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

Освітньо-професійна програма Бізнес-адміністрування
Спеціальність 073 Менеджмент
Ступінь вищої освіти Магістр

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ
Завідувач кафедри _____
Тетяна ВОРОНЬКО-НЕВІДНИЧА
26 грудня 2022 року

КВАЛІФІКАЦІЙНА РОБОТА

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

виконав здобувач вищої освіти денної форми навчання

Кривчун Ростислав Юрійович

Керівник кваліфікаційної роботи Вікторія Медвідь

Полтава – 2022 року

ЗМІСТ

ВСТУП

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

Вивченням питання інформаційної безпеки займалися такі вчені, як: Абрамчук М., Богуш В., Герасименко А., Гуцу С., Деркач М., Дячков Д., Живко З., Захаркін О., Козак А., Кормич Б., Ліпкан В., Максименко Ю., Маркіна І., Марущак А., Ортинський В., Сороківська О., Петрик В. Нашинець-Наумова А., Шевченко С. та ін.

Метою кваліфікаційної роботи є обґрунтування теоретичних положень та розробка практичних рекомендацій щодо управління інформаційною безпекою підприємства в сучасному бізнес-середовищі. Це обумовило необхідність розв'язання наступних **завдань**:

дослідити сутнісну характеристику інформаційної безпеки підприємства;

охарактеризувати систему управління інформаційною безпекою

підприємства;

здійснити загальну характеристику підприємства;

провести організаційно-економічний аналіз показників господарської діяльності підприємства;

оцінити управління інформаційною безпекою підприємства;

надати рекомендації щодо вдосконалення процесу забезпечення захисту інформації в підприємстві;

удосконалити систему управління інформаційною безпекою підприємства.

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

Предметом виступають теоретичні, методичні положення та практичні рекомендації щодо процесу управління інформаційною безпекою підприємства в сучасному бізнес-середовищі.

Інформаційна база кваліфікаційної роботи формувалась на основі праць вітчизняних та зарубіжних вчених у галузі інформаційної безпеки, законодавчих і нормативно-правових документів України, матеріалів науково-практичних конференцій, статистичних даних комітету статистики України, статистичної звітності досліджуваного підприємства. Обробку та аналіз інформації здійснено за допомогою сучасних програмних продуктів.

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

Методи дослідження. У роботі використано метод узагальнення та порівняння; метод аналогії, порівняння та інтегрування; метод аналізу некількісних показників; метод графічного зображення аналітичних даних.

Елементи наукової новизни одержаних результатів дослідження полягають у подальшому розвитку теоретико-методичних аспектів і науково-

практичних рекомендацій відносно управління інформаційною безпекою підприємства в сучасному бізнес-середовищі, а саме: досліджено сутнісну характеристику інформаційної безпеки підприємства та охарактеризовано систему управління інформаційною безпекою підприємства.

Практична значущість кваліфікаційної роботи полягає у вдосконаленні управління інформаційною безпекою підприємства в сучасному бізнес-середовищі шляхом вдосконалення процесу забезпечення захисту інформації в підприємстві та удосконалення системи управління інформаційною безпекою підприємства.

Апробація результатів роботи. Основні положення і результати досліджень за темою кваліфікаційної роботи оприлюдненні у формі тез доповідей на: VI Всеукр. наук.-практ. інтернет-конфер. «Управління ресурсним забезпеченням господарської діяльності підприємств реального сектору економіки» (Полтава, 17 листопада 2021 р.), Всеукр. наук.-практ. інтернет-конфер. «Управління ресурсним забезпеченням господарської діяльності підприємств реального сектору економіки» (Полтава, 27 жовтня 2022 р.), та публікації статті у фаховому виданні [25, 32, 61]:

1. Яснолоб І.О., Кривчун Р.Ю. Управління інформаційною безпекою у сучасному бізнес-середовищі. *Управління ресурсним забезпеченням господарської діяльності підприємств реального сектору економіки* : матер. VI Всеукр. наук.-практ. інтернет-конфер. з міжн. участю, 17 листопада 2021 р. Полтава : ПДАУ, 2021. С. 266-268.

2. Кривчун Р.Ю. Модель системи інформаційної безпеки підприємства. *Управління ресурсним забезпеченням господарської діяльності підприємств реального сектору економіки* : матер. VII Всеукр. наук.-практ. інтернет-конф. з міжн. участю, 27 жовтня 2022 р. Полтава : ПДАУ, 2022. С. 121-122.

3. Медвідь В.Ю., Правдивець О.М., Кривчун Р.Ю. Теоретико-методичні засади формування системи управління інформаційною безпекою підприємства. *Агросвіт*. 2022. № 24 (2022). https://www.nayka.com.ua/index.php/agrosvit/issue/archive.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА В СУЧАСНОМУ БІЗНЕС-СЕРЕДОВИЩІ

1.1. Сутнісна характеристика інформаційної безпеки підприємства

Усі підприємства мають розуміти та планувати, як саме вони будуть йти до свого успіху, але на цьому шляху, вагомим елементом є його можливість забезпечити безпеку своєї конфіденційної інформації.

Часті зміни в економіках країн постійно змінюють та надають нові вимоги до якості безпеки. Слідкування за новинками в плані безпеки та зломів системи є пріоритетним завданням тих, хто займається організацією безпеки на підприємстві.

Мінімізація ризиків викрадення даних є основною причиною виникнення та створення інформаційної безпеки на підприємстві. Адже чим складніша система інформаційної безпеки на підприємстві, тим важче зловмисниками заволодіти конфіденційною інформацією. Чим дорожчим буде планування та організація зломів, фізичних викрадень або фізичного знищення даних, тим більше зловмисники будуть задумуватися про кінцевий результат своєї неправомірної діяльності і чи варто зламувати дані того чи іншого підприємства, адже вартість отриманої інформації може не перекрити їхні витрати на підготовку вторгнення.

Інформація – це сукупність певних даних, які описують стан керованої й керуючої підсистем та зовнішнього середовища; результат і предмет праці менеджменту підприємства. Потенційна ефективність та найвища обґрунтованість управлінських дій і рішень будуть при умові отримання достовірної й повної інформації, яка якісно і оперативно буде оброблена. Одночасно інформація є об'єднуючою ланкою між суб'єктом та об'єктом управління, між підприємством і зовнішнім середовищем. Вона поступово

переходить в категорію товару, набуваючи якості споживчої вартості.

Сучасний стан науково-технічного та економічного прогресу характеризується надзвичайно стрімким розвитком інформаційних систем і технологій й застосуванням у повсякденному житті, діяльності підприємства, управлінні країною. Інформатизація – це соціально-економічний, науково-технічний і організаційний процес: формування найоптимальніших умов з метою задоволення інформаційних потреб; реалізації прав населення, органів місцевого самоврядування та органів державної влади, суспільства; управління на основі застосування інформаційних систем, ресурсів, технологій, використовуючи комунікаційну й обчислювальну техніку.

Інформація – це абстрактне судження, яке поєднує у собі велику кількість значень в залежності від контексту. Простіше кажучи, інформація є змістом даних, які отримав той, хто шукав відповіді на свої запитання.

Інформація буває різноманітною: хибною, правдивою та повною нісенітницею. В залежності від отриманих даних інформація виділяється доступністю для отримувача. Прикладом обмеження є шифр, код – те, що обмежує коло осіб, які зможуть отримати певну інформацію. Інформація може виступати в ролі товару, вона також легко купується і продається (в залежності від попиту на ту чи іншу інформацію).

Варто зазначити, що основними властивостями інформації є цінність, достовірність та актуальність. У свою чергу часовими властивостями інформації постають актуальність, оперативність й ідентичність.

Безпека – це умови, в яких знаходиться складна система, в цих умовах зовнішні та внутрішні чинники, не призводять до негативних процесів, які є згубними для складної системи відповідних потреб, знань і уявлень.

Відповідно, захист інформації – це процес, який спрямований на забезпечення інформаційної безпеки, визначальними факторами якої є загроза (потенційна причина, що знижує рівень інформаційної безпеки системи, тобто потенційно здатну привести до негативних наслідків) і ризик (збиток системи або організації) [30].

Захисту підлягає будь документована інформація, неправомірне поводження з якою може завдати шкоди її власнику, користувачеві або іншій особі. Захисту потребує не тільки конфіденційний документ, а й відкритий правовий акт необхідно зберегти в цілісності та безпеці від стихійного лиха чи викрадача.

Саме тому інформаційна безпека є частиною проблеми інформаційного забезпечення функціонування будь-якого суб'єкта господарювання.

Інформаційна безпека – найважливіший елемент системи економічної безпеки підприємництва, основа процесу його управління. Без неї неможливо сформувати цілі управління, оцінити ситуацію, визначити проблему, підготувати і прийняти рішення, проконтролювати хід його виконання.

У науковій літературі поки відсутній єдиний підхід до змісту поняття «інформаційна безпека». Для одних воно відображає стан, для інших процес, діяльність, здатність, систему гарантій, властивість, функцію. З метою упорядкування різних поглядів ми вирішили їх класифікувати за критерієм ознаки, що визначає зміст даного поняття. Таким чином, нами були виокремлені такі напрями підходів. Наприклад, деякі науковці характеризують інформаційну безпеку як «стан захищеності інформаційного середовища, який відповідає інтересам держави, якого забезпечується формування, використання і можливості розвитку незалежно від впливу внутрішніх та зовнішніх інформаційних загроз». А також деякі українські дослідники, які вважають за необхідне визначати інформаційну безпеку як стан захищеності. Інші дослідники визначають інформаційну безпеку як стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації, тоді як Додонов О.Г. визначає інформаційну безпеку як стан захищеності інформаційного простору, що забезпечує формування та розвиток цього простору в інтересах

особистості, суспільства та держави [42]. Ряд представників цього напряму розглядають інформаційну безпеку як стан, що характеризується відсутністю небезпеки, тобто чинників та умов, які загрожують безпосередньо індивіду, спільноті, державі з боку інформаційно-комунікаційного середовища. Прибічники такого підходу вважають інформаційну безпеку станом і процесом захищеності особи, суспільства, держави від реальних або потенційних загроз. Водночас, на нашу думку, розглядати безпеку лише в якості стану не зовсім доречно, тому що це не відображає динамізму як самої безпеки, так і тієї системи, для якої безпека виступає функцією її подальшого розвитку та існування [21].

Зубок М. зазначає, що інформаційна безпека – багатогранна, можна навіть сказати, багатовимірна сфера діяльності, де успіх може принести тільки системний, комплексний підхід. Спектр інтересів суб'єктів, пов'язаних з використанням інформаційних систем, можна розділити на наступні категорії: забезпечення доступності, цілісності і конфіденційності інформаційних ресурсів та підтримуючої інфраструктури. Іноді до основних складових інформаційної безпеки включають також захист від несанкціонованого копіювання інформації [20].

Згідно з визначенням Архипова О. і Скиби А. інформаційна безпека залежить не тільки від комп'ютерів, але і від підтримуючої інфраструктури, до якої можна віднести системи електричного та теплопостачання, кондиціонери, засоби комунікацій і, звичайно, обслуговуючий персонал. Ця інфраструктура має самостійну цінність, але нас цікавитиме лише те, як вона впливає на виконання інформаційною системою її функцій [4].

Інформаційна безпека є процесом, а не станом, оскільки має враховувати майбутнє. Тому дане поняття варто розглядати через призму ознак, таких як властивість, стан, а також управління небезпеками і загрозами у випадку, коли забезпечується мінімізація впливу негативних факторів. Тобто думка деяких авторів, які вважають, що інформаційна безпека є захистом інформації є дещо неповною. Зазначимо, що

інформаційна безпека є більш широким поняттям за своєю сутністю і багатоаспектною сферою діяльності, ефективність якої може бути лише при застосуванні системно-комплексного підходу.

Інформаційна безпека підприємства відображає захищеність інформаційного середовища та ефективність інформаційного забезпечення процесу управління на підприємстві [62].

Розглянувши різні визначення поняття «інформаційна безпека» можна охарактеризувати основні її ключові положення:

стан захищеності інтересів працівників підприємства в інформаційному бізнес середовищі;

відносини, пов'язані із захистом важливих інтересів від реальних та потенційних загроз в інформаційному просторі;

захищеність правил встановлених законом, за допомогою яких відбуваються інформаційні процеси;

захищеність інформаційного простору підприємства;

нероздільна частина економічної, політичної, оборонної та інших складових безпеки підприємства.

Враховуючи вищезазначене, схему забезпечення інформаційної безпеки у підприємстві можна представити наступним чином (рис. 1.1).

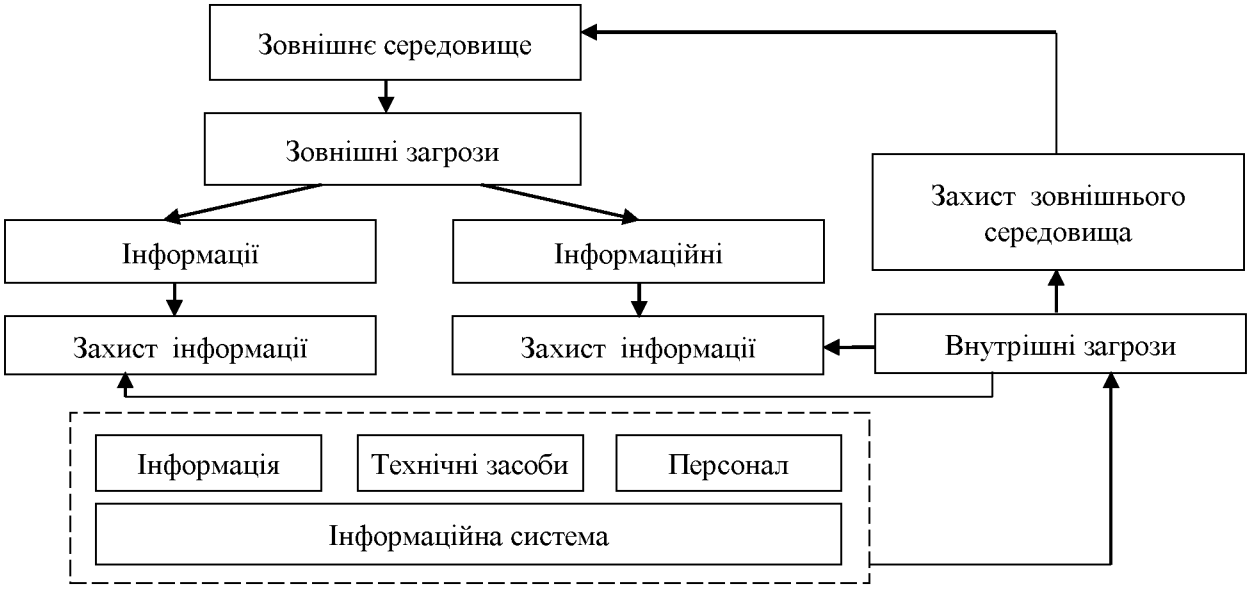

Рис. 1.1. Загальна схема забезпечення інформаційної безпеки підприємства [27]

Заходи із забезпечення інформаційної безпеки спрямовані на охорону конфіденційної інформації, а також включають контрзаходи (пошук даних про конкурентів, партнерів і контрагентів) [3]. Варто зазначити, що уся цінна інформація підприємства підлягає захисту. У першу чергу, це інформація, яка є комерційною таємницею.

На думку Аніловської Г.Я., одним із методів забезпечення інформаційної безпеки підприємства є стандартизація інформаційної структури інформаційної системи, елементами якої виступають форми існування і подання інформації у цілому, а зв'язками – операції перетворення інформації в системі. Стандартизація цього типу полягає у запровадженні єдиних правил введення, зберігання, аналізу, оброблення інформації [2].

Денисенко М.П. і Колос І.В. зазначають, що метою інформаційного забезпечення управління є своєчасне надання необхідної і достатньої інформації для прийняття управлінських рішень, що забезпечують ефективну діяльність як підприємства в цілому, так і його структурних підрозділів. Виділяють такі основні складові в системі інформаційного забезпечення управління підприємством: інформаційні ресурси, інформаційні технології, технічні засоби та програмне забезпечення [10].

З метою захисту інформації необхідно здійснювати певні дії на мікро- та макрорівнях. Важливе значення у забезпеченні інформаційної безпеки відіграє формування відповідних відділів і підрозділів підприємства, оскільки інформаційно-аналітична робота є однією із головних внутрішньовиробничих функціональних складових безпеки підприємства.

Внутрішньовиробнича інформаційна складова забезпечує здійснення результативного інформаційно-аналітичного забезпечення діяльності суб'єкта господарювання. Відповідні структурні підрозділи підприємства виконують функції, що у сукупності характеризують процес створення та захисту інформації. До них належать наступні(рис. 1.2).

Підприємство постійно отримує інформацію, яка відрізняться джерелами її формування. Виділяють наступні види інформації:

відкрита офіційна інформація;

ймовірна нетаємну інформацію, яка отримується від неформальних контактів працівників підприємства з носіями такої інформації;

ймовірна таємну інформацію, яка отримується від неформальних контактів працівників підприємства з носіями такої інформації.

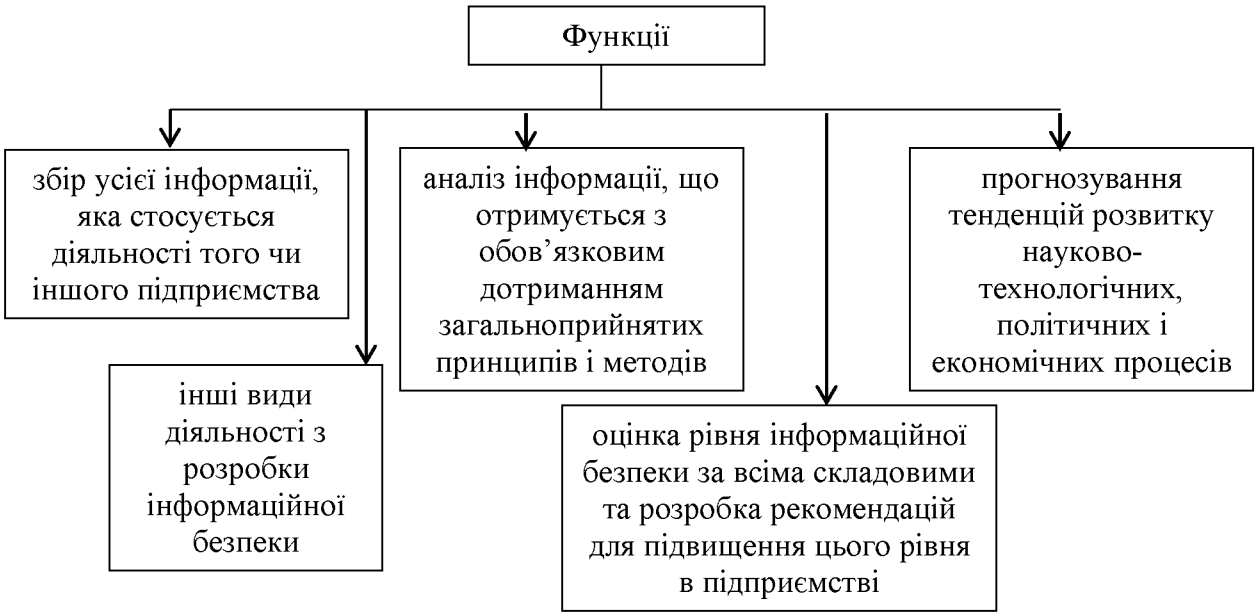

Рис. 1.2. Функції, які характеризують процес створення та захисту інформації [29]

Позавиробнича інформаційна складова характеризується надійністю взаємодії з економічними контрагентами.

Забезпечення інформаційної безпеки на мікрорівні полягає у створенні таких структурних одиниць підприємства, як інформаційно-аналітичний підрозділ та Служба захисту інформації. До завдань Служби захисту інформації належить: своєчасне виявлення загроз інформації; виявлення й максимальне перекриття потенційно можливих каналів і методів несанкціонованого доступу до інформації; відпрацьовування механізмів оперативного реагування на загрози, використання засобів і методів виявлення й нейтралізації джерел загроз безпеці компанії; організація спеціального діловодства, що виключає несанкціоноване одержання конфіденційної інформації [4].

1.2. Система управління інформаційною безпекою підприємства

Формування системи управління інформаційною безпекою гарантує ефективність, якщо буде сформована на основі міжнародних стандартів ISO/IEC 27001:2005 та ISO/IEC 17799:2005.

Стандарт ISO/IEC 27001:2005 [13] визначає вимоги, яких має дотримуватися підприємство при формуванні інформаційної безпеки підприємства. Вона слідкує за визначення, мінімізацію, керування небезпекою та загрозами, якими може пошкоджуватися інформація, сприяє вибору ефективної та адекватної системи захисту інформації на підприємстві.

Завдяки стандарту ISO/IEC 27001:2005 [13] на підприємстві можливо:

сформувати вимоги та цілі, направлені на інформаційну безпеку;

гарантування впевненості в тому, що керування ризиками в сфері інформаційної безпеки є ефективним та доцільним. Запевнитися в тому, що підприємство діє згідно чинного законодавства і решті нормативних документів;

втілити в життя контроль за функціонуванням системи управління інформаційної безпеки;

виявляти та відстежувати всі існуючі способи управління інформаційною безпекою;

отримання інформації керівництвом щодо стану процесу управління захистом інформації;

регламентацію політики безпеки для внутрішньої та зовнішньої аудиторії шляхом поділу їх на рівні;

забезпечення партнерів та постачальників усією необхідною інформацією про стандарти, процедури та політику підприємства.

Стандарт ISO/IEC 17799:2005 формує принципи та є головним при розробці, впровадженні, супроводі та покращенні системи керування інформаційною безпекою, описує механізм визначення цілей контролінгу і його вартості у таких сферах [13]:

політика безпеки (визначення принципів керування і способів, які забезпечують захист інформації);

управління безперервністю бізнес-процесів (виключення сторонніх втручань в ділові операції, захист процесів під час обробки інформації, від втручання серйозних неполадок чи форс-мажорів);

дотримання правових норм (винятки в порушеннях цивільного та кримінального права, встановлених законом зобов'язань, регуляторних чи контрактних зобов'язань, дотримання вимог безпеки);

організація активів та ресурсів (керування захистом інформації всередині підприємства) [19];

фізична безпека і безпека навколишнього середовища (виключення несанкціонованого втручання в конфіденційну інформацію);

класифікація і управління активами (знаходження та захист інформаційних ресурсів);

захист персоналу (зменшення ризиків, спричинених помилками оператора, крадіжками, шахрайством чи несанкціоновано використаним обладнанням);

керування доступом (контроль за доступом до інформації);

керування засобами зв'язку та важливим обладнанням;

розробка та обслуговування систем (долучення додаткових засобів захисту до інформаційної системи) [22];

Модель системи інформаційної безпеки підприємства – це поєднання внутрішніх та зовнішніх факторів, те як вони впливають на загальний стан інформаційної безпеки на підприємстві та забезпечення безпеки ресурсів. Організаційна побудова моделі системи управління інформаційною безпекою підприємства зображена на рис. 1.3.

Об'єктами захисту є інформаційні та матеріальні ресурси:

- документація, яка збережена на паперових носіях;
- технічні засоби зв'язку та комунікації;
- усна інформація;

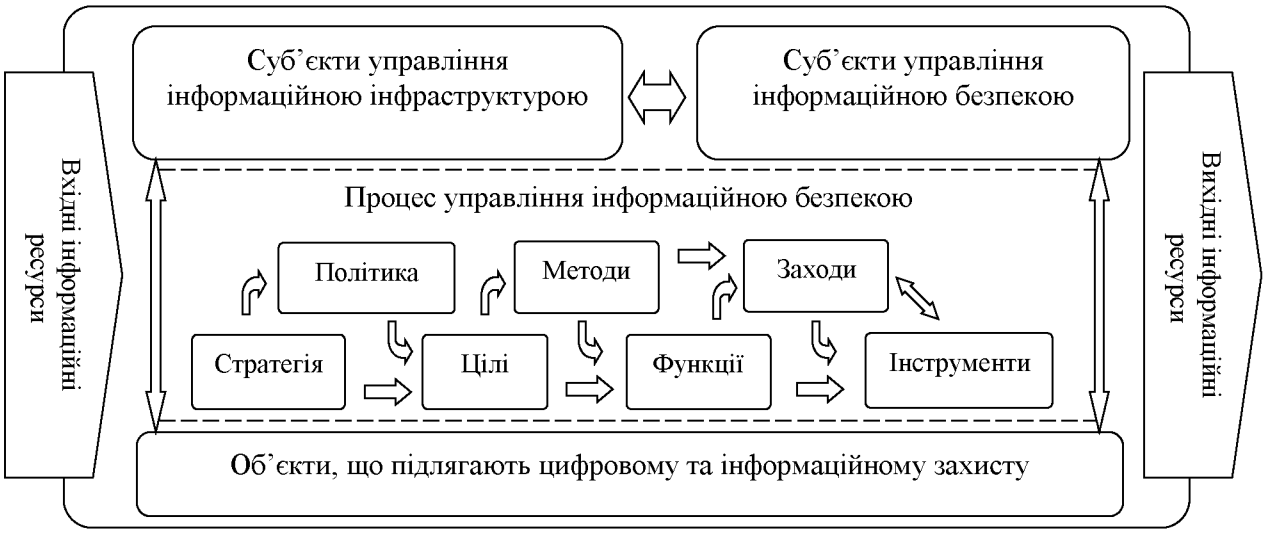

Рис. 1.3. Організаційна модель системи управління інформаційною безпекою підприємства [6]

- відцифрована інформація, яка може зберігатися та передаватися на різні носії;

- приміщення, в яких проводяться наради та обговорення, зберігання і обробка інформації;

- інформаційні системи загалом, сюди відносяться і системи зв'язку;

- документи, які зберігаються на технічних та програмних засобах;

- програмні засоби.

Усі загрози, з якими зіштовхується підприємство, можна класифікувати за природою їх виникнення, тобто вони можуть бути випадковими або ж навмисними. В залежності від методу боротьби з ними виділяють внутрішні та зовнішні загрози [24].

Зовнішніми загрозами є:

- діяльність конкурентів, яка спрямована на перехоплення та обробку важливої інформації;

- випадкові дії працівників сторонніх організацій, які потягли за собою збої у системі інформаційної безпеки;

- умисне знищення, руйнація або ж навмисна модифікація інформації;

- катастрофи і стихійні лиха, непередбачувані ситуації, збої, аварії;

Внутрішніми загрозами є:

- некоординована діяльність структур підприємства, яка спрямована на захист інформації;

- персонал підприємства навмисно знищує інформацію;

- випадкові помилки працівників, застарілість техніки, збої в роботі інформаційної системи;

- грубі порушення правил збору, накопичення, обробки, перетворення, зберігання, відтворення і передавання інформації.

Існує декілька видів порушень [28]:

- організаційні види порушень (об'єднують в собі несанкціонований доступ до бази і масових даних, доступ зловмисників до активного мережевого обладнання чи серверів, неправильне розміщення засобів захисту та запобіжників при несанкціонованому доступі або ж помилки при керуванні ними, крадіжка чи небажане ознайомлення із конфіденційною інформацією в паперових чи електронних носіях, розкрадання конфіденційних даних;

- організаційно-правові порушення (спричинені відсутністю об'єднаної політики підприємства, яка була б спрямована на сферу захисту інформації, недотримання вимог нормативних документів, режимів доступу, зберігання і знищення даних);

- фізичні види порушень (нанесення шкоди апаратним засобам, автоматизованим системам, лініям зв'язку, комунікаційному обладнанню, незаконне привласнення або неправомірне ознайомлення із конфіденційною інформацією на носіях або їх викрадення [29].

- радіоелектронні види порушень (застосування електронних засобів, які спрямовані на перехоплення та дешифрування потоків інформації, фото чи відео фіксація моніторів та обладнання, поширення дезінформації у локальних мережах, передача даних чужими лініями зв'язку.

Щоб протистояти загрозам та припинити порушення на підприємстві, необхідно організувати процес управління ризиками, який є основою під час побудови системи інформаційної безпеки на підприємстві.

Формування надійної системи інформаційної безпеки – це широкий спектр процедур, спрямованих на мінімізацію внутрішніх та зовнішніх загроз, які обмежені у часі та ресурсах [37].

У свою чергу процес керування ризиками включає в себе наступні елементи: опис бізнес-процесів, виявлення ризиків, оцінку ризиків, планування заходів, реалізацію заходів, оцінку ефективності.

Опис бізнес-процесів (аналіз та спостереження за бізнес процесами, визначення критеріїв за якими формуватиметься політика мінімізації ризиків, постійна ідентифікація бізнес процесів) [53].

Виявлення ризиків (виявлення ступеня схильності підприємства до загроз, які можуть призвести до вагомої шкоди. Саме для цього і необхідний аналіз бізнес процесів та обговорення з експертами у галузі безпеки. Результатом даного аналізу є класифікація потенційних ризиків).

Стандартними інформаційними ризиками є: копіювання конфіденційної інформації із локальних місць, умисне пошкодження інформації з метою її знищення, копіювання секретних документів для передачі їх конкурентам, незаконний вхід у корпоративну мережу, умисне знищення техніки та обладнання [41].

Оцінка ризиків (виокремлення усіх потенційних ризиків із їхніми якісними та кількісними оцінками, які можуть призвести до збитків, виділення ризиків, які не прослідковуються на підприємстві).

Відповідно оцінка ризиків відбувається за наступними етапами:

- опис об’єктів та способів захисту;
- пошук ресурсу і обчислення його кількісних показників;
- аналіз загроз, які можуть зашкодити інформаційній безпеці;
- визначення ступеня вразливості;
- пошук та оцінка засобів забезпечення інформаційної безпеки, які підприємство може використати.

Планування заходів, основною метою яких є встановлення термінів та перелік робіт, які спрямовані на мінімізацію збитків у разі настання

критичних моментів [51].

Реалізація заходів, тобто виконання всіх запланованих робіт, які пов'язані із мінімізацією ризиків, контроль за якістю отриманих результатів та термінів їх виконання.

Оцінка ефективності – це системний процес, який спрямований на отримання оцінки та об'єктивних матеріалів про поточний стан системи, після проведення всіх запланованих операцій, співвідношення досягнутих результатів із запланованими [56].

Отже, управління інформаційною безпекою є досить важкою, відповідальною та клопіткою роботою. Для безпечної діяльності підприємства необхідно ідентифікувати та управляти величезною кількістю інформації. Діяльність, яка спрямована на безпеку, тісно пов'язана із процесом управління ризиками. Необхідно слідкувати за власними інформаційними ресурсами та уважно аналізувати зовнішню інформацію.

Варто зазначити, що основними цілями інформаційної безпеки є:

конфіденційність, тобто інформація обмежена у доступі і доступна лише обмеженому колу осіб;

виключення несанкціонованого доступу до інформації, коли сторонні особи не можуть ознайомитися або отримати доступ до конфіденційної інформації;

цілісність інформації і належних до неї процесів означає, що інформація повинна бути перевіреною, нерозірваною на «шматки», піддаватися обробці, введенню чи виведенню та не повинна піддаватися ніяким змінам під час даних процесів;

доступність інформації, тобто інформація має бути своєчасною, надійною і, у разі необхідності, бути доступною для уповноважених чи довірених осіб;

встановлення на облік усіх процесів, які пов'язані з ризиком.

У подальшому цілі реалізуються під час вирішення наступних задач:

додавання до системи терміну інформаційної безпеки;

облік та класифікація інформаційних ресурсів організації;

вибір осіб які відповідають за інформаційну безпеку;

визначення ризиків інформаційної безпеки та способів їх мінімізації;

формування групи яка матиме доступ до інформаційних ресурсів;

розробка методів та способів оцінки ризиків, для управління ними;

обирання технічних та адміністративних заходів, які спрямовані на зниження та протидію ризикам;

впровадження заходів, спрямованих на інформаційну безпеку, періодичний контроль за можливими ризиками;

гарантування безпеки працівників та фізичної безпеки;

впровадження нових вимог до інформаційної системи, спираючись на інформаційну безпеку;

контролінг за інформаційною безпекою на підприємстві;

Фактори, які впливають на систему інформаційної безпеки [23]:

- загрози, які мають можливість виникнення та виникають під час формування інформаційної безпеки;

- вразливість інформаційної безпеки, яка прямим чином може призвести до прямих загроз;

- ризики, які є відображенням можливих втрат у разі, якщо загроза стане дійсністю;

Варто зазначити, що виокремлюють чотири рівні впровадження системи керування інформаційною безпекою:

формування політики галузевих ризиків;

аналіз ризиків для підприємства;

формування кінцевої мети;

формування політики ризиків включає формування основ керування ними, для всієї організації загалом. Дані принципи спираються на цілі підприємства, його стратегію, вимоги, запропоновані законодавством і певними стандартами, спрямованими на інформаційну безпеку [17].

Висновки до розділу 1

У першому розділі кваліфікаційної роботи досліджено теоретичні аспекти управління інформаційною безпекою підприємства:

1. Інформація – це сукупність певних даних, які описують стан керованої й керуючої підсистем та зовнішнього середовища; результат і предмет праці менеджменту підприємства. Безпека – це умови, в яких знаходиться складна система, в цих умовах зовнішні та внутрішні чинники, не призводять до негативних процесів, які є згубними для складної системи відповідних потреб, знань і уявлень.

Інформаційна безпека підприємства відображає захищеність інформаційного середовища та ефективність інформаційного забезпечення процесу управління на підприємстві. Вона є найважливішим елементом системи економічної безпеки підприємництва, основа процесу його управління.

2. Організаційна модель системи управління інформаційною безпекою підприємства передбачає наявність класичних складових для забезпечення захисту інформаційної інфраструктури товариства: суб'єктів управління інформаційною інфраструктурою та суб'єктів управління інформаційною безпекою, об'єктів, що підлягають цифровому та інформаційному захисту, а також власне процесу управління, який передбачає включення стратегії, політики інформаційної безпеки (неформалізованих), цілей, методів, функцій, заходів та інструментів.

РОЗДІЛ 2
АНАЛІЗ ПІДПРИЄМСТВА ЯК СИСТЕМИ УПРАВЛІННЯ

2.1. Загальна характеристика підприємства

Об'єктом дослідження було обрано підприємство, яке займається рослинництвом, обробляючи 3541 га землі у Миргородському районі. Розташування господарства не створює проблем у реалізації продукції власного виробництва, а також у забезпеченні добривами, машинами, матеріалами та насінням. Підприємство знаходиться на території, рельєф якої є рівнинним із слабо пологими і пологими схилами. На території основні масиви ріллі розміщені в південно-східній частині землекористування і придатні для вирощування зернових і технічних культур.

Предметом економічної діяльності підприємства є:

виробництво, заготівля, зберігання, реалізація, переробка, транспортування сільгосппродукції;

оренда земельних ділянок сільськогосподарського та не сільськогосподарського призначення для ведення товарного сільськогосподарського виробництва.

Підприємство має в своїй структурі має такі виробничі підрозділи:

– токове господарство;
– тракторно-рільнича бригада № 1, 2;
– складське господарство;
– ремонтна майстерня.

Стабільний фінансовий стан сільськогосподарського підприємства робить досягнення даної мети можливою в довгостроковій перспективі. Метою діяльності підприємства, функціонуючого в ринкових умовах – це виробництво та реалізація сільськогосподарської продукції, а також надання учасникам підприємства та іншим особам послуг щодо ведення сільського господарства та здійснення інших, пов'язаних з ним видів діяльності.

Досліджуване підприємство – це відкрита система, яка може існувати лише за умови активної взаємодії з навколишнім середовищем. Воно вибирає з проміжного та загального зовнішнього середовища основні фактори виробництва і, перетворюючи їх на продукцію (товари, послуги, інформацію) та відходи, передає знов у зовнішнє середовище. Умовою життєздатності системи є корисний (вигідний) обмін між «входом» і «виходом».

Система управління організацією включає сукупність усіх служб організації, всіх підсистем та комунікацій між ними, а також процесів, що забезпечують функціонування організацією.

Вищим органом управління товариства є Збори учасників товариства. Загальні збори учасників товариства мають право приймати рішення з усіх питань діяльності товариства, у тому числі й з тих, що передані до компетенції виконавчого органу (директора).

Організаційна структура управління – це форма поділу праці, що закріплює певні функції управління за відповідними структурними підрозділами апарата управління. Головне призначення організаційної структури – забезпечити ефективну діяльність управлінського персоналу. До його складу на підприємстві входять: керівник підприємства, керівники підрозділів, фахівці, обслуговуючий персонал.

Організаційна структура управління підприємства (додаток А) є засобом сприяння досягнення менеджерами своїх цілей. Оскільки цілі є похідними від загальної стратегії підприємства, тісний зв'язок стратегії та структури цілком логічний. Відповідно до організаційної структури підприємства розробляється система управління підприємством. У підприємстві застосовується лінійна структура управління.

У цілому в підприємстві спостерігається низький рівень спеціалізації, нечисленні правила, за якими здійснюється діяльність, та централізацію повноважень у руках однієї особи – власника. Проста організація є «малоступеневою». Вона переважно складається з двох-трьох вертикальних рівнів та аморфної групи уповноважених службовців, які мають право

централізовано приймати рішення. Вона мобільна, потребує незначних витрат. На ефективність діяльності підприємства впливає результативність прийняття рішень.

В управлінні підприємством застосовуються різні показники. Їх використання відображає особливості діяльності підприємства, дає змогу вести певну аналітичну роботу, на основі якої ухвалюються управлінські рішення відповідно до обраної стратегії. Основними ресурсами підприємства є земля, праця та капітал.

Земля – це головний засіб, без якого неможливо здійснити виробництво продукції тваринництва і рослинництва. Земельні угіддя – це земельні ділянки, що систематично використовуються для певних господарських цілей та відрізняються за природно-історичними ознаками. Сільськогосподарські угіддя – частини землі, що використовуються для сільськогосподарського виробництва. Угіддя розрізняються за природними особливостями і призначенням. До основної категорій відноситься рілля – землі, що систематично оброблюються і використовуються для посіву різноманітних сільськогосподарських культур.

Структура сільськогосподарських угідь підприємства залежить від зональних особливостей і характеризує якість землі підприємства як засобу виробництва (табл. 2.1).

Таблиця 2.1

Склад і структура земельного фонду, 2017-2021 рр.

Показники	Роки					Структура 2020 р., %	2021 р. до 2017 р., %
	2017	2018	2019	2020	2021		
Загальна земельна площа у власності і користуванні, га	3611	3615	3598	3529	3541	100,00	-1,94
Площа сільсько-господарських угідь – всього, га	3611	3615	3598	3527	3539	99,94	-1,99
у т.ч. рілля	3051	2969	3146	3225	3252	91,84	6,59

Аналіз даних табл. 2.1 показує, що загальна земельна площа підприємства в 2021 р. становила 3541 га. Площа ріллі – 3252 га, або 91,84 %

у структурі загальної земельної площі підприємства, що говорить про високий коефіцієнт розораності земель. У порівнянні з 2017 р. її площа збільшилась на 6,59 %.

Спеціалізація сільськогосподарського виробництва органічно поєднана з його розміщенням. Вона є формою суспільного поділу праці і знаходиться в постійному взаємозв'язку та взаємозумовленості. Розміщення характеризує кількісний бік суспільного поділу праці і вказує, які види продукції, в якому розмірі й на яких площах виробляються на тій чи іншій території. Спеціалізація демонструє якісний бік суспільного поділу праці і вказує, виробництво яких саме видів продукції є переважаючим на даній території. Це ефективна форма організації сільського господарства, яка дає можливість зосередити виробництво певних видів продукції на окремих територіях і підприємствах і одержати завдяки цьому кращих результатів господарської діяльності.

Випуск і реалізація продукції впливає на фінансові результати роботи сільськогосподарського підприємства. Крім того, реалізація виробничої продукції – це основне джерело формування доходу підприємства. Тому техніко-економічний аналіз роботи підприємства починається з аналізу випуску та реалізації продукції, у вивченні обсягу виробництва, темпів його зростання, тобто у оцінці виконання плану виробництва та реалізації продукції.

Проаналізуємо спеціалізацію сільськогосподарського підприємства в табл. 2.2.

Результати розрахунків, які подані у табл. 2.2 дають змогу зазначити, що перше місце в структурі товарної продукції підприємства за останні п'ять років займало виробництво кукурудзи на зерно – 65,3 %, друге – виробництво соняшнику 20,0 %, третє – соя 8,6 %.

Отже, виробничий напрямок досліджуваного підприємства можна охарактеризувати як зерново-технічний.

Розрахуємо рівень спеціалізації за формулою:

$$К_с = 100 / \sum V_i (2N_i - 1) \quad (2.1)$$

Таблиця 2.2

Склад і структура товарної продукції підприємства, 2017-2021 рр.

Види продукції	Вартість продукції, тис. грн					Вартість за 5 роки, тис. грн	Питома вага, %	Місце за питомою вагою
	Роки							
	2017	2018	2019	2020	2021			
Пшениця озима	1767,4	2173,4	2128,0	-	-	6068,8	2,1	5
Кукурудза на зерно	25959,4	28377,3	37343,1	51836,6	44284,4	187800,8	65,3	1
Ячмінь озимий	626,1	-	300,0	-	-	926,1	0,3	7
Культури зернобобові сушені	1030,2	-	-	-	1422,6	2452,8	0,9	6
Соняшник	11042,3	9096,9	7516,1	14709	15120,5	57484,8	20,0	2
Соя	5657,7	7673,1	5426,2	5907,7	-	24664,7	8,6	3
Ріпак озимий	3175,5	1262,3	3576,2	-	-	8014	2,8	4
Разом по рослинництву	49258,6	48583	56289,6	72453,3	60827,5	287412	100,0	х
Всього по господарству	49258,6	48583	56289,6	72453,3	60827,5	287412	100,0	х

де Кс – коефіцієнт рівня спеціалізації;

V – питома вага товарної продукції;

Ni – питома вага товарної продукції;

і – місце продукції за питомою вагою.

Кс = 100 / [65,3 * (2 * 1 – 1) + 20,0 * (2 * 2 – 1) + 8,6 * (2 * 3 – 1) + 2,8 * (2 * 4 – 1) + 2,1 * (2 * 5 – 1) + 0,9 * (2 * 6 – 1) + 0,3 * (2 * 7 – 1)] = 100 / 216,7 = 0,46

Таким чином, за результатами проведених розрахунків Кс = 0,46. Значення даного коефіцієнта свідчить про середній рівень спеціалізації досліджуваного підприємства, який зумовлений, насамперед, спеціалізацією на галузі рослинництва.

Отже, здійснивши загальну характеристику досліджуваного підприємства, у наступному підрозділі кваліфікаційної роботи здійснимо організаційно-економічний аналіз показників господарської діяльності досліджуваного підприємства.

2.2. Організаційно-економічний аналіз показників господарської діяльності підприємства

Головним джерелом розвитку економіки та найбільш важливим елементом продуктивних сил є люди, їх освіта, майстерність, підготовка, мотивація діяльності. Існує непересічна залежність конкурентоспроможності економіки, рівня добробуту населення від якості трудового потенціалу підприємства.

Трудові ресурси є надзвичайно важливим ресурсом кожного підприємства, від якості та ефективності якого, зазвичай, залежать результати діяльності підприємства і його конкурентоспроможність.

Проаналізуємо динаміку показників загальної структури персоналу підприємства в табл. 2.3.

Таблиця 2.3

Характеристика та динаміка загальної структури персоналу підприємства за категоріями зайнятих, 2017-2021 рр., осіб

Категорія зайнятих	Роки					2021 р. до 2017 р.	
	2017	2018	2019	2020	2021		
	Кількість, осіб	Кількість, осіб	Кількість, осіб	Кількість, осіб	Кількість, осіб	абсолютне відхилення, (+;-)	відносне відхилення, %
Управлінський персонал	14	14	13	13	12	-2	-14,3
У тому числі: Керівники	5	5	4	4	4	-1	-20,0
Спеціалісти	9	9	8	8	8	-1	-11,1
Технічні працівники	-	-	1	1	-	0	0
Виробничий персонал	55	53	56	50	50	-5	-9,1
Разом	69	67	69	63	62	-7	-10,1

Отже, у досліджуваному підприємстві чисельність управлінського персоналу дещо зменшилася (на 2 особи) і становить 12 осіб, у тому числі 4 керівники та 8 спеціалістів.

Виробничий персонал підприємства у 2021 році становив 50 осіб, що дорівнює значенню 2017 року.

Так загалом у 2017 р. персонал налічував 69 осіб, а у 2021 р. – 62 особи, що на 10,1 % менше.

Для оцінки персоналу досліджуваного підприємства доцільно проаналізувати вікову структуру працівників (табл. 2.4).

Таблиця 2.4

Характеристика та динаміка вікової структури персоналу підприємства, 2017-2021 рр.

Вікові категорії	2017 р.		2018 р.		2019 р.		2020 р.		2021 р.		Відхилення (+; -) у % 2021 р. від 2017 р.	
	кількість, осіб	частка,%	кількість, осіб	частка,%	кількість, осіб	частка,%	кількість, осіб	частка,%	кількість, осіб	частка,%	Абсолютне	Відносне
Молодь віком 15-24 років	2	2,9	2	3,0	2	2,9	2	3,2	2	3,2	0	0,3
29-40 років	34	49,3	33	49,3	33	47,8	31	49,2	30	48,4	-4	-0,9
41-50 років	27	39,1	27	40,3	29	42,0	27	42,9	27	43,5	0	4,4
Передпенсійні роки	3	4,3	2	3,0	2	2,9	2	3,2	2	3,2	-1	-1,1
Пенсійні роки	3	4,3	3	4,5	3	4,3	1	1,6	1	1,6	-2	-2,7
Разом	69	100	67	100	69	100	63	100	62	100	-7	х

Отже, проаналізувавши вікову структуру персоналу досліджуваного підприємства слід відмітити, що переважну більшість складають працівники 29-40 років. Так, кількість працівників віком 29-40 років в 2017 році складала 34 особи, що становило 49,3 % від усієї кількості працюючих. В 2021 році їх кількість склала 30 осіб – 48,4 % в загальній структурі персоналу підприємства.

Найменшу чисельність у віковій структурі персоналу становлять працівники категорії «пенсійні роки» – 3 особи у 2017 році і по 1 особа у 2021 році.

Наявність у трудовому колективі людей різного віку, з різним стажем праці веде до кращої організації взаємодопомоги та обміну досвідом між його членами та до покращення групової роботи у підприємстві.

Такий колектив забезпечує молодим працівникам можливість оволодіння професією та навичками спільної праці і разом з тим дає змогу задовольнити потреби висококваліфікованих працівників у передаванні їх професійного та життєвого досвіду молодим працівникам. При наявності в колективі людей різного віку знижується ризик конфліктних ситуацій, оскільки літні люди частіше схильні до компромісів, толерантності, пошуків шляхів до згоди і примирення.

Управління персоналом в досліджуваному підприємсті здійснює директор. Стимулювання праці – це сукупність форм і методів забезпечення і підвищення матеріальної та моральної зацікавленості персоналу в досягненні певних індивідуальних і колективних результатів. Існуюча система стимулювання праці у підприємстві складається з грошового та морального стимулювання виробничого й управлінського персоналу.

Праця працівників аграрної сфери, як ніяких інших працівників, дуже важка і потребує великого напруження усіх духовних та фізичних сил. Для повного розкриття і можливості використання цих сил потрібний постійний та сталий чинник стимулювання до праці – раціональне поєднання мотивів і стимулів матеріального, морального та психологічного характеру. Тобто затрачена праця має забезпечувати належний заробіток. Під системою оплати праці в досліджуваному підприємстві розуміється взаємозв'язок між показниками, що характеризують норму праці та рівень її оплати в межах і вище норм праці, що гарантує отримання працівником заробітної плати, яка відповідає фактичним досягнутим результатам та узгодженої між робітником і роботодавцем ціною його робочої сили.

Отже, результат діяльності підприємства значною мірою залежить від формування системи стимулювання персоналу, яка полягає у здійсненні об'єктивної кількісної та якісної оцінки трудової активності працівника і визначенні відповідної винагороди. Винагородження працівника може бути матеріальним і моральним, і задовольняти ті чи інші види потреб, тому його форми і розмір мають відповідати затраченим зусиллям.

Важливе значення для розвитку підприємства мають основні засоби. Основні виробничі засоби – це грошовий вираз знарядь праці. Вони беруть участь у процесі виробництва тривалий час, зберігаючи при цьому натурально-речову форму.

За характером участі у виробництві основні засоби поділяються на виробничі і невиробничі основні засоби та виробничі основні засоби несільськогосподарського призначення. За сучасних умов інтенсифікація виробництва, підвищення конкурентоспроможності підприємств потребують постійного удосконалення їхньої технічної бази, що сприяє підвищенню ефективності використання основних виробничих засобів. Підвищення якості управління пов'язане з опануванням сучасних методів оцінювання стану основних виробничих засобів, аналізу та планування їхнього розвитку, формуванням комплексного підходу до оцінювання взаємовпливу показників фінансово-господарської діяльності підприємств та показників використання основних виробничих засобів.

Дослідження активів досліджуваного підприємства подано у табл. 2.5.

Таблиця 2.5

Аналіз ефективності складу і розміщення активів підприємства за 2017-2021 рр.

Активи	Звітні роки										Відхилення 2021 р. до 2017 р.	
	2017		2018		2019		2020		2021			
	тис. грн	%	тис. грн	%	тис. грн	%	тис. грн	%	тис. грн	%	(+,-)	(%)
Оборотні активи	69573	78,6	109773	86,1	86047	75,5	86218	75,6	121741	82,9	52168	4,3
Необоротні активи	18946	21,4	17656	13,9	27952	24,5	29355	25,7	25120	17,1	6174	-4,3
Разом	88519	100,0	127429	100	114033	100	114033	100	114033	100	25514	х

З наведених показників помітно, що за весь досліджуваний період в підприємстві переважають оборотні активи, але помітний поступовий спад їхньої відсоткової частки з 86,1 % у 2018 році до 82,9 % у 2021 році. Причинами зменшення даного показника можуть бути переоцінка об'єктів

активів, погашення кредитів чи продаж основних засобів.

Необоротні активи становлять 17,1 % у 2021 році, що на 6174 тис. грн більше, ніж у 2017 році. Дане явище можна пояснити збільшенням вартості нематеріальних активів та основних засобів.

Аналіз забезпеченості і руху основних засобів досліджуваного підприємства наведений у табл. 2.6.

Таблиця 2.6

Наявність і рух основних засобів підприємства, 2017-2021 рр.

Показники	Роки					2021 р. до 2017 р., %
	2017	2018	2019	2020	2021	
Основні засоби, тис. грн на початок року	11980	17520	17443	22130	28212	(в 2,4 рази)
на кінець року	17520	17443	22130	28212	23370	33,4
Середньорічна вартість основних засобів, тис. грн	14750,0	17481,5	19786,5	25171,0	25791,0	74,9
Знос основних засобів, тис. грн на початок року	10406	18848	16385	19968	25112	(в 2,4 рази)
на кінець року	12848,0	16385,0	19968,0	25112,0	29408,0	(в 2,3 рази)
Середньорічний знос основних засобів, тис. грн	11627,0	17616,5	18176,5	22540,0	27260,0	(в 2,3 рази)
Рівень зносу , % на початок року	86,9	107,6	93,9	90,2	89,0	2,5
на кінець року	73,3	93,9	90,2	89,0	125,8	71,6
Середньорічний рівень зносу основних засобів, %	80,1	100,8	92,1	89,6	107,4	34,1

Таким чином, у 2021 р. основні засоби на кінець року становили 28212 тис. грн., що 2,4 рази більше, ніж у 2017 р. В той же час середньорічна вартість основних засобів зросла в 2,4 рази.

Середньорічний рівень зносу основних засобів показує, на який відсоток профінансовані за рахунок зносу заміна і відновлення основних засобів. Даний показник має тенденцію до збільшення з 80,1 % до 107,4 % протягом досліджуваного періоду, що демонструє погіршення стану матеріально-технічної бази підприємства.

Іншою складовою активів товариства є оборотні активи, аналіз динаміки яких представлено в табл. 2.7.

Основну частину оборотних активів складає дебіторська заборгованість

–57,3 %. Її значення у 2017 р. було 18619 тис. грн, тобто 26,8 %. Зростання дебіторської заборгованості свідчить про наявність та зростання підприємницького ризику та зменшення поточної ліквідності.

Таблиця 2.7

Склад оборотних активів підприємства, 2017-2021 рр.

Види основних засобів	Роки										Відхилення 2021 р. до 2017 р.,	
	2017		2018		2019		2020		2021			
	тис. грн	%	тис. грн	%	тис. грн	%	тис. грн	%	тис. грн	%	(+,-) тис. грн	%
Запаси, з них	50936	73,2	66611	60,7	46761	54,3	48872	56,7	46772	38,4	-4164,0	-34,8
виробничі запаси	15002	21,6	23753	21,6	11628	13,5	13031	15,1	491	0,4	-14511,0	-21,2
незавершене виробництво	6255	9,0	19587	17,8	29864	34,7	14850	17,2	21628	17,8	15373,0	8,8
готова продукція	17167	24,7	14152	12,9	5151	6,0	20945	24,3	20553	16,9	3386,0	-7,8
товари	12512	18,0	9119	8,3	118	0,1	46	0,1	100	0,1	-12412,0	-17,9
Дебіторська заборгованість	18619	26,8	42506	38,7	37465	43,5	37326	43,3	69716	57,3	51097,0	30,5
Гроші та їх еквіваленти	18	0,0	656	0,6	1821	2,1	20	0,0	552	0,5	534,0	0,4
Інші оборотні активи	0	0,0	0	0,0	0	0,0	0	0,0	4701	3,9	4701,0	3,9
Разом	69573,0	100,0	109773,0	100,0	86047,0	100,0	86218,0	100,0	121741,0	100,0	52168,0	x

Запаси теж складають значну частину оборотних активів з питомою вагою 38,4 % у 2021 р., проте її значення зменшується на 34,2 % порівняно з 2017 р., що є позитивною тенденцією для прискорення ділової активності. Варто зазначити, що більшість запасів (17,8 %) у 2021 р. складає незавершене виробництво, і його питома вага зменшується на 8,8 % порівняно з 2017 р.

Наступним етапом аналізу досліджуваного підприємства є дослідження його основних показників виробничо-фінансової діяльності (табл. 2.8, рис. 2.1).

Здійснивши аналіз основних показників виробничо-фінансової діяльності підприємства за 2017-2021 рр., можна зробити висновок, що протягом досліджуваного періоду підприємство було прибутковим. Однак у 2018-2020 рр. чистий прибуток зменшився майже удвічі, а у 2021 році підприємству вдалося підвищити цей показник до рівня 2017 року.

Таблиця 2.8

Основні показники виробничо-фінансової діяльності підприємства за 2017-2021 рр.

Зміст операції	Роки					Відхилення 2021 р. до 2017 р., %
	2017	2018	2019	2020	2021	
Чистий дохід від реалізації продукції (товарів, робіт, послуг), тис. грн	97651	69716	103317	85141	110979	13,6
Собівартість реалізованої продукції (товарів, робіт, послуг), тис. грн	73091	54369	87587	62176	79710	9,1
Чистий прибуток (збиток), тис. грн	12211	7589	4139	7757	12120	-0,7
Рівень рентабельності (збитковості) виробництва продукції – всього, %	12,5	10,9	4,0	9,1	10,9	-12,7

Собівартість реалізованої продукції постійно збільшувалась протягом досліджуваного періоду. Так, у 2021 р. показник становив 79710 тис. грн, що на 9,1 % більше у порівнянні з 2017 р. Це явище спричинене здорожчанням сировини та комунальних послуг в країні.

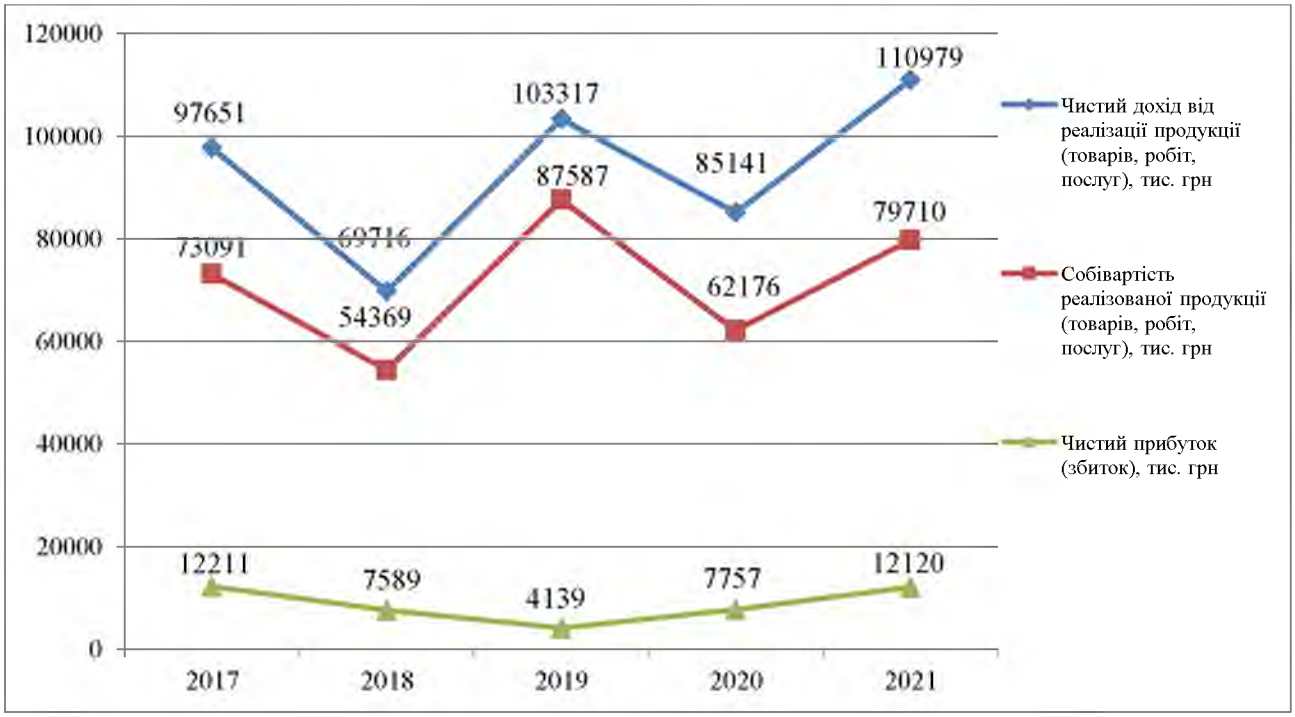

Рис. 2.1. Основні показники виробничо-фінансової діяльності підприємства за 2017-2021 рр.

Таким чином, можна зробити висновок, що вцілому ТОВ Агрофірма «Зоря-Агро» працює досить ефективно, злагоджено, відповідає умовам ринку

та попиту на дані види продукції.

У наступному підрозділі кваліфікаційної роботи буде проведена оцінка управління інформаційною безпекою досліджуваного підприємства.

2.3. Оцінка управління інформаційною безпекою підприємства

Управління інформаційною безпекою досліджуваного підприємства – це комплекс досить складних, розгалужених, режимних, технічних, профілактичних та унікальних заходів, спрямованих на забезпечення захисту підприємства як від зовнішніх так і внутрішніх загроз.

Тому надзвичайно важливим аспектом дослідження захисту інформації в системі інформаційної безпеки підприємства є оцінка зовнішніх та внутрішніх загроз інформаційній безпеці.

Найвагомішими зовнішніми загрозами інформаційній безпеці досліджуваного підприємства є шкідливе програмне забезпечення та спам, який часто є носієм шкідливого програмного забезпечення. Атаки з використанням шкідливого програмного забезпечення – це найнебезпечніший інструмент, що володіє високою ефективністю. Його застосування практично в половині випадків призводить до витоку інформації. Збільшується частка працівників, які зіткнувся з фішинговими атаками. Незначними є кількість мережевих вторгнень, відмов в обслуговуванні, випадки промислового шпигунства. За всіма іншими пунктами зовнішні загрози демонструють мінімальну кількість випадків. Основним наслідком будь-якої атаки в разі її успішного здійснення стає втрата підприємством конфіденційної інформації.

У свою чергу основними внутрішніми загрозами є: вразливість програмного забезпечення, неналежний обмін інформацією через мобільні пристрої, випадкові витоки від працівників та навмисні витоки інформації з вини співробітників, викликані в основному незнанням затверджених у

досліджуваному підприємстві правил.

Таким чином, основними групами дестабілізуючих факторів інформаційної безпеки підприємства визначаємо:

групу людського фактору, до якої відносимо персонал, зовнішніх осіб та конкурентів;

групу технічних факторів, яка включає: вірусне програмне забезпечення, шпигунські інформаційні системи, засоби пошкодження або виведення з ладу технічно-апаратних засобів, а також програмні та технічні засоби реалізації інформаційних загроз;

групу факторів природнього середовища, до якої відносяться природні та неконтрольовані фактори.

Варто зазначити, що всі данні, якими володіє досліджуване підприємство та платформа, якою користується підприємство знаходиться на серверах, доступ до серверної кімнати мають лише адміністратори IT. Вхід проводиться за допомогою складного графічного пароля, який знають лише адміністратори IT, у серверній встановлені камери, які ведуть запис цілодобово та оснащені власним джерелом енергії і в разі вимкнення електроживлення, о працюватимуть так само як і графічний пароль для входу в серверну.

Генерування всіх паролів та ключів проводиться системними адміністраторами підприємства, нові паролі та логіни видаються керівникам кожні 3-4 місяці, у разі зависання програм чи обладнання, лише системні адміністратори мають право проводити обслуговування та ремонт обладнання, ніякі сторонні особи до ремонту, діагностики та обслуговування технічного обладнання чи оновлення програм доступу не мають.

Загалом інформаційна система управління досліджуваного підприємства сформована стандартно та характерна базовим комплексом елементів (рис. 2.2).

Загалом інформаційна система товариства є нескладною за побудовою та місить лише найбільш необхідні елементи, які забезпечують прийняття, накопичення, обробку, зберігання та надання інформаційних ресурсів, та які є

відносно простими за своїм функціоналом.

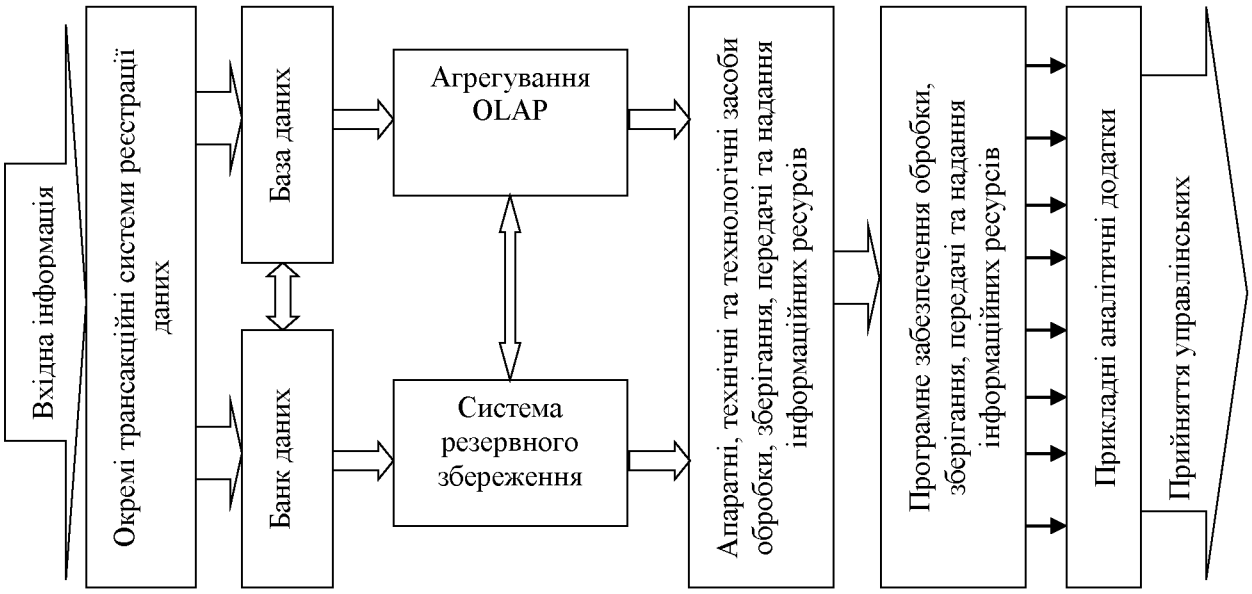

Рис. 2.2. Модель інформаційної системи управління підприємства, 2022 р.

Аналізуючи систему управління інформаційною безпекою досліджуваного підприємства доцільно визначити її функціональну модель, яку подано на рис. 2.3. Дана модель є стандартною та забезпечує реалізацію загальноприйнятого алгоритму інформаційного захисту.

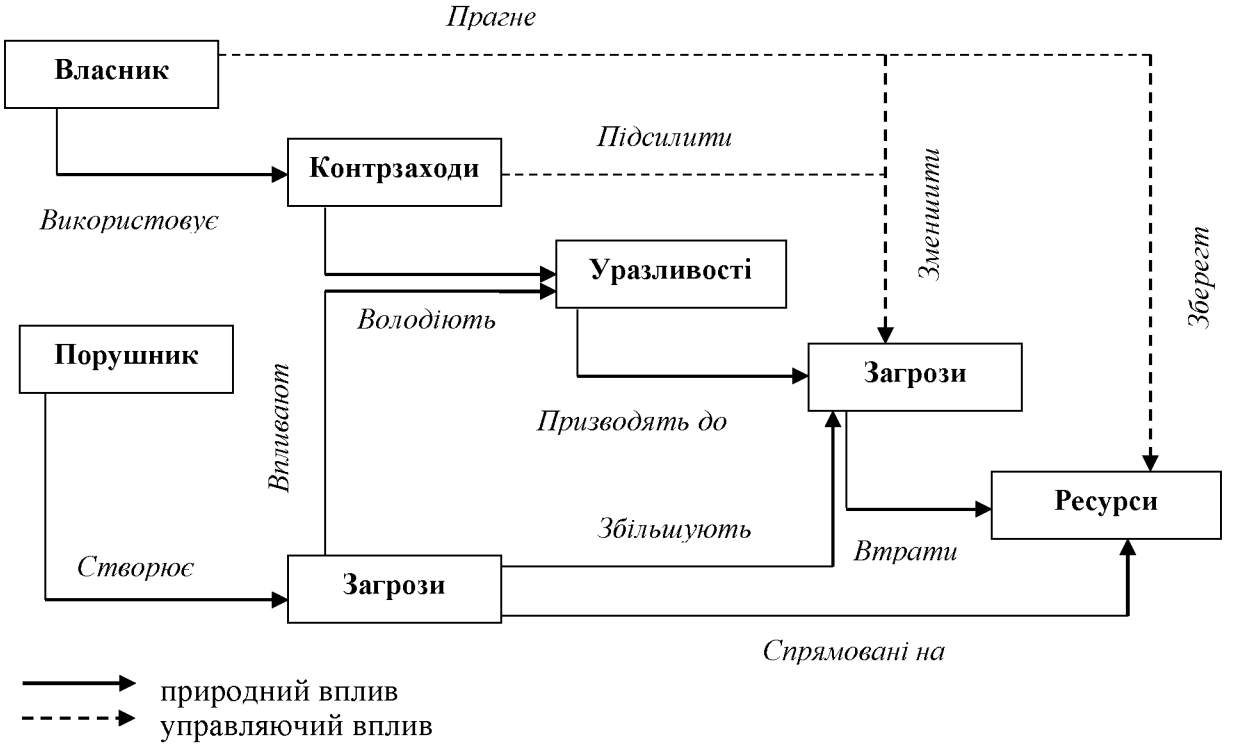

Рис. 2.3. Функціональна модель системи управління інформаційною безпекою підприємства, 2022 р.

Загалом усю інформацію, яка стосується досліджуваного підприємства можна поділити на три види:

інформація, що відноситься до комерційної таємниці (заробітна плата, технології виробництва, договори з постачальниками і споживачами, банки та бази даних);

інформація, що потребує захисту (трудові договори, особисті справи працівників, зміст регістрів бухгалтерського обліку та внутрішньої бухгалтерської звітності, інші документи і розробки для внутрішнього користування);

відкрита інформація (інформація в мережі Internet, інформація в соціальних мережах та месенджерах, статут).

За захист інформації відповідають працівники різних структурних підрозділів підприємства різних рівнів. На оперативному рівні відповідальність несе кожен із провідних фахівців. На тактичному рівні – фахівці, які відповідають за захист комерційної таємниці, що стосується окремих видів діяльності досліджуваного підприємства. Стратегічний рівень формує модель та політику захисту даних і визначає пріоритетні напрямки розвитку системи управління інформаційною безпекою підприємства. На даному рівні відповідальними є директор та загальні збори учасників. Таким чином, загальну структуру системи управління інформаційної безпеки досліджуваного схематично зображено на рис. 2.4.

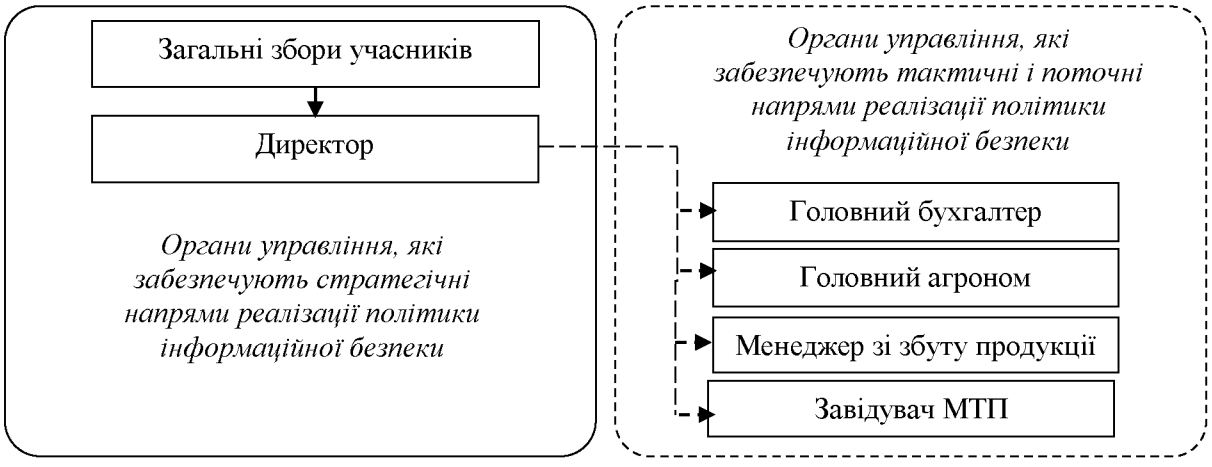

Рис. 2.4. Загальна структуру системи управління інформаційної безпеки підприємства

Аналіз системи управління інформаційною безпекою підприємства варто продовжити визначенням коефіцієнтів, що характеризують рівень захисту інформації досліджуваного підприємства за 2017-2021 рр. (табл. 2.9).

Таблиця 2.9

Показники рівня інформаційної безпеки підприємства, 2017-2021 рр.

Статті витрат	2017 р.	2018 р.	2019 р.	2020 р.	2021 р.	Відхилення 2021 р. до 2017 р.	
						(+; -)	%
Коефіцієнт технічного захисту інформації	0,73	0,64	0,85	0,57	0,89	0,16	21,92
Коефіцієнт програмної захищеності інформації	0,86	0,79	0,84	0,87	0,87	0,01	1,16
Коефіцієнт фінансового захисту інформації	0,08	0,1	0,11	0,09	0,07	-0,01	-12,50
Коефіцієнт фінансування інформаційних служб підприємства	0,03	0,02	0,05	0,03	0,02	-0,01	-33,33
Коефіцієнт правової захищеності інформації	0,22	0,26	0,19	0,17	0,11	-0,11	-50,00
Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства	0,76	0,59	0,64	0,79	0,81	0,05	6,58
Коефіцієнт підготовленості персоналу до розпізнавання загроз	0,58	0,64	0,55	0,71	0,68	0,1	17,24
Оцінка інформації, що надається особам, що приймають рішення (ОПР), інформаційною службою підприємства	0,25	0,26	0,31	0,22	0,2	-0,05	-20,00
Коефіцієнт точності інформації	0,89	0,81	0,82	0,78	0,85	-0,04	-4,49
Коефіцієнт суперечливості інформації	0,54	0,62	0,55	0,57	0,57	0,03	5,56
Коефіцієнт своєчасності надання інформації	0,45	0,39	0,4	0,41	0,43	-0,02	-4,44
Коефіцієнт надійності інформації	0,65	0,63	0,71	0,63	0,61	-0,04	-6,15

Результати розрахунків коефіцієнтів дали змогу визначити, що значення коефіцієнту технічного захисту інформації зросло у 2021 р. порівняно з 2017 р. на 0,16 або на 21,92 %.

Коефіцієнт програмної захищеності інформації дещо збільшився на 0,01 або ж на 1,16 % протягом досліджуваного періоду.

Коефіцієнт фінансування інформаційних служб підприємства показує скільки витрат йде на утримання працівників, які мають відношення до забезпечення інформаційної безпеки. Даний показник зменшився на 33,3 % протягом досліджуваного періоду.

Коефіцієнт фінансового захисту інформації не відповідає нормативному значенню і зменшився на 12,5 % у 2021 порівняно з 2017 р. Коефіцієнт правової захищеності не задовольняє умови правового захисту інформаційних ресурсів досліджуваного підприємства і зменшився на 50,0 % протягом досліджуваного періоду. Негативним моментом також є зниження коефіцієнтів: своєчасності надання інформації на 4,44 %, точності інформації на 4,49 %, надійності інформації на 6,15 %, що є оберненим до зростанням коефіцієнту суперечливості інформації на 5,56 %.

У той же час збільшується значення коефіцієнту підготовленості персоналу до розпізнавання загроз на 17,24 % протягом досліджуваного періоду, що є позитивним моментом, однак цього не достатньо для формування ефективної системи інформаційної безпеки.

Висновки до розділу 2

Проаналізувавши підприємство як систему управління, доцільно зробити наступні висновки:

1. Підприємство має лінійну структуру управління. Основними відділами підприємства є токове господарство; тракторно-рільничі бригади №1, 2; складське господарство; ремонтна майстерня.

Виробничий напрямок досліджуваного підприємства можна охарактеризувати як зерново-технічний: перше місце в структурі товарної продукції підприємства за останні п’ять років займало виробництво кукурудзи на зерно – 65,3 %, друге – виробництво соняшнику 20,0 %, третє – соя 8,6 %.

2. У досліджуваному підприємстві чисельність управлінського

персоналу дещо зменшилася (на 2 особи) і становить 12 осіб, у тому числі 4 керівники та 8 спеціалістів. Виробничий персонал підприємства у 2021 році становив 50 осіб, що дорівнює значенню 2017 року. Загалом у 2017 р. персонал налічував 69 осіб, а у 2021 р. – 62 особи, що на 10,1 % менше.

Протягом досліджуваного періоду підприємство було прибутковим. Однак у 2018-2020 рр. чистий прибуток зменшився майже удвічі, а у 2021 році підприємству вдалося підвищити цей показник до рівня 2017 року.

Вцілому підприємство функціонує ефективно, злагоджено та відповідає умовам ринку та попиту на дані види продукції.

3. Відповідальність за збереження інформації покладена на директора і окремих фахівців, оскільки підрозділу, який би забезпечував цей процес у структурі досліджуваного підприємства немає.

Протягом аналізованого періоду найбільш значимими зовнішніми загрозами для товариства визначено шкідливе програмне забезпечення та спам, який часто є носієм шкідливого програмного забезпечення. Основними внутрішніми загрозами інформаційної безпеки є: вразливість програмного забезпечення, випадкові витоки від працівників та навмисні витоки інформації з вини співробітників.

РОЗДІЛ 3
НАПРЯМИ УДОСКОНАЛЕННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА В СУЧАСНОМУ БІЗНЕС-СЕРЕДОВИЩІ

3.1. Рекомендації щодо вдосконалення процесу забезпечення захисту інформації в підприємстві

Сьогодні застосування сучасних технологій забезпечує успіх бізнесу. Тому на перший план виходить інформаційна безпека підприємства. Відповідно, щоб захистити свій бізнес від неправдивої інформації як керівництво, так і кожен працівник досліджуваного підприємства повинні дотримуватися правил проти кібератак. Для того щоб досліджуване підприємство не стало ціллю кіберзлочинців, пропонуються основні правила необхідного забезпечення інформаційної безпеки підприємства (рис. 3.1).

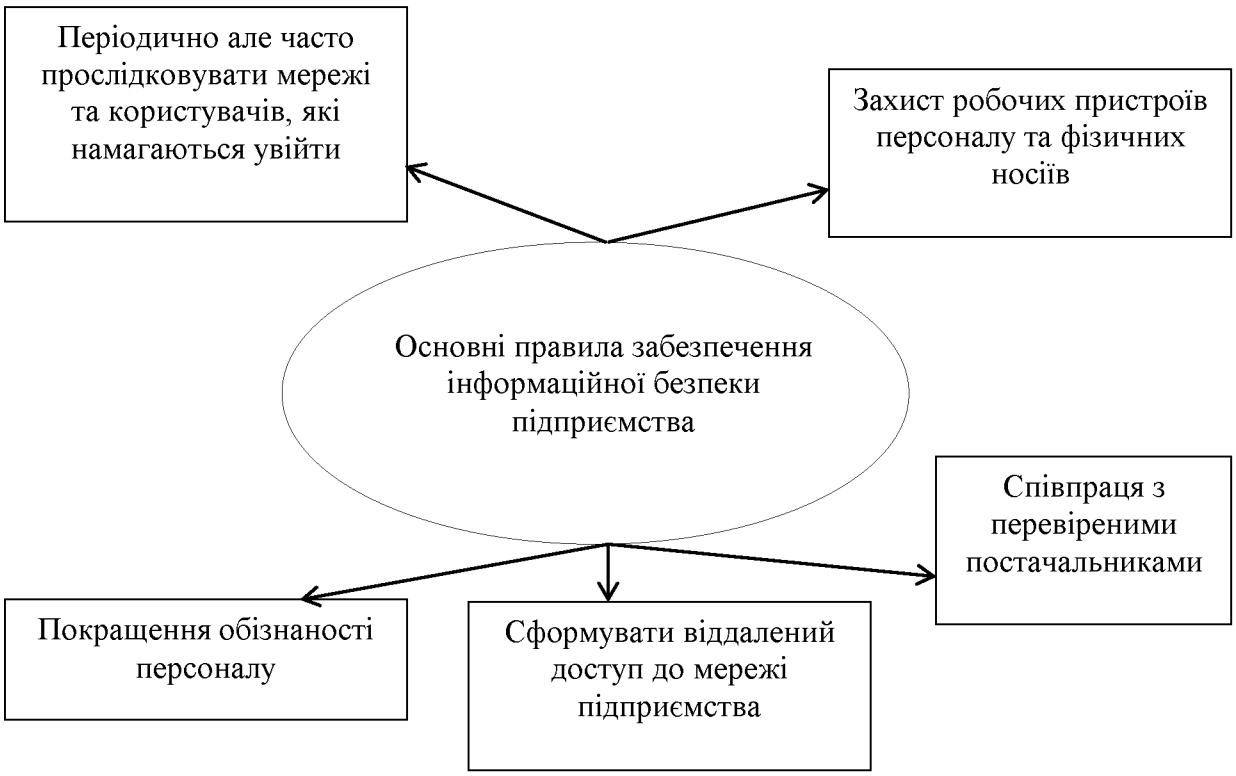

Рис. 3.1. Основні правила забезпечення інформаційної безпеки підприємства

По перше, своєчасно та достовірно інформувати своїх співробітників про поточні зміни в підприємстві, загрозу банкрутства або перспективи розвитку. Кіберзлочинці, як правило, хочуть отримати доступ до даних підприємства через її «найслабкішу точку» – недосвідченого персоналу. Для початку вони надсилають настільки «справжній» фейковий звіт, що працівник відкриває його, не дізнавшись про шкідливу роботу.

У такому випадку розвиток подій може бути різним: до пристрою завантажуються шкідливі (шпигунські) програми, віруси, трояни. Тому для зміцнення інформаційної безпеки, перш за все, необхідно повідомляти персонал про поточні загрози та методи захисту від них. Кожен працівник підприємства повинен усвідомлювати необхідність захисту даних клієнтів та внутрішньої інформації. Керівництво має задумуватися про регулярність проводити тренінги, що стосуються забезпечення інформаційної безпеки в усіх структурних підрозділах, працівники яких задіяні у процесі захисту даних.

По друге, захистити свої робочі комп'ютери і носії інформації. Дані, які не є захищеними піддаються шкідливому програмному забезпеченню і комерційним кібератакам. Тому що в разі крадіжки чи втрати корпоративних смартфонів, носіїв інформації, ноутбуків працівник втрачає усі дані підприємства.

З метою запобігання таких ситуацій варто: не залишати комп'ютер увімкненим і завжди виходити з системи та джерел, які містять конфіденційні дані; встановлювати правила для файлів, носіїв інформації, електронних листів та шифрувати усі корпоративні дані (в результаті, якщо функціональний пристрій втрачено, то зловмисники не зможуть отримати дані підприємства); регулярно створювати резервні копії файлів, що дозволить у будь-який час отримати інформацію.

По третє, надійний контроль в організації. Адже з міркувань безпеки підприємства негласні дані повинні зберігатися на окремих серверах, які забезпечують додатковий захист через брандмауери або інші служби

безпеки. Це зменшує ризик втрати даних. Також треба стежити за користувачами, які намагаються отримати доступ до вашої мережі або здійснюють покупки. Це дозволяє адміністраторам швидко викривати підозрілу поведінку та реагувати на неї.

По четверте, надійна співпраця. Кожна угода про надання послуг, постачання або іншу співпрацю має містити конкретні вимоги безпеки. Багато постачальників хмарних послуг регулярно переглядають різні заходи щодо загроз, щоб відповідати галузевим стандартам інформаційної безпеки. Постачальник послуг повинен мати рівень безпеки, відповідний партнерству.

По п'яте, захист віддаленого доступу. Високошвидкісний доступ до Інтернету та сучасна трудова етика в організації дозволяють багатьом офісним працівникам працювати з дому.

Такий режим роботи з року в рік стає все більш популярним. Особливо сьогодні можливість безпечної дистанційної роботи для підприємства є великою перевагою. Будь-який пристрій співробітника або клієнта, що забезпечує віддалений доступ до корпоративної мережі, повинен відповідати стандартам інформаційної безпеки, які вимагають:

підключення до віртуальної приватної мережі (VPN).

використання двохфакторної аутентифікації під час входу або підключення до VPN.

доступу до віртуальної машини як варіанту підключення за замовчуванням, якщо це можливо.

використання комплексного рішення безпеки для захисту від зловмисників, шпигунського програмного забезпечення та інших загроз, а також запобігання фішинговим атакам.

Враховуючи вищезазначене, можна виділити основні етапи в процесі організації захисту інформації підприємства (рис. 3.2).

Як правило, усі здійснювані кіберзлочини мають єдину послідовність дій кіберзлочинців, що зумовлює необхідність поетапного управління ризиками діджиталізації (рис. 3.3).

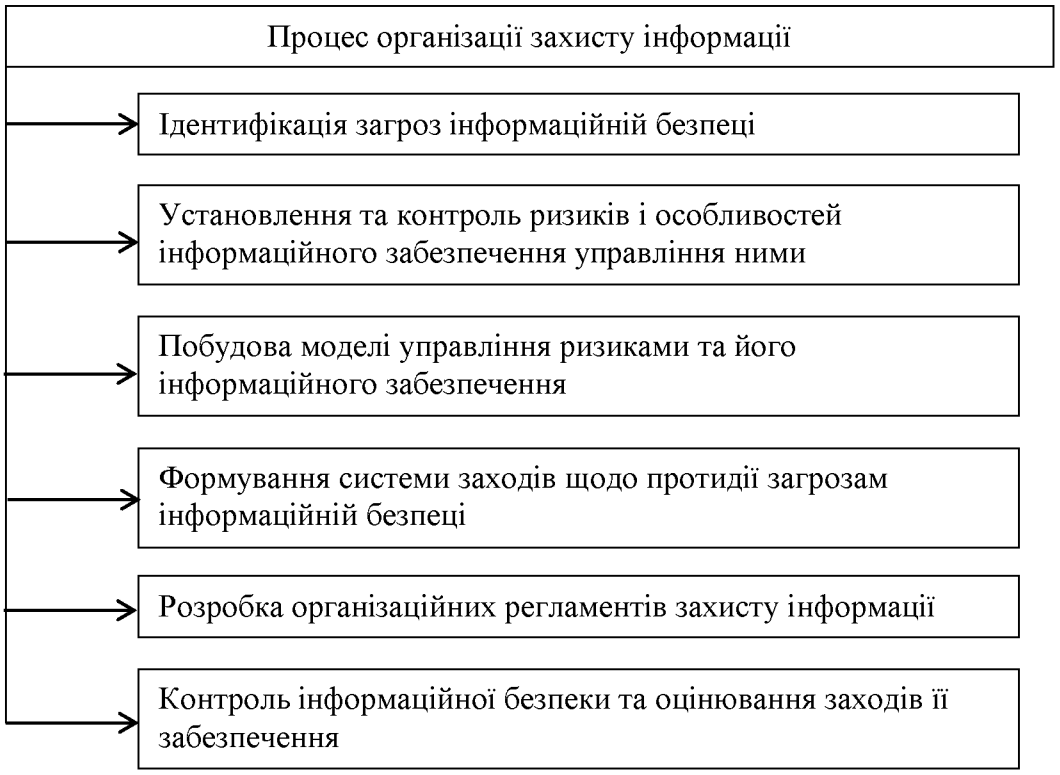

Рис. 3.2. Процес організації захисту інформації підприємства

Зокрема, метою попереджувального етапу є оцінка (розвідка) можливого впливу кіберризиків. На етапах фактичного проникнення кіберзлочинців у середину інформаційної оболонки необхідним є реакційний етап негайного блокування кіберінциденту (чи кібератаки), а на захисному етапі – максимально можливе збереження доступного обсягу інформації та її перенесення на інші носії чи хмарні сховища.

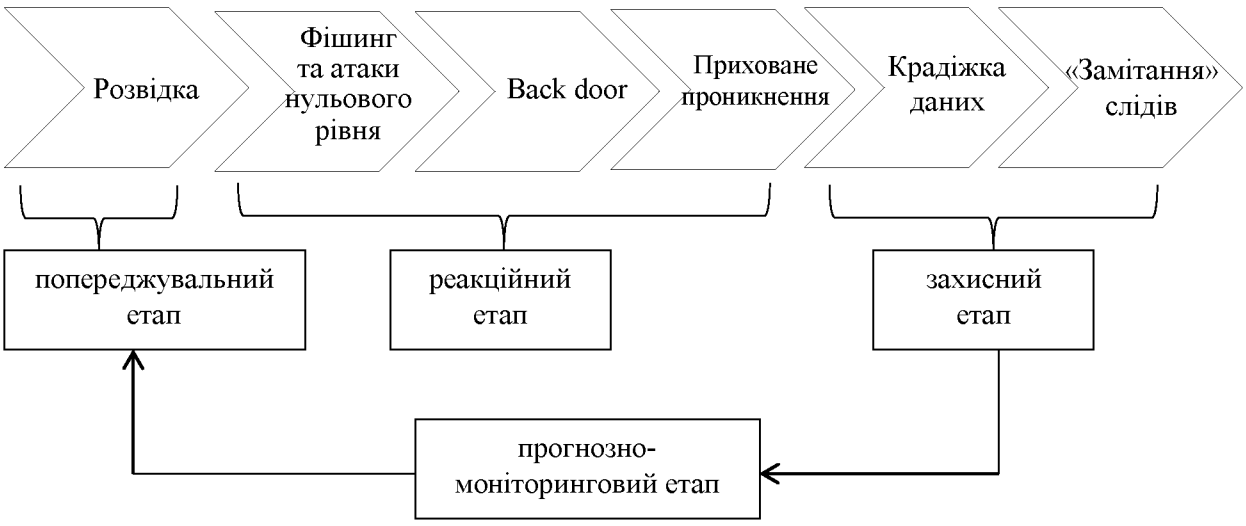

Рис. 3.3. Модель реагування і нівелювання кіберзагроз інформаційної безпеки підприємства на різних стадіях кібератак

Мета прогностично-моніторингового етапу – постійне відстежування вже відомих і потенційних діджиталізаційних ризиків та прогнозування сценаріїв їхнього впливу на інформаційну і, як наслідок, економічну безпеку підприємств.

У результаті попереджувального, реакційного, захисного та прогнозно-моніторингового етапу кіберзахисту можливе поступальне планування і реалізація відновлювальних заходів унаслідок впливу кібератак на економічну безпеку в коротко-, середньо- та довгостроковій перспективі (табл. 3.1).

Таблиця 3.1

Відновлювальні заходи внаслідок впливу кібератак на інформаційну безпеку підприємства

Рівень реагування	Період реагування	Заходи
Короткостроковий (оперативний)	Дні / тижні	Пошук компромісів захисту від кібератак
		Діагностика заходів кіберзахисту і їх організаційного забезпечення
		Комунікативна взаємодія з контрагентами
		Забезпечення безперервності бізнес-процесів
Середньостроковий (перманентний)	Тижні / місяці	Побудова інфраструктури кіберзахисту й архітектури кібер-менеджменту
		Перманентна взаємодія з адвокатськими та судовими інституціями сфери кіберзахисту
		Моніторинг та оцінювання ймовірних небезпек на основі оцінки попередніх і потенційних кіберзагроз
Довгостроковий (стратегічний)	Місяць / роки	Збільшення інвестицій у розробку або придбання кіберпрограм інформаційної безпеки
		Відновлення бізнесу, який зазнав шкоди внаслідок кібератак у попередні періоди
		Формування банку (архіву) даних кіберзахисту

Отже, повна автоматизація сучасної мережі, застосування хмарних технологій зберігання інформації дасть змогу побудувати надійні інформаційні зв’язки між структурними підрозділами підприємства. Проте, це можливо лише за умови розробки ефективних стратегій формування кібербезпеки облікового простору, навчання персоналу і збільшення витрат на кіберзахист підприємств.

Таким чином, для того щоб досліджуване підприємство не стало

жертвою хакерської атаки потрібно дотримуватися всіх правил інформаційної безпеки. Тоді підприємство матиме значно менші збитки та неполадки бізнес-процесів.

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

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

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

Слід відзначити, що виключеного з багатофакторної моделі коефіцієнту програмної захищеності інформації здійснено через найменше серед інших факторів показником коефіцієнту кореляції. Проте, цей фактор, має не менш важливе значення для створення системи належного захисту інформаційної інфраструктури досліджуваного підприємства. Тому програмне забезпечення разом з технічним забезпеченням визначають основу

функціонування інформаційної системи будь-якого підприємства.

Визначено, що прогнозне значення чистого прибутку підприємства на 2023 р. становить 11,55 % (додаток Д).

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

3.2. Удосконалення системи управління інформаційною безпекою підприємства

Сьогодні багато українських підприємств вирішують завдання створення системи інформаційної безпеки, яка відповідала б «найкращим практикам» і стандартам у сфері інформаційної безпеки та відповідала сучасним вимогам захисту інформації за параметрами конфіденційності, цілісності та доступності. Причому, це питання є важливим не тільки для «молодих» підприємств, що розвивають свій бізнес з використанням сучасних інформаційних технологій управління. Не менш, а швидше і більш важливою ця проблема є для підприємств і організацій, які давно працюють на ринку, які приходять до необхідності модернізувати існуючу у них систему інформаційної безпеки.

З метою вирішення завдань та встановлених цілей потрібно проводити заходи на різних рівнях інформаційної безпеки.

На *адміністративному* рівні з метою формування системи інформаційної безпеки варто розробити та затвердити політику інформаційної безпеки, яка передбачає сукупність правил, законів та норм поведінки, що спрямовані на захист інформації та асоційованих із нею ресурсів.

Політика інформаційної безпеки має узгоджуватися з існуючими правилами та законами, існуючих в підприємстві. Чим надійніша система, тим суворішою і різноманітнішою має бути політика безпеки. Залежно від сформульованої політики можна обирати конкретні механізми, які забезпечують безпеку системи.

Організаційний рівень захисту інформації. Враховуючи зауваження до управління інформаційною безпекою досліджуваного підприємства у попередньому розділі, варто запропонувати наступні заходи для покращення процесу захисту інформації:

організація навчання персоналу навичкам роботи з новими програмними продуктами за участю кваліфікованих спеціалістів;

розробка необхідних заходів спрямованих на вдосконалення системи економічної, соціальної та інформаційної безпеки підприємства;

проведення інструктажу з метою усвідомлення кожним працівником всієї важливості та конфіденційності довіреної йому інформації, тому що, як правило, причиною розголошення конфіденційної інформації є недостатнє знання працівниками правил захисту комерційних секретів і нерозуміння необхідності їх ретельного дотримання;

контроль за дотриманням правил зберігання корпоративної документації підприємства;

строгий контроль за дотриманням працівниками правил роботи з конфіденційною інформацією;

планова перевірка та обслуговування всіх інформаційних систем та інформаційної інфраструктури;

планове проведення зборів, семінарів, обговорень з питань інформаційної безпеки підприємства;

призначення постійного системного адміністратора.

Варто зазначити, що програмно-технічні засоби є одними з головних елементів реалізації інформаційного захисту підприємства, тому потрібно запровадити і застосовувати такі заходи задля підвищення його рівня:

призначення паролів користувачів (з метою регулювання доступу користувачів до інформаційних ресурсів підприємства потрібно скласти перелік користувачів, які матимуть змогу входити у систему під своїм логіном та паролем. Так, за допомогою ОС Windows, встановленої на сервері, можна створити перелік користувачів з відповідними паролями, які необхідно роздати працівникам та провести їм відповідний інструктаж. Також необхідно ввести термін дії пароля, після якого користувачеві буде запропоновано змінити пароль. Обмежити кількість спроб входу до системи з неправильним паролем);

введення запиту паролів у програмі 1С: Підприємств при роботі з базами даних, при зміні даних., що можна зробити за допомогою програмних засобів;

розмежування доступу до файлів та каталогів, що буде здійснюватися системним адміністратором, який дозволить доступ до відповідних дисків, папок та файлів для кожного користувача конкретно;

регулярне сканування робочих станцій та оновлення баз антивірусної програми, що дозволить виявляти та нейтралізувати шкідливі програми, ліквідувати причини заражень;

встановлення та забезпечення функціонування засобів антивірусного захисту;

встановлення на комп'ютер-сервер мережевого екрану Agnitum Outpost FireWall, який блокує атаки з Інтернету, перевагою якого є контроль з'єднання комп'ютера з іншими, при цьому блокуючи хакерів та запобігаючи несанкціонованому зовнішньому та внутрішньому доступу до мережі.

Враховуючи зазначене, комплексна модель менеджменту захисту інформації досліджуваного підприємства повинна створюватися з використанням пакетного інформаційного забезпечення на програмно-керованих технічних засобах загального користування.

Інформаційна система підприємства повинна бути оснащена штатними і, при необхідності, додатковими позаштатними засобами технічного захисту

інформації, які при їхньому спільному використанні утворюватимуть комплекс засобів і механізмів захисту, що забезпечують потрібний рівень захищеності інформаційних ресурсів підприємства, тобто спроможності системи інформаційної безпеки протистояти впливам загроз (рис. 3.4).

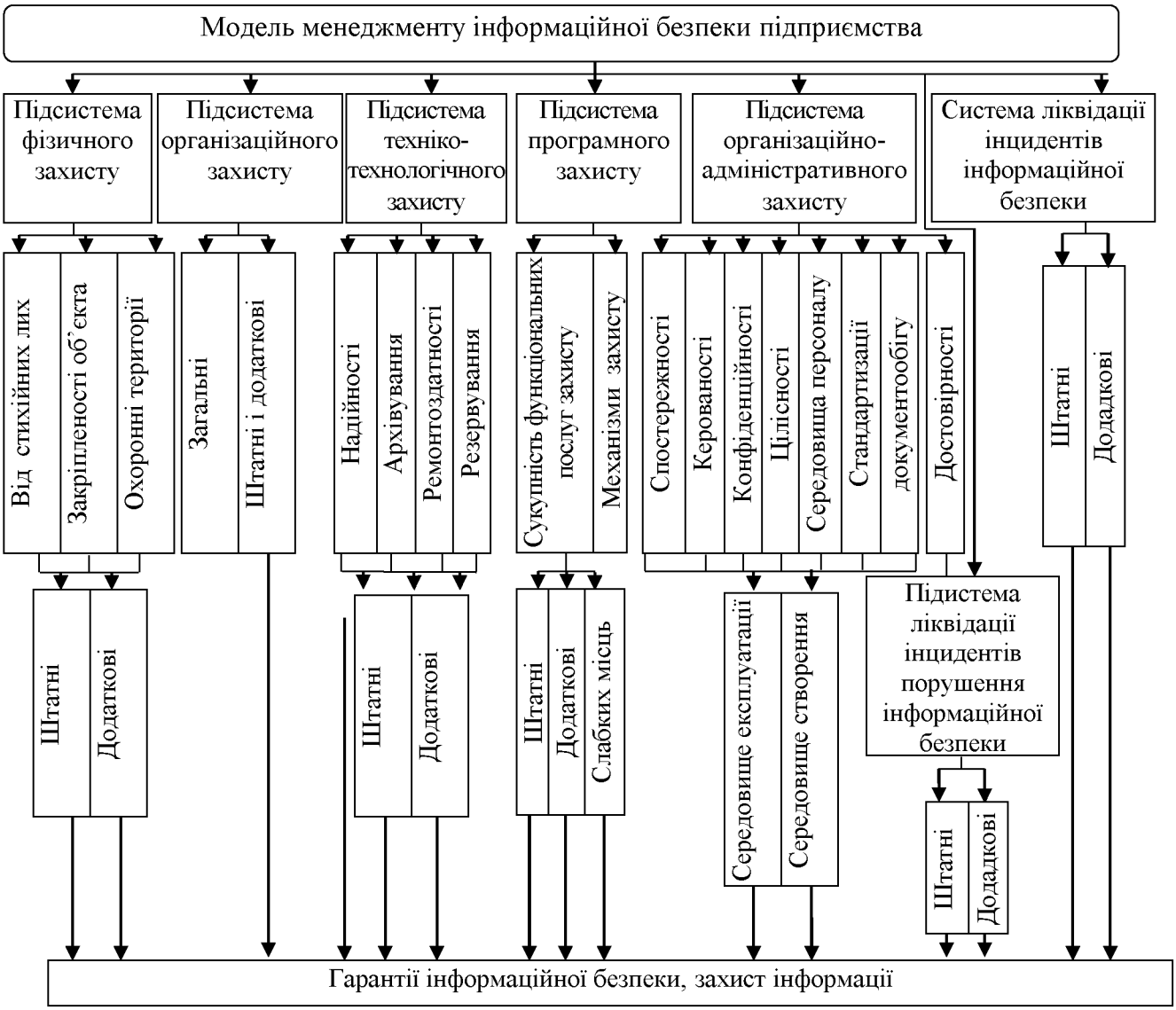

Рис. 3.4. Пропонована модель комплексної системи інформаційної безпеки підприємства [на основі 45]

В межах пропонованої моделі менеджменту інформаційної безпеки підприємства, сукупність функціональних послуг захисту повинен передбачати набір елементарних функцій, виконання яких у середовищі експлуатації дозволяє протистояти певній множині загроз для інформації.

Відтак, до штатних елементів захисту в межах кожної із зазначених підсистем доцільно включити функції захисту від: несанкціонованого впливу

через штатні елементи доступу; позаштатного впливу через штатні елементи або додаткові програмні та технічні засоби; позаштатного впливу на параметри інформаційного середовища; впливу з використанням позаштатних програмними та програмно-технічними засобів на програмні елементи товариства; впливу позаштатних технічних або програмно-технічних засобів на апаратну частину інформаційної системи; витоку інформації через побічні канали; інформаційно-вразливого режиму, модифікації функцій, і як результату послуг, які надаються інформаційною системою товариства; збоїв та відмов у функціонуванні інформаційної системи, баз та банків даних; загроз у підсистемах, які забезпечують збереження інформаційних ресурсів, в тому числі і на фізичних носіях.

Також до штатних функціональних послуг пропонованої системи менеджменту інформаційної безпеки доцільно включити заходи ліквідації настання наслідків від реалізованих загроз та систему менеджменту техніко-технологічного захисту інформації на підприємстві.

Отже, ефективне формування та впровадження формування комплексної моделі менеджменту інформаційної безпеки підприємства передбачає виконання основних умов, зокрема: інформаційна безпека повинна формуватися на основі цілей виробничо-господарської діяльності; стратегічні функції менеджменту інформаційної безпеки повинні виконуватися вищим керівництвом підприємства, спеціалізований орган – адміністратор з питань інформаційної безпеки, який входить до відділу інформаційних технологій повинен забезпечувати виконання оперативних й тактичних функцій управління інформаційною безпекою; необхідно розробити та постійно використовувати систему моніторингу оцінювання ризиків порушення інформаційної безпеки, виникнення загроз, вразливостей інформаційного середовища; рівень захищеності інформаційних ресурсів та має базуватися на цінності й важливості цих ресурсів; необхідна політика інформаційної безпеки, яка б базувалась на основах інформаційної культури поведінки та ознайомлення з нею керівників та співробітників товариства;

дотримання світових та вітчизняних стандартів інформаційної безпеки.

На основі узагальнення зазначених пропозицій, модель функціональної побудови системи управління інформаційною безпекою досліджуваного підприємства потрібно модифікувати відповідно до вигляду відображеного на рис. 3.5.

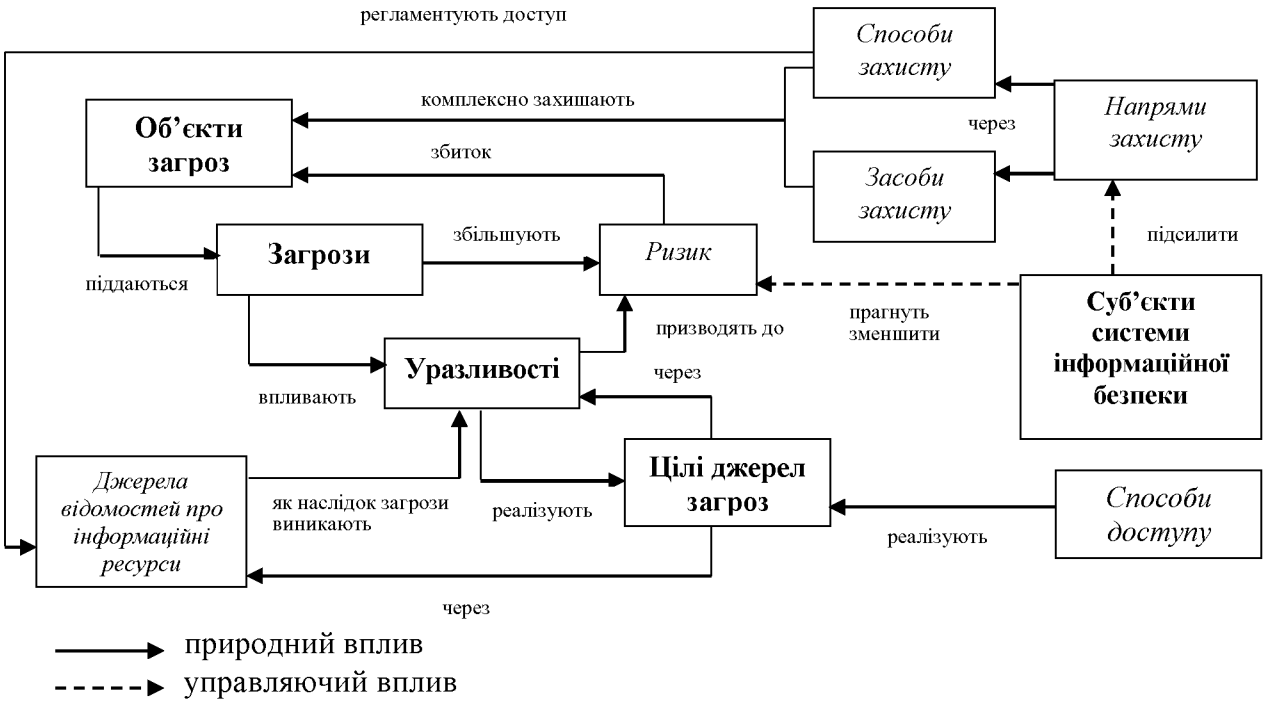

Рис. 3.5. Пропонована функціональна модель управління інформаційною безпекою підприємства [сформовано на основі 6]

Зазначена модель, на відміну від існуючої на товаристві, має більш широкий функціонал та спрямована на одночасне застосування декількох напрямів забезпечення інформаційної безпеки та одному або декількох рівнях, що за незмінних програмних, апаратних та техніко-технологічних засобах матиме значно вищу ефективність захисту інформаційної інфраструктури підприємства.

Метою процесу менеджменту інформаційної безпеки товариства повинно стати, перш за все, визначення та оцінка ефективності пропонованої модель менеджменту інформаційної безпеки, а також визначення додаткових уточнюючих вимог для модифікації та оптимізації системи інформаційного захисту з метою забезпечення її релевантності за зміни умов функціонування підприємства.

Висновки до розділу 3

За результатами рекомендаційного розділу кваліфікаційної роботи слід зазначити:

1. Встановлено, що базовими аспектами будь-якої інформаційної системи сільськогосподарського підприємства є техніко-технологічне устаткування, програмне забезпечення та кадровий потенціал, який здійснює процеси управління інформаційним захистом. Запропоновано розглядати напрями оптимізації системи захисту інформації в підприємстві саме в зазначених площинках шляхом формування багатофакторної виробничої регресії. Характеризуючи коефіцієнти кореляції, то можна простежити, що кожен із факторів (коефіцієнт технічного захисту інформації, коефіцієнт програмної захищеності інформації та коефіцієнт підготовленості персоналу до розпізнавання загроз) суттєво впливає на рентабельність діяльності. Вдосконалення даних напрямів дозволить отримати прогнозне значення рентабельності – 11,55 %.

2. Враховуючи існуючі інформаційні, технічні, програмні засоби та, звичайно, фінансові ресурси підприємства, з метою покращення рівня інформаційного захисту, керівництву пропонується впровадити комплексну модель управління інформаційною безпекою. Пропонована модель повинна враховувати й основні напрями забезпечення захисту інформаційної інфраструктури за певними рівнями, враховуючи концепцію «глибинного захисту». Зважаючи на зазначене, модель повинна створюватися з використанням пакетного інформаційного забезпечення на програмно-керованих технічних засобах загального користування. Водночас, реалізацію основних напрямів управління інформаційною безпекою за різними рівнями та базовими напрямами доцільно забезпечити нормативно-організаційними та методичними засобами, серед яких особливе місце повинні політика, стратегія, модель поведінки працівника, навчання персоналу та інші.

ВИСНОВКИ

Результати проведеного дослідження кваліфікаційної роботи на тему «Управління інформаційною безпекою підприємства в сучасному бізнес-середовищі» дають змогу зробити наступні висновки:

1. Інформація – це сукупність певних даних, які описують стан керованої й керуючої підсистем та зовнішнього середовища; результат і предмет праці менеджменту підприємства. Безпека – це умови, в яких знаходиться складна система, в цих умовах зовнішні та внутрішні чинники, не призводять до негативних процесів, які є згубними для складної системи відповідних потреб, знань і уявлень.

Інформаційна безпека підприємства відображає захищеність інформаційного середовища та ефективність інформаційного забезпечення процесу управління на підприємстві. Вона є найважливішим елементом системи економічної безпеки підприємництва, основа процесу його управління.

2. Організаційна модель системи управління інформаційною безпекою підприємства передбачає наявність класичних складових для забезпечення захисту інформаційної інфраструктури товариства: суб'єктів управління інформаційною інфраструктурою та суб'єктів управління інформаційною безпекою, об'єктів, що підлягають цифровому та інформаційному захисту, а також власне процесу управління, який передбачає включення стратегії, політики інформаційної безпеки (неформалізованих), цілей, методів, функцій, заходів та інструментів.

3. Підприємство має лінійну структуру управління. Місія діяльності – виробництво та реалізація сільськогосподарської продукції, а також надання учасникам підприємства та іншим особам послуг щодо ведення сільського господарства та здійснення інших, пов'язаних з ним видів діяльності. Повноваження директора визначені Статутом товариства. Повноваження головних спеціалістів визначені Посадовою інструкцією. Контроль за

діяльністю директора товариства з обмеженою відповідальністю здійснюється ревізійною комісією, що утворюється зборами учасників товариства з трьох осіб. Основними відділами підприємства є токове господарство; тракторно-рільничі бригади №1, 2; складське господарство; ремонтна майстерня.

Виробничий напрямок досліджуваного підприємства можна охарактеризувати як зерново-технічний: перше місце в структурі товарної продукції підприємства за останні п'ять років займало виробництво кукурудзи на зерно – 65,3 %, друге – виробництво соняшнику 20,0 %, третє – соя 8,6 %.

4. У досліджуваному підприємстві чисельність управлінського персоналу дещо зменшилася (на 2 особи) і становить 12 осіб, у тому числі 4 керівники та 8 спеціалістів. Виробничий персонал підприємства у 2021 році становив 50 осіб, що дорівнює значенню 2017 року. Загалом у 2017 р. персонал налічував 69 осіб, а у 2021 р. – 62 особи, що на 10,1 % менше.

Протягом досліджуваного періоду підприємство було прибутковим. Однак у 2018-2020 рр. чистий прибуток зменшився майже удвічі, а у 2021 році підприємству вдалося підвищити цей показник до рівня 2017 року.

Вцілому підприємство функціонує ефективно, злагоджено та відповідає умовам ринку та попиту на дані види продукції.

5. Відповідальність за збереження інформації покладена на директора і окремих фахівців, оскільки підрозділу, який би забезпечував цей процес у структурі досліджуваного підприємства немає.

Протягом аналізованого періоду найбільш значимими зовнішніми загрозами для товариства визначено шкідливе програмне забезпечення та спам, який часто є носієм шкідливого програмного забезпечення. Основними внутрішніми загрозами інформаційної безпеки є: вразливість програмного забезпечення, випадкові витоки від працівників та навмисні витоки інформації з вини співробітників.

6. Встановлено, що базовими аспектами будь-якої інформаційної

системи сільськогосподарського підприємства є техніко-технологічне устаткування, програмне забезпечення та кадровий потенціал, який здійснює процеси управління інформаційним захистом. Запропоновано розглядати напрями оптимізації системи захисту інформації в підприємстві саме в зазначених площинках шляхом формування багатофакторної виробничої регресії. Характеризуючи коефіцієнти кореляції, то можна простежити, що кожен із факторів (коефіцієнт технічного захисту інформації, коефіцієнт програмної захищеності інформації та коефіцієнт підготовленості персоналу до розпізнавання загроз) суттєво впливає на рентабельність діяльності. Вдосконалення даних напрямів дозволить отримати прогнозне значення рентабельності – 11,55 %.

7. Враховуючи існуючі інформаційні, технічні, програмні засоби та, звичайно, фінансові ресурси підприємства, з метою покращення рівня інформаційного захисту, керівництву пропонується впровадити комплексну модель управління інформаційною безпекою. Пропонована модель повинна враховувати й основні напрями забезпечення захисту інформаційної інфраструктури за певними рівнями, враховуючи концепцію «глибинного захисту». Зважаючи на зазначене, модель повинна створюватися з використанням пакетного інформаційного забезпечення на програмно-керованих технічних засобах загального користування. Водночас, реалізацію основних напрямів управління інформаційною безпекою за різними рівнями та базовими напрямами доцільно забезпечити нормативно-організаційними та методичними засобами, серед яких особливе місце повинні політика, стратегія, модель поведінки працівника, навчання персоналу та інші.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ананченко О.Є. Питання формування організаційної структури системи управління інформаційною безпекою підприємства. *Сучасний захист інформації*. 2016. № 1. С. 79-83.

2. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. URL: http://www.nbuv.gov.ua/portal/chem_biol/nvnltu/18_9/270_Anilowska_18_ 9.pdf

3. Ареф'єва О.В. Інформаційний базис управління економічною безпекою підприємства. *Науковий вісник НЛТУ України*. 2015. Вип. 25.4. С. 190-193.

4. Архипов О., Скиба А. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації. *Захист інформації*. 2013. Т. 15, № 4. С. 366-375.

5. Архипов О., Теплицька Т. Адаптивний підхід до управління інформаційною безпекою. *Молодий вчений*. 2019. № 11 (75). С. 668-672.

6. Бехтер Л. А. Загрози інформаційної безпеки та захист інформації як складова економічної безпеки сільськогосподарських підприємств. *Агросвіт*. 2020. № 12. С. 66-70.

7. Борсуковський Ю.В. Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. *Кібербезпека: освіта, наука, техніка*. 2020. № 4 (8). С. 34-48.

8. Бурячок В.Л., Гулак Г.М, Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : підручник. К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. 449 с.

9. Голубєв В.О. Інформаційна безпека : проблеми боротьби з кіберзлочинами : монографія. Запоріжжя : ЗІДМУ, 2003. 250 с.

10. Денисенко М.П., Колос І.В. Інформаційне забезпечення ефективного управління підприємством. *Економіка та держава*. 2006. № 7. С. 19-24.

11. Дзьобань О.П., Соснін О.В. Інформаційна безпека: нові виміри загроз, пов'язаних із інформаційно-комунікаційною діяльністю. *Гуманітарний вісник Запорізької державної інженерної академії*. 2015. Вип. 61. С. 24-34.

12. ДСТУ ISO/IEC 27000:2019 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. ДП УкрНДНЦ наказ від 16.10.2019 р. № 312. URL: http://online.budstandart.com/ua/catalog/docpage.html?id_doc=85795

13. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. ДП УкрНДНЦ наказ від 18.12.2015 р. № 193. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66910

14. Дячков Д.В. Методичні підходи до оцінки інформаційної безпеки підприємства. Вісник *Сумського національного аграрного університету : Серія «Економіка і менеджмент»*. 2017. № 12 (74). С. 87-92.

15. Дячков Д.В. Характеристика сучасних загроз системі управління інформаційною безпекою аграрних підприємств. *Бізнес-навігатор*. 2019. Вип. 6.1-1. С. 172-177.

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

17. Залевська І. Інформаційна безпека: нові підходи до визначення поняття. *Освіта регіону*. 2010. № 4. С. 216-219.

18. Захаров Є. Інформаційна безпека: що захищаємо? *Свобода висловлювань і приватність*. 2013. № 4. С. 3-6.

19. Збожинський С. Інформаційна безпека під час застосування цифрових технологій. *Юридична газета*. 2017. С. 18-19.

20. Зубок М. Інформаційна безпека в підприємницькій діяльності: підручник. Київ, 2015. 216 с.

21. Інформація та документація. Базові поняття. Терміни та визначення:

ДСТУ 2398-94. Чинний від 1995-02-01. К. : Держспоживстандарт України, 1995. I, 45 с. (Національний стандарт України).

22. Кавун С.В. Інформаційна безпека: підручник. Харків: ХНЕУ, 2009. 368 с.

23. Калетнік В., Калетнік Н. Інформаційна безпека і кіберзахист як сучасна інтелектуальна зброя. *Молодий вчений*. 2021. С. 305-311.

24. Кісілевич-Чорнойван О.М. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять. *Юриспруденція: теорія і практика*. 2009. С. 11-18.

25. Кривчун Р.Ю. Модель системи інформаційної безпеки підприємства. *Управління ресурсним забезпеченням господарської діяльності підприємств реального сектору економіки* : матер. VII Всеукр. наук.-практ. інтернет-конф. з міжн. участю, 27 жовтня 2022 р. Полтава : ПДАУ, 2022. С. 121-122.

26. Кримчак Л. А. Інформаційне забезпечення управління економічною безпекою зовнішньоекономічної діяльності вітчизняних підприємств. *Вісник Хмельницького національного університету. Економічні науки*. 2018. № 6(1). С. 274-276.

27. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник. К. : КНТ, 2006. 280 с.

28. Лосєв І. Інформаційна безпека: як укріпити. *День*. 2014. С. 19.

29. Маракова І.І., Сиропятов О.А. Інформаційна безпека комплексних систем зв'язку.*Ukrainian Information Security Research Journal*. 2006. Т.8, № 4.

30. Маркіна І.А., Дячков Д.В. Основи формування системи менеджменту інформаційної безпеки підприємства. *Проблеми і перспективи розвитку підприємництва*. 2016. № 3(1). С. 80-88.

31. Марущак А.І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. *Державна безпека України*. 2011. № 21. С. 92-95.

32. Медвідь В.Ю., Правдивець О.М., Кривчун Р.Ю. Теоретико-

методичні засади формування системи управління інформаційною безпекою підприємства. *Агросвіт*. 2022. № 24 (2022). https://www.nayka.com.ua/index.php/agrosvit/issue/archive.

33. Міронова Ю.В., Роїк О.М., Фіголь І.В. Управління інформаційною безпекою у плодоовочевих переробних підприємствах. *Економіка АПК*. 2015. № 2. С. 63-68.

34. Момот Т.В., Зубенко А.В., Вершиніна Д.М. Інформаційно-аналітичне забезпечення безпеко-орієнтованого управління підприємств будівельної галузі. *Вісник Хмельницького національного університету. Економічні науки*. 2021. № 1. С. 192-196.

35. Мужанова Т.М. Організаційне забезпечення інформаційної безпеки підприємства : основні засади. *Сучасний захист інформації*. 2016. № 2. С. 78-82.

36. Мужанова Т.М. Особливості менеджменту персоналу у системі управління інформаційною безпекою підприємства. *Економіка. Менеджмент. Бізнес*. 2015. № 3. С. 93-98.

37. Нестеренко О. Свобода інформації чи інформаційна безпека? *Свобода висловлювань і приватність*. 2011. № 1. С. 3-9.

38. Нехай В.А., Нехай В.В. Інформаційна безпека як складова економічної безпеки підприємств. *Науковий вісник Міжнародного гуманітарного університету* : зб. наук. пр. Одеса. Серія Економіка і менеджмент. 2017. №24(2). С. 137-140.

39. Обидєннова Т.С., Гусаров О.О., Антипцева О.Ю. Методи прийняття управлінських рішень в умовах розроблення, впровадження та функціонування системи менеджменту інформаційної безпеки. *Проблеми системного підходу в економіці*. 2019. Вип. 2 (70). С. 153-157.

40. Панченко В.А. Управління інформаційною безпекою держави та підприємств: правові та організаційні аспекти. *Актуальні проблеми правознавства*. 2020. Вип. 1. С. 103-109.

41. Потапенко О.К. Державна інформаційна політика та безпека. *Вісник*

Київського національного університету імені Тараса Шевченка. Філософія. Політологія. 2011. Вип. 102. С. 48-51.

42. Про електронні документи та електронний документообіг: Закон України : прийнятий ВРУ 22.05.2003 р. № 851–IV. Відомості Верховної Ради України. 2003 р. №44. С. 1175-1176.

43. Про основи національної безпеки України: Закон України від 19 червня 2003 року № 964-IV. Відомості Верховної Ради України. 2003. № 39. Ст. 351.

44. Про концепцію національної програми інформатизації: Закон України від 4 лютого 1998 року № 75/98-ВР. Відомості Верховної Ради України. 1998. № 27-28. Ст. 182.

45. Про національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-ВР. Відомості Верховної Ради України. 1998. № 27-28. Ст. 181.

46. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163 – VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19.

47. Русіна Ю.О., Острякова В.Ю. Удосконалення системи управління інформаційною безпекою на підприємстві. *Міжнародний науковий журнал «Інтернаука»*. 2017. № 14. С. 135-139.

48. Світлична В.Ю., Вершиніна Д.М. Організаційні аспекти реалізації інформаційно-аналітичного забезпечення безпекоорієнтованого управління будівельними підприємствами. *Комунальне господарство міст. Серія : Економічні науки*. 2019. Т. 7. С. 31-36.

49. Северина С.В. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету*. 2016. №1. С. 155-160.

50. Смачило Т.В., Кахній М.І. Теоретичні засади управління системою інформаційної безпеки підприємства. *Молодий вчений*. 2016. № 12.1. С. 969-972.

51. Солодка О. Окремі аспекти правового змісту поняття

«інформаційна безпека». *Часопис Київського університету права*. 2008. № 1. С. 89-93.

52. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи. *Вісн. Хмельниц. нац. ун-ту. Сер.: Екон. науки*. 2010. № 2. Т. 2. С. 32-35.

53. Степанов В. Інформаційна безпека в умовах реалізації інформаційної політики. *Вісник Національної академії державного управління при Президентові України*. 2019. № 4. С. 71-76.

54. Трахтенгерц Е.О. Комп'ютерні системи підтримки прийняття управлінських рішень. *Проблеми управління*. К. : Інститут космічних досліджень НАН та НКА України, 2013. №1. С. 13 -27.

55. Ушатов В., Сєвєрінов О. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки. *Global Cyber Security Forum* : матеріали I міжнародного науково-практичного форуму, 14-16 листопада 2019 р. Харків : ХНУРЕ, 2019. С. 104-105.

56. Федулова С.О. Інформаційна безпека та захист інтелектуальної власності на бази даних. *Економічний вісник ДВНЗ «Український державний хіміко-технологічний університет»*. 2016. С. 189-193.

57. Філатова І.О. Інформаційно-аналітичне забезпечення клієнто-орієнтованого стратегічного управління в системі корпоративної безпеки підприємств будівельної галузі. *Сучасний стан наукових досліджень та технологій в промисловості*. 2018. № 2. С. 50-56.

58. Цвілій О.О. Безпека інформаційних технологій: сучасний стан стандартів ISO27k системи управління інформаційною безпекою. *Телекомунікаційні та інформаційні технології*. 2014. №2. С. 73.

59. Чередниченко А.О. Категорії інформаційної безпеки та категорії «інформаційної системи» в системі корпоративного управління підприємств будівельної галузі. *Вісник економіки транспорту і промисловості*. 2014. Вип. 45. С. 216-220.

60. Якименко Ю.М., Мужанова Т.М., Легомінова С.В. Системний

аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії FireEye. *Кібербезпека: освіта, наука, техніка*. 2021. № 4. С. 36-50.

61. Яснолоб І.О., Кривчун Р.Ю. Управління інформаційною безпекою у сучасному бізнес-середовищі. *Управління ресурсним забезпеченням господарської діяльності підприємств реального сектору економіки* : матер. VI Всеукр. наук.-практ. інтернет-конфер. з міжнародною участю, 17 листопада 2021 р. Полтава : ПДАУ, 2021. С. 266-268.

62. Alberts C.J., Behrens S.G., Pethia R.D., Wilson W.R. Operationally critical threat, asset and vulnerability evaluation, 1999. 84 p

63. Zhang R., Cai L., Pan J. Resource Management for Multimedia Services in High Data Rate Wireless Networks. *Springer International Publishing AG*, Cham, Switzerland, 2017. 140 p.