та інші аспекти, і можуть мати об'єктивний або суб'єктивний характер. Суб'єктивні загрози, у свою чергу, поділяються на випадкові (ненавмисні) та навмисні дії. З метою формування адекватної моделі загроз, необхідно ідентифікувати основні види загроз інформаційній безпеці, які можуть бути реалізовані стосовно автоматизованої системи підприємства, та врахувати їх при розробці моделі.

До об'єктивних загроз належать:

зміни умов фізичного середовища, спричинені стихійними лихами та аваріями (такими як землетруси, повені, пожежі або інші непередбачувані події);

функціональні порушення та відмови в роботі апаратного забезпечення та технічних засобів автоматизованої системи;

негативні наслідки помилок, допущених на етапах проектування та розробки компонентів автоматизованої системи (технічних засобів, технології обробки інформації, програмного забезпечення, засобів захисту, структур даних тощо);

помилкові дії персоналу (користувачів) автоматизованої системи під час її експлуатації.

До суб'єктивних навмисних загроз належать навмисні дії (спроби) потенційних порушників.

Наступним кроком є визначення повного переліку потенційних загроз та їхня класифікація відповідно до наслідків їхнього впливу на інформацію. Зокрема, необхідно ідентифікувати, порушення яких саме властивостей інформації є метою загрози (конфіденційності, цілісності та доступності), а також які загрози спрямовані на порушення спостережності та керованості автоматизованої системи.

До випадкових загроз суб'єктивного характеру (дії, що здійснюються персоналом або користувачами внаслідок неуважності, недбалості, недостатньої обізнаності тощо, без навмисного шкідливого наміру) належать:

дії, що спричиняють відмову функціонування АС (або її окремих компонентів), руйнування програмних, апаратних та інформаційних ресурсів (таких як обладнання, канали зв'язку, видалення даних, ПЗ тощо);

ненавмисне пошкодження носіїв інформації;

несанкціонована зміна режимів функціонування АС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестових або технологічних процесів, що можуть призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

ненавмисне зараження ПЗ комп'ютерними вірусами;

недотримання вимог організаційних заходів захисту, встановлених чинними розпорядчими документами АС;

помилки при введенні даних до системи, виведення даних на некоректні адреси пристроїв, внутрішніх та зовнішніх абонентів тощо;

будь-які дії, що можуть призвести до розголошення конфіденційної інформації, атрибутів розмежування доступу, втрати цих атрибутів тощо;

неправомірне встановлення та використання ПЗ, забороненого політикою безпеки (наприклад, навчальних та ігрових програм, системного та прикладного забезпечення тощо);

наслідки некваліфікованого використання засобів захисту інформації.

До навмисних загроз суб'єктивного характеру, спрямованих на дестабілізацію роботи АС (або її окремих елементів), виведення її з ладу, несанкціоноване проникнення та отримання доступу до її ресурсів, належать:

фізичне пошкодження АС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

порушення функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, заземлення, охоронної сигналізації, вентиляції тощо);

порушення режимів роботи АС (апаратного та програмного забезпечення);

впровадження та використання комп'ютерних вірусів, апаратних і програмних закладок, підслуховуючих пристроїв та інших засобів розвідки;

використання методів перехоплення побічних електромагнітних випромінювань і наведень, акустично-електричних перетворень інформаційних сигналів;

використання персоналу АС з корисливою метою (шантаж, підкуп тощо);

крадіжка носіїв інформації, виробничих відходів (роздруківок, записів тощо);

несанкціоноване копіювання носіїв інформації;

зчитування залишкової інформації з оперативної пам'яті комп'ютерів, зовнішніх накопичувачів;

отримання облікових даних з подальшим їх використанням для маскування під легітимного користувача («маскарад»);

неправомірне підключення до каналів зв'язку, перехоплення переданих даних, аналіз трафіку тощо;

впровадження та використання ПЗ, забороненого політикою безпеки, або несанкціоноване використання ПЗ, що може надати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж).

Загалом же потенційні загрози інформації, що обробляється в АС для підприємства представлені у додатку Т, таблиці Т.1.

Наступним етапом стане формування моделі порушника об’єкта інформаційної діяльності для підприємства. Під порушником розуміється фізична особа, яка здійснила спробу виконання заборонених операцій, незалежно від її мотивації. Ці дії можуть бути зумовлені помилкою через недостатню обізнаність, ненавмисним характером, або ж мати навмисний зловмисний намір (корисливий інтерес) чи здійснюватися без такої мети (задля розваги, самоствердження), з метою самоствердження або помсти, з використанням різноманітних способів, методів, можливостей та засобів.

Порушник може застосовувати широкий спектр методів та засобів для отримання доступу до інформації з обмеженим доступом. У випадку, коли дії порушника є навмисними та зумовлені корисливими мотивами, його ідентифікують як зловмисника. Зловмисники, як правило, проводять ретельний аналіз систем безпеки в інформаційно-технологічній системі перед здійсненням спроби проникнення. Найчастіше використовується неформалізована модель порушника (зловмисника), яка описує причини та мотиви його дій, наявні можливості, рівень знань, цілі, основні шляхи досягнення цих цілей (способи реалізації загроз), місце та характер дії, можливу тактику тощо. Для досягнення запланованих цілей зловмисник повинен докласти певних зусиль та витратити відповідні ресурси.

Порушниками АС можуть виступати як внутрішні особи (персонал та користувачі системи), так і зовнішні особи (сторонні).

До можливих внутрішніх порушників належать:

кінцеві користувачі (оператори системи) (перший рівень);

технічний та обслуговуючий персонал (третій рівень);

співробітники відділу розробки та супроводження ПЗ (четвертий рівень);

співробітники служби безпеки АС (перший рівень);

керівники різних рівнів (перший рівень).

До можливих зовнішніх порушників (сторонніх осіб) належать:

технічний персонал, що обслуговує будівлю (перший рівень);

клієнти (перший рівень);

представники організацій-конкурентів (другий рівень);

відвідувачі з різних причин (другий рівень).

Порушники класифікуються відповідно до рівня можливостей, що надаються їм штатними засобами комп'ютерної системи. Виділяється 4 рівні таких можливостей, причому дана класифікація є ієрархічною, тобто кожен наступний рівень включає в себе функціональні можливості попереднього.

Перший рівень визначає базовий рівень взаємодії з комп'ютерною системою, що обмежується можливістю запуску попередньо визначеного набору завдань (програм), які реалізують заздалегідь запрограмовані функції обробки інформації.

Другий рівень характеризується можливістю розробки та запуску власних програм з новими функціями обробки інформації.

Третій рівень визначає можливість управління функціонуванням комп'ютерної системи, включаючи вплив на базове ПЗ системи, її апаратну конфігурацію та склад обладнання.

Четвертий рівень охоплює весь спектр можливостей осіб, залучених до проектування, реалізації та ремонту апаратних компонентів комп'ютерної системи, аж до інтеграції власних засобів з новими функціями обробки інформації до складу системи.

Передбачається, що на своєму рівні порушник є висококваліфікованим фахівцем, який володіє повною інформацією про комп'ютерну систему та застосовуваний комплекс засобів захисту. Несанкціонований доступ до

інформації може здійснюватися порушником як під час активної роботи АС, так і в періоди її неактивності, або ж шляхом комбінування обох часових інтервалів. У комплексній системі захисту інформації на виділеному об’єкті передбачаються, розглядаються і розробляються усі 4 рівні порушників (табл. 3.1).

Таблиця 3.1

Модель порушника для підприємства

№	Користувач АС	Рівень порушника
1.	Внутрішні	
1.1	Оператор системи	I
1.2	Співробітники відділу розробки і супроводження ПЗ	IV
1.3	Персонал	I
2.	Зовнішні	
2.1	Працівник служби охорони	III
2.2	Працівник комунальних служб	III
2.3	Конкуренти	IV
2.3	Клієнт	III

Для прийняття обґрунтованих рішень щодо інвестицій у систему захисту необхідно оцінити потенційні збитки від порушень безпеки, зокрема витоку інформації, та ймовірність їхнього виникнення. Вартість системи захисту слід співвідносити з можливими втратами та їхньою вірогідністю. Зважаючи на складність кількісної оцінки реальної цінності інформації, перевага надається якісним експертним оцінкам.

3.2. Модернізація виробництва шляхом впровадження заходів інформаційної безпеки

Впровадження інформаційної безпеки прямо впливає на економічну ефективність модернізації виробництва, переводячи витрати на безпеку з пасивних (накладних) у стратегічні (інвестиційні) витрати:

зниження операційних збитків – захист АСУ ТП від атак мінімізує ризик простоїв, псування партій пива та аварій, це забезпечує безперервність виробництва (Business Continuity);

зростання конкурентоспроможності – наявність надійних систем захисту (особливо даних про якість і походження сировини) підвищує довіру споживачів та партнерів, що є важливим елементом репутаційного капіталу;

забезпечення відповідності (Compliance) – дотримання національних стандартів та міжнародних норм (наприклад, стандартів якості харчової промисловості) дозволяє підприємству виходити на нові ринки, витрати на штрафи та судові процеси через порушення захисту даних значно перевищують витрати на превентивну інформаційну безпеку.

Модернізація виробництва підприємства шляхом впровадження заходів інформаційної безпеки (ІБ) є актуальним і багатоаспектним процесом. Модернізація виробництва не зводиться лише до оновлення обладнання. У сучасному бізнес-середовищі вона включає:

Технологічну модернізацію: встановлення нових АСУ ТП (автоматизованих систем управління технологічними процесами), сенсорів, контролерів та обладнання для підвищення ефективності броварства (затирання, фільтрації, ферментації);

Організаційну модернізацію: перебудову бізнес-процесів, впровадження ERP/MES систем (планування ресурсів підприємства/системи управління виробництвом) та систем управління якістю (наприклад, HACCP);

Інформаційну модернізацію: цифрову трансформацію, що передбачає збір, обробку, зберігання та захист великих обсягів даних (Big Data) про якість сировини, процес ферментації, логістику та продажі.

Впровадження інформаційної безпеки є не просто додатковим заходом, а фундаментом успішної інформаційної модернізації. Без інформаційної безпеки, будь-яка інша технологічна модернізація створює додаткові вразливості, а не переваги.

Для модернізації виробництва підприємства шляхом впровадження заходів інформаційної безпеки покладемо в основу кілька ключових теоретичних підходів:

Модель «Тріада КІД» (CIA Triad). Це класична модель, за якою визначаються основні цілі інформаційної безпеки для підприємства:

конфіденційність (confidentiality) – забезпечення нерозголошення критичної інформації. Для підприємства це рецептури, комерційна таємниця, дані про клієнтів і постачальників, а також фінансова інформація;

цілісність (integrity) – гарантування точності та повноти даних, що особливо критично для харчової промисловості. Порушення цілісності даних у системі управління якістю або АСУ ТП може призвести до виробництва неякісної, небезпечної продукції або зупинки лінії.

доступність (availability) – забезпечення безперебійного доступу до ІТ-систем і технологічних процесів. У пивоварній галузі простої через кібератаки (наприклад, атака програм-вимагачів) призводять до псування сировини, порушення циклу ферментації та значних фінансових втрат.

Теорія управління ризиками (Risk Management Theory). Згідно з даною теорією модернізація інформаційної безпеки підприємства має базуватися на систематичній оцінці ризиків, зокрема:

ідентифікації активів, тобто визначення критичних ІТ-активів (АСУ ТП, ERP, сервери рецептур);

визначення загроз і вразливостей, тобто оцінка ймовірності зовнішніх (хакерські атаки, шпигунство) та внутрішніх (несанкціонований доступ, помилки персоналу) загроз;

обробка ризиків, тобто впровадження захисних заходів (контролів) згідно з принципом, що вартість захисту не повинна перевищувати вартість активу або потенційних збитків.

Модернізація виробництва збільшує кількість точок входу (сенсори, мережа) і, відповідно, кіберризиків, що робить впровадження інформаційної безпеки обов'язковим елементом модернізації.

Шестикроковий процес створення плану управління ризиками проекту для підприємства передбачає визначення переліку потенційних ризиків, імовірності виникнення цих ризиків та їхнього негативного впливу, шляхів запобігання або пом'якшення ризиків, розгляд непередбачуваних ситуацій та встановлення точок запуску для активізації заходів у разі настання непередбачуваної ситуації.

На основі власного проекту «Модернізація виробництва підприємства» (додаток У) було складено список потенційних ризиків проекту та розставлено їх за пріоритетом, використовуючи показник «Високий-Середній-Низький» (табл. 3.2).

Таблиця 3.2

Матриця ризиків проекту на етапі впровадження заходів модернізації виробництва підприємства, за 2025-2026 рр.

ВПЛИВ				
високий	Різкі зміни законодавства ІБ Кібератака під час перехідного періоду	Затримка постачання обладнання/ПЗ Нестача фінансування під час реалізації	Опір персоналу змінам
середній	Відмова ключового постачальника ПО	Технічна несумісність нового ПЗ зі старими системами	Низький рівень ІТ-компетенцій персоналу
низький			
	низька	середня	висока
	ЙМОВІРНІСТЬ		

На основі аналізу даної матриці було обрано три найнебезпечніші ризики для підприємства та визначено превентивні заходи по їх недопущенню, визначені можливі непередбачувані ситуації, а також точки запуску коригування (коли необхідно розпочинати реалізацію коригуючих заходів), відобразивши у табл. 3.3. Реєстр ризиків аналізується щотижнево на статусній

нараді. У разі появи нового ризику – він вноситься в реєстр і призначається відповідальний.

Таблиця 3.3

Управління потенційними ризиками для підприємства на етапі впровадження заходів модернізації виробництва підприємства, за 2025-2026 рр.

№	Найнебезпечніші ризики	Превентивні заходи	Непередбачувані ситуації	Точка запуску коригування
1.	Опір персоналу змінам	- навчання перед впровадженням; - роз'яснювальна HR-комунікація; - тестовий запуск на 1 відділі	- саботаж нових процедур ІБ; - ігнорування нових політик безпеки	якщо >25% працівників не виконує нові правила
2.	Затримка постачання	- договори з альтернативними постачальниками; - резерв по термінах 2–4 тижні	-митні затримки; - відсутність товару у всіх постачальників	затримка >7 календарних днів
3.	Нестача фінансування	- деталізація бюджету за етапами; - резерв 10%; - поетапна оплата	- підвищення цін на ПЗ; - курсові коливання	перевищення бюджету етапу на >15%

Концепція кіберстійкості (Cyber Resilience). Цей підхід, що є розвитком інформаційної безпеки та може бути застосовуваним після впровадження розробленого нами проекту з модернізації виробництва підприємства, передбачає, що атаки неминучі. Головна мета – не лише запобігти, але й забезпечити здатність системи:

швидко виявляти інциденти;

обмежувати їхній вплив;

відновлювати нормальну роботу підприємства з мінімальними втратами часу та даних.

Для підприємства це означає наявність плану відновлення після інциденту (Disaster Recovery Plan), який охоплює не лише IT, але й технологічний цикл.

Для такого підприємства, як пивоварний завод, що реалізує складні проекти з модернізації виробництва шляхом впровадження заходів

інформаційної безпеки ієрархічна структура робіт (Work Breakdown Structure, WBS) є необхідним фундаментом для успішного виконання, контролю та завершення проєкту.

Ієрархічна структура робіт (WBS) є ключовим інструментом управління проєктами, що забезпечує структуроване та повне охоплення всіх робіт, необхідних для реалізації проєкту на підприємстві зображена у додатку Ф на рис. Ф.1. WBS допомагає чітко визначити 100% обсягу робіт, запобігає дублюванню зусиль. Кожен елемент роботи в WBS (пакет робіт) виконується лише один раз, забезпечуючи, що ресурси не витрачаються даремно, наприклад, на повторну закупівлю чи проєктування. На основі найнижчого рівня WBS (пакетів робіт) можна точно оцінити необхідні ресурси (людські, фінансові, матеріальні, час). Це критично для фінансового планування інвестиційного проекту, WBS дозволяє визначити тривалість кожного окремого завдання та їхню залежність (логічний зв'язок). Це є основою для побудови календарного графіка (діаграми Ганта) та визначення критичного шляху проєкту, що важливо для уникнення простоїв виробництва. План-графік робіт по проекту, що описує всі контрольні точки та роботи із призначеними датами початку та завершення, взаємозв’язку завдань необхідних для реалізації проєкту модернізації виробництва на підприємстві шляхом впровадження заходів інформаційної безпеки зображений у додатку Х таблиці Х.1.

Вартісний план проекту складає 250000 грн, який розподілений за часом освоєння на 6 місяців та складається с наступних статей витрат:

закупівля обладнання засобів ІБ (українські постачальники) 150000 грн;

монтаж та налаштування 40 000 грн;

навчання персоналу 60000 грн;

Параметрами та критеріями досягнення якості проекту, щодо яких відбуватиметься контроль якості отриманих результатів, що сформовані у плані якості проекту є працездатність впровадженої системи інформаційної безпеки підтверджена тестуванням і актами приймання.

Всі учасники проекту проєкту модернізації виробництва із зазначенням строків їх зайнятості по проекту та відсотка завантаженості розміщені та вказані у табл. 3.4.

Таблиця 3.4

Учасники проекту із зазначенням строків їх зайнятості по проекту та відсотка завантаженості, за 2025-2026 рр.

Учасник	Роль	Відповідальність	Завантаженість
Заступник директора	Керівник проекту	Загальне керівництво проектом, прийняття рішень	100%
Відділ ІТ	Виконавець технічних робіт	Монтаж, конфігурація, тестування систем ІБ	50%
Планово-економічний відділ	Відповідальний за бюджет і закупівлі	Контроль бюджету, оплати постачальникам	20%
Служба управління персоналом	Відповідальний за навчання	відповідає за організацію навчання персоналу	30%

Команда проекту та план управління нею зображені на рис. 3.1.

Рис. 3.1. Організаційна структура управління командою проекту на підприємстві

Для підприємства, особливо під час модернізації виробництва чи впровадження нових систем (як-от ІБ), використання матриці RACI є критично необхідним для уникнення плутанини та забезпечення ефективної комунікації. Матриця відповідальності, або матриця RACI (RACI Matrix), є важливим інструментом управління проєктами, який використовується для чіткого визначення та документування ролей і рівня участі зацікавлених сторін (Stakeholders) у виконанні завдань, досягненні результатів або ухваленні

рішень у рамках проєкту чи процесу. У складних проєктах, де задіяні різні відділи (виробництво, IT, фінанси, логістика), часто виникає проблема розмивання відповідальності («хто це мав робити?»). Матриця RACI усуває цю плутанину, чітко призначаючи одного Відповідального (A) та конкретних Виконавців (R) для кожного завдання (завдання з WBS). Назва RACI є акронімом, де кожна літера відповідає за певний рівень відповідальності або участі:

A – Accountable – відповідальний за роботу, яку будуть виконувати інші люди, це відповідальність за наслідки делегування, її делегувати неможливо, за наслідки завжди відповідає один;

R – Responsible – відповідальний за власне виконання роботи чи її результат.

Оскільки лише одна особа є Відповідальною (A), процес затвердження рішень не затримується через узгодження з багатьма особами. Це прискорює проходження критичних етапів проєкту модернізації на підприємстві. Завдяки WBS та RACI, керівництво підприємства може точно бачити, які ресурси задіяні, скільки часу вони витрачають на консультації, а скільки – на безпосереднє виконання (R). Це дозволяє виявляти перевантаження ключових фахівців. Впровадження RACI для підприємства (табл. 3.5) є організаційною складовою модернізації, яка гарантує, що технічні та технологічні зміни будуть реалізовані структуровано, контрольовано та ефективно.

Таблиця 3.5

Матриця відповідальності (RACI) учасників проекту

Завдання	Керівник проекту	Відділ IT	Планово-еконо-мічний відділ	Служба управління персонлом
Аналіз стану ІБ	A	R	-	-
Закупівля обладнання	A	-	R	-
Монтаж систем	A	R	-	-
Навчання персоналу	A	R	-	R
Оплати і бюджет	A	-	R	-

Для оцінювання взаємозв'язку між витратами на інформаційну безпеку та величиною чистого прибутку доцільно застосувати аналіз парної регресії, де змінна X представляє витрати на інформаційну безпеку, а змінна Y - показники чистого прибутку (додаток Ц). На рисунку 3.2 подано графічне відображення динамічної залежності прибутку від зміни обсягів фінансування заходів з інформаційної безпеки підприємства.

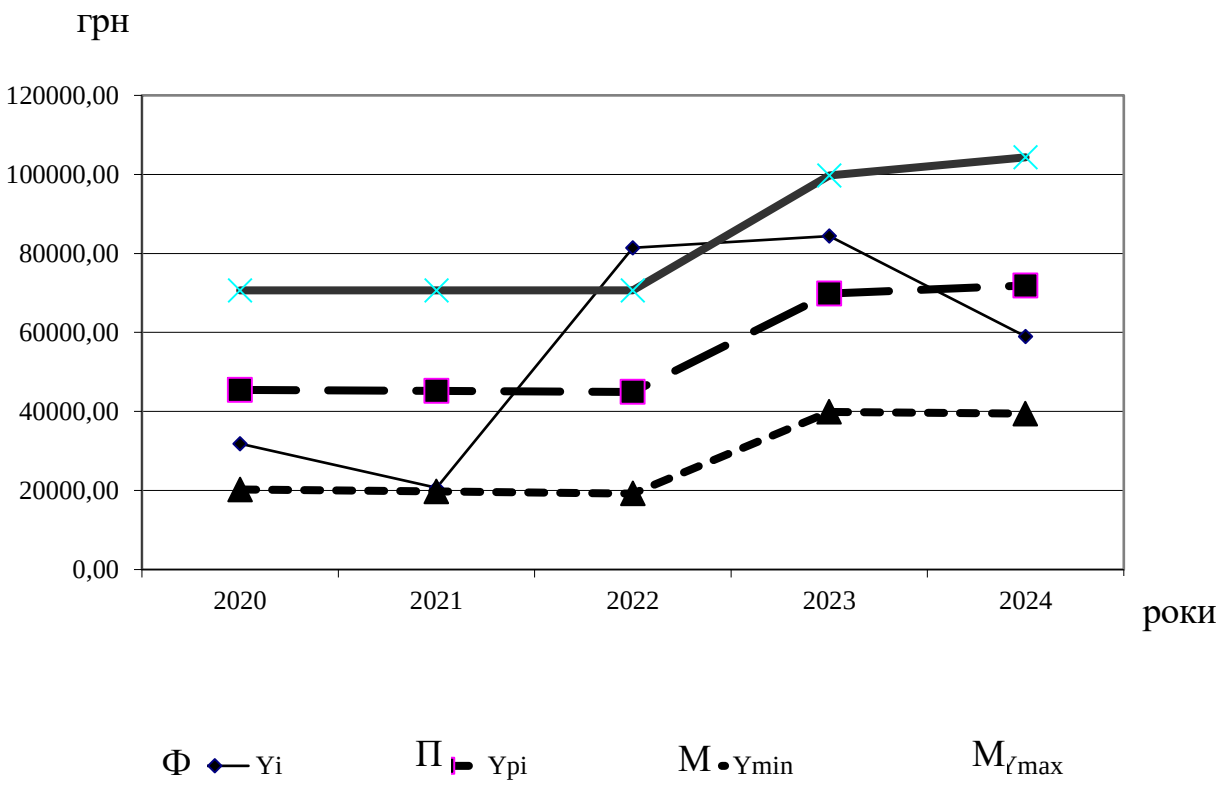

Рис. 3.2. Динаміка зміни показників залежності зміни прибутку від витрат на інформаційну безпеку підприємства, за 2020-2024 рр.

Результати розрахунків, наведені у додатку Ц, демонструють істотний зв'язок між аналізованими показниками. З урахуванням міжнародних стандартів та нормативних кодексів у сфері інформаційної безпеки, а також середніх показників діяльності промислових підприємств України, встановлено, що формування комплексної системи інформаційної безпеки здатне забезпечити зростання чистого прибутку на рівні 1–1,5 %.

Відповідно до проведеного аналізу модернізації виробництва шляхом впровадження заходів інформаційної безпеки, очікуване збільшення чистого прибутку підприємства становитиме лише 0,2 %. Поясненням відносно невисоких результатів приросту у порівнянні з очікуваним, що усталився у вітчизняній та міжнародній практиці, є те, що досліджуваний період діяльності підприємства припав на досить складний період для виявлення стійких тенденцій та закономірностей для всіх українських підприємств, а саме, перші 2 роки дослідження припали на мирний період діяльності підприємства, з початком широкомасштабної війни росії проти України, перед більшістю українських підприємств постали нові виклики, як на фоні різкого падіння курсу гривні, великої інфляції, порушення логістичних ланцюжків, здорожчання сировини та витратних матеріалів, необхідність підтримки армії, волонтерських ініціатив, місцевих громад, так і, особливо для підприємств, що випускають алкогольну продукцію, обмеження на її продаж у зв'язку з комендантськими годинами та регіонами наближеними до бойових дій та особливо починаючи з 2024 року досить відчутне падіння попиту серед населення, як із причин падіння купівельної спроможності, зміни структури споживання та надання пріоритету товарам першої необхідності, а також зменшення продажів у HoReCa через закриття або обмеження роботи закладів. Проте, незважаючи на відносно скромні очікувані фінансові показники, доцільність проведення даних заходів продиктована підвищенням кількості кібератак на підприємства харчової промисловості, потребою в нових системах захисту інформації та безперервності бізнес-процесів як у воєнний час, так і в післявоєнну відбудову України.

Таким чином, модернізація виробництва підприємства через впровадження заходів інформаційної безпеки – це інвестиція, що забезпечує довгострокову стійкість, цілісність критичних активів та економічну безперервність діяльності підприємства.

Висновки до розділу 3

Таким чином, у третьому розділі кваліфікаційної роботи були отримані наступні результати:

1. Узагальнені потенційні загрози інформації, що обробляється в АС, результатом чого стала розробка моделі загроз для інформації та сформована модель порушника для об'єкта інформаційної діяльності підприємства.

2. Модернізація виробництва підприємства шляхом впровадження заходів інформаційної безпеки є не просто додатковим заходом, а фундаментом успішної інформаційної модернізації. Без інформаційної безпеки, будь-яка інша технологічна модернізація створює додаткові вразливості, а не переваги. Для модернізації виробництва покладена в основу модель «Тріада КІД» (CIA Triad), за якою визначені основні цілі інформаційної безпеки для підприємства: конфіденційність (C), цілісність (I), доступність (A). Застосована теорія управління ризиками (Risk Management Theory), шляхом розробки плану управління ризиками, який передбачає визначення переліку потенційних ризиків, імовірності виникнення цих ризиків та їхнього негативного впливу, шляхів запобігання або їх пом'якшення, розгляд непередбачуваних ситуацій та встановлення точок запуску для активізації заходів у разі настання непередбачуваної ситуації. Результатом цього стала розробка матриці ризиків підприємства та визначено превентивні заходи по їх недопущенню.

3. На основі власного проекту «Модернізація виробництва підприємства» була розроблена ієрархічна структура робіт (WBS), що є необхідним фундаментом для успішного виконання, контролю та завершення проєкту. Розроблений календарний план-графік робіт по проекту з модернізації виробництва, визначені всі учасники проєкту із зазначенням строків їх зайнятості по проекту та відсотка завантаженості, визначений план управління командою проекту та створена матриця відповідальності (RACI Matrix) учасників проекту, що є критично необхідним для уникнення плутанини та забезпечення ефективної комунікації на підприємстві під час впровадження заходів інформаційної безпеки.

ВИСНОВКИ

На основі виконаного дослідження на тему: «Управління інформаційною безпекою підприємства в сучасному бізнес-середовищі» доцільно зробити наступні висновки.

1. Розглянуто сутність, роль та значення системи управління інформаційною безпекою підприємства в ринкових умовах господарювання. Досліджені основні принципи інформаційної безпеки, методи запобігання та ліквідації загроз інформаційній безпеці, класи загроз інформаційної безпеки організації.

2. Зроблений огляд тенденцій та досвід з управління інформаційною безпекою в Україні. Розкрита та охарактеризована спеціально орієнтована методика прийняття управлінських рішень на базі технологій інформаційного менеджменту «Бізнес-довідка» («конкурентна розвідка»).

3. Розглянуті загальні відомості про підприємство, проаналізована організаційна структура управління, виконаний аналіз управління персоналом.

4. Проведений комплексний аналіз техніко-економічних показників діяльності підприємства. Так, зокрема, був зроблений висновок про те, що підприємство за 2020-2024 роки діяльності має досить потужне та міцне фінансове становище. Проте недоліком в роботі підприємства є надмірна величина не використовуваних належним чином вільних грошових коштів, що може свідчити про не досить високу ефективність управління оборотним капіталом на підприємстві.

5. Виконаний аналіз системи управління інформаційною безпекою підприємства, який дозволяє зробити висновок, що товариство в цілому захищене достатньо добре, проте не позбавлено деяких недоліків. Підприємство має базовий рівень організації інформаційної безпеки, який відповідає мінімальним вимогам для виробничого підприємства середнього розміру. До основних досягнень можна віднести: наявність правової бази та

функціональний захист, а також можемо підкреслити свідомість персоналу. Зокрема, впроваджено необхідні локальні нормативні документи, що регламентують доступ до інформації, використання корпоративних ресурсів та політику конфіденційності, що відповідає вимогам законодавства України. Забезпечено базовий захист мережевої інфраструктури (міжмережеві екрани, антивірусне програмне забезпечення) та резервне копіювання критично важливих даних (бухгалтерський облік, виробничі рецептури). Зафіксовано відносно високий рівень обізнаності ключових співробітників відділу ІТ та бухгалтерії щодо основних загроз (фішинг, шкідливе ПЗ).

6. В основі комплексу заходів щодо інформаційної безпеки підприємства були узагальнені потенційні загрози інформації, що обробляється в АС, результатом чого стала розробка моделі загроз для інформації та сформована модель порушника для об’єкта інформаційної діяльності підприємства.

7. Модернізація виробництва підприємства шляхом впровадження заходів інформаційної безпеки є не просто додатковим заходом, а фундаментом успішної інформаційної модернізації. Без інформаційної безпеки, будь-яка інша технологічна модернізація створює додаткові вразливості, а не переваги. Для модернізації виробництва покладена в основу модель «Тріада КІД» (CIA Triad), за якою визначені основні цілі інформаційної безпеки для підприємства: конфіденційність (C), цілісність (I), доступність (A). Застосована теорія управління ризиками (Risk Management Theory), шляхом розробки плану управління ризиками, який передбачає визначення переліку потенційних ризиків, імовірності виникнення цих ризиків та їхнього негативного впливу, шляхів запобігання або їх пом’якшення, розгляд непередбачуваних ситуацій та встановлення точок запуску для активізації заходів у разі настання непередбачуваної ситуації. Результатом цього стала розробка матриці ризиків підприємства та визначено превентивні заходи по їх недопущенню.

8. На основі власного проекту «Модернізація виробництва підприємства» була розроблена ієрархічна структура робіт (WBS), що є

необхідним фундаментом для успішного виконання, контролю та завершення проєкту. Розроблений календарний план-графік робіт по проекту з модернізації виробництва, визначені всі учасники проєкту із зазначенням строків їх зайнятості по проекту та відсотка завантаженості, визначений план управління командою проекту та створена матриця відповідальності (RACI Matrix) учасників проекту, що є критично необхідним для уникнення плутанини та забезпечення ефективної комунікації на підприємстві під час впровадження заходів інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Господарський кодекс України : Закон України від 16.01.2003 № 436-IV *Відомості Верховної Ради України.* – 2003. – № 18–22. – Ст. 144.

2. Наказ КМУ від 29.04.2021 №439-р. Стратегія кібербезпеки України. – URL: https://zakon.rada.gov.ua/laws/show/447/2021

3. Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV *Відомості Верховної Ради України.* – 2003. – № 40–44. – Ст. 356.

4. Азаров А. М. Кібербезпека бізнес-процесів: стратегії та моделі управління. Київ: Ліра-К. 2023. 380 с.

5. Барановський О. М., Захарченко В. А. Економічна безпека та управління ризиками в інформаційному просторі. Львів: Новий Світ-2000. 2024. 412 с.

6. Бачило І. Д., Черкашина А. О. Інформаційна безпека підприємства: теорія та практика. К.: Центр учбової літератури. 2020. 248 с.

7. Береза А. В. Моделювання загроз інформаційній безпеці підприємств у непередбачуваному середовищі. *Вісник економічної науки України*. 2023. №1. С. 45–51.

8. Бєляєв В. М. Інформаційна безпека підприємства: організаційно-правовий та економічний аспекти. Харків: Право. 2022. 315 с.

9. Боголюбський О.Є. Сучасні проблеми управління інформаційною безпекою підприємства. *Менеджмент XXI століття: глобалізаційні виклики:* матеріали IX Міжнародної науково-практичної конференції. 15 травня 2025р. Полтава: ПДАУ. 2025. С. 599-601.

10. Бондаренко С. В. Менеджмент інформаційної безпеки: підручник. К.: НАУ. 2022. 280 с.

11. Борисенко М. А. Роль CISO у формуванні культури кіберстійкості компанії. *Економіка та управління підприємствами*. 2022. №3. С. 112–119.

12. Бутенко В. І. Ризики в інформаційних системах. Харків: ХНУРЕ. 2020. 150 с.

13. Величко Р. С. Забезпечення інформаційної безпеки в контексті віддаленої роботи. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство*. 2024. Вип. 52. С. 87–93.

14. Власенко С. В., Мельник І. Р. Цифрова трансформація та захист даних в умовах глобалізації. Одеса: Гельветика. 2021. 290 с.

15. Герасименко П. Л. Вплив цифрового тіньового ринку на інформаційну безпеку бізнесу. *Актуальні проблеми економіки*. 2021. №11. С. 160–168.

16. Гордієнко І. А. Кібербезпека і управління в цифрову епоху. К.: Академперіодика. 2021. 230 с.

17. Гуменюк О. О. Управління кіберризиками підприємства: методологічний підхід. Вінниця: Дім книги. 2025. 350 с.

18. Дзюба І. А. Оцінка ефективності інвестицій в системи інформаційної безпеки. *Фінанси України*. 2023. №7. С. 78–85.

19. Демчук П. В., Коваль Л. І. Інформаційна безпека: навчальний посібник. Київ: Центр навчальної літератури. 2020. 256 с.

20. Дячков Д. В. Характеристика сучасних загроз системі управління інформаційною безпекою аграрних підприємств. *Науково-виробничий журнал «Бізнес-навігатор»*. 2019. Випуск 6.1-1 (56). С. 172–177.

21. Дячков Д. В. Формування моделі політики інформаційної безпеки на основі концепцій «глибинного захисту». *Підприємництво і торгівля : збірник наукових праць. Львів : Видавництво Львівського торговельно-економічного університету.* 2019. Вип. 25. С. 116–121..

22. Дячков Д. В. Розробка методологічних засад оцінювання та діагностики інформаційної безпеки підприємств агропродовольчої сфери. *Український журнал прикладної економіки.* 2019. Том 4. № 3. С. 188–197. (0,87 друк. арк.).

23. Дячков, Д. В. Стратегічні напрями управління інформаційною безпекою підприємств агропродовольчої сфери. *Український журнал прикладної економіки.* 2019. Том 4. № 4. С. 70–78.

24. Задорожна Н. О. Інтеграція штучного інтелекту в системи моніторингу кіберзагроз. *Проблеми економіки*. 2024. №2. С. 145–152.

25. Іванов А. В. Безпека інформаційних систем у менеджменті. Дніпро: Арт-Прес. 2023. 301 с.

26. Кавун С. І. Економічна безпека підприємства: інформаційний аспект. Х.: Ун-т внутр. Справ. 2020. – 198 с.

27. Касьянова Н. В. Інформаційна безпека організації: ризики, захист, управління. Одеса: ОНУ. 2019. 235 с.

28. Кириленко С. В. Особливості управління інцидентами інформаційної безпеки в умовах воєнного стану. *Науковий журнал «Кібербезпека та інформаційний менеджмент»*. 2022. Вип. 4. С. 22–30.

29. Климко А. М., Савченко Г. Л. Стратегічний менеджмент інформаційної безпеки. Київ: Кондор. 2024. 400 с.

30. Ковальчук О. П. Система управління інформаційною безпекою: моделі, методи. Львів: ЛНУ. 2019. 208 с.

31. Колісник В. П. Комплексний захист інформації в корпоративних мережах. Чернівці: Букрек. 2022. 320 с.

32. Кузьменко О. П. Формування політики інформаційної безпеки як елемент корпоративного управління. *Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку*. 2021. Вип. 1. С. 190–197.

33. Лисиця Ю. С. Аналіз сучасних міжнародних стандартів (ISO/IEC 27001) та їх застосування в українському бізнесі. *Економічний часопис – XXI*. 2023. №9-10. С. 105–110.

34. Марчук В. І. Фактори підвищення кіберстійкості малих та середніх підприємств. *Вісник Київського національного університету імені Тараса Шевченка. Економіка*. 2024. Вип. 6. С. 55–61.

35. Нікітін Л. М. Застосування ризик-орієнтованого підходу в управлінні інформаційною безпекою. *Економіст*. 2020. №8. С. 70–75.

36. Нестеренко О. Г. Роль інформаційної безпеки в стратегії розвитку підприємства. Економіка. 2021. №7. С. 45–52.

37. Омельченко Т. Р. Хмарні технології та управління безпекою даних: виклики та рішення. *Науковий вісник Одеського національного економічного університету*. 2022. Вип. 1. С. 130–136.

38. Пархоменко І. І. Управління ризиками інформаційної безпеки. К.: КНЕУ. 2018. 187 с.

39. Петренко О. В. Аудит інформаційної безпеки: стандарти та практика. Київ: Знання. 2021. 288 с.

40. Полозова Т. В. Формування системи показників оцінки рівня інформаційної безпеки підприємства / Т. В. Полозова, О. В. Стороженко, М. Ю. Журавель // *Вісник економіки транспорту і промисловості.* 2011. № 33. С. 171-177

41. Попова І. В. Розвиток системи управління безперервністю бізнесу (BCM) через призму кібербезпеки. *Збірник наукових праць НАН України. Економіка*. 2025. Вип. 1. С. 90–97.

42. Сазонова Т.О., Боголюбський О.Є. Стратегічне управління інформаційною безпекою підприємства. *Менеджмент XXI століття: глобалізаційні виклики*: матеріали IX Міжнародної науково-практичної конференції, 15 травня 2025 р. Полтава: ПДАУ. 2025. С. 546-548.

43. Саєнко Ю. О. Гібридні загрози та захист економічних інтересів підприємств. Ужгород: Закарпаття. 2025. 340 с.

44. Сидоренко А. М. Проблеми захисту персональних даних в українському бізнесі в умовах GDPR. *Право та безпека інформаційних технологій*. 2023. №5. С. 45–53.

45. Скрипник А. І., Горбунов Ю. В. Інформаційна безпека в сучасних IT-системах. Х.: Фоліо. 2021. 310 с.

46. Тарасов С. В. Аудит інформаційної безпеки: навчальний посібник. Дніпро: ДНУ. 2020. 215 с.

47. Ткаченко В. П. Впровадження системи DLP для запобігання витоку комерційної таємниці. *Інформаційні технології та безпека*. 2021. №2. С. 75–82.

48. Харченко О. М. Захист критичної інформаційної інфраструктури: державний та корпоративний рівні. *Стратегічні пріоритети*. 2024. Вип. 3. С. 115–123.

49. Чумак Л. І. Соціальна інженерія як загроза інформаційній безпеці та методи протидії. *Вісник економічної теорії та міжнародних відносин*. 2020. №4. С. 180–187.

50. Шевченко А. А. Безпека інформації в ІТ-проєктах. Запоріжжя: ЗНУ. 2022. 192 с.

51. Шевчук Р. О. Управління доступом та ідентифікацією (IAM) у сучасній ІТ-архітектурі. *Інтелект XXI*. 2023. Вип. 6. С. 150–157.

52. Шматько Л. В. Політика інформаційної безпеки підприємства. К.: НАДУ. 2019. 170 с.

53. Федорова Л. В. Управління інформаційною безпекою на основі міжнародних стандартів. Львів: Магнолія. 2020. 295 с.

54. Andress M. The Basics of Information Security. Syngress, 2020. 304 p.

55. Whitman M. E., Mattord H. J. Principles of Information Security. 6th ed. Cengage Learning. 2021. 720 p.

ДОДАТКИ