ЗАТВЕРДЖЕНО

Наказ Вищого навчального закладу Укоопспілки «Полтавський університет економіки і торгівлі» 08 липня 2015 року № 152-Н

Форма № П-4.04

ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД УКООПСПІЛКИ
«ПОЛТАВСЬКИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТОРГІВЛІ»

Навчально-науковий інститут заочно-дистанційного навчання

Форма навчання заочна

Кафедра економічної кібернетики, бізнес-економіки та інформаційних систем

Допускається до захисту
Завідувач кафедри д.е.н., проф.
_____М.Є. Рогоза
(підпис, ініціали та прізвище)

«_____»_____ 2020 р.

ДИПЛОМНА РОБОТА

на тему:

«Моделювання інформаційної безпеки підприємства»
(за матеріалами ТОВ «Нова Пошта»)

(повна назва підприємства)

зі спеціальності 051 Економіка
освітня програма «Економічна кібернетика»

Виконавець роботи Кропивка Ольга Григорівна
(прізвище, ім'я, по батькові)

_____
(підпис, дата)

Науковий керівник доцент, к.е.н. Кузьменко Олександра Костянтинівна
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

_____
(підпис, дата)

Полтава 2021

ЗАТВЕРДЖЕНО
Наказ Вищого навчального закладу Укоопспілки «Полтавський університет економіки і торгівлі»
08 липня 2015 року № 152-Н

Форма № П-4.03

ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД УКООПСПІЛКИ
«ПОЛТАВСЬКИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТОРГІВЛІ»

ЗАТВЕРДЖУЮ:
Завідувач кафедри
_____М.Є. Рогоза
(підпис, ініціали та прізвище)
«_____» _____ 2019 р.

ЗАВДАННЯ ТА КАЛЕНДАРНИЙ ГРАФІК
ВИКОНАННЯ ДИПЛОМНОЇ РОБОТИ

на тему «Моделювання інформаційної безпеки підприємства»
Студентом спеціальності 051 Економіка, *освітня програма* «Економічна кібернетика»
Прізвище, ім'я, по батькові Кропивка Ольга Григорівна
Затверджена наказом ректора № 257-Н від „19" грудня 2019 року

Зміст роботи	Термін виконання	Фактичне виконання
1. Підбір і вивчення літературних джерел	до 25.12.2019 р.	виконано
2. Складання і затвердження розгорнутого плану роботи	до 15.01.2020 р.	виконано
Написання розділу 1. «Теоретичні положення щодо забезпечення інформаційної безпеки підприємства»	до 01.03.2020 р.	виконано
3. Збір і обробка інформації, необхідної для виконання роботи	до 01.04.2020 р.	виконано
Написання розділу 2. «Аналіз діяльності ТОВ «Нова Пошта»	до 30.06.2020 р	виконано
Написання розділу 3. «Моделювання інформаційної безпеки»	до 15.10.2010 р.	виконано
4. Розробка та обґрунтування пропозицій	до 20.10.2020 р.	виконано
5. Оформлення тексту роботи	до 05.11.2020 р.	виконано
6. Подання роботи науковому керівнику	до 10.12.2020 р.	виконано
7. Доопрацювання роботи з урахуванням зауважень і пропозицій	до 25.01.2021 р.	виконано
8. Подання роботи на кафедру	до 07.02.2021 р.	виконано

Дата видачі завдання «20» грудня 2019 р.
Студент(ка) _____
(підпис)
Науковий керівник _____ к.е.н., доцент Кузьменко О.К.
(підпис) (науковий ступінь, вчене звання, ініціали та прізвище)

Результати захисту дипломної роботи
Дипломна робота (проект)
оцінена на _____
(балів, оцінка за національною шкалою, оцінка за ECTS)
Протокол засідання ЕК № ____ від «____» _____ 2020 р.
Секретар ЕК_____ _____
(підпис) (ініціали та прізвище)

Зміст

Вступ

У сучасному суспільстві інформація стала одним із найважливіших стратегічних ресурсів, що забезпечує подальший розвиток підприємства. Саме тому інформація, як і решта ресурсів, потребує особливого захисту. Проблема інформаційної безпеки набула особливого значення в сучасних умовах широкого застосування автоматизованих інформаційних систем. У зв'язку із зростаючою роллю інформаційних ресурсів у житті сучасного суспільства, а також через реальність численних загроз проблема інформаційної безпеки вимагає до себе постійної і значної уваги. Системний характер впливу на інформаційну безпеку великої сукупності різних обставин, які мають до того ж різну фізичну природу, що переслідують різні цілі і викликають різні наслідки, приводять до необхідності комплексного підходу при вирішенні цієї проблеми.

Загалом інформація пронизує всі сфери життя суспільства, створюючи нову основу розвитку економіки, культури і взагалі нову характеристику соціуму. Вивченням питання інформаційної безпеки займалися такі вчені, як С. Ф. Гуцу [13], Б. А. Кормич [26], А. І. Марущак [32], О. А. Сороківська [46].

Проте проблема інформаційної безпеки підприємства залишається недостатньо дослідженою. Це пов'язано з тим, що автори значну увагу приділяють забезпеченню інформаційної безпеки держави, а також з відсутністю цілеспрямованого підходу до проблеми в цілому у тих учених, які розглядали роль інформації в діяльності підприємства.

Метою роботи є обґрунтування концептуальних засад та розробка практичних рекомендацій щодо моделювання системи інформаційної безпеки підприємства. Тому, у роботі поставлено і вирішено такі завдання:

охарактеризувати основні положення інформаційної безпеки;

дослідити технологію забезпечення інформаційної безпеки підприємства;

розглянути основні моделі інформаційної безпеки;

виконати загальну характеристику та фінансовий аналіз результатів

діяльності ТОВ «Нова Пошта»;

виконати аналіз ризиків інформаційної безпеки на ТОВ «Нова пошта»;

запропонувати методичні рекомендації щодо оцінювання стану інформаційної безпеки підприємства;

змоделювати процеси системи захисту інформації ТОВ «Нова Пошта» на основі теорії графів і методології IDF0.

Об'єкт дослідження – процес забезпечення інформаційної безпеки на ТОВ «Нова Пошта».

Предмет дослідження – моделі та методики дослідження системи інформаційної безпеки підприємства.

Методи дослідження. У роботі використано наукові праці вітчизняних і зарубіжних учених, де відображені фундаментальні положення щодо безпеки, системи інформаційної безпеки підприємства. Теоретико-методологічною базою дослідження є загальнонаукові та спеціальні методи пізнання. Для досягнення мети та виконання завдань були використані такі методи та підходи: системний підхід – до оцінювання стану господарської діяльності суб'єкта господарювання; процесно-функціональний – для моделювання процесів системи забезпечення інформаційною безпекою підприємства; методи аналізу, синтезу, індукції, дедукції, узагальнення – для обґрунтування сутності теоретичних понять, графічний – для відображення стану розвитку підприємства та фінансового аналізу діяльності ТОВ «Нова Пошта».

Інформаційною базою дослідження є законодавчі та нормативні акти, що регулюють умови діяльності галузі зв'язку, офіційні статистичні матеріали Державної служби статистики України, інформаційні джерела урядових інституцій, наукові праці закордонних і вітчизняних вчених, які досліджували проблеми інформаційної безпеки на підприємствах, матеріали вибіркових досліджень та соціологічних опитувань, Інтернет – ресурси та результати особистих досліджень автора.

Практичне значення одержаних результатів полягає у розробці системи

захисту інформації на підприємстві. Основні наукові положення дипломної роботи подано у вигляді рекомендацій, які можна використовувати на практиці.

Результати дослідження схвалено та прийнято до впровадження у Вищому навчальному закладі Укоопспілки «Полтавський університет економіки і торгівлі».

Дипломна робота є самостійно виконаним завершеним науковим дослідженням. Наукові результати, які представлено в дипломній роботі, та ті, що оприлюднені у наукових виданнях, отримані автором самостійно.

Дипломна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, що налічує 55 найменувань, додаток. Обсяг основного тексту роботи становить 91 сторінок.

Розділ 1. Теоретичні положення щодо забезпечення інформаційної безпеки підприємства

1.1. Основні положення інформаційної безпеки

Сьогодні інформація перестала бути лише технічною категорією. Впровадження та розповсюдження новітніх технологій посприяло тому, що інформація перетворилася на економічну категорію, стала одним з найважливіших елементів ринку та фактором, що регулює рівень розвитку не тільки виробництв, а й економіки загалом, адже переважна більшість економічних зв’язків набувають форми обміну інформацією. У ринковій економіці інформація стає товаром і її отримання, збереження, передача та використання повинні підпорядковуватися законам товарно-грошових відносин, тобто інформація стає об'єктом та інструментом управління. Інформаційні впливи можуть спричиняти результат не відразу, а через тривалий час. Визначальним фактором життєдіяльності сучасного суспільства стає глобалізація інформаційних ресурсів. Тому важливими на цей час є питання, що належать до інформаційної сфери та їх впливи на економіку. А отже виникає необхідність забезпечення та регулювання інформаційної безпеки різних сфер діяльності [36, с. 63].

В основному, інформаційну безпеку визначають як різновид соціальної діяльності, який полягає в створенні державними і недержавними інституціями необхідних умов для розвитку національних інтересів в інформаційній сфері [36, с. 63].

Об’єктами інформаційної безпеки можуть бути: свідомість, психіка людей; інформаційні системи різного масштабу і різного призначення. До соціальних об'єктів інформаційної безпеки звичайно відносять особистість, колектив, суспільство, державу, світове товариство [40].

На рисунку 1.1 наведено види безпеки та рівні на яких здійснюється управління інформаційною безпекою.

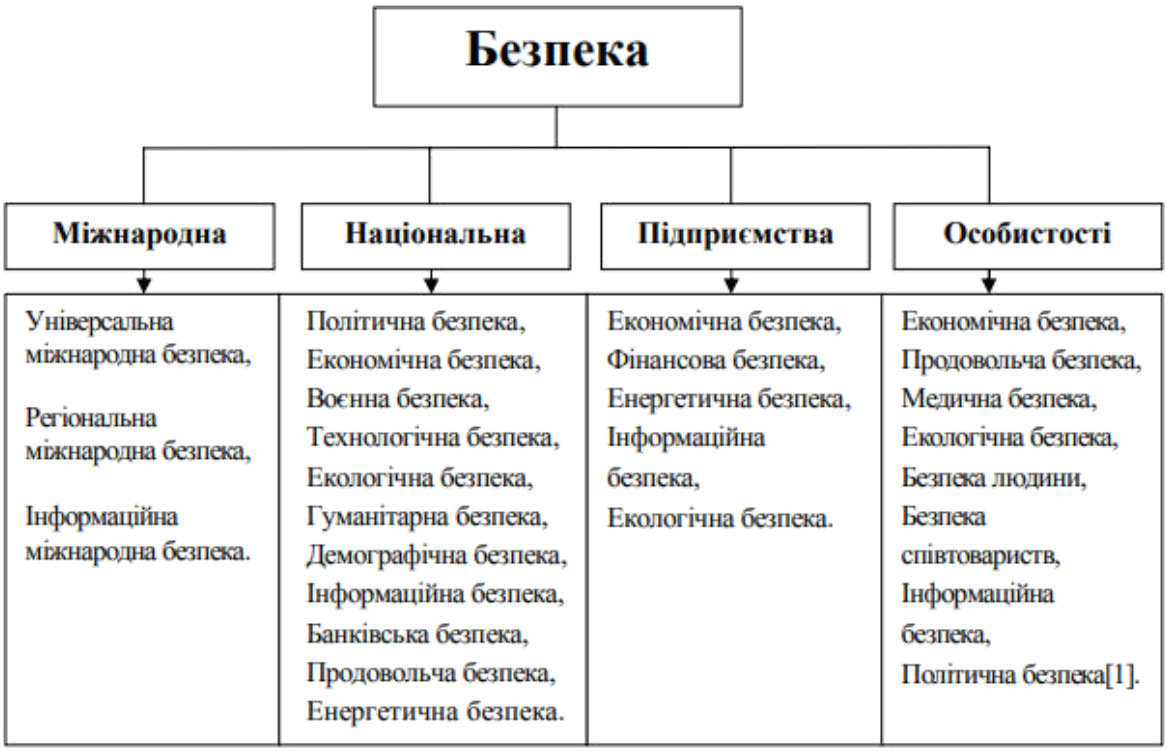


Рисунок 1.1 – Види безпеки [36, с. 63].

Міжнародна інформаційна безпека – характеризується, як взаємодія учасників міжнародних відносин для підтримання тривалого миру на основі захисту світового кіберпростору разом із засобами масової інформації, глобальної інфраструктури та суспільної свідомості від реальних інформаційних загроз [22].

Інформаційна безпека, як складова національної безпеки – стан захищеності життєво-важливих інтересів людини, суспільства і держави, коли запобігається нанесення шкоди через:

неповноту, невчасність та невірогідність інформації, що використовується;

негативний інформаційний вплив;

негативні наслідки застосування інформаційних технологій;

несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [45].

Інформаційна безпека, як складова безпеки підприємства – діяльність керівництва підприємства з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує нормальне функціонування та розвиток підприємства [45].

Інформаційна безпека, як складова особистої безпеки особи – характеризується як стан захищеності особистості, соціальних груп та об'єднань людей від впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору [45].

Відповідно до умов функціонування у динамічному ринковому середовищі, інформаційна безпека підприємства представляє собою характеристику стану джерел інформації що гарантує певний рівень інформаційно-аналітичного забезпечення, який базується на захисті інформаційного середовища і обумовлює отримання ефективного та результативного інформаційного продукту [15, с. 159].

У науковій літературі відсутній єдиний погляд на зміст поняття «інформаційна безпека» та «інформаційна безпека підприємства» [17, 157–158]:

Цимбалюк В. характеризує інформаційну безпеку як стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації [52, с. 3].

Фурашев В. вважає, що інформаційна безпека – це вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності [50; 14, с. 48].

Гуцу С. пропонує розглядати інформаційну безпеку як стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [14, с. 35].

Литвиненко О. під інформаційною безпекою розуміє єдність трьох складових: забезпечення захисту інформації; захисту та контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності [31, с. 9].

Цікавим та водночас дискусійним є визначення Кормича Б., який зазначає, що інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією України умови існування і розвитку людини, всього суспільства та держави [25, с. 241].

Харченко Л., Ліпкан В., Логінов О. визначили, що інформаційна безпека – це складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України [51, с. 32].

Таким чином, інформаційну безпеку слід розглядати як забезпечення реалізації національних інтересів за допомогою різних засобів, що є в її розпорядженні.

До основних функціональних цілей економічної безпеки належать:

- забезпечення високої фінансової ефективності роботи, фінансової стійкості та незалежності підприємства;

- забезпечення технологічної незалежності та досягнення високої конкурентоспроможності технічного потенціалу того чи іншого суб'єкта господарювання;

- досягнення високої ефективності менеджменту, оптимальної та ефективної організаційної структури управління підприємством;

- досягнення високого рівня кваліфікації персоналу та його інтелектуального потенціалу, належної ефективності корпоративних НДДКР;

- мінімізація руйнівного впливу результатів виробничо-господарської діяльності на стан навколишнього середовища;

- якісна правова захищеність усіх аспектів діяльності підприємства;

- забезпечення захисту інформаційного поля, комерційної таємниці і досягнення необхідного рівня інформаційного забезпечення роботи всіх підрозділів підприємства та відділів організації;

- ефективна організація безпеки персоналу підприємства, його капіталу та майна, а також комерційних інтересів.

Головна та функціональні цілі зумовлюють формування необхідних структуроутворюючих елементів і загальної схеми організації економічної безпеки.

Загальна схема процесу організації економічної безпеки включає такі дії (заходи), що здійснюються послідовно або одночасно:

а) формування необхідних корпоративних ресурсів (капіталу, персоналу, прав інформації, технології та устаткування);

б) загальностратегічне прогнозування та планування економічної безпеки за функціональними складовими;

в) стратегічне планування фінансово-господарської діяльності підприємства;

г) загально-тактичне планування економічної безпеки за функціональними складовими;

д) тактичне планування фінансово-господарської діяльності підприємства;

е) оперативне управління фінансово-господарською діяльністю підприємства;

ж) здійснення функціонального аналізу рівня економічної безпеки;

з) загальна оцінка досягнутого рівня економічної безпеки.

Тільки здійснення в необхідному обсязі зазначених дій (заходів) можна буде досягти належного рівня економічної безпеки підприємства.

Щодо поняття «інформаційна безпека підприємства» необхідно зазначити, що воно є надзвичайно актуальним на сучасному етапі розвитку інформаційних технологій, який супроводжується введенням інформаційних

систем у всі сфери діяльності людини, постійною взаємодією підприємств на теренах саме інформаційного простору [17, с. 158–159].

Сороківська О. визначає інформаційну безпеку підприємства як суспільні відносини щодо створення і підтримки на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [47].

Танцюра М. характеризує інформаційну безпеку підприємства як збереження конфіденційності, цілісності та доступності інформації: доступність – це властивість бути досяжним та придатним до використання авторизованими сутностями; цілісність – це властивість захищеності точності та повноти даних; конфіденційний – це властивість захищеності інформації від неавторизованого використання фізичними особами, сутностями та процесами. Інформаційні активи – це знання чи дані, які мають цінність для організації [48, с. 452].

Марущак А. визначає інформаційну безпеку підприємства як цілеспрямовану діяльність його органів та посадових осіб з використанням дозволених сил і засобів щодо досягнення стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток [33, с. 94].

Отже, зміст інформаційної безпеки ґрунтується на двох її аспектах:

1. Інформаційна безпека – це стан захищеності інформаційного середовища.

2. Забезпечення захисту інформації – це діяльність, яка спрямована на запобігання витоку інформації, що захищається, недопущення несанкціонованих і ненавмисних дій на неї.

Існує декілька підходів до визначення поняття «інформаційна безпека підприємства»:

1) полягає в здійсненні цілеспрямованої діяльності органів управління та посадових осіб підприємства з використанням дозволених сил і засобів по

досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток [8];

2) заснований на виділенні системних параметрів і функціонального блоку. «Інформаційна безпека – захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин» [10]. Системними параметрами виступають сама інформація і інфраструктура, під якою слід розуміти всі системи забезпечення, починаючи від електропостачання, закінчуючи обслуговуючим персоналом. Функціональний блок – це загрози інформаційній системі і збиток, яким не можна нехтувати внаслідок порушення стану інформаційної безпеки.

Тобто, інформаційна безпека, виступаючи в якості однієї з основ економічної безпеки компанії, і питання, пов'язані з її забезпеченням, представляють сьогодні один з життєво-необхідних аспектів ведення успішної підприємницької діяльності в умовах агресивної ринкової економіки. Говорячи про агресивність сучасної економічної системи, слід враховувати процеси перетворення структури активів підприємств у бік переважання інформаційних активів над матеріальним капіталом.

Відповідно до цих тенденцій в компаніях розвиваються і ускладнюються інформаційні системи і системи комунікацій. Їх основним завданням є забезпечення таких умов для економічної діяльності підприємства, в яких досягається максимальна ефективність всіх внутрішніх процесів в умовах динамічного навколишнього середовища підприємства та активної конкурентної боротьби. Забезпечення інформаційної безпеки в цілому веде до значної економії витрат, коштів і ресурсів підприємства, тоді як збиток, що наноситься внаслідок навмисних дій і ненавмисних помилок, призводить до значних матеріальних втрат. Наприклад, розкриття особливих умов технологічних процесів призводить до появи аналогічних продуктів у конкурентів, в результаті такого порушення інформаційної безпеки

підприємство втрачає частину ринку, відповідно падає виручка і знижується прибуток. Якщо ж інформаційні активи є ключовим фактором конкурентоспроможності підприємства, то порушення інформаційної безпеки веде до катастрофічних наслідків для підприємства [35].

Специфіка забезпечення інформаційної безпеки підприємства проявляється в трьох базових ознаках [35]:

Конфіденційність інформації – властивість інформаційних ресурсів, в тому числі інформації, пов'язане з тим, що вони не стануть доступними і не будуть розкриті для неуповноважених осіб.

Цілісність інформації – незмінність інформації в процесі її передачі або зберігання.

Доступність інформації – властивість інформаційних ресурсів, в тому числі інформації, що визначає можливість їх отримання і використання на вимогу уповноважених осіб.

Функціональні ознаки забезпечення інформаційної безпеки підприємства полягають у формуванні таких умов:

1. Суворе виконання зобов'язань: підтвердження всіх дій, вчинених в інформаційній системі, і подій, запропонованих до вчинення, таким чином, що ці дії і події не можуть бути пізніше скасовані, за винятком випадків, передбачених регламентом.

2. Реалізація підзвітності та ідентифікації: забезпечення однозначної ідентифікації всіх суб'єктів інформаційної системи і користувачів інформації, що мають певні права доступу до неї, і реєстрації всіх скоєних дій, пов'язаних з отриманням і обробкою інформації.

3. Досягнення достовірності: підтвердження відповідності здійснюваних операцій регламентованими діями і результатами.

4. Забезпечення достовірності: формування умов, що гарантують фактичну ідентичність інформаційних ресурсів заявленим параметрам.

При цьому, способи і засоби забезпечення інформаційної безпеки зводяться до трьох сфер: апаратне забезпечення, програмне забезпечення,

канали комунікації. Безпосередні процедури і механізми захисту інформації розподілені між захистом фізичного рівня, персональний захист і організаційний захист.

Таким чином, концепція інформаційної безпеки може бути представлена у вигляді структурної схеми, що відбиває її базові та функціональні ознаки, способи і засоби забезпечення інформаційної безпеки, процедури і механізми захисту інформації. Концепція інформаційної безпеки відображена у вигляді схеми на рисунку 1.2.

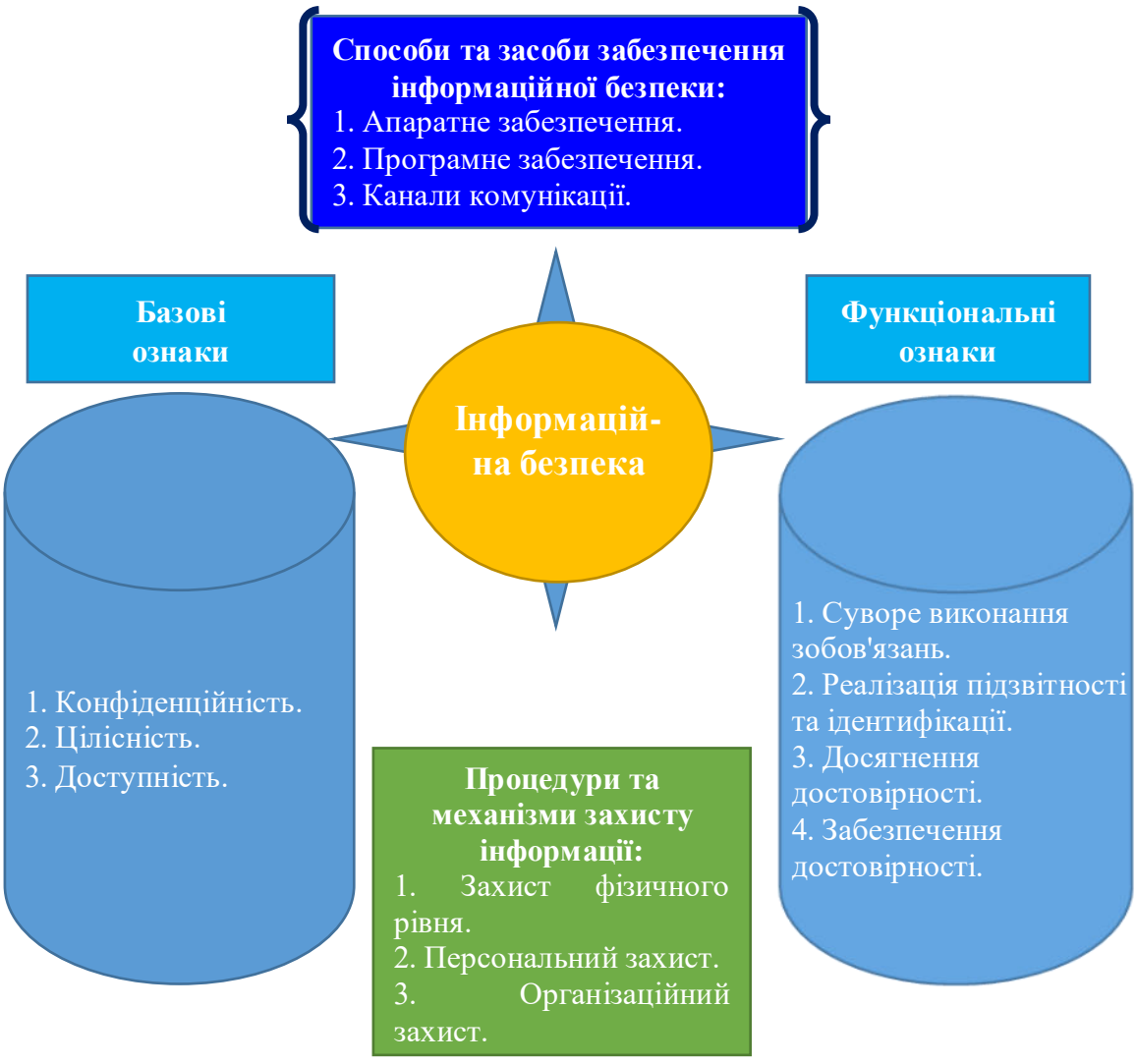


Рисунок 1.2 – Концепція інформаційної безпеки

Оскільки, зараз підприємства активно впроваджують інформаційні технології в свою діяльність, забезпечення інформаційної безпеки стає

вельми актуальним питанням для підприємств, в інтересах яких мінімізувати загрози інформаційній безпеці.

Об'єктивною умовою виникнення поняття інформаційної безпеки є поява загроз нанесення шкоди майновим і іншим інтересам в результаті впливу безпосередньо на інформацію або на засоби комунікації, за якими вона передається. В даний час розвиток інформаційних технологій призвело до появи широкої різноманітності як засобів обробки і передачі даних, так і можливостей їх розкрадання і використання в корисливих цілях. Внаслідок цього компанії повинні забезпечувати захист власної інформації для запобігання промислового шпигунства і нанесення іншої шкоди своїм інтересам, мінімізуючи потенційні і усуваючи існуючі загрози своєї інформаційної безпеки [35].

Відповідно до концепції забезпечення інформаційної безпеки підприємства тільки виявлення і контроль повного спектру загроз дозволяє побудувати ефективну систему захисту інформації.

По відношенню до інформаційної системі підприємства, загрози інформаційної безпеки можуть бути внутрішніми або зовнішніми. Внутрішні представляють собою порушення регламенту підприємства щодо використання інформаційних ресурсів підприємства, використання даних компанії в особистих цілях, занесення співробітниками вірусу в інформаційну мережу, розкрадання конфіденційних даних. Зовнішні загрози є наслідком дій суб'єктів, що не мають відношення до компанії, найбільш типовими прикладами є хакерська атака на інформаційну систему і саботаж підтримуючої інфраструктури.

За мотивацією загрози поділяють на навмисні і ненавмисні. До ненавмисних загроз відносять факти випадкового видалення даних персоналом, форс-мажорні обставини, пов'язані з роботою інформаційної системи, стихійні лиха, що ведуть до поломки апаратного забезпечення. Навмисні загрози мають на меті нанесення відчутного збитку підприємству, а

суб'єкти, що здійснюють такі дії, слідують чітким планам щодо подолання можливого захисту.

Залежно від мети загрози виділяють дії, спрямовані на отримання даних, знищення даних, зміна даних, порушення роботи програмного забезпечення, контроль над роботою програмного забезпечення та інші. Найбільше значення мають загрози, спрямовані на отримання закритих, конфіденційних даних підприємства для подальшого їх використання в нелегальних цілях, наприклад, розкрадання даних з комерційних контрактів, патентів, винаходів або розробок з метою їх подальшого перепродажу конкурентам.

Функціональна класифікація загроз інформаційній безпеці оперує чотирма критеріями (табл. 1.1).

Таблиця 1.1

Функціональні загрози інформаційної безпеки [35]

№	Критерій інформаційної безпеки	Загрози інформаційної безпеки
1	2	3
1.	Загальна інформаційна безпека	За базовим ознаками доступності, цілісності, конфіденційності, проти яких загрози спрямовані в першу чергу.
2.	Компоненти інформаційних систем	На ці компоненти безпосередньо спрямовані загрози: дані, програми, апаратура, що підтримує інфраструктуру.
3.	Спосіб здійснення	Випадкові / навмисні дії / загрози. Дії / загрози природного / техногенного характеру.
4.	Розташування джерела загроз	Усередині інформаційної системи або поза нею.

З огляду на багатогранність сучасних інформаційних систем, можна погодитися з твердженням, що «нельзя защититься от всех мыслимых и немыслимых угроз информационной безопасности хотя бы потому, что невозможно предусмотреть действия злоумышленников, не говоря уж обо всех ошибках пользователей» [34]. Формуючи інформаційну систему і виконуючи конкретні кроки, спрямовані на попередження загроз інформаційній безпеці, необхідно опрацьовувати заходи прямого захисту від відомих загроз і забезпечувати можливість оперативного реагування на ті

загрози, для яких заходи захисту не передбачені базовим регламентом. Для обох випадків існує ряд загальних методів захисту, які забезпечують зниження шкоди, що завдається інформаційній системі внаслідок порушення інформаційної безпеки, дозволяють знизити ймовірність реалізації максимального широкого спектру загроз і убезпечити підприємство від різних зовнішніх атак і помилок внутрішніх користувачів. Відповідно до концепції інформаційної безпеки вони поділяються на апаратні, програмні та комунікаційні.

Отже, сьогодні спостерігається критично високе значення інформаційних активів підприємств в контексті їх переважаючого значення по відношенню до вартості матеріальних ресурсів організації. З огляду на рівень сучасного розвитку інформаційних технологій, питання забезпечення захисту інформації стають однією з фундаментальних детермінант економічної безпеки підприємства. Інформаційна безпека виступає єдиним можливим напрямком для попередження нанесення збитків економічним інтересам підприємства шляхом організації захисту від існуючих і потенційних загроз інформаційних ресурсів підприємства.

1.2. Технологія забезпечення інформаційної безпеки підприємства

На сучасному етапі традиційні ресурси втрачають своє першорядне значення. Інформація постає головним ресурсом і товаром науково-технічного та соціально-економічного розвитку світового співтовариства. Інформація не тільки впливає на прискорення розвитку науки, техніки та різних галузей народного господарства, а й відіграє значну роль в процесах забезпечення охорони, збереження власності, спілкування тощо. Водночас, застосування технологій обробки інформаційних ресурсів потребує підвищеної уваги до питань інформаційної безпеки. Руйнування інформаційного ресурсу, його тимчасова недоступність або несанкціоноване

використання можуть завдати значних матеріальних збитків. Без належного ступеня захисту інформації впровадження інформаційних технологій може виявитися економічно невигідним в результаті значних втрат конфіденційних даних, що зберігаються і обробляються в комп'ютерних мережах. Тому проблема забезпечення інформаційної безпеки діяльності підприємства є актуальною [15, с. 158–159].

Враховуючи різні погляди на проблематику формування технології забезпечення інформаційної безпеки, науковці визначили основні аспекти для її ефективного впровадження та застосування, які полягають у [2, 3, 4, 9, 23, 55]:

розмежуванні доступу до робочих місць, як адміністративними заходами (розмежування доступу в приміщення), так і з використанням різних систем захисту від несанкціонованого доступу;

виділенні на підприємстві посадової особи (адміністратора з безпеки), відповідальної за функціонування систем захисту інформаційних ресурсів;

розробці та контролі практичного здійснення заходів щодо забезпечення безпечного функціонування систем захисту;

періодичному контролі цілісності систем захисту і дотримання режиму охорони приміщень, в яких розташовані системи захисту;

періодичному контролі журналів операцій, автоматично створюваних програмними модулями, що входять в системи захисту;

зберіганні резервних копій ключових носіїв всіх операторів, що працюють в системах захисту;

запобіганні отримання зловмисниками ключових носіїв і їх тиражування власниками;

можливості довести неправомірні дії користувачів і обслуговуючого персоналу інформаційної системи;

захисті мережевої інфраструктури на основі виділеної локальної мережі або на основі віртуальної приватної мережі;

захисті серверів, автоматизованих робочих місць та телекомунікаційного обладнання інформаційних систем від

несанкціонованого доступу до їх ресурсів, шкідливого програмного забезпечення і мережевих атак, здійснюваних із зовнішніх мереж;

застосуванні засобів і систем захисту, які мають дозвільні сертифікати.

Очевидно, що впровадження ефективної технології забезпечення інформаційної безпеки на підприємстві призводить до поліпшення контролю за використанням різних видів ресурсів, підвищення загального рівня безпеки та структурування інформаційних ресурсів.

При цьому, під системою безпеки розуміють організовану сукупність спеціальних органів, служб, засобів, методів і заходів, що забезпечують захист життєво-важливих інтересів особистості, підприємства і держави від внутрішніх і зовнішніх загроз (рис. 1.3) [27].

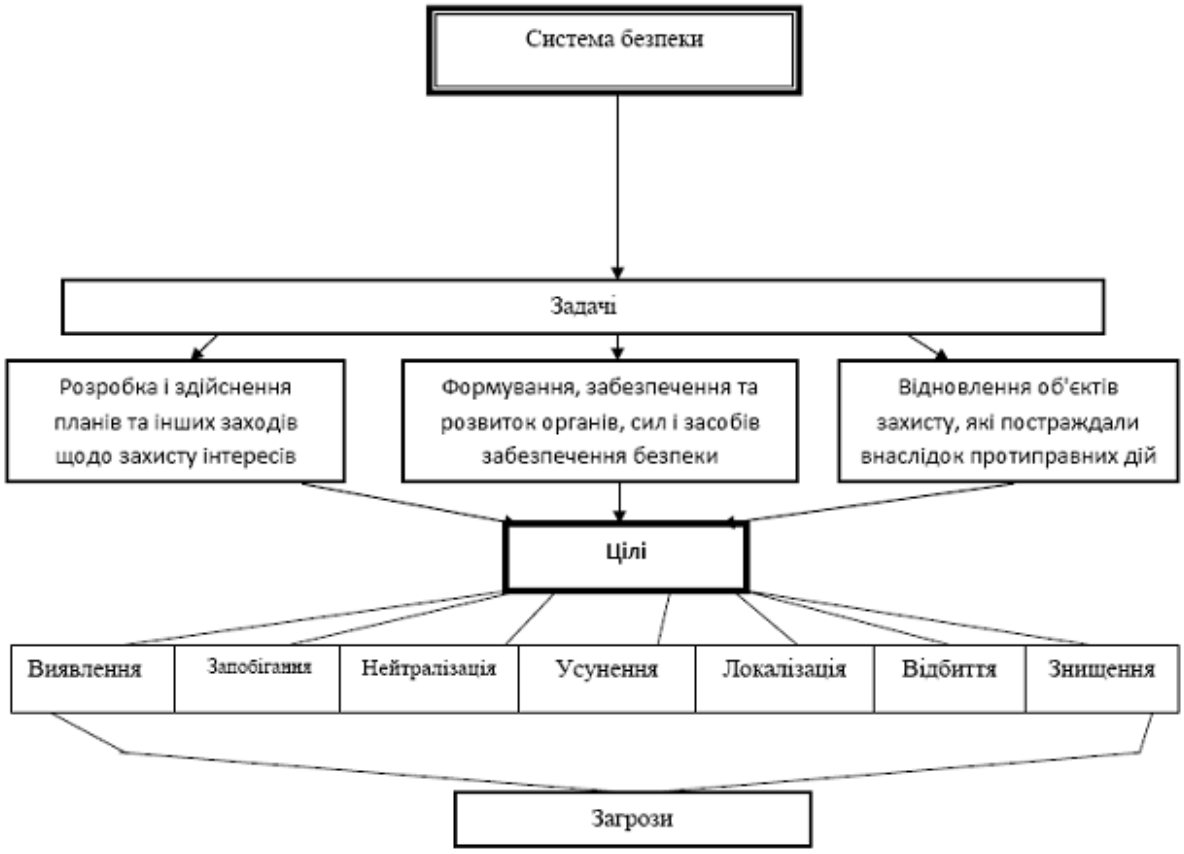


Рисунок 1.3 – Функціональна система інформаційної безпеки [53]

Отже, якщо розуміти інформаційну безпеку як «стан захищеності інформаційного середовища суспільства, що забезпечує її формування,

використання і розвиток в інтересах громадян, організацій» [21], тоді під загрозою – «сукупність факторів та умов, що виникають в процесі взаємодії об'єкта безпеки з іншими об'єктами, а також складових його компонентів між собою і здатних чинити на нього негативний вплив» [53]. Тобто, вона виступає в якості можливості вирішення протиріччя у взаємодії об'єкта безпеки з іншими об'єктами, компонентів об'єкта безпеки, що у стадії дисгармонії чи конфлікту, шляхом насильницької зміни в бік погіршення властивостей об'єкта безпеки, або його компонентів, тобто шляхом нанесення шкоди.

При цьому, між загрозою і небезпекою нанесення шкоди завжди існують відносини заподіяння, які визначаються як обумовлена сутністю взаємодіючих об'єктів, елементів системи, зв'язок між явищами, при якій одне явище, зване причиною, за наявності певних умов неминуче породжує, викликає інше явище, зване слідством. Загроза завжди породжує небезпеку. Небезпека може бути визначена як стан, в якому знаходиться об'єкт безпеки внаслідок появи загрози. Відмінність між ними полягає в тому, що небезпека є властивістю об'єкта безпеки, а загроза – властивістю об'єкта взаємодії або знаходяться у взаємодії елементів об'єкта безпеки, виступаючих як джерело загроз. Загроза знаходиться у відношенні заподіяння не тільки з небезпекою, але і з очікуваною шкодою – наслідками негативної зміни умов існування, які необхідно подолати для відновлення необхідних умов – в тому сенсі, що очікувана шкода визначає величину небезпеки [53].

Загрози інформаційній безпеці – це можливі дії або події, які можуть вести до порушень інформаційної безпеки [53]. Види загроз інформаційній безпеці дуже різноманітні і мають безліч класифікацій (рис. 1.4).

Відповідно до наведеної класифікації загроз за видом об'єкта впливу вони поділяються на загрози власне інформації, загрози персоналу об'єкта та загрози діяльності щодо забезпечення інформаційної безпеки об'єкта. При більш детальному розгляді загроз інформації, їх можна поділити на загрози носіям конфіденційної інформації, місцям їх розміщення (розташування), каналам

передачі (системам інформаційного обміну), а також інформації, що зберігається в документованому (електронному) вигляді на різних носіях. За характером порушення, як один із варіантів класифікації, зображено на рисунку 1.5.

Рисунок 1.4 – . Види загроз інформаційної безпеки [53]

Таким чином, встановлено, що дія загроз інформаційній безпеці об'єкта направлено на створення можливих каналів витоку інформації, що захищається (передумов до її витоку) і безпосередньо на витік інформації.

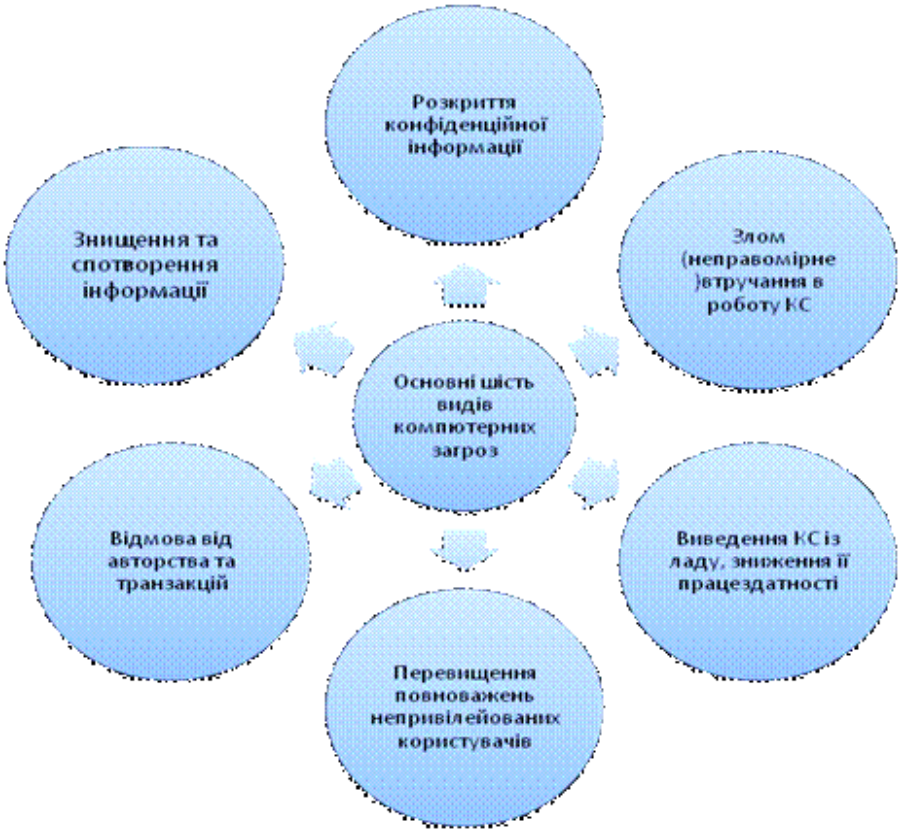


Рисунок 1.5 – Шість основних загроз інформаційній безпеці (класифікація за характером порушення) [53]

В загальному вигляді структура системи інформаційної безпеки підприємства включає засоби, підсистеми, програмну та технічну частини, автоматизовану систему обробки інформації, методи оцінки інформаційної захищеності підприємства (рис. 1.6).

Елементами цієї системи є: правовий, організаційний, інженерно-технічний захист інформації, а основною її характеристикою – комплексність. Структура системи, склад і зміст елементів, їх взаємозв’язок залежать від об’єму і цінності інформації, що захищається, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи. Технологію забезпечення інформаційної безпеки підприємства

можна представити як взаємодію складових: інформаційне забезпечення процесу управління на підприємстві; захист інформаційного середовища підприємства; діагностика рівня інформаційної безпеки [19].

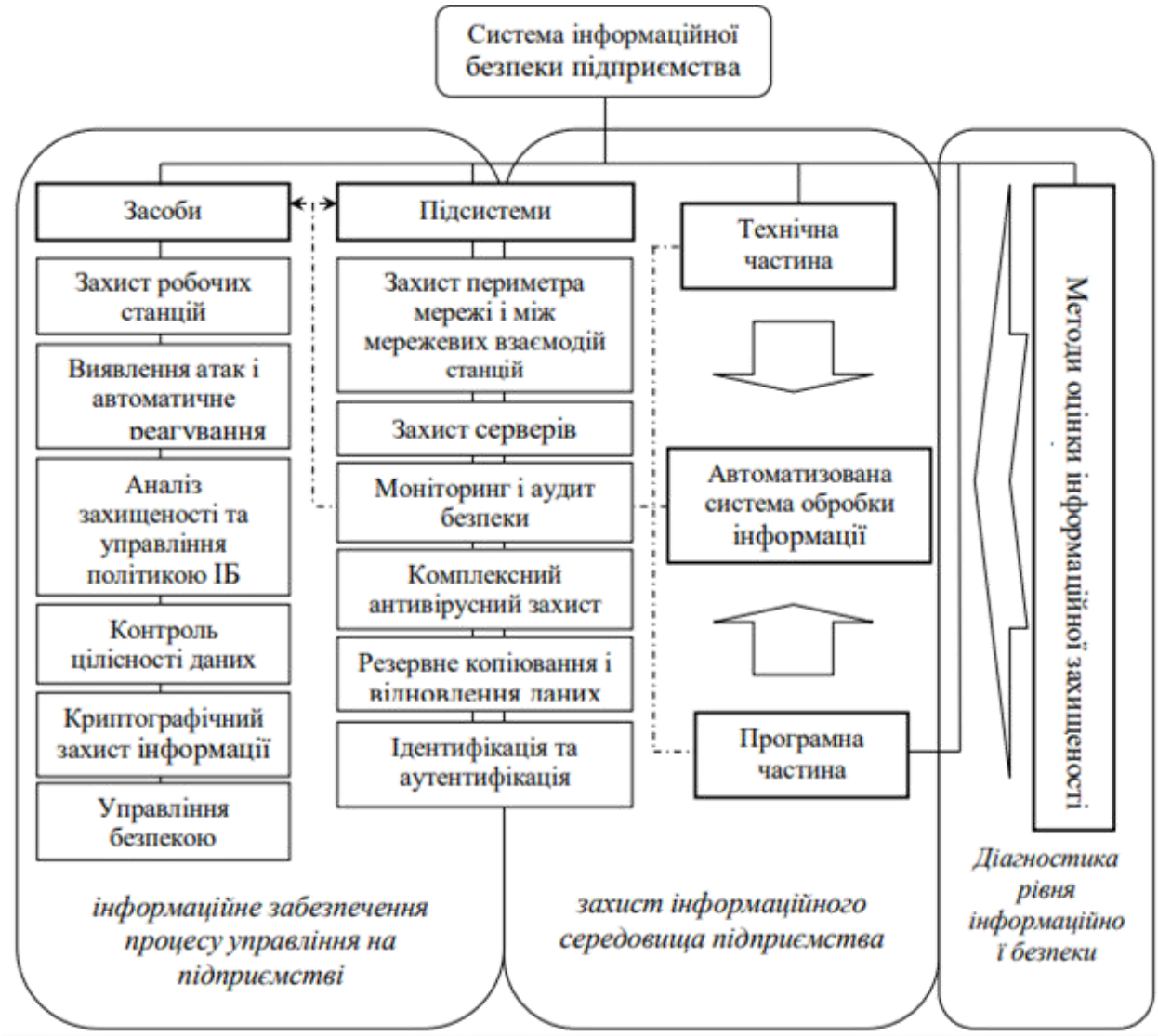


Рисунок 1.6 – Структура системи захисту інформаційної системи підприємства [1515, с. 160]

При побудові моделі системи інформаційної безпеки повинні враховувати взаємозв’язок між складовими. Наприклад, вихід з ладу будь-якого обладнання може призвести до втрати даних або виходу з ладу іншого критично важливого елемента системи. Подібні взаємозв’язки визначають основу технології побудови моделі організації з точки зору інформаційної безпеки.

Створення ефективної системи інформаційної безпеки є неможливим без чіткого визначення загроз інформації, що охороняється. Під загрозами інформації з обмеженим доступом прийнято розуміти потенційні або реально можливі дії стосовно інформаційних ресурсів, що призводять до неправомірного оволодіння інформацією [17, с. 159].

Джерелами зовнішніх загроз є: несумлінні конкуренти; злочинні угруповання і формування; окремі особи та організації адміністративно-управлінського апарату. Джерелами внутрішніх загроз можуть бути: адміністрація підприємства; персонал; технічні засоби забезпечення виробничої і трудової діяльності. Фахівці свідчать, що, в середньому, 82% загроз створюються співробітниками підприємства або за їх прямої або опосередкованої участі; 17% загроз виникає ззовні – зовнішні загрози; 1% загроз створюється випадковими особами [33].

Основними загрозами інформації є розголошення, витік і несанкціонований доступ до її джерел.

До формальних каналів поширення інформації належать [17]:

- ділові зустрічі, наради, переговори та інші форми спілкування;
- обмін офіційними діловими, науковими і технічними документами, засобами передачі офіційної інформації (пошта, телефон, телеграф, факс).

Неформальними каналами поширення інформації є [17]:

- особисте спілкування (зустрічі, переписка, телефонні переговори);
- виставки, семінари, конференції, з'їзди, колоквіуми та інші масові заходи;
- засоби масової інформації (преса, інтерв'ю, радіо, телебачення).

Як правило, причиною розголошення конфіденційної інформації є [17]:

- слабке знання (або незнання) вимог захисту конфіденційної інформації;
- помилковість дій персоналу через низьку виробничу кваліфікацію;

- відсутність системи контролю за оформленням документів, підготовкою виступів, реклами і публікацій;
- злісне, навмисне невиконання вимог захисту комерційної таємниці.

Попередження можливих загроз і протиправних дій може бути забезпечене всілякими засобами, починаючи від створення клімату глибоко усвідомленого відношення співробітників до проблеми безпеки і захисту інформації до створення глибокої, «ешелонованої» системи захисту фізичними, апаратними, програмними і криптографічними засобами. Попередження загроз можливе і шляхом одержання інформації про протиправні акти, які готуються, плановані розкрадання, підготовчі дії й інші елементи злочинних вчинків. У попередженні загроз важливу роль відіграє інформаційно-аналітична діяльність служби безпеки на основі глибокого аналізу криміногенного стану й діяльності конкурентів і зловмисників [17, 160].

Виявлення загроз – це дії з визначення конкретних загроз та їхніх джерел, які приносять той або інший вид збитку. До таких дій відносять виявлення фактів розкрадання або шахрайства, а також розголошення конфіденційної інформації або випадків несанкціонованого доступу до джерел комерційних секретів. Виявлення має на меті проведення заходів щодо збирання, нагромадження й аналітичного оброблення відомостей щодо можливої підготовки злочинних вчинків з боку кримінальних структур або конкурентів на ринку збуту [17, с. 160].

Припинення або локалізація загроз – це дії, спрямовані на усунення діючої загрози і конкретних злочинних вчинків. Ліквідація наслідків має на меті відновлення стану, що передував настанню загрози. Усі ці способи мають на меті захистити інформаційні ресурси від протиправних зазіхань і забезпечити [17, с. 160]:

запобігання розголошенню і витоку конфіденційної інформації;

заборону несанкціонованого доступу до джерел конфіденційної інформації;

збереження цілісності, повноти і доступності інформації;

дотримання конфіденційності інформації;

забезпечення авторських прав.

Найбільш загальними принципами захисту будь-якого виду інформації, що охороняється, є [17, с. 160]:

захист інформації організує і проводить власник інформації або уповноважені ним особи (юридичні або фізичні);

захистом інформації власник охороняє свої права на володіння і розпорядження інформацією, прагне захистити її від незаконного заволодіння і використання на шкоду його інтересам;

захист інформації здійснюється шляхом проведення комплексу заходів для обмеження доступу до захищеної інформації, що захищається, і створення умов, що виключають або суттєво ускладнюють несанкціонований, незаконний доступ до засекреченої інформації та її носіїв.

Отже, захист інформації – це діяльність власника інформації або уповноваженої ним особи з: забезпечення своїх прав на володіння, розпорядження і управління захищеною інформацією; запобігання витоку і втрати інформації; збереження повноти, вірогідності, цілісності захищеної інформації, її масивів і програм обробки; збереження конфіденційності або таємності захищеної інформації, відповідно до правил, установлених законодавчими й іншими нормативними актами [17, с. 160].

З цією метою, запропоновані рекомендації, які слід застосовувати при формуванні технології захисту інформаційної системи підприємства [15, с. 160–161]:

механізми захисту інформаційної системи повинні бути прості для технічного обслуговування і «прозорі» для користувачів;

кожен користувач повинен мати мінімальний набір «привілеїв», необхідних для інформаційної взаємодії;

можливість відключення «механізмів» захисту інформаційної системи в «особливих» випадках, коли механізми «заважають» інформаційній взаємодії користувачів;

незалежність «механізмів» захисту від самої системи; розробники повинні враховувати, найгірші наміри користувачів та передбачати здійснення серйозних помилок при використанні інформаційних технологій.

Для проведення якісного аудиту інформаційної безпеки підприємства повинна бути надана вичерпна інформація про інформаційну інфраструктуру підприємства і методах її захисту. Класифікація та складна система взаємозв'язків методів, засобів, одиниць оцінки, гарантій оцінки, забезпечення єдності оцінки та довіри наведені у таблиці 1.2.

Постійна робота в сфері підтримки інформаційної безпеки на належному рівні є необхідною умовою ефективності підприємницької діяльності. Водночас безпека інформаційної системи має розглядатися як важлива складова загальної безпеки підприємства. Таким чином, захист інформаційних ресурсів підприємства є одним з ключових завдань в умовах підвищення рівня внутрішніх і зовнішніх загроз інформаційної безпеки, що можуть безпосередньо вплинути на його фінансову діяльність і стійкість на ринку. Щоб зберегти бізнес, розвиватися і бути конкурентоспроможним, підприємствам необхідно створити ефективну систему управління інформаційною безпекою. Наведена технологія забезпечення інформаційної безпеки зорієнтована на вирішення питань надійної аутентифікації користувачів і серверів, захист конфіденційної інформації при її передачі по каналах зв'язку, контроль справжності та цілісності електронних документів, забезпечення юридично-значимого електронного документообігу, захищеного обміну електронними документами як всередині підприємства так і з зовнішніми користувачами.

Основними принципами забезпечення інформаційної безпеки є наступні [53]: системності; комплексності; безперервності захисту; розумної

достатності; гнучкості управління і застосування; відкритості алгоритмів і механізмів захисту; простоти застосування захисних заходів і засобів.

За способами здійснення всі заходи забезпечення безпеки комп'ютерних систем підрозділяють на:

Таблиця 1.2

Методи, засоби оцінки інформаційної захищеності підприємства [49]

№ з/п	Вид захисту інформації	Методи та засоби оцінки	Одиниці оцінки	Гарантії оцінки	Забезпечення єдності оцінки та довіри
1	*2*	*3*	*4*	*5*	*6*
1	Криптографічний	Розрахункові. Стійкість системи шифрування	Час розкриття методом прямого перебору	Теоретичне доведення, експеримент	Досягнута продуктивність. Обчислювальної техніки
2	Від витоку технічними каналами	Інструментальні. Метрологічні вимірювальні прилади	Відношення сигнал/шум. С/Ш=Іс-Іш	Клас вимірювальних приладів, похибка вимірювання	Державна метрологічна система
3	Від НСД до комп'ютерних систем	Експертні оцінки, аудит дослідження	Одиниці умовних шкал	Кваліфікація експертів	Система державної експертизи
4	Від фізичного НСД до носіїв інформації	Експертні оцінки, моделювання, атестація, аудит	Ймовірність подолання рубежів охорони	Кваліфікація експертів	Система атестації КЗЗ – комплексів засобів захисту
5	Організаційні заходи (від людського фактору)	Експертні оцінки, атестація, аудит	Одиниці умовних шкал	Кваліфікація експертів	Система атестації КЗЗ
6	Від вірусів	Експертиза. Статистичні дослідження. Оцінка ризиків	Ймовірності, математичне очікування, дисперсія	Довірчий інтервал (критерій Пірсона тощо)	Сертифікація. Система збору й аналізу статистичних даних
7	За допомогою брандмауерів				
8	Система виявлення атак				

правові (законодавчі). До правових заходів захисту інформації належать діючі в країні закони, укази, положення, інструкції та інші нормативні акти, які регламентують правила поводження з інформацією обмеженого використання і відповідальності за їх порушення. Цим вони перешкоджають несанкціонованому використанню інформації і є стримуючим фактором для потенційних порушників;

морально-етичні. До морально-етичних заходів протидії відносяться всілякі норми поведінки, які традиційно склалися або складаються в суспільстві у міру поширення комп'ютерів в країні. Ці норми бувають як неписаними (загальновизнані норми чесності, патріотизму), так і оформленими в якийсь звід правил чи приписів;

організаційно-адміністративні. Організаційно-адміністративні заходи захисту регламентують процеси функціонування ІС (інформаційних систем); використання ресурсів ІС; діяльність персоналу інформаційної служби на підприємстві; порядок взаємодії користувачів із системою, з тим, щоб найбільшою мірою ускладнити чи виключити можливість реалізації загроз безпеці. Включають в себе: розробку правил обробки інформації в інформаційній системі; сукупність дій при проектуванні та обладнанні обчислювальних центрів та інших об'єктів інформаційної системи (облік впливу стихії, пожеж, охорона приміщень); сукупність дій при підборі й підготовці персоналу (перевірка нових співробітників, ознайомлення їх з порядком роботи з конфіденційною інформацією, з мірами відповідальності за порушення правил її обробки; створення умов, при яких персоналу було б невигідно допускати зловживання); організацію надійного пропускного режиму; організацію обліку, зберігання, використання та знищення документів і носіїв з конфіденційною інформацією; розподіл реквізитів розмежування доступу (паролів, повноважень); організацію прихованого контролю за роботою користувачів і персоналу інформаційної системи; сукупність дій при проектуванні, розробці, ремонті та модифікації устаткування і програмного забезпечення (сертифікація використовуваних

технічних і програмних засобів, суворе санкціонування, розгляд і затвердження всіх змін, перевірка на задоволення вимогам захисту, документальна фіксація змін);

фізичні. До фізичних мір захисту відносяться різні механічні, електро- і електромеханічні пристрої або споруди, спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і доступу порушників (турнікети, колючий дріт, кодові замки, системи охоронно-пожежної сигналізації);

апаратно-програмні. До апаратно-програмних заходів захисту відносяться різні електронні пристрої та спеціальні програми, які реалізують самостійно або в комплексі з іншими засобами наступні способи захисту: ідентифікацію і аутентифікацію суб'єктів інформаційної системи; розмежування доступу до ресурсів ІС; контроль цілісності даних; забезпечення конфіденційності даних; аудит подій, що відбуваються в інформаційній системі; резервування ресурсів і компонентів інформаційної системи.

Таким чином, в сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки комплексною системою захисту інформації, яка повинна бути: безперервною, плановою, цілеспрямованою, конкретною, активною, надійною. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в критичних ситуаціях.

1.3. Моделі інформаційної безпеки

Відомо [5; 5; 7, ст. 36], що будь-яка організаційна модель інформаційної безпеки підприємства має ієрархічну структуру, що складається з багатьох елементів, механізмів захисту інформаційних ресурсів, логічних, адміністративних і фізичних компонент, процедур реалізації бізнес-процесів і їх конфігурацій, які працюють спільно, забезпечуючи потрібний рівень реалізації

бізнес-цілей діяльності підприємства. Кожна модель може мати свої відмінності у структурі [55, ст. 87], але всі вони мають певні ієрархічні рівні, кожен з яких підтримує вищий і захищає нижчий рівень. Оскільки організаційна модель інформаційної безпеки може мати складну ієрархічну структуру (рис. 1.7), то різні підприємства можуть наповнювати її різними технологіями захисту своїх інформаційних ресурсів, адекватними методами і процедурами їх підтримки для досягнення потрібного рівня захищеності [38].

Реалізація ефективної організаційної моделі інформаційної безпеки підприємства вимагає зваженого підходу і застосування всіх компонент і процедур для забезпечення без- перервності бізнес-процесів підприємства, стійкого його перебігу та запобігання потенційним загрозам і небезпекам [18]. Деякі компоненти моделі (наприклад, списки контролю доступу, методи шифрування) є програмно-технічними, а інші – фізичними і адміністративними (наприклад, розроблення політики інформаційної безпеки підприємства і забезпечення її відповідності нормативним документам), але кожен має важливе місце в рамках загальної мети діяльності підприємства [5; 12, с. 315]. Якщо одна компонента відсутня або реалізується не повною мірою, то це може негативно вплинути на всю ієрархічну структуру інформаційної безпеки підприємства.

Оскільки організаційна модель інформаційної безпеки підприємства складається з різних ієрархічних рівнів [7], то кожен з них має забезпечити виконання різних функціональних цілей захисту інформаційних ресурсів [11], які мають досягатися в різні терміни та за різні проміжки часу. Цілі можуть бути щоденними (операційними), середньо-терміновими (тактичними) і довготерміновими (стратегічними). Теж саме відбувається і у сфері планування інформаційної безпеки підприємства [1]. Щоденні (операційні) цілі пов'язані з продуктивністю роботи АСУ підприємством і виконанням поточних завдань, що забезпечують передбачене функціонування відповідних бізнес-процесів. Середньо-термінові (тактичні) цілі стосуються, наприклад, об'єднання всіх робочих станцій АСУ та

відповідних інформаційних ресурсів у один домен, щоб забезпечити можливість їхнього централізованого контролю. Прикладом довготермінових (стратегічних) цілей може бути переведення всіх філій на зв'язок з головним офісом за допомогою VPN-з'єднань, об'єднання всіх безпровідних технологій для отримання єдиного підходу до забезпечення інформаційної безпеки підприємства [12, с. 315–316].

Рисунок 1.7 – Організаційна модель інформаційної безпеки підприємства та її компоненти [12, с. 316]

Стратегічне планування передбачає роботу з планами, які знаходяться на одному рівні з бізнес-цілями діяльності підприємства і цілями захищеності його інформаційних ресурсів. Оскільки цілі такого планування довготермінові, тому вони мають як широкий горизонт реалізації, так і достатню глибину прогнозування подальшої діяльності. Стратегічне планування, зазвичай, містить такі цілі [39, с. 138]:

забезпечити правильне розуміння допустимих ризиків проведення інформаційних атак зловмисниками, організувати їх прогнозування та здійснити облік;

забезпечити відповідність комплексну системи захисту інформації вимогам чинного законодавства та регуляторів інформаційної безпеки;

інтегрувати обов'язки працівників підприємства щодо забезпечення інформаційної безпеки в їх безпосередню та повсякденну діяльність;

розробити модель компетентності працівників підприємства для забезпечення можливості реалізації бізнес-цілей його діяльності та поліпшення його інформаційної безпеки;

використовувати інформаційну безпеку підприємства як бізнес-перевагу над конкурентами, щоб привернути більше клієнтів і закріпити свій стан на ринку товаровиробників.

Тактичне планування належить до діяльності менеджерів підприємства та підтримки їхніх дій, які необхідні для досягнення широких цілей, висунутих у процесі стратегічного планування. Загалом, тактичні плани мають дещо коротші терміни планування, набагато вужчий горизонт реалізації та значно меншу глибину прогнозування порівняно із стратегічними планами [12, с. 316].

Оперативне планування – це конкретні плани і прогнози, терміни і цілі, припускає вказання дієвих заходів, встановлення жорстких термінів і графіків виконання робіт [39, с. 141]. Це конкретні дії реалізації тактичних і стратегічних планів, які потрібно зробити для досягнення бізнес-цілей діяльності підприємства. Зазвичай оперативне планування зводиться до [46]:

оцінювання ризиків успішного проведення інформаційних атак зловмисниками, а також нанесення потенційних збитків підприємству від них;

усунення негативного впливу змін у системі захисту інформації на продуктивність роботи працівників підприємства;

підтримка і впровадження захисних заходів з поліпшення інформаційної безпеки підприємства;

постійне сканування вразливостей і встановлення програмних оновлень;

контроль відповідності дій працівників підприємства та потенційних клієнтів встановленій політиці інформаційної безпеки.

Такий підхід до планування називається горизонтом планування. При цьому політика інформаційної безпеки підприємства працює краще тоді, якщо оперативні, тактичні та стратегічні бізнес-цілі діяльності підприємства конкретно визначені та взаємодіють між собою, підтримуючи одне одного.

Створення моделі управління захистом інформації ґрунтується на послідовному визначенні об’єктів управління, цілей і завдань управління, показників і критеріїв ефективності управління, функцій управління, складу системи та організаційної структури управління, на розробці методів і засобів управління [16].

Проблеми інформаційної безпеки істотно залежать від типу інформаційних систем і сфери їх застосування. У локальних системах малого масштабу систему захисту побудувати набагато простіше, ніж в системах розподіленого типу, що пояснюється особливостями цих систем, основними з яких є: територіальна розосередженість компонентів системи і як наслідок наявність обміну інформацією між ними; широкий спектр способів подання, зберігання і передачі інформації; одночасна участь в процесах опрацювання інформації великою кількістю користувачів з різними правами доступу; використання різнорідних програмно-технічних засобів обробки і систем телекомунікацій [42]. Саме тому, автор роботи [16] запропоновав структурну модель інформаційної безпеки систем розподіленого типу, яка відображена на рисунку 1.8. Ця структурна модель передбачає, що рішення проблеми безпеки в інформаційних системах розподіленого типу полягає в аналізі наступних основних компонентів [16]:

визначення основних завдань захисту інформації,

визначенні суб’єктів інформаційних процесів,

класифікації основних можливих загроз безпеки,

визначенні рівнів вразливості інформаційних систем,

визначенні джерел інформації,

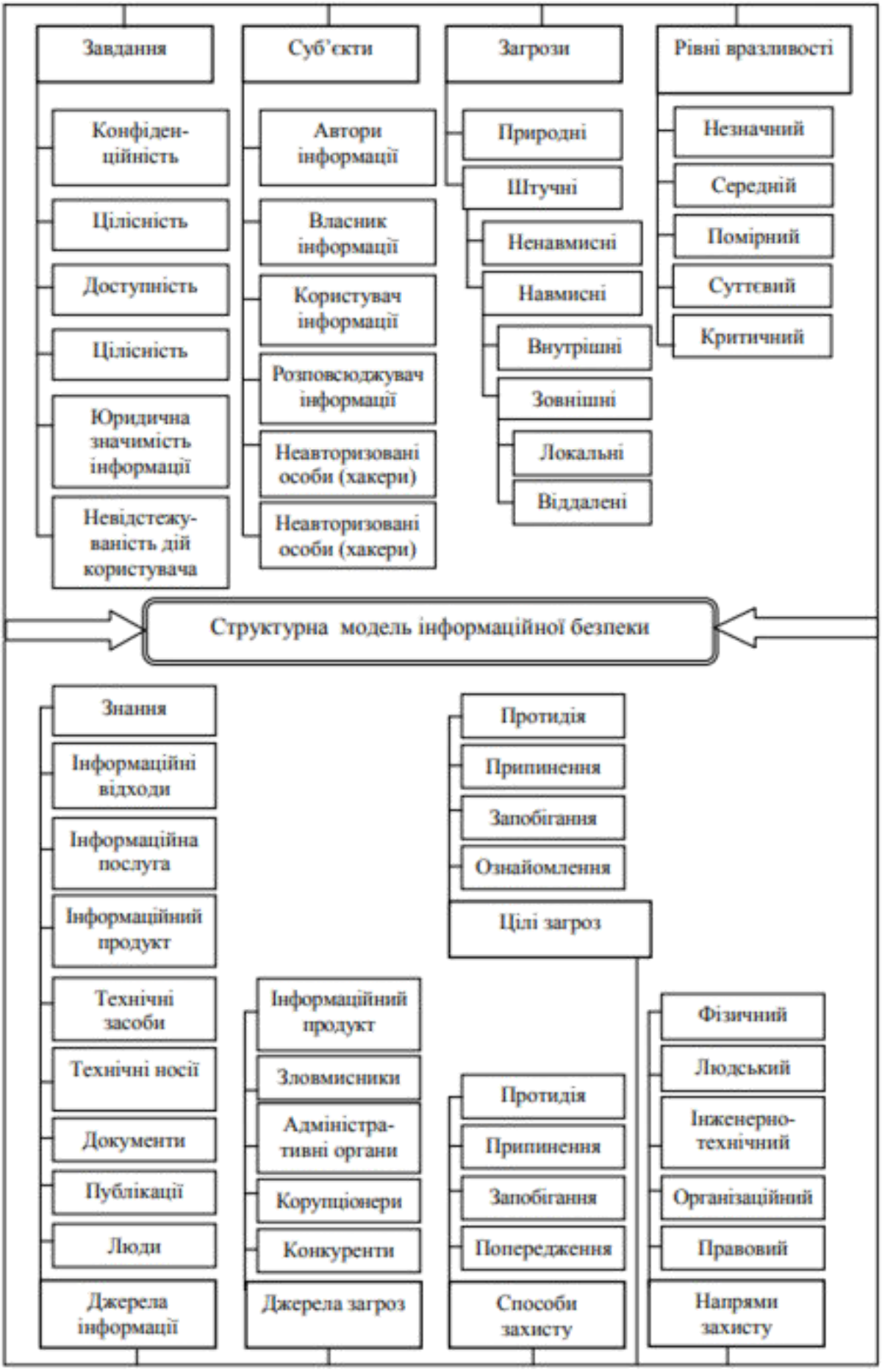


Рисунок 1.8 – Структурна модель інформаційної безпеки [16]

ознайомленні з особливостями джерел загроз,

досліджені способів та напрямів захисту та цілей захисту.

При цьому, забезпечення безпеки інформації полягає у вирішенні трьох взаємопов'язаних завдань [43, с. 17]:

конфіденційність – полягає в захисті інформації в процесі її створення, зберігання, обробки та обміну від ознайомлення з нею особами, які не мають права доступу до неї;

цілісність – полягає в захисті від навмисної або ненавмисної зміни інформації та алгоритмів її обробки особами, які не мають на те права;

доступність – полягає в наданні користувачам всієї наявної в системі інформації відповідно до встановлених їм правам.

Основними суб'єктами в інформаційних процесах є: автори і власники інформації, авторизовані користувачі інформації, неавторизовані особи (особи, які намагаються отримати самовільний доступ до інформації), окремі співробітники або колективи, які беруть участь в розробці, забезпеченні працездатності програмно-технічних засобів інформаційних систем і наповненні системи інформацією. Системи захисту повинні забезпечувати захист прав авторів і власників інформації та одночасно надавати доступ до інформації користувачам відповідно до їх прав [16].

Під загрозою безпеки інформаційних систем розуміється потенційно можлива дія, подія або процес, який за допомогою впливу на інформацію та інші компоненти системи може завдати шкоди інтересам суб'єктів [16].

Джерелами загроз виступають конкуренти, злочинці, корупціонери, адміністративно-управлінські органи.

Джерела загроз переслідують при цьому наступні цілі: ознайомлення з відомостями, що охороняються, їх модифікація в корисливих цілях і знищення для нанесення прямих матеріальних збитків.

Неправомірне заволодіння конфіденційною інформацією можливо шляхом її розголошення джерелами відомостей, за рахунок витоку інформації через технічні засоби та через несанкціонований доступ до

відомостей, що охороняються.

Джерелами конфіденційної інформації є люди, їх знання, документи, публікації, технічні носії інформації, технічні засоби забезпечення виробничої та трудової діяльності, продукція, послуги і відходи виробництва.

Основними напрямками захисту інформації є правовий, організаційний, інженерно-технічний, людський, фізичний захист інформації як індикатори комплексного підходу до забезпечення інформаційної безпеки.

Засобами захисту інформації є фізичні засоби, апаратні засоби, програмні засоби та криптографічні методи. Останні можуть бути реалізовані як апаратно, програмно, так і змішано-програмно-апаратними засобами.

В якості засобів захисту виступають всілякі заходи, шляхи, способи і дії, що забезпечують попередження протиправних дій, їх запобігання, припинення та протидія несанкціонованому доступу.

Окрім системного підходу, доцільно врахувати і положення процесного підходу до моделювання систем інформаційної безпеки. Сутність процесного підходу до формування моделі інформаційної безпеки полягає в тому, що захист інформації розглядається як особливий вид діяльності в організації, який здійснюється при моделюванні, проектуванні як сукупність процесів захисту інформації:

наявність мети процесу, тобто бажаного результату захисту інформації, що досягається при здійсненні процесу;

зміни предметної області, в якій реалізується процес. По суті, реалізація процесу завжди пов'язана зі зміни системи та є цілеспрямованим переходом цієї системи з існуючого в бажаний стан;

обмеженість необхідних ресурсів на виконання операцій і дій, що складають процес;

безперервність процесу. Процес є модель функції захисту, яка здійснюється організацією протягом усього свого існування;

комплексність та розмежування процесу. Комплексність процесу передбачає врахування всіх внутрішніх і зовнішніх факторів, які прямо

або опосередковано впливають на розвиток процесу і результати процесу [42, с. 128–129].

У той же час кожен процес має чітко визначені межі предметної області, наприклад процес аналізу загроз, процес сертифікації засобів захисту, процеси стратегічного управління безпекою тощо.

Формалізуючи модель інформаційної безпеки у математичному вигляді, доцільно визначити її функціональну залежність від завдань захисту інформації, суб'єктів інформаційних процесів, загроз безпеки, рівнів вразливості інформаційних систем, джерел інформації, джерел загроз, способів захисту, напрямів захисту, цілей захисту [16]:

$$S_{mis} = f[\{W(MIS_{sub})\}, \{W(MIS_{task})\}, \{W(MIS_{threats})\}, \{W(MIS_{level})\}, \{W(MIS_{sourceinf})\}, \{W(MIS_{sourcethreat})\}, \{W(MIS_{wayprotect})\}, \{W(MIS_{directprotect})\}, \{W(MIS_{goal})\}], \quad (1.1)$$

де S_{mis} – стан системи інформаційної безпеки;

$\{W(MIS_{sub})\}$ – сукупність суб'єктів системи інформаційної безпеки;

$\{W(MIS_{task})\}$ – сукупність завдань системи інформаційної безпеки;

$\{W(MIS_{threats})\}$ – сукупність загроз системи інформаційної безпеки;

$\{W(MIS_{level})\}$ – рівні вразливості системи інформаційної безпеки;

$\{W(MIS_{sourceinf})\}$ – сукупність джерел інформації системи інформаційної безпеки;

$\{W(MIS_{sourcethreat})\}$ - сукупність джерел загроз системи інформаційної безпеки;

$\{W(MIS_{wayprotect})\}$ – сукупність способів захисту інформаційних ресурсів;

$\{W(MIS_{directprotect})\}$ – сукупність напрямів захисту інформаційних ресурсів;

$\{W(MIS_{goal})\}$ – сукупність цілей захисту інформаційних ресурсів.

Інформаційна безпека є функцією з множини області значень складових системи інформаційної безпеки. Постійне зростання потреби в

інформації обумовлює необхідність нарощування та ефективного використання інформаційних ресурсів, формування інформаційного потенціалу організаційних утворень, що виступає основною передумовою зміни стану системи інформаційної безпеки, перебудови або вдосконаленні її моделі.

При будь-якій зміні стану організації як соціально-економічної системи, зміну моделі системи інформаційної безпеки (ΔS_{mis}) можна виразити рівнянням [16]:

$$\Delta S_{mis} = \Delta S_{in} ; \Delta S_{ext}, \quad (1.2)$$

де ΔS_{in} – зміна стану системи інформаційної безпеки через взаємодію із зовнішнім середовищем;

ΔS_{ext} – зміна стану системи інформаційної безпеки, що відбуваються всередині самої системи без впливу зовнішнього середовища.

Отже, вищезазначена формалізація моделі процесу інформаційної безпеки розглядає захист інформації як сукупність процесів. Захист інформації здійснюється відповідно до заздалегідь визначеної та постійно змінюваної мети захисту, яка пов’язана з затратами фінансових, енергетичних, трудових, матеріальних та інших ресурсів, з врахуванням обмежень зовнішнього середовища. Бажаний результат захисту інформації досягається більш ефективно, в тому випадку, якщо пов’язані ресурси і діяльність розглядаються і управляються як процес. Процес, як категорія, використовується як засіб структурування діяльності суб’єкту захисту інформації.

Таким чином, модель захисту інформації для інформаційних систем розподіленого типу, дозволяє визначити:

основні завдання щодо забезпечення безпеки, виявити суб'єкти в інформаційних процесах,

визначити типи загроз і рівнів уразливості;

побудувати ефективну систему захисту інформації, застосувати адекватні засоби і методи безпеки на всіх рівнях інформаційних процесів.

Висновки до розділу 1

У першому розділі роботи проаналізовано основні теоретичні положення інформаційної безпеки. Встановлено, що відповідно до умов функціонування, у динамічному ринковому середовищі, інформаційна безпека підприємства представляє собою характеристику стану джерел інформації що гарантує певний рівень інформаційно-аналітичного забезпечення, який базується на захисті інформаційного середовища і обумовлює отримання ефективного та результативного інформаційного продукту. Доведено, що інформаційну безпеку слід розглядати як забезпечення реалізації національних інтересів за допомогою різних засобів, що є в її розпорядженні. Відзначено, що зміст інформаційної безпеки ґрунтується на двох її аспектах: інформаційному та забезпечення захисту інформації. Наведено базові та функціональні ознаки забезпечення інформаційної безпеки підприємства.

Отже, сьогодні спостерігається високе значення інформаційних активів підприємств в контексті їх переважаючого значення по відношенню до вартості матеріальних ресурсів організації. З огляду на рівень сучасного розвитку інформаційних технологій, питання забезпечення захисту інформації стають однією з фундаментальних детермінант економічної безпеки підприємства. Інформаційна безпека виступає єдиним можливим напрямком для попередження нанесення збитків економічним інтересам підприємства шляхом організації захисту від існуючих і потенційних загроз інформаційних ресурсів підприємства.

Охарактеризовано технологію забезпечення інформаційної безпеки підприємства. Доведено, що в сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки комплексною системою захисту

інформації, яка повинна бути: безперервною, плановою, цілеспрямованою, конкретною, активною, надійною. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в критичних ситуаціях.

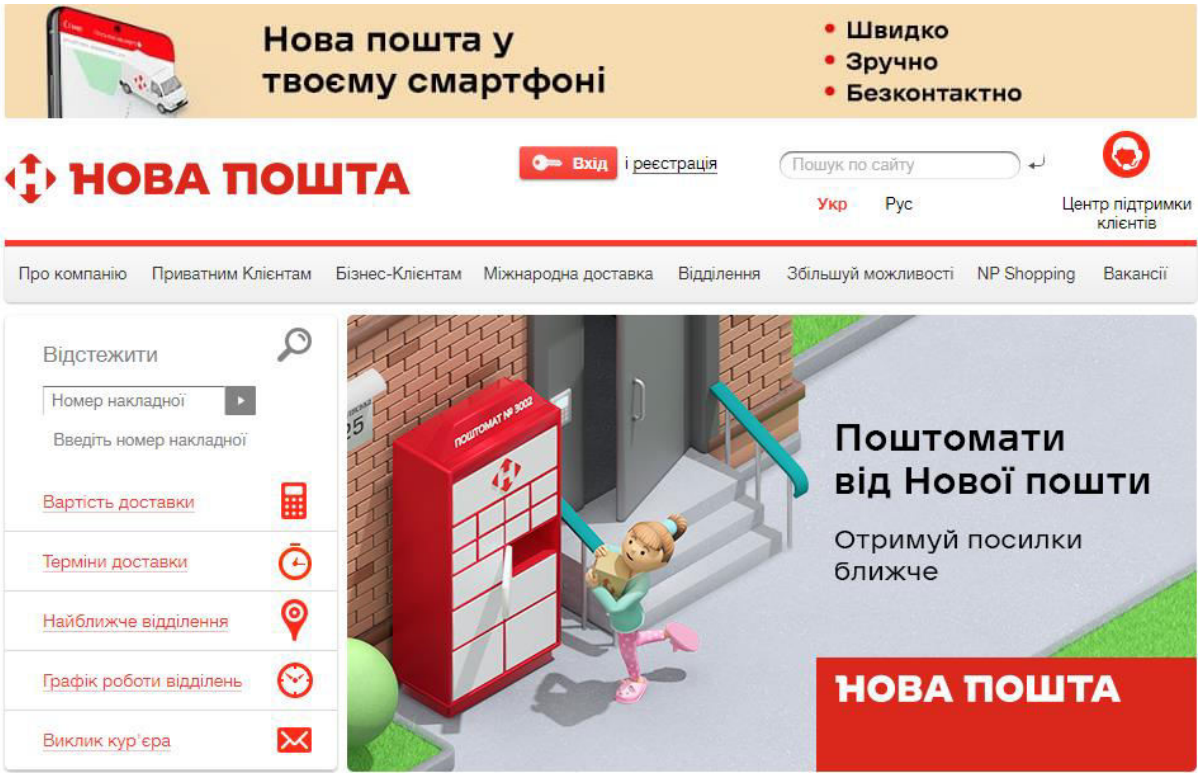
Наведено та охарактеризовано моделі інформаційної безпеки. Отже, структурна модель інформаційної безпеки передбачає, що рішення проблеми безпеки в інформаційних системах розподіленого типу полягає в аналізі наступних основних компонентів: визначення основних завдань захисту інформації, визначенні суб'єктів інформаційних процесів, класифікації основних можливих загроз безпеки, визначенні рівнів вразливості інформаційних систем, визначенні джерел інформації, ознайомленні з особливостями джерел загроз, дослідженні способів та напрямів захисту та цілей захисту. При цьому, забезпечення безпеки інформації полягає у вирішенні трьох взаємопов'язаних завдань: збереженні конфіденційності, цілісності та доступності. Функціональна модель процесу інформаційної безпеки розглядає захист інформації як сукупність процесів. Захист інформації здійснюється відповідно до заздалегідь визначеної та постійно змінюваної мети захисту, яка пов'язана з затратами фінансових, енергетичних, трудових, матеріальних та інших ресурсів, з врахуванням обмежень зовнішнього середовища. Бажаний результат захисту інформації досягається більш ефективно, в тому випадку, якщо пов'язані ресурси і діяльність розглядаються і управляються як процес. Процес, як категорія, використовується як засіб структурування діяльності суб'єкту захисту інформації.

У роботі доведено, що створення системи інформаційної безпеки є масштабною роботою, яка вимагає серйозних зусиль. Тому, насамперед, необхідно найбільш точно визначити ризики, які існують для інформаційної безпеки підприємства, і не вживати додаткових заходів забезпечення

безпеки, якщо це реально не відобразиться на підвищенні рівня зростання самого підприємства.

Розділ 2. Аналіз діяльності ТОВ «Нова Пошта»

2.1. Характеристика діяльності ТОВ «Нова Пошта»



ТОВ «Нова Пошта» [37]:

це великий поштовий оператор зв'язку, який працює на ринку України в кожному регіоні;

це найбільш популярна транспортна українська компанія, що надає послуги з експрес-доставки документів, різних вантажів, а також посилок фізичних осіб та бізнес – посилок;

є однім з найкрупніших роботодавців в Україні (на сьогодні, у компанії працюють більше, ніж 28 тис. працівників);

входить до групи компаній «Нова Пошта», яка надає клієнтам, бізнесу та приватним фізичним особам, повний спектр логістичних та пов'язаних з ними послуг. До цієї групи входять як українські, так і зарубіжні компаній, а саме «Нова Пошта», «НП Логістик», «ПОСТ ФІНАНС» та «Нова Пошта

Глобал». Сама група «Нова Пошта» входить у ТОП-100 крупніших платників податків в Україні. Тільки за 2019 рік компанія перерахувала до бюджетів всіх рівнів країни більше ніж 4,3 млрд грн податків та зборів;

має найсучасніші сортувальні термінали, розташовані у місті Києві, а також у містах Львів та Хмельницький. Такі термінали здатні обробляти від 14 – 20 тисяч посилок усього за одну годину.

Заснована у 2001 році «Нова Пошта» – українська компанія, що забезпечує сервіс експрес-доставки документів, вантажів і посилок для фізичних та юридичних осіб.

Група «Нова Пошта» пропонує своїм клієнтам – як юридичним особам, так і приватним особам - повний спектр логістичних і поштових послуг. У Групу входять українські та закордонні підприємства, які схематично представлені на рисунку 2.1, зокрема «Нова Пошта», «НП Логістик», «ПОСТ ФІНАНС» і «Нова Пошта Ітернешнл».

Рис. 2.1 Структура Групи «Нова Пошта»

«Нова Пошта» – лідер логістичного ринку експрес-перевезень, що забезпечує просту доставку кожному клієнту – у відділення, поштомати, на

адресу – і дозволяє тисячам підприємців створювати і розвивати бізнес не лише в Україні, але й за кордоном.

Мережа підприємства нараховує понад 2671 відділень по всій території України, а кількість відправлень перевищила 146 млн., за 2018 рік.

«НП Логістик» – компанія, що надає послуги фулфілменту: зберігання товару на складах, комплектацію та відправку замовлень отримувачу.

«ПОСТ ФІНАНС» – завдяки небанківській фінансовій установи, клієнти компанії можуть здійснювати грошові перекази та операції з електронними грошима.

«Нова Пошта Інтернешнл» розвиває та виходить на міжнародну мережу, щоб надавати клієнтам послуги експрес-доставки не лише в Україні, але й за кордоном [37].

Група «Нова Пошта» працює із дотриманням усіх норм українського законодавства. У сукупності, Група перерахувала в бюджет країни близько 1,5 млрд грн податків і зборів за останні роки.

ТОВ «Нова Пошта» перший український оператор з впровадження експрес-перевезень – повного комплексу надання послуг з доставки документів, вантажів, грошових переказів.

Компанія кожного року отримує різні нагороди та займає лідируючі позиції українського ринку, наприклад, має нагороди: «Золота Фортуна «Якість третього тисячоліття»» та «Народне визнання «Бренд року»».

ТОВ «Нова Пошта» працює під гаслом – «Ми там, де вам зручно!» (рис. 2.2).

В процесі сортування поштової кореспонденції запроваджена 5-ти значна індексація – якісне, просте, прискорене обслуговування клієнтів. Технічне забезпечення процесу виробництва використовує нові сучасні технології, сучасну техніку, транспорт, сучасний ремонт, розширення поштових мереж [37].

ТОВ «Нова Пошта» має корпоративний Інтернет-портал (www.novaposhta.ua), що сприяє взаємозв'язку інформаційних ресурсів всіх підрозділів підприємства.

Використання нових технологій дозволяє компанії надавати сучасні послуги – доставку товарів та вантажів з інтернет-магазинів; зберігання вантажів (певний термін); зворотня доставка (повернення); упаковка вантажу (різні види упаковки).

В компанії Нова Пошта розвиваються фінансові та банківські послуги – оформлюються фінансові документи й приймається готівка. Широкий спектр послуг компанії включає більше ніж 70 видів послуг.

Рисунок 2.2 – Цінності компанії Нова Пошта [37]

«Нова Пошта» учасник міжнародних проектів: «Система реєстрації й контролю проходження пошти в Україні», «Міжнародна фінансова система», «Постійний контроль якості».

Значна увага компанії приділяється забезпеченню та підвищенню рівня високої кваліфікації персоналу (курси, тренінги, семінари, навчальні центри).

Місія підприємства – спрощувати життя своїм клієнтам, робивши доставку легкою для життя і бізнесу. Для цього команда «Нова Пошта» впроваджує та удосконалює нові продукти і послуги, орієнтуючись на світові стандарти та кращий міжнародний досвід.

Окрім відправки та отримання посилок та вантажів, у відділеннях «Нова Пошта» можна замовити, додаткові послуги, що розроблені з урахуванням побажань клієнтів.

На рисунку 2.3 зображено кількість відділень розташованих у всіх куточках України.

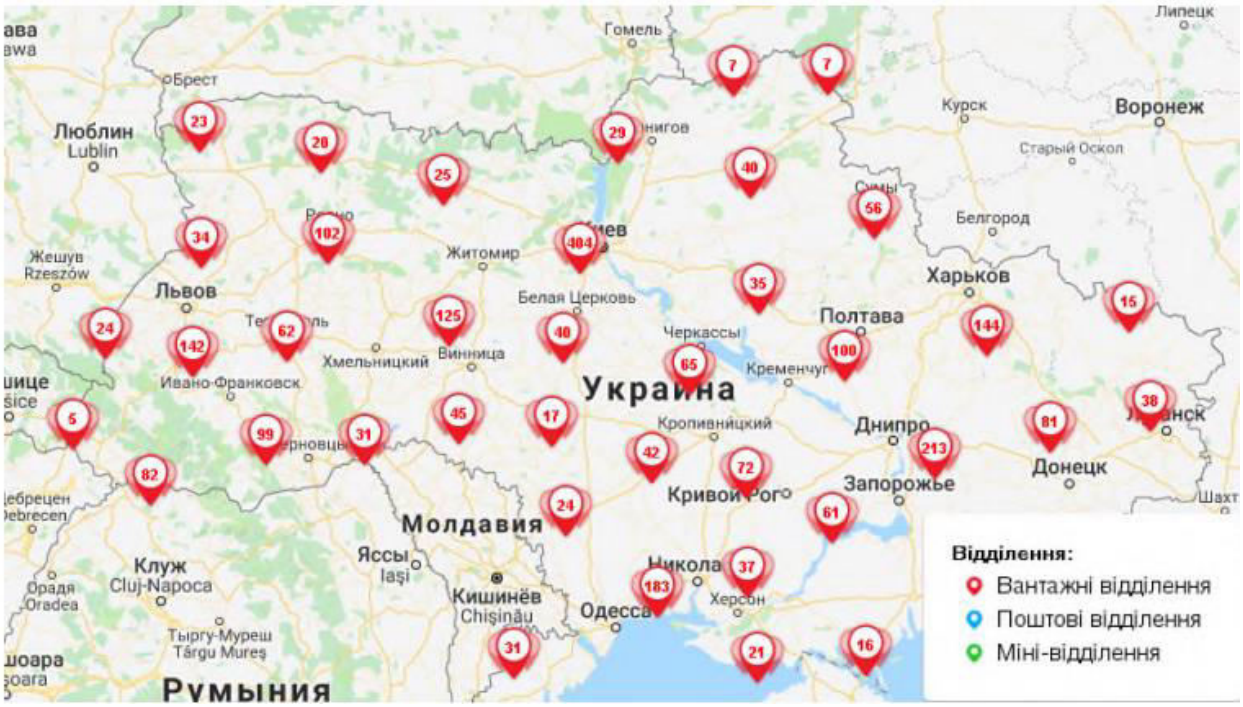


Рисунок 2.3 – Георгафія розташування відділень ТОВ «Нова Пошта»

Отже, як показує історія динамічного розвитку, вже понад 20 років компанія пропонує своїм клієнтам зручну, доступну та якісну послугу – доставку вантажів і кореспонденції в будь-яку точку України.

Компанія використовує в своїй діяльності нові технології та послуги з доставки товарів (вантажів): склад-склад, двері-двері, склад-двері, двері-склад [37].

Додаткові послугт які пропонує ТОВ «Нова Пошта» є такі [37]:

1. Доставка та повернення вантажів до роздрібних мереж – передбачає доставку товару клієнта в будь-які торгово-роздрібні мережі (супермаркети, філіали, представництва, мережі автозаправок тощо) у будь-яку точку України.

Цей вид партнерства дозволяє оптимізувати і спростити логістичні та організаційні процеси, відповідно до специфіки задоволення клієнтів.

2. Доставка палетованного вантажу – передбачає формування палети з окремих вантажів або перевезення сформованих палет за зниженими тарифами.

3. Доставка автомобільних шин і дисків – передбачає перевезення шин і дисків за зниженими цінами.

4. Зворотня доставка – передбачає повернення документів за вантаж відправнику.

5. Післяплата за товар – передбачає розрахунок за вантаж, суму вартості якого відправник доручає одержати транспортній компанії. Одержана сума надходить на банківський рахунок відправника.

6. Виклик машини – передбачає надання відправнику відповідного транспорту на обумовлений час під завантаження.

7. Переадресація – передбачає зміну типу послуги або адреси доставки вже оформленого вантажу за бажанням клієнта відправника.

8. Підйом вантажу на поверх – передбачає підйом вантажу на поверх при доставці за адресою. Маса одного місця вантажу не повинна перевищувати 75 кг. Замовити послугу може тільки клієнт відправника. Якщо вага

відправлення по одній товарно-транспортній накладній менше 30 кг, послуга надається безкоштовно (без попереднього замовлення).

9. Зберігання вантажу – передбачає зберігання вантажу у відділенні ТОВ «Нова Пошта» 1 (один) календарний місяць з дня надходження вантажу. Безкоштовно вантаж може зберігатися протягом 5-ти робочих днів, включаючи день, коли він мав бути одержаний отримувачем. За зберігання вантажу на складі більше 5-ти днів нараховується доплата у розмірі 20% від вартості перевезення вантажу, без урахування суми комісії за кожний наступний робочий день.

10. Упаковка вантажу – передбачає пакування вантажу у найбільш зручний вид упаковки. Зазначимо, що послуга надається в кожному відділенні ТОВ «Нова Пошта». Пакування вантажу застосовується для уникнення пошкоджень при транспортуванні, складуванні, зберіганні, а також для захисту від впливу зовнішнього середовища.

Види упаковки: фірмові пакети, розраховані на 1-2 кг; картонний конверт; картонні коробки різних розмірів; мішок поліпропіленовий; обрешетування дерев'яне; палетування. Для захисту відправлення існують додаткові види пакування: картонні коробки різних розмірів з ущільнювачем; повітрянопухирчаста плівка; стрейч-плівка; поролон; гофро-картон.

Впроваджена програма лояльності збільшує можливості – це винагорода активним клієнтам ТОВ «Нова Пошта». Мета її полягає в нарахуванні балів за кожну послугу з використанням карти учасника і подальшим обміном накопичених балів на послуги компанії та спеціальні подарунки.

Організаційна структура управління підприємством є основою системи управління, яка визначає склад, підпорядкованість та взаємодію її елементів, окреслює необхідну кількість управлінського персоналу, здійснює його розподіл за підрозділами, регламентує адміністративні, функціональні та інформаційні взаємовідносини між працівниками апарату управління та підрозділами, встановлює права, обов'язки й відповідальність менеджерів [44].

Організаційна структура управління ТОВ «Нова Пошта» наведена на рис. 2.4, яка дуже разголужена. Із організаційної структури підприємства ТОВ «Нова Пошта», бачимо, що кожен підрозділ самостійний, але безпосередньо взаємно пов'язаний з іншими підрозділами організаційної системи підприємства. Результати роботи будь-якого підрозділу апарату управління оцінюються показниками, що характеризують реалізацію ними своїх цілей і завдань. По кожній підсистемі формуються «ієрархія» послідовності, а також правил роботи, охоплюючи всю організацію від верху до низу.

Проаналізуємо кожен із відділів компанії [37]:

Фінансово-бухгалтерський відділ в компанії ТОВ «Нова Пошта» працює з різними категоріями і групами клієнтів, розробляючи та втілюючи фінансові системи та інструменти, які забезпечують прибутковість компанії. Їх вплив є визначним при виборі стратегічного напрямку, розробки портфоліо чи планів розширення.

Бухгалтерський відділ забезпечує досягнення бізнес-результатів компанії, при веденні точних та своєчасних облікових записів згідно вимог законодавства. На основі даних бухгалтерського, податкового та управлінського обліку, компанія щодня приймає рішення щодо найвигідніших інвестицій, їх окупності та подальших планів.

Департамент логістики. Даний відділ підпорядковує найбільшу завантаженість, яка впливає на ефективну роботу ТОВ «Нова Пошта». Оскільки в їх обов'язках є контроль міжміської логістики, міської логістики та термінальної логістики.

ІТ-відділ. Без ІТ – відділу неможливе ефективне управління сучасними інформаційними системами. За його допомогою забезпечується безперервна робота ІТ – інфраструктури і таким чином активне функціонування всього бізнесу.

Основні функції ІТ-відділу:

- дослідження і відстеження новітніх інформаційних технологій;

- забезпечення безперебійної роботи устаткування і користувачів;

- проектування, розробка, впровадження та супровід програмних продуктів;

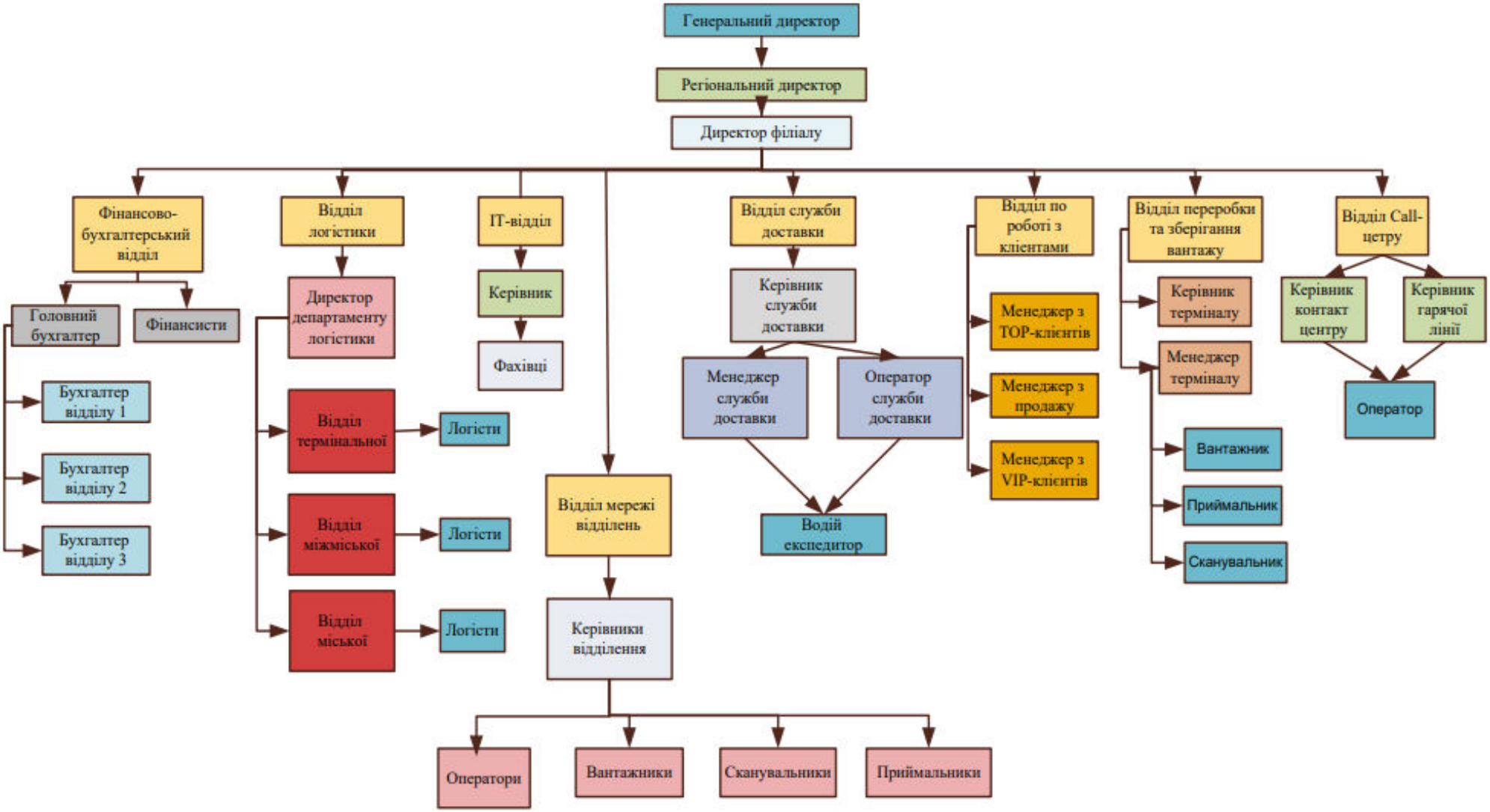


Рисунок 2.4 – Організаційна структура ТОВ «Нова Пошта» (складено на основі документації підприємства)

- регулярне відстеження ситуації в бізнесі для задоволення інформаційних потреб компанії;

- формування потреб в капіталовкладеннях в технологічну інфраструктуру;

- підтримання високого рівня освіченості співробітників в сфері інформаційних технологій.

Відділ мережі відділень. Відділення ТОВ Нова Пошта є самостійним структурним підрозділом організації до яких звертаються по питанням отримання та відправлення вантажу.

Основними завданнями відділень є:

- прийом, огляд та видача вантажу клієнтові;

- надання цілісної та ефективної упаковки для відправлення вантажу;

- прийом заяв на переадресування, повернення вантажу, зміни дати доставки та зміни даних щодо одержувача вантажу;

- надання клієнтові інформації щодо роботи організації.

Відділ по роботі з клієнтами. Основне завдання цього відділу полягає у виконанні поставлених планів продажу, пошуку нових та обслуговування вже існуючих клієнтів з дотриманням високих стандартів клієнтського сервісу. Менеджери відділу особисто зустрічаються з клієнтом, розроблюють комерційну пропозицію, узгоджують його потреби, за необхідності заключають договір та супроводжують клієнта на всіх етапах співпраці з нами.

Таким чином можна зазначити, що компанія «Нова Пошта» – надійний партнер для більше ніж 80000 компаній, серед яких національні виробники та роздрібні мережі, мережі автозаправок, інтернет-магазини, представництва іноземних компаній та багато інших.

2.2. Аналіз фінансових результатів діяльності ТОВ «Нова Пошта»

Для визначення виробничого та фінансового потенціалу підприємства необхідно провести комплексний економічний аналіз його діяльності.

Прибутковість компанії показує результативність діяльності з надання послуг з експрес-доставки товарів. Показники доходності ТОВ «Нова Пошта» послуг за період 2016-2019 рр. проаналізуємо в таблиці 2.1 [29].

Таблиця 2.1

Показники доходності ТОВ «Нова Пошта» послуг за 2016-2019 рр.

Роки / Назва показника	2016	2017	2018	2019
1	2	3	4	5
Письмова кореспонденція	13408,07	3674,68	15754,65	14593,10
Грошові перекази	4126,25	5525,72	5596,99	5397,32
Посилки	4538,77	4305,72	2477,01	1994,96
Періодичні видання	5088,81	6399,12	5757,73	4697,23
Доставка з Інтернет – магазинів	11888,21	23169,33	34554,40	36696,48
Торгівельна діяльність	24280,23	10042,94	5435,24	4326,99
Зберігання вантажу	3378,96	3452,00	3834,82	4189,99
Послуги електрозв'язку	207,27	302,60	1838,04	1637,08
Інші послуги	2072,63	2229,89	4713,41	1935,35
Загальна сума	68764,20	69549,00	79881,30	75424,50

Примітка. Сформовано на основі [29]

Дослідження показало, що з 2016-2019 рр. показники прибутку компанії «Нова Пошта» збільшуються з кожним роком (рис. 2.5) [29].

Проаналізуємо показники витрат ТОВ «Нова Пошта» за період з 2016–2019 рр. Вагомі значення мають показник оплати праці, витрати купівельної вартості, витрати на утримання транспорту, сплата податків, амортизаційні витрати тощо (табл. 2.2).

Перемінні витрати (закупівля матеріалів), транспортні витрати, витрати за споживання електроенергії визначаються у відсотковому значенні від

наданого обсягу послуг (робіт). З аналізу бачимо, що показник характеризує ефективність діяльності компанії – в 2018 р. 105,5%, а в 2019 р. 112,8%.

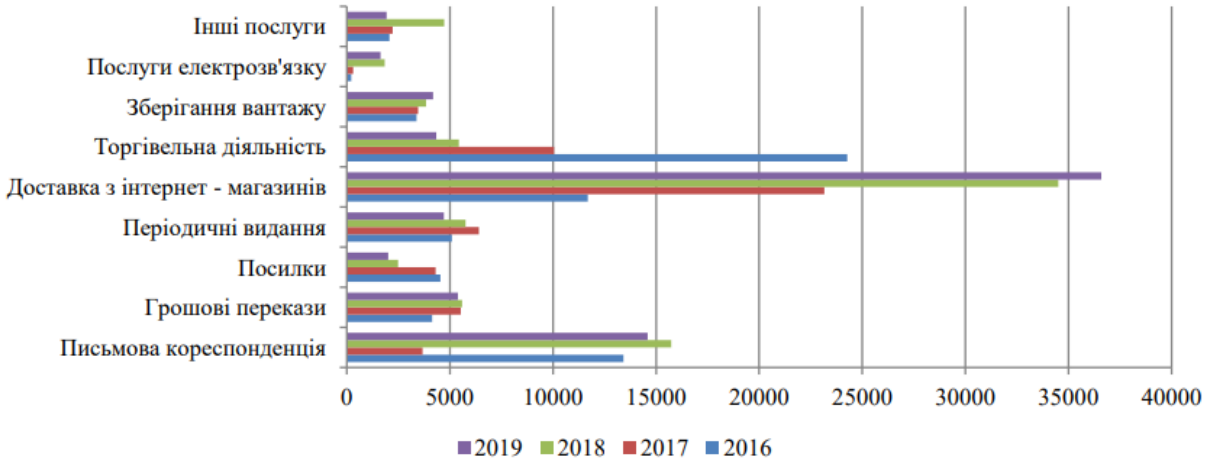


Рисунок 2.5 – Динаміка доходів ТОВ «Нова Пошта» послуг за 2016–2019 рр.

Таблиця 2.2

Показники витрат ТОВ «Нова Пошта» за 2016-2019 рр, *тис грн*

Роки / Назва показника	2016	2017	2018	2019
1	2	3	4	5
Заробітна плата і нарахування на ФОП	24233,92	24655,86	28060,25	26551,85
Витрати на утримання транспорту	2403,35	2555,63	2964,52	2365,23
Обслуговування технічних засобів	565,23	566,34	570,70	582,10
Опалення і електроенергія	1365,28	1689,67	1970,54	1752,32
Амортизація	1975,95	1843,74	2170,25	1624,21
Плата банку за готівку	1273,35	1240,00	1387,52	1420,20
Купівельна вартість	12224,52	12485,36	15244,21	17210,56
Податки	3320,20	3284,21	3447,20	3074,00
Витрати на матеріали	730,25	794,32	848,21	872,54
Перерахунок ПДВ	850,60	904,32	1410,25	1478,14
Оплата послуг електрозв'язку	542,25	596,65	680,85	772,35
Оренда	410,20	460,20	410,20	410,20
Всього	49373,1	50628,3	58153,1	54993,7

Примітка. Сформовано на основі [29]

Аналіз динаміки витрат ТОВ «Нова Пошта» за 2016–2019 рр. показав збільшення економічних показників. Як свідчать дані фінансової звітності, що наведені у таблиці 2.3, група компаній ТОВ «Нова Пошта» у звітному 2019 році отримала 13,453 млрд грн чистого доходу від реалізації своїх послуг, що на 27,94% більше, ніж у звітному 2018 році та на 70,29% більше, ніж у попередньому 2017 році відповідно [37] (рис. 2.6).

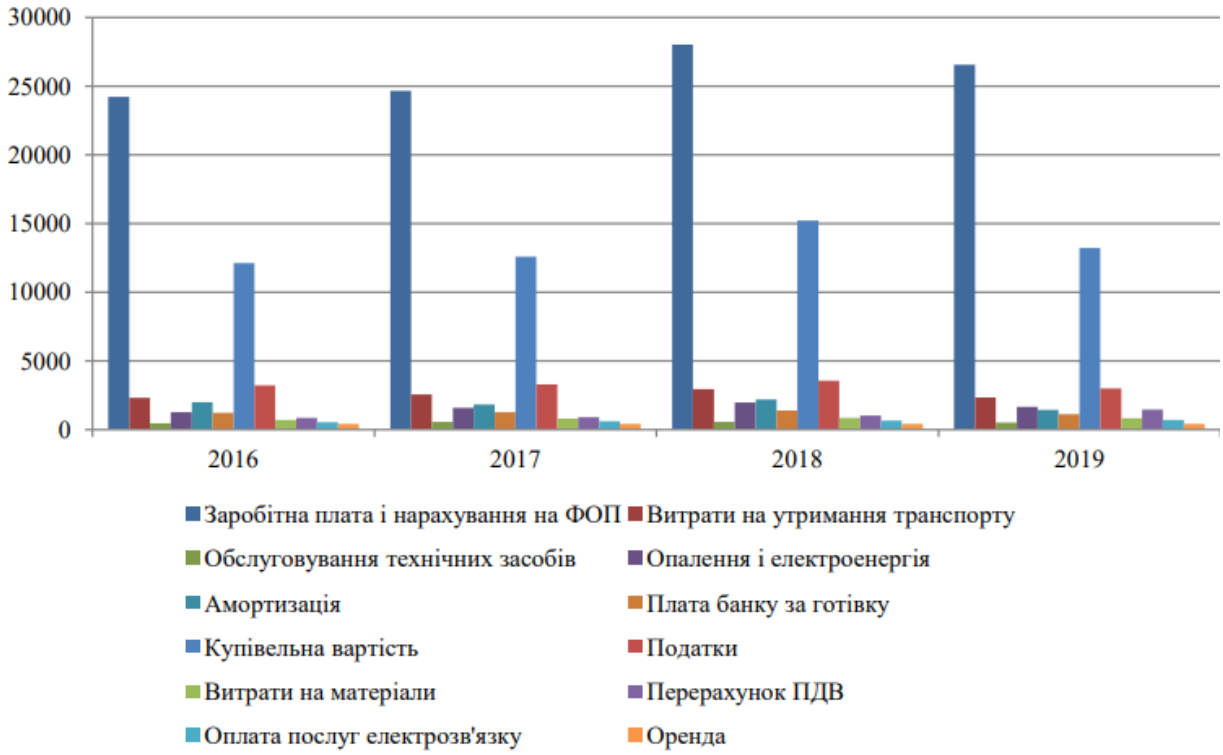


Рисунок 2.6 – Динаміка витрат ТОВ «Нова Пошта» за 2016–2019 рр. [29]

Таблиця 2.3

Показники доходу ТОВ «Нова Пошта» за 2017–2019 р., млрд. грн

млнд грн

Роки / Назва показника	2017	2018	2019
1	2	3	4
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	7,900	10,515	13,453
Валовий прибуток	1,700	1,964	2,948
Прибуток від операційної діяльності	570	493,7	1,024
Прибуток до оподаткування	500	510,6	868,3

Чистий прибуток	430	452,6	782,9

Примітка. Сформовано на основі [29]

Чистий прибуток компанії ТОВ «Нова Пошта» в 2019 році становив 782,954 млн грн, що на 72,97% більше порівняно з попереднім звітним 2018 роком та на 82,06% більше, ніж у попередньому 2017 році відповідно. Операційний прибуток компанії минулого року становив 1,024 млрд грн проти 493,746 млн грн роком раніше, а валовий – 2,949 млрд грн (1,965 млрд грн), данні свідчать про те, що компанія аналізує свою попередню діяльність та здійснює антикризове управління (рис. 2.7).

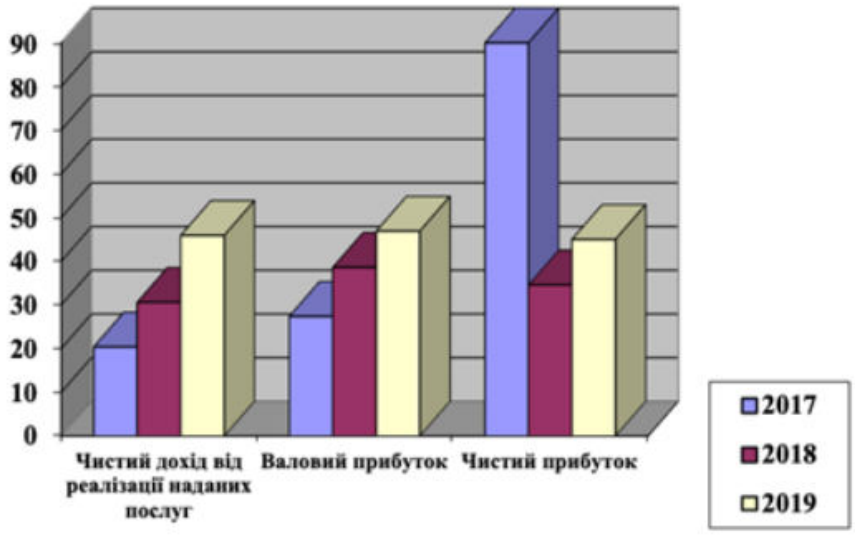


Рисунок 2.7 – Темпи зростання прибутковості ТОВ «Нова Пошта» за період 2017-2019 р.

Загальна сума витрат ТОВ «Нова Пошта» збільшилася на 2427,8 млрд. грн у звітному 2019 році у порівнянні із звітним 2018 роком, відповідно загальна сума витрат збільшилася у звітному 2019 році у порівнянні із звітним 2017 роком на 5074,6 млрд. грн. [37]. Основну частку в витратах компанії займають витрати на оплату праці та інші операційні витрати. Це абсолютно нормальний процес, наведені дані повністю відповідають загальному нарощуванню обсягів наданих послуг у звітному 2019 році, а також постійним збільшенням працівників компанії.

Показники економічної діяльності ТОВ «Нова Пошта» за період 2017 – 2019 р. подано у таблиці 2.4.

Таблиця 2.4

Основні економічні показники діяльності
ТОВ «Нова Пошта» за період 2017–2019 р.

Назва показника	Роки			Темп зростання 2018/2017, %	Темп зростання, 2019/2018, %
	2017	2018	2019		
1	*2*	*3*	*4*	*5*	*6*
Середньорічна вартість основних виробничих фондів, млрд. грн	355	475	1328	133,8	279,5
Середньорічна величина оборотних активів, млрд.грн	975	1650	2100	169,2	127,3
Фондовіддача	22,25	22,10	10,13	99,3	45,8
Рентабельність активів, %	22,6	18,1	15,1	80,1	83,4
Коефіцієнт оборотності оборотних активів	8,1	6,36	6,40	78,5	100,6
Рентабельність оборотних активів, %	35,0	29,0	34,2	82,6	117,9

Примітка. Сформовано на основі [29]

Всі показники рентабельності діяльності підприємства ТОВ «Нова Пошта» за 2017–2019рр. досить високі, що є позитивним фактором. Компанія щорічно нарощує обсяги наданих послуг, особливо за останній 2019 рік. Темпи зростання обсягу наданих послуг перевищують темпи зростання витрат, що є позитивним моментом в діяльності компанії й веде до зростання прибутку від наданих послуг. ТОВ «Нова Пошта» має резерви для збереження і зміцнення свого становища на ринку. Показники вартості оборотних активів значно збільшилися у звітному 2019р. році в порівнянні із звітними 2018р. та 2017р., що свідчить про розширення обсягів виробництва. Зниження показника рівня фондовіддачі було обумовлене значним зростанням вартості основних виробничих фондів у 2019 р. у порівнянні із звітними 2018р. та 2017р. Зниження показника фондовіддачі у 2019 році у порівнянні із 2018 та 2017 році було спричинено впровадженням нової техніки, вартість якої на одиницю продукцію вище, але експлуатаційні

витрати значно нижче і в цілому така техніка ефективніша, ніж стара, тому у цьому випадку падіння показника фондовіддачі виправдало та не несе негативну інформацію щодо динаміки успішної роботи підприємства. Показник рентабельності активів дає змогу зрозуміти – наскільки ефективно керівництво компанії розподіляє наявні активи для отримання максимального прибутку. Показник рентабельності оборотних активів достатньо високий та впевнено тримає своє середнє значення останні три роки роботи компанії. Це свідчить про те, що компанія дуже успішно генерує свої наявні оборотні активи для отримання прибутку.

Отже, за даними аналізу фінансово-господарської діяльності, було встановлено, що підприємство працює з високою рентабельністю. При цьому показники прибутку і рентабельності мають позитивну динаміку, що характеризує діяльність підприємства, як успішну. Організація є фінансово стійким, і не має труднощів з погашенням заборгованості. Показники абсолютної та поточної ліквідності компанії ростуть станом на 2019 рік, що говорить про те, що компанія має можливість не тільки погашати свої строкові зобов'язання, а й володіє значно вищими ресурсами, що можуть перекрити зобов'язання компанії перед кредиторами. Рівень ризику рентабельності активів компанії низький, компанія має високий прибуток з достатнім запасом міцності. Компанія не обтяжена високим рівнем кредиторської заборгованості, що говорить про те, що у разі необхідності компанія може залучити нові кредити, не обтяжуючи себе вже існуючими боргами.

2.3. Аналіз ризиків інформаційної безпеки на ТОВ «Нова пошта»

Оскільки, на підприємстві ТОВ «Нова Пошта» впроваджено електронний документообіг – це дає можливість співробітникам контролювати переміщення документів, зменшити надмірність даних на

паперових носіях, управляти збереженням і обробкою інформації. Всі ці фактори змушують працювати підприємство швидше і з більшою віддачою, підвищують ефективність його роботи. У той же час, при всіх перевагах, електронний документообіг створює нові ризики, і недбале ставлення до його захисту призводить до нових інформаційних загроз.

Загрози інформаційної безпеки для системи електронного документообігу є наступні:

загроза цілісності (її модифікація або знищення інформації);

загроза конфіденційності – це будь-яке недотримання правил розмежування доступу;

загроза доступності (працездатності системи) – різні загрози, здійснення яких призведе до порушення або зупинки роботи системи.

Під ризиком інформаційної безпеки вважають ймовірність того, що ця загроза зможе скористатися вразливістю активу або групи активів і тим самим завдасть збиток організації.

Існують різні методи оцінки ризиків інформаційної безпеки та управління ними [6].

Оцінка ризиків на підприємстві може бути виконана за наступним чином:

1. Оцінка активів – необхідно визначити, які ресурси потребують захисту, класифікувати їх.

2. Аналіз джерел проблем – побудова моделі порушника; побудова моделі загроз; ідентифікація вразливостей.

3. Оцінка ризиків – класифікуються результати попереднього етапу.

4. Прийняття рішення – базується на звіті про аналіз ризиків.

Після оцінки ризиків необхідно розробити раціональний комплекс засобів захисту, який забезпечить необхідний рівень інформаційної безпеки з повним перекриттям всіх виявлених загроз. Існують кількісні, якісні і змішані методи аналізу ефективності системи захисту інформації. У якості інструментальних засобів для аналізу та оцінки ризиків використовують:

CORAS, CRAMM, FRAP, RiskWatch, Microsoft Security Assessment Tool (MSAT), ГРИФ.

Пропонуємо, для аналізу ризиків використати розрахункову методику оцінки ризиків інформаційної системи, матричний підхід до аналізу ризиків.

Проведемо оцінку:

На першому етапі «Ідентифікація активів» - сформовано список активів організації. Процес збору адміністратором інформаційної безпеки даних, для аналізу ризиків, відбувався шляхом опитування співробітників підприємства. В якість активів ТОВ «Нова Пошта» було визначено: персональні дані, комерційна таємниця, електронні документи, електронна пошта, АРМ, бази даних, сервер. Таким чином, було сформовано (при зборі даних для аналізу ризиків за матричною методологією [1]) три матриці: матрицю вразливостей (містить зв'язок між активами і слабкими місцями в організації), матрицю загроз (відношення між слабкими місцями та загрозами), матрицю контролю (зв’язки між загрозами та засобами керування).

Значення кожної клітинки матриці показує оцінку відношення між елементом рядка і стовпця. В основному, використовують таку систему оцінок, як «низька», «середня» і «висока».

При формуванні номенклатури активів, слабких місць та загроз, було використано наступну шкалу оцінки взаємозалежностей активів (загроз) і слабких місць (вразливостей):

0 – немає впливу; 1 – слабкий вплив;

3 – помірний вплив; 9 – сильний вплив.

Ранжування пріоритету вразливостей проведено за наступною шкалою:

1 і 2 – неважлива;

3 – важлива, але не ключова;

4 – важлива, але знаходиться під впливом ключової;

5 – ключова.

Отже, отримані матриці активів та загроз ТОВ «Нова Пошта» наведені у таблицях 2.5–2.6.

Таблиця 2.5

Матриця активів

	Активи і витрати	Персональні дані	Комерційна таємниця	Електронні документи	Електронна пошта	ПК співробітників (АРМ)	Всього	Розряд
Уразливості, пріоритет - >		**5**	**4**	**3**	**2**	**1**		
Локальна обчислювальна мережа	**5**	3	3	3	0	0	36	**2**
База даних (БД)	**4**	9	3	9	0	0	84	**4**
Передача даних через інтернет	**5**	9	9	9	9	3	129	**5**
Перерва в подачі енергії	**2**	1	1	3	1	9	29	**1**
Апаратно-програмні збої	**3**	3	3	9	3	9	69	**3**
Людський фактор (помилки користувача)	**5**	9	9	9	9	9	135	**6**

Таблиця 2.6

Матриця загроз

	Уразливості	Людський фактор (помилки користувача)	Передача даних через Інтернет	Бази даних	Апаратно-програмні збої	Локальна обчислювальна мережа	Перерва в подачі енергії	Всього	Розряд
Уразливості, пріоритет ->		**6**	**5**	**4**	**3**	**2**	**1**		
Шкідливе програмне забезпечення	**4**	9	9	9	9	3	0	168	**5**
Втрата інформації (вірус)	**3**	9	9	9	3	1	0	146	**3**
Пожежа	**2**	1	0	3	0	1	3	23	**1**
Персонал	**5**	9	3	3	3	3	3	99	**2**
Хакерські атаки (перехоплення, спотворення, знищення, підміна маршрутів слідування інформації)	**4**	9	9	9	0	9	0	153	**4**

Сукупні дані про погрози і відповідні засоби управління додаються в матрицю контролю, представлену в таблиці 2.7

Таблиця 2.7

Матриця активів

Загрози	Шкідливе програмне забезпечення	Хакерські атаки	Втрата інформації (вірус)	Персонал	Пожежа	Всього	Розряд
Управлінські дії, пріоритет - >		**5**	**4**	**3**	**2**	**1**		
Електронний цифровий підпис	**5**	0	9	1	9	0	57	**6**
Парольний захист на ресурси	**5**	0	3	0	9	0	30	**4**
Використання ліцензійного ПЗ	**5**	9	1	1	1	0	54	**5**
Антивірусне ПЗ	**4**	0	0	3	9	0	27	**3**
Трудовий договір з пунктом про нерозголошення інформації	**4**	0	0	3	9	0	27	**3**
Маршрутизатор (роутер)	**3**	0	3	3	0	0	21	**2**
Протипожежна сигналізація	**3**	0	0	0	0	9	9	**1**

На другому етапі «Визначення ризиків невідповідності законодавству в області інформаційної безпеки». Присвоюється значення «1», якщо немає, то – «0». Всі вимоги, яким присвоєно значення «1», підсумовуються, інші значення не враховуються (табл. 2.8).

Отже, рівень ризику невідповідності вимогам до інформаційної безпеки на ТОВ становить $R_n = 0,25$ (табл. 2.9).

Таблиця 2.8

Ризик невідповідності законодавству в області інформаційної безпеки

Вимоги законодавства	Виконання вимог
1	2
Реєстрація в якості оператора персональних даних	1
Розробка і прийняття документів, що регламентують питання надання доступу і захист персональних даних	1
Оформлення допусків співробітників до персональних даних	0
Формування переліку оброблюваних персональних даних	1
Класифікація інформаційної системи обробки персональних даних	1
Підготовка інформаційної системи обробки персональних даних до атестації за вимогами безпеки	1
Вживання заходів щодо захисту персональних даних	1
Сертифікація системи захисту інформації у складі інформаційної системи обробки персональних даних	0
Сертифікація заходів системи захисту інформації у складі інформаційної системи обробки персональних даних	1
Встановлення вимог до надійності і безпеки використовуваних в інформаційних системах апаратних і програмних засобів	1
Перевірка на відповідність вимогам надійності і безпеки використовуваних в інформаційних системах апаратних і програмних засобів	1
Введення обмежень на придбання і використання окремих видів апаратних і програмних засобів в інформаційній системі	0
Технічні (в т.ч. програмні) засоби обмеження доступу в інформаційних системах не створювати загрозу або завдавати шкоди здоров'ю і майну інших осіб	1
Обов'язок щодо забезпечення конфіденційності відомостей, що становлять професійну таємницю	1
Всього	11

Таблиця 2.9

Значення ризику невідповідності вимогам законодавства

Сума виконаних вимог	Ризик невідповідності вимогам законодавств
13–14	0,01
8–12	0,25
Менше або рівне 7	0,5

Не виконуються	0,9

На наступному етапі розробляється модель загроз. Визначається ймовірність виникнення несприятливих подій і актуальність загроз інформаційної безпеки. По завершенню етапу формується список актуальних загроз на кожен актив або групу активів.

Таким чином, для ТОВ маємо наступний список актуальних загроз: шкідливе програмне забезпечення, втрата інформації через віруси, пожежа, персонал, хакерські атаки (перехоплення, спотворення, підміна, знищення, підміна маршрутів слідування інформації).

На останньому етапі – проводиться кількісна оцінка ризиків. Для цього:

1) обираються актуальні загрози – за допомогою моделі загроз складається список актуальних загроз. Ідентифіковані активи зіставляються з спрямованими на них погрозами;

2) визначаються ймовірності виникнення загроз. При цьому, на один актив можуть впливати одночасно декілька загроз. Тому, слід з'ясувати ймовірність того, що хоча б одна загроза реалізується по відношенню до заданого активу. Ймовірність реалізації хоча б однієї загрози з сукупності ймовірностей загроз $y_1, y_2, \ldots y_n$, де n – кількість загроз, дорівнює різниці між одиницею і добутком ймовірностей протилежних подій.

Отже, для ТОВ маємо наступні ймовірності реалізації актуальних загроз – таблиця 2.10.

Таблиця 2.10

Ймовірність реалізації актуальних загроз

Загроза інформаційній безпеці	Значення ймовірності реалізації загроз
Шкідливе програмне забезпечення	0,3
Втрата інформації через віруси	0,45
Пожежа	0,1
Персонал	0,75
Хакерські атаки (перехоплення, спотворення, підміна, знищення, підміна маршрутів слідування	0,65

інформації)	

Ймовірність реалізації хоча б однієї загрози зі списку актуальних загроз $R_{угр} = 0,9934$;

3) визначаються цінності активів – ця величина знаходиться в діапазоні від 0 до 1 (показує відношення ціни активів до вартості всього бізнесу).

Визначену оцінку для ТОВ – представлено у таблиці 2.11;

4) визначаються можливості застосування організаційних і технічних вразливостей. Ймовірність застосування організаційних вразливостей проводиться експертними методом. В процесі виконання аналізу всіх організаційних заходів, виконуваних, присвоюється значення «1», а тим, що не виконуються «0». Аналіз організаційних заходів захисту інформації ТОВ наведені у таблиці 2.12;

Таблиця 2.11

Оцінка цінностей компанії ТОВ «Нова Пошта»

Назва активу	Значення оцінки цінностей активу
Персональні данні	0,7
Комерційна таємниця	0,6
Електронні документи	0,55
Електронна пошта	0,5
АРМ	0,35
Бази даних	0,4
Сервер	0,45

Таблиця 2.12

Аналіз організаційних заходів захисту інформації

Організаційні заходи захисту інформації	Оцінка виконання організаційних заходів щодо захисту інформації
1	2
Організаційна інфраструктура інформаційної безпеки	1
Координація питань інформаційної безпеки	1
Розподіл обов'язків по забезпеченню	1

Організаційні заходи захисту інформації	Оцінка виконання організаційних заходів щодо захисту інформації
1	2
інформаційної безпеки	
Призначення відповідальних за кожен актив або процедуру безпеки	0
Отримання доступу до засобів обробки інформації з боку керівництва та адміністраторів засобів управління	1
Перевірка сумісності з іншим програмним забезпеченням і компонентами системи апаратних засобів	1
Співпраця організацій в області інформаційної безпеки	1
Незалежна перевірка (аудит) інформаційної безпеки	0
Включення вимог безпеки до договорів зі сторонніми особами та організаціями	0
Залучення сторонніх організацій до обробки інформації (Аутсорсинг)	0
Включення вимог безпеки за договором на аутсорсинг	0
Облік активів	1
Інвентаризація активів	1
Класифікація інформації	1
Облік питань безпеки в посадові обов'язки і при прийомі на роботу персоналу	1
Навчання користувачів	1
Контроль доступу до зони контролю	1
Управління передачею даних і операційною діяльністю	1
Безпека електронної пошти	0
Контроль доступу до інформації	1
Управління безперервністю бізнесу	0
Всього	14

Таким чином (табл. 2.13), коефіцієнт уразливості організаційних заходів захисту $K_o = 0{,}01$.

Таблиця 2.13

Ймовірність реалізації актуальних загроз

Сума заходів захисту, що виконуються	Коефіцієнт уразливості організаційних заходів захисту
14–17	0,01
9–13	0,25
Менше або рівне 8	0,5
Не виконуються	0,9

Оцінка технічних вразливостей проведено експертним методом, в ході якого були проаналізовані технічні заходи захисту інформації, які виконуються на ТОВ. В процесі виконання аналізу всім технічним заходам, виконуваних, присвоюється значення «1», які не виконуються «0». Аналіз результатів технічних заходів захисту інформації ТОВ «Нова Пошта» наведений у в таблиці 2.14.

Таблиця 2.14

Аналіз технічних заходів захисту інформації

Технічні заходи захисту інформації	Оцінка виконання технічних заходів захисту інформації
1	2
Реалізація дозволеної кількості допуску виконавців до інформації та документів у системі	1
Розмежування доступу користувачів і обслуговуючого персоналу до інформаційних ресурсів, програмних засобів обробки (передачі) і захисту інформації	1
Контроль за діями користувачів	0
Реєстрація дій користувачів інформаційної системи	1
Розв'язка ланцюгів електроживлення об'єктів захисту за допомогою захисних фільтрів, які блокують (пригнічують) інформативний сигнал	0
Використання захищених каналів зв'язку	0
Криптографічне перетворення інформації, що обробляється і передаються засобами	1

Технічні заходи захисту інформації	Оцінка виконання технічних заходів захисту інформації
1	2
обчислювальної техніки і зв'язку	
Запобігання впровадження в автоматизовані системи програм-вірусів	1
Запобігання впровадження в автоматизовані системи програмних вкладок	0
Всього	5

Таким чином (таблиця 2.15), коефіцієнт уразливості технічним заходам захисту $K_m = 0{,}5$;

Таблиця 2.15

Ймовірність реалізації актуальних загроз

Сума заходів захисту, що виконуються	Коефіцієнт уразливості технічних заходів захисту
11–12	0,01
7–10	0,25
Менше або рівне 6	0,5
Не виконуються	0,9

5) визначення чисельного значення ризику (рис. 2.16). Ризик реалізації хоча б однієї загрози з усього переліку актуальних загроз із урахуванням наявності вразливостей по відношенню до конкурентного активу визначається загальній формулі:

$$R = R_{угр} \cdot R_n \cdot C \cdot \frac{K_0 + K_t}{2} \cdot 100\%,$$

де R – чисельна величина ризику реалізації загроз інформаційної безпеки;

$R_{угр}$ – ймовірність реалізації хоча б однієї загрози з усього переліку актуальних загроз;

R_n – ризик невідповідності вимогам законодавства;

C – цінність активу;

K_0 – ймовірність використання організаційних вразливостей;

K_t – ймовірність використання технічних вразливостей.

Таблиця 2.16

Ризики реалізації загроз інформаційній безпеці для активів компанії ТОВ «Нова Пошта»

Назва активу	Значення ризику реалізації загроз інформаційній безпеці, %
Персональні данні	4,433
Комерційна таємниця	3,799
Електронні документи	3,483
Електронна пошта	3,166
АРМ	2,216
Бази даних	2,533
Сервер	2,849

На останньому етапі «Визначення допустимого рівня ризику», з таблиці 2.16 маємо значення ризику реалізації загроз інформаційній безпеці не менше 5%, це означає, що ризик реалізації загроз інформаційної безпеки є допустимим для всіх активів. Слід звернути увагу, що високий ризик реалізації загроз інформаційній безпеці, пов'язаний з персональними даними організації.

Таким чином, в результаті оцінки маємо список ранжируваних засобів контролю за підсумковим впливом на актуальні загрози інформаційної безпеки ТОВ «Нова Пошта».

Даний аналіз дозволяє врахувати засоби захисту, які необхідно тримати на постійному контролі для відстеження можливого впливу актуальних загроз на активи організації. Маємо зручні шаблони, які можливо поступово вдосконалюватися з збільшенням кількості доступної інформації; інструмент для проведення прозорого аналізу процесів, адаптуючись до постійно-мінливих загроз, уразливості та активам.

Таким чином, управління ризиками інформаційної безпеки дозволяє швидше реагувати на зміни в системі управління та контролювати ситуацію. Використання сучасних інструментів оцінки ризиків інформаційної безпеки

допомагає зміцнити «слабкі місця» в системі управління компанією та підвищити ефективність фінансово-господарської діяльності.

Аналіз ризиків інформаційної безпеки підприємства дозволить підтримувати дані про безпеки підприємства в актуальному стані, оперативно розробляти рекомендації щодо зниження рівня ризику і вживати ефективних заходів по усуненню можливих (або виявлених) загроз.

Висновок до розділу 2

Другий розділ дипломної роботи присвячено аналізу діяльності ТОВ «Нова Пошта». Охарактеризовано діяльність ТОВ «Нова Пошта». Відзначено, що ТОВ «Нова Пошта» – це: великий поштовий оператор зв'язку, який працює на ринку України в кожному регіоні; найбільш популярна транспортна українська компанія, що надає послуги з експрес-доставки документів, різних вантажів, а також посилок фізичних осіб та бізнес – посилок; є однім з найкрупніших роботодавців в Україні; має найсучасніші сортувальні термінали.

За даними аналізу фінансово-господарської діяльності, було встановлено, що підприємство працює з високою рентабельністю. При цьому показники прибутку і рентабельності мають позитивну динаміку, що характеризує діяльність підприємства, як успішну. Організація є фінансово стійким, і не має труднощів з погашенням заборгованості. Показники абсолютної та поточної ліквідності компанії ростуть станом на 2019 рік, що говорить про те, що компанія має можливість не тільки погашати свої строкові зобов'язання, а й володіє значно вищими ресурсами, що можуть перекрити зобов'язання компанії перед кредиторами. Рівень ризику рентабельності активів компанії низький, компанія має високий прибуток з достатнім запасом міцності. Компанія не обтяжена високим рівнем кредиторської заборгованості, що говорить про те, що у разі необхідності

компанія може залучити нові кредити, не обтяжуючи себе вже існуючими боргами.

Виконано аналіз ризиків інформаційної безпеки на ТОВ «Нова пошта». Встановлено, що оскільки, на підприємстві ТОВ «Нова Пошта» впроваджено електронний документообіг, то це дає можливість співробітникам контролювати переміщення документів, зменшити надмірність даних на паперових носіях, управляти збереженням і обробкою інформації. У той же час, при всіх перевагах, електронний документообіг створює нові ризики, і недбале ставлення до його захисту призводить до нових інформаційних загроз.

Проведено аналіз ризиків системи захисту інформаційної безпеки підприємства на основі матричного підходу. Даний аналіз дозволив врахувати засоби захисту, які необхідно тримати на постійному контролі для відстеження можливого впливу актуальних загроз на активи організації. Відзначено, що отримано зручні шаблони, які можливо поступово вдосконалюватися з збільшенням кількості доступної інформації; інструмент для проведення прозорого аналізу процесів, адаптуючись до постійно-мінливих загроз, уразливості та активам.

Розділ 3. Моделювання інформаційної безпеки

3.1. Методичні рекомендації щодо оцінювання стану інформаційної безпеки підприємства

Для забезпечення захисту інформаційного середовища підприємства необхідне систематичне виконання наступних етапів (рис. 3.1.):

аналіз загроз інформаційній безпеці;

планування та розробка заходів щодо забезпечення інформаційної безпеки;

оперативна реалізація запланованих дій.

Рисунок 3.1 – Схема функціонування системи інформаційної безпеки підприємства

Діагностику рівня інформаційної безпеки підприємства пропонується проводити за трьома ключовими напрямками (рис. 3.2): оцінка програмно-технічної захищеності інформації; оцінка інформаційної надійності персоналу; оцінка інформації, що надається особам, що приймають рішення, інформаційною службою підприємства.

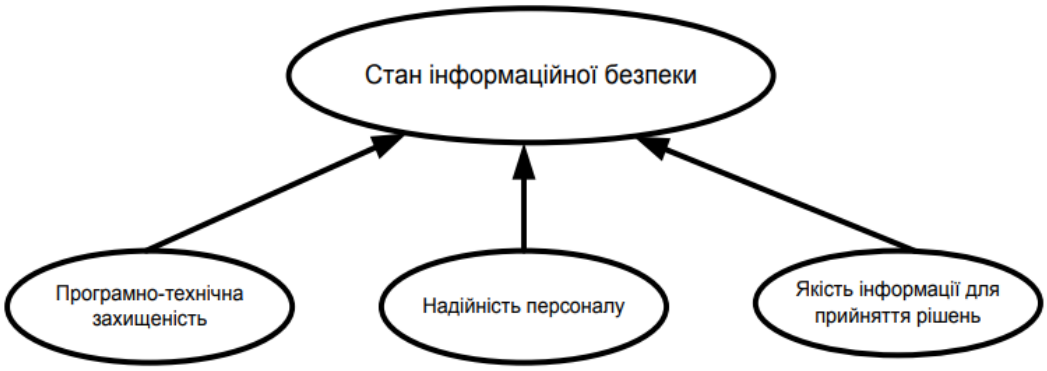


Рисунок 3.2 – Визначення стану інформаційної безпеки підприємства

У попередніх розділах було доведено, що кількісний аналіз та моделювання є тими інструментальними засобами, які дають змогу оцінити, виокремити, нехай і наближено, суттєві ризики з несуттєвих (надуманих). Однак у більшості випадків одного лише якісного аналізу недостатньо для ідентифікації та виокремлення суттєвих чинників ризику й нехтування несуттєвими (надуманими). З цією метою необхідно здійснювати кількісний аналіз небезпеки.

Методи експертних оцінок включають комплекс логічних і математико-статистичних методів і процедур, пов’язаних з діяльністю експерта по переробці необхідної для аналізу і прийняття рішень інформації. Центральною «фігурою» експертної процедури є сам експерт – це фахівець, який використовує свої здібності (знання, вміння, досвід, інтуїцію) для знаходження найбільш ефективного рішення.

Експерти, що залучаються для оцінки небезпеки, в тому числі і інформаційної, повинні: мати доступ до всієї наявної в розпорядженні розробника інформації; володіти достатнім рівнем креативності мислення та необхідними знаннями у відповідній предметній області; бути вільним від особистих переваг щодо проекту (не лобіювати його).

Методи експертних оцінок, що застосовуються для аналізу небезпеки: запитальники; SWOT-аналіз; роза і спіраль ризиків; оцінка ризику стадії проекту; метод Дельфі.

Інформація може існувати в самих різних формах. Її можна друкувати або писати на папері, зберігати на електронних носіях, пересилати за традиційною або електронною поштою, показувати у фільмах або передавати в усній розмові. Яку б форму не приймала інформація і які б кошти не використовувалися для її передачі та зберігання, необхідно завжди забезпечувати відповідний рівень її захисту.

Інформаційна безпека досягається шляхом впровадження сукупності необхідних засобів захисту, до числа яких можуть входити політики, рекомендації, інструкції, організаційні структури і програмні функції. Ці засоби необхідно реалізувати для того, щоб гарантувати виконання вимог до безпеки в конкретній організації.

У пункті 2.3 було виконано аналіз рівня інформаційної безпеки підприємства ТОВ «Нова Пошта», але пропонуємо до тієї методики ще використати наступну систему оцінки рівня інформаційної безпеки:

1. Оцінка програмно-технічної захищеності інформації:

Коефіцієнт технічного захисту інформації:

$$K_{ТЗ} = I \cdot A_{НВ}$$

де $I \cdot A_{НВ}$ - кількість не відвернутих інформаційних атак.

Коефіцієнт програмної захищеності інформації:

$$K_{ПЗ} = \frac{Ч_{бф}}{Ч_{нф}}$$

де $Ч_{бф}$ – час безперебійного функціонування корпоративної інформаційної системі, год.

$Ч_{нф}$ – нормативний час функціонування корпоративної інформаційної системи, год.

Коефіцієнт фінансового захисту інформації:

$$K_{фз} = \frac{В_{з.ін}}{В_{пр.ін}}, \qquad 0{,}15 - зростання,$$

де $В_{з.ін}$ – витрати на захист інформаційних ресурсів, грн.;

$В_{пр.ін}$ – витрати на придбання інформаційних ресурсів, грн.

Коефіцієнт фінансування інформаційних служб підприємства

$$К_{фін} = \frac{В_{фін}}{В_з}, \qquad 0{,}5 - 0{,}15 - зростання,$$

де $В_{фін}$ – витрати на фінансування інформаційних служб підприємства, грн.;

$В_з$ – загальні витрати підприємства.

2. Оцінка інформаційної надійності персоналу:

Коефіцієнт правової захищеності інформації

$$К_{пр.з} = \frac{I}{I_{юр.з}}, \qquad 1 - зменшення,$$

де I – обсяг інформації, розголошення якої може спричинити негативні наслідки для підприємства, %

$I_{юр.з}$ – загальний обсяг юридично захищеної інформації, %

Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства:

$$К_{д.р.} = \frac{ЧП_1}{ЧП_з}, \qquad 1 - зростання,$$

де $ЧП_1$ – чисельність працівників, які мають доступ до комерційної таємниці, що працюють на підприємстві більше одного року, ос.;

$ЧП_З$ – загальна чисельність працівників, що мають доступ до комерційної таємниці, ос.

Коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку підприємства:

$$К_{н.п.} = \frac{ЧПз.зв - ЧП_{вип}}{ЧП_{з.зв}.}, \qquad 1 - зростання$$

де $ЧП_{вип}$ – чисельність працівників, звільнених за причиною витоку інформації, ос.;

ЧПз.зв – загальна чисельність звільнених працівників, ос.

Коефіцієнт підготовленості персоналу до розпізнавання погроз:

$$K_{п.п.} = \frac{ЧПз. - ЧП_п}{ЧП_з.}, \qquad 1 - зростання$$

де $ЧП_п$ – чисельність працівників, ненавмисні дії яких призвели до витоку інформації завдяки низькому рівню підготовки персоналу до розпізнавання загроз безпеки, ос.;

ЧПз – загальна чисельність працівників, що мають доступ до закритої інформації, ос.

3. Оцінка інформації, що надається особам, що приймають рішення (ОПР), інформаційною службою підприємства:

Коефіцієнт повноти інформації:

$$K_{п.ін} = \frac{I_н}{I_{необ}}, \qquad 1 - зменшення$$

де $I_н$ – обсяг інформації, що є в розпорядженні ОПР, %;

$I_{необ}$ – обсяг інформації, необхідної для ухвалення обґрунтованого рішення, %

Коефіцієнт точності інформації:

$$K_{п.ін} = \frac{I_р}{I_н}, \qquad 1 - зростання$$

де $I_р$ – обсяг релевантної інформації, %

$I_н$ – загальний обсяг наявної в розпорядженні ОПР інформації, %

Коефіцієнт суперечливості інформації:

$$K_{с.ін} = \frac{I_{ухв}}{I_з}, \qquad 1 - зростання$$

де $I_{ухв}$ – кількість незалежних свідчень на користь ухвалення рішення, %;

$I_з$ – загальна кількість незалежних свідчень у сумарному обсязі релевантної інформації, %.

Коефіцієнт своєчасності надання інформації:

$$K_{с.н.ін} = \frac{I_{с.н.}}{I_{необ}}, \qquad 1 - зростання$$

де $I_{с.н.}$ – обсяг своєчасно наданої ОПР інформації, %;

$I_{необ}$ – обсяг інформації, необхідної для ухвалення обґрунтованого рішення, %

Коефіцієнт надійності інформації:

$$K_{н.ін} = \frac{I_{н.д.}}{I_{з.н.}}, \qquad 1 - зростання$$

де $I_{н.д.}$ – обсяг інформації, наданої ОПР з надійних джерел, %;

$I_{з.н.}$ – загальний обсяг наданої ОПР інформації, %

При цьому, будь-яка організація повинна визначити свої вимоги до безпеки. При оцінці вимог використовуються три основні показники.

Першим показником служить оцінка небезпек, з якими стикається організація. Шляхом оцінки небезпек визначаються загрози для інформації, її вразливість та ймовірність виникнення загроз, а також можливий збиток.

Другий показник - це законодавчі, нормативні та договірні вимоги, які повинна дотримуватися організація, її партнери по бізнесу, підрядники та постачальники послуг.

Третій показник – це певний набір принципів, цілей і вимог до обробки інформації, розроблених організацією для підтримки своєї діяльності.

Визначення вимог до безпеки проводиться шляхом методичної оцінки ризиків. Витрати на підтримку безпеки необхідно збалансувати з шкодою для бізнесу, який може виникнути при порушенні безпеки.

Методи оцінки небезпек можуть застосовуватися до всієї організації або лише до її частин, а також до окремих інформаційних системам, системних компонентів і сервісів, в залежності від того, що виявиться найбільш практичним, реалістичним і корисним.

Важливими методами аналізу стану забезпечення інформаційної безпеки є методи опису і класифікації. Для здійснення ефективного захисту системи управління інформаційною безпекою слід, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними.

У якості розповсюджених методів аналізу рівня забезпечення інформаційної безпеки використовуються методи дослідження причинних зв'язків. За допомогою даних методів виявляються причинні зв'язки між загрозами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи по їх нейтралізації. У числі даних методів причинних зв'язків можна назвати наступні: метод схожості, метод розбіжності, метод сполучення схожості і розбіжності, метод супроводжувальних змін, метод залишків.

Таким чином, змоделюємо систему захисту інформації на ТОВ «Нова Пошта».

3.2. Моделювання процесів системи захисту інформації на основі теорії графів і методології IDF0

Отже, в попередніх розділах було доведено, що серед найпоширеніших загроз інформаційній безпеці є: небажаний контент, несанкціонований доступ, витік інформації, втрата даних, шахрайство. При цьому найбільшу загрозу представляє крадіжка інформації, що вимагає впровадження системи безпеки інформації на підприємстві.

В основу створення системи захисту інформації покладемо такі теорії, як теорії ймовірностей і випадкових процесів; теорії графів, автоматів та мереж Петрі; теорія нечітких множин; теорії ігор та конфліктів; теорія катастроф; еволюційне моделювання; формально-евристичний підхід;

ентропійний підхід. При цьому, використаємо методи моделювання, заснованих на неформальній теорії систем, таких як методи структурування, методи оцінювання та методи пошуку оптимальних рішень.

Враховуючи роботу [41] система захисту інформації може бути представлена у вигляді орієнтованого графа, де вершинам відповідають компоненти інформаційної системи, а ребрам – інформаційні потоки між ними. При цьому використовують опис трактів проходження, де послідовно вказується джерело інформації, проміжна апаратура і одержувач інформації, а також вид переданої інформації. Таким чином, побудова матриць суміжності та інцидентності дозволяє визначити компоненти інформаційної системи, які обробляють інформацію різних рівнів конфіденційності з метою подальшого посилення захисту від потенційних загроз інформаційній безпеці.

Для моделювання системи захисту інформації з точки зору поточного опису процесів доцільно використовувати методології IDEF [54] – технологію опису бізнес-процесів в цілому як множини взаємозалежних дій або функцій. Отже, цей підхід дозволить провести передпроєктне дослідження процесів системи з необхідним рівнем деталізації для подальшого виявлення «вузьких» місць і розробити заходи для реінжинірингу відповідних процесів.

Процес забезпечення інформаційної безпеки розіб’ємо на такі підпроцеси:

аналіз вхідних даних,

розподіл за рівнями захисту інформації,

усунення загроз,

обробка інформації засобами для захисту інформації.

Далі, у рамках методології IDEF функціонування системи захисту інформації зручно зобразити як в нотації IDEF0, що дозволяє описати логічні відносини між окремими процесами системи (рис. 3.3).

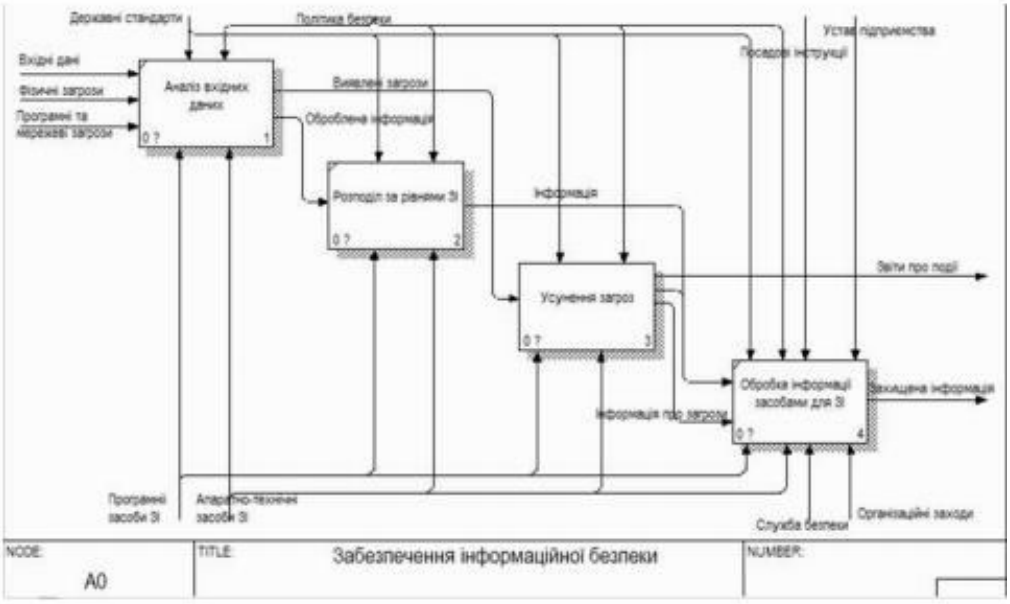


Рисунок 3.3 – Діаграма IDEF0 «Забезпечення інформаційної безпеки»

З точки зору розробки системи захисту інформації найбільш проблемним є процес «Усунення загроз» (рис. 3.4), який можна розбити на наступні підпроцеси: класифікація загроз за категоріями, розробка системи захисту інформації, реалізація системи захисту інформації, планові перевірки для виявлення загроз.

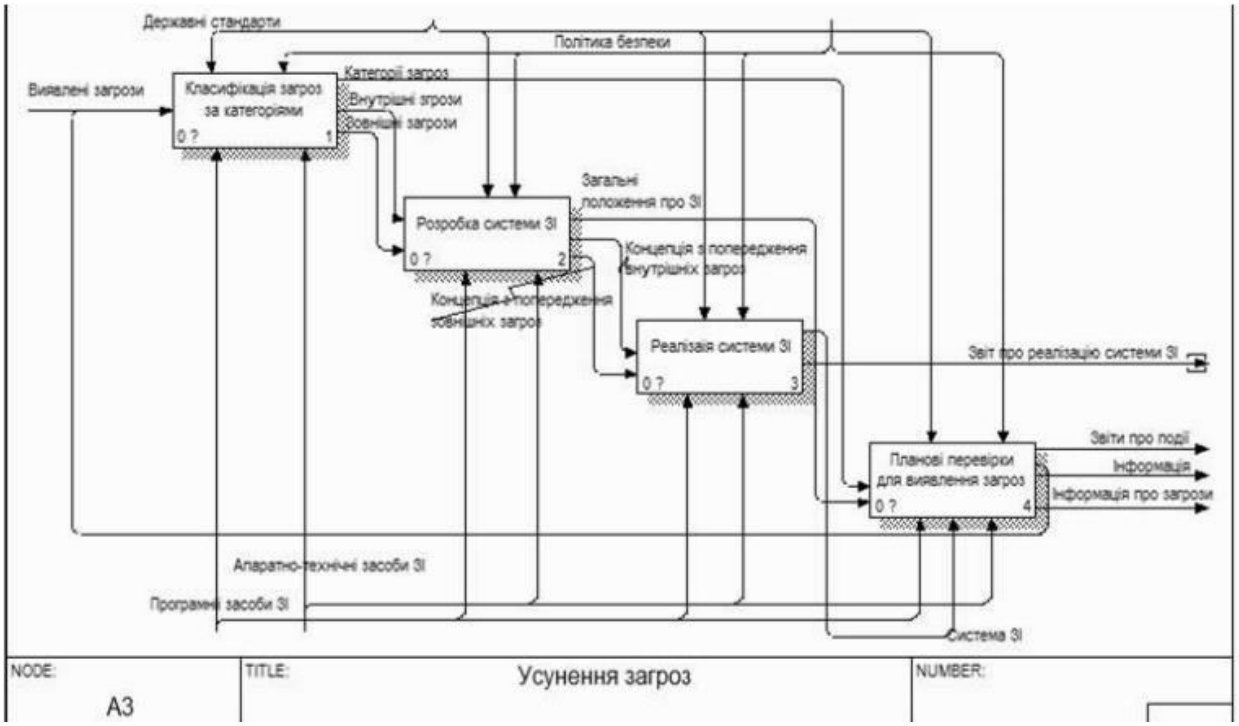


Рисунок 3.4 – Діаграма IDEF0 «Усунення загроз»

Розглянемо декомпозицію процесу «Розробка системи захисту інформації» із використанням теорії графів, а саме моделі системи захисту з повним перекриттям.

Модель системи захисту з повним перекриттям може бути представлена у вигляді трьох множин:

множини загроз $T = \{t_i\}$,

множини об'єктів захисту $O = \{o_j\}$,

множини механізмів захисту $M = \{m_k\}$.

Тобто систему захисту інформації можна зобразити як тридольний граф [20, с. 846–853]:

$$\{T,O,M\}. \quad (3.1)$$

Отже, враховуючи математичну модель (3.1) розіб'ємо процес «Розробка системи захисту інформації» на наступні підпроцеси (рис. 3.5):

визначення актуальних загроз – на виході отримуємо множину загроз $T=\{t_i\}$;

визначення інформаційних ресурсів для захисту – на виході отримуємо множину об'єктів захисту $O=\{o_j\}$;

визначення механізмів захисту інформації – на виході отримуємо механізмів захисту $M=\{m+\}$;

розробка документів, регламентуючих захист інформації;

створення цілісної системи захисту інформації.

Однак ця модель системи захисту інформації не враховує можливостей здійснення загроз для системи і шляхів захисту від них. Тому, в модель введемо ще два елементи:

Першим елементом є набір вразливостей $V=\{v_r\}$, що визначають можливість здійснення загрози T щодо об'єкту захисту O, визначається як:

$$\{T \cdot O\}: v_r = <ti,oj>. \quad (3.2)$$

Другим елементом є набір бар’єрів $B=\{b_l\}$, що визначають шлях здійснення загрози T, перекритий механізмом захисту M, визначається як:

$$\{V \cdot M\}: b_l = <t_i, o_j, m_k>. \quad (3.3)$$

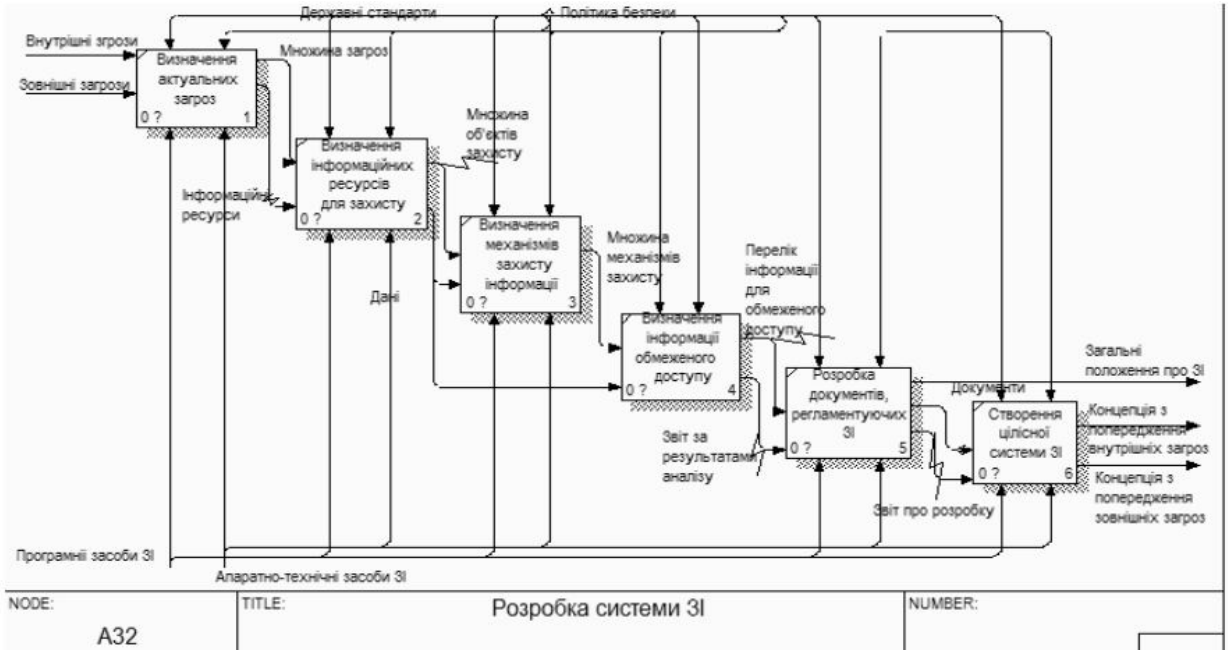


Рисунок 3.5 – Діаграма IDEF0 «Розробка системи захисту інформації» (AS-IS)

Таким чином, враховуючи (3.1) – (3.2) та [20] система захисту інформації може бути представлена моделлю, що складається з п'яти елементів:

$$\{T,O,M,V,B\}. \quad (3.4)$$

Отже, у такій системі для будь-якої уразливості існує бар'єр, який її усуває, тобто для всіх можливих загроз безпеці існують механізми захисту, що перешкоджають здійсненню цих загроз.

Також необхідно враховувати, що реальна система захисту інформації може забезпечити лише певний ступінь опірності загрозам безпеки. Тому, кожен елемент множини бар’єрів b_l поставимо у відповідний набір:

$$<P_l, L_l, R_l>, \quad (3.5)$$

де P_l – ймовірність появи загрози;

L_l – величина збитку при вдалому здійсненні загрози щодо об'єктів захисту;

R_l – ступінь опірності механізму захисту m_k, що характеризується ймовірністю його подолання.

Для оцінки проєктованої системи використаємо ще величину захищеності S, яка згідно з [20] розраховується за формулою (3.6):

$$S = 1/Risk_0, \tag{3.6}$$

де $Risk_0$ – сума всіх залишкових ризиків ($0<[P_k,L_k]<1$; $0<[R_k]<1$).

Залишкові ризики характеризують надійність кожного бар'єра і пов'язані з можливістю виконання загрози t_i щодо об'єкта захисту o_j при використанні механізму захисту m_k:

$$Risk_l = P_k L_k (1 - R_k). \tag{3.7}$$

Таким чином, враховуючи наведену математичну модель (3.7), сформуємо наступні заходи з реінжинірингу процесів системи захисту інформації, а саме процесу «Розробка системи захисту інформації»:

визначити вразливість системи, тобто можливість здійснення кожної загрози щодо кожного об'єкту захисту;

визначити бар'єри системи, тобто всі шляхи здійснення загрози, перекриті одним з механізмів захисту;

проаналізувати захищеність системи із урахуванням залишкових ризиків кожного бар'єру та їхньої сумарної величини.

Запропоновані заходи з реінжинірингу системи відображено на діаграмі IDEF0 «Розробка системи захисту інформації» для варіанта «TO-BE» (рис. 3.6).

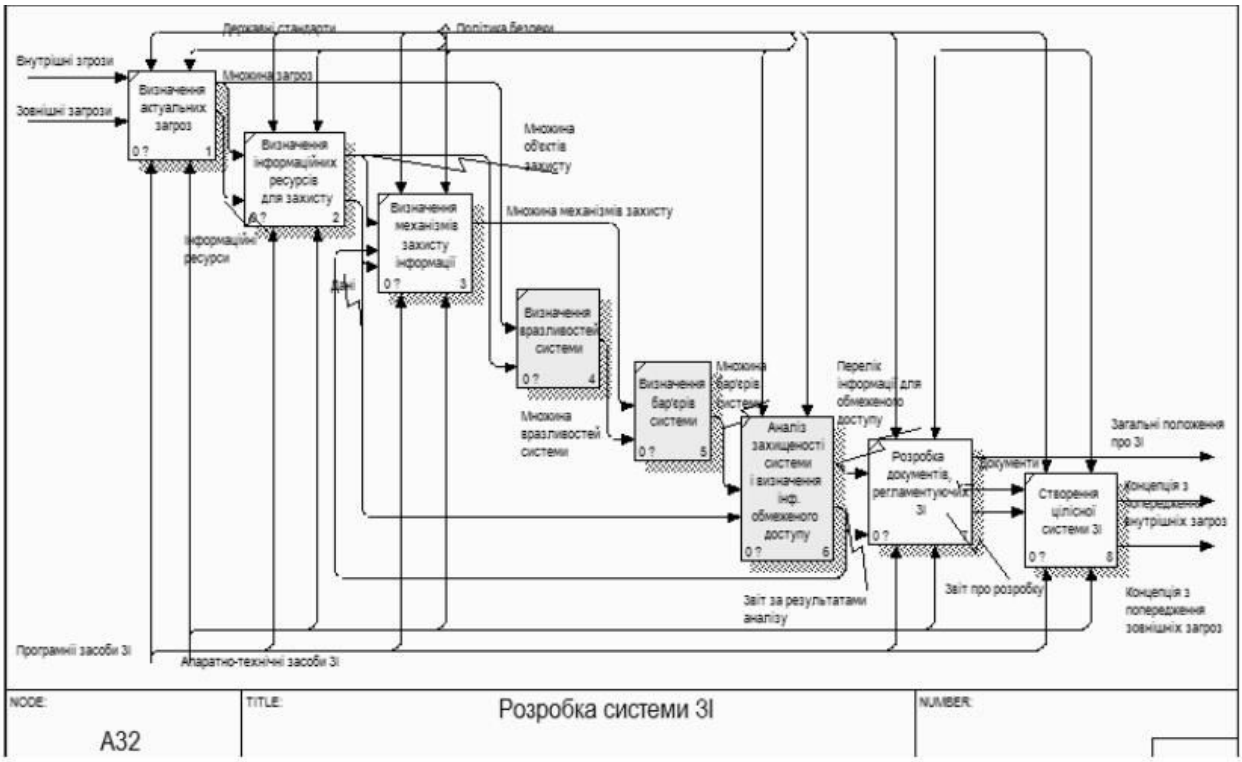


Рисунок 3.6 – Діаграма IDEF0 «Розробка системи захисту інформації» (TO-BE)

Таким чином, на основі використання теорії графів, а саме комбінації моделі системи захисту із повним перекриттям та ризик-орієнтованої моделі, було побудовано ефективну модель системи захисту інформації з використанням методології IDEF.

3.3. Обґрунтування економічної ефективності

Для визначення ефективності необхідно розрахувати:

– експлуатаційні витрати для зниження ризику за допомогою засобів захисту;

– витрати на інформаційну безпеку при застосуванні методу оцінки ризиків;

– можливі витрати на запровадження необхідних мір та зменшення ризику з можливими втратами;

Система вимог щодо зменшення ризику повинна бути настільки сповнена, щоб її виконання дозволяло повністю охоплювати усі можливі істотні ризики та загрози. Тільки в цьому випадку можна буде виміряти рівень довіри до безпеки використовуваної системи рівнем виконання вимог.

При виконанні системи вимог інформаційної безпеки необхідно враховувати виникнення наступних проблем:

– виконання всіх можливих вимог щодо забезпечення інформаційної безпеки може бути неможливо через занадто високу вартість їх реалізації;

– вимоги щодо безпеки можуть не виконуватися через відсутність досить ефективного контролю за виконанням вимог;

– вимоги можуть не виконуватися, оскільки вони погано засвоєні виконавцями.

У всіх трьох випадках контроль за виконанням вимог може дати великий позитивний ефект. Якщо частина вимог не може бути реалізована через нестачу коштів на їх реалізацію, контроль повинен дозволити не випускати з виду існуючі проблеми і вирішувати їх у міру появи коштів на підвищення інформаційної безпеки з урахуванням показників важливості вирішення зазначених проблем. При відсутності ефективного контролю за виконанням вимог з боку виконавців можуть проявлятися тенденції оптимізувати свою роботу за рахунок ігнорування деяких вимог з безпеки. Тому постійний контроль за виконанням вимог крім іншого покликаний переконати виконавців важливістю виконання вимог.

В системах, де організований контроль всіх вимог, як правило, крім великого числа інструкцій, наказів, законодавчих та підзаконних актів, в яких формуються вимоги, складаються списки вимог по підконтрольним структурам і процесам. Наявність такого роду списків дозволяє як контролерам, так і виконавцям швидше зрозуміти вимоги, швидше освоювати систему вимог і, відповідно, краще їх виконувати

Розрахунок витрат на впровадження системи управління ризиками інформаційної безпеки підприємства:

Обстеження підприємства:

В0 = 5000 грн.;

Проектування системи захисту:

В1= 5000 грн.;

Налаштування системи захисту:

В2 = 3000 грн.;

Розробка правил кореляції для сценаріїв виявлення інцидентів:

В3 = 4000 грн.;

Розробка регламенту реагування на інциденти безпеки:

В4 = 3000 грн.;

Розробка інструкцій оператора/аналітика/користувача:

В5 = 2000 грн.;

Вартість реалізації проекту рівна сумі наданих послуг і відповідно, розраховується за формулою:

В= В0+В1+В2+В3+В4 + В5 = 5000+5000+3000+4000+3000+2000=22000.

Отже, орієнтовна вартість реалізації проекту системи аналізу ризиків інформаційно безпеки: 22000 грн.

Висновок до розділу 3

Третій розділ дипломної роботи присвячено моделюванню інформаційної безпеки ТОВ «Нова Пошта». Запропоновано методичні рекомендації щодо оцінювання стану інформаційної безпеки підприємства.

На основі математичної моделі системи захисту з повним перекриттям проведено моделювання системи захисту інформації. Наведено удосконалену математичну модель, яка враховує вразливості та бар’єри системи, надані рекомендації з оцінки захищеності проектованої системи.

Запропоновано основні заходи з реінжинірингу процесів системи захисту інформації, які базуються на удосконаленій математичній моделі.

Побудовано діаграму забезпечення інформаційної безпеки та виконано її декомпозицію із використанням методології IDEF.

Виконано порівняльний аналіз діаграм для варіантів AS-IS та TO-BE.

Виконано обґрунтування економічної ефективності запропонованих дій. Отже, розрахунок витрат на впровадження системи управління ризиками інформаційної безпеки підприємства:

Обстеження підприємства: B0 = 5000 грн.

Проектування системи захисту: B1= 5000 грн.

Налаштування системи захисту:B2 = 3000 грн.

Розробка правил кореляції для сценаріїв виявлення інцидентів: B3 = 4000 грн.

Розробка регламенту реагування на інциденти безпеки: B4 = 3000 грн.

Розробка інструкцій оператора/аналітика/користувача: B5 = 2000 грн.

Отже, орієнтовна вартість реалізації проекту системи аналізу ризиків інформаційно безпеки: 22000 грн.

Висновки

У першому розділі роботи проаналізовано основні теоретичні положення інформаційної безпеки. Доведено, що інформаційну безпеку слід розглядати як забезпечення реалізації національних інтересів за допомогою різних засобів, що є в її розпорядженні. Відзначено, що зміст інформаційної безпеки ґрунтується на двох її аспектах: інформаційному та забезпечення захисту інформації. Наведено базові та функціональні ознаки забезпечення інформаційної безпеки підприємства. Наголошено, що інформаційна безпека виступає єдиним можливим напрямком для попередження нанесення збитків економічним інтересам підприємства шляхом організації захисту від існуючих і потенційних загроз інформаційних ресурсів підприємства.

Досліджено технологію забезпечення інформаційної безпеки підприємства. Доведено, що в сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки комплексною системою захисту інформації, яка повинна бути: безперервною, плановою, цілеспрямованою, конкретною, активною, надійною. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в критичних ситуаціях.

Розглянуто моделі інформаційної безпеки. Відзначено, шо структурна модель інформаційної безпеки передбачає, що рішення проблеми безпеки в інформаційних системах розподіленого типу полягає в аналізі наступних основних компонентів: визначення основних завдань захисту інформації, визначенні суб’єктів інформаційних процесів, класифікації основних можливих загроз безпеки, визначенні рівнів вразливості інформаційних систем, визначенні джерел інформації, ознайомленні з особливостями джерел загроз, дослідженні способів та напрямів захисту та цілей захисту. При цьому, забезпечення безпеки інформації полягає у вирішенні трьох

взаємопов'язаних завдань: збереженні конфіденційності, цілісності та доступності. Функціональна модель процесу інформаційної безпеки розглядає захист інформації як сукупність процесів. Захист інформації здійснюється відповідно до заздалегідь визначеної та постійно змінюваної мети захисту, яка пов'язана з затратами фінансових, енергетичних, трудових, матеріальних та інших ресурсів, з врахуванням обмежень зовнішнього середовища. Бажаний результат захисту інформації досягається більш ефективно, в тому випадку, якщо пов'язані ресурси і діяльність розглядаються і управляються як процес. Процес, як категорія, використовується як засіб структурування діяльності суб'єкту захисту інформації.

У роботі доведено, що створення системи інформаційної безпеки є масштабною роботою, яка вимагає серйозних зусиль. Тому, насамперед, необхідно найбільш точно визначити ризики, які існують для інформаційної безпеки підприємства, і не вживати додаткових заходів забезпечення безпеки, якщо це реально не відобразиться на підвищенні рівня зростання самого підприємства.

Виконано загальну характеристику та фінансовий аналіз результатів діяльності ТОВ «Нова Пошта». Відзначено, що ТОВ «Нова Пошта» – це: великий поштовий оператор зв'язку, який працює на ринку України в кожному регіоні; найбільш популярна транспортна українська компанія, що надає послуги з експрес-доставки документів, різних вантажів, а також посилок фізичних осіб та бізнес – посилок; є однім з найкрупніших роботодавців в Україні; має найсучасніші сортувальні термінали.

За даними аналізу фінансово-господарської діяльності, було встановлено, що підприємство працює з високою рентабельністю. При цьому показники прибутку і рентабельності мають позитивну динаміку, що характеризує діяльність підприємства, як успішну. Організація є фінансово стійким, і не має труднощів з погашенням заборгованості. Показники абсолютної та поточної ліквідності компанії ростуть станом на 2019 рік, що

говорить про те, що компанія має можливість не тільки погашати свої строкові зобов'язання, а й володіє значно вищими ресурсами, що можуть перекрити зобов'язання компанії перед кредиторами. Рівень ризику рентабельності активів компанії низький, компанія має високий прибуток з достатнім запасом міцності. Компанія не обтяжена високим рівнем кредиторської заборгованості, що говорить про те, що у разі необхідності компанія може залучити нові кредити, не обтяжуючи себе вже існуючими боргами.

Виконано аналіз ризиків інформаційної безпеки на ТОВ «Нова пошта». Встановлено, що оскільки, на підприємстві ТОВ «Нова Пошта» впроваджено електронний документообіг, то це дає можливість співробітникам контролювати переміщення документів, зменшити надмірність даних на паперових носіях, управляти збереженням і обробкою інформації. У той же час, при всіх перевагах, електронний документообіг створює нові ризики, і недбале ставлення до його захисту призводить до нових інформаційних загроз. Запропоновано аналіз ризиків системи захисту інформаційної безпеки підприємства провести на основі матричного підходу. Даний аналіз дозволив врахувати засоби захисту, які необхідно тримати на постійному контролі для відстеження можливого впливу актуальних загроз на активи організації. Відзначено, що отримано зручні шаблони, які можливо поступово вдосконалюватися з збільшенням кількості доступної інформації; інструмент для проведення прозорого аналізу процесів, адаптуючись до постійно-мінливих загроз, уразливості та активам.

Запропоновано методичні рекомендації щодо оцінювання стану інформаційної безпеки підприємства. На основі математичної моделі системи захисту з повним перекриттям проведено моделювання системи захисту інформації. Наведено удосконалену математичну модель, яка враховує вразливості та бар'єри системи, надані рекомендації з оцінки захищеності проектованої системи.

Запропоновано основні заходи з реінжинірингу процесів системи захисту інформації, які базуються на удосконаленій математичній моделі. Побудовано діаграму забезпечення інформаційної безпеки та виконано її декомпозицію із використанням методології IDEF.

Виконано порівняльний аналіз діаграм для варіантів AS-IS та TO-BE.

Виконано обґрунтування економічної ефективності запропонованих дій. Отже, розрахунок витрат на впровадження системи управління ризиками інформаційної безпеки підприємства: обстеження підприємства – 5000 грн., проектування системи захисту – 5000 грн., налаштування системи захисту – 3000 грн., розробка правил кореляції для сценаріїв виявлення інцидентів – 4000 грн., розробка регламенту реагування на інциденти безпеки – 3000 грн., розробка інструкцій оператора/аналітика/користувача – 2000 грн.. Отже, орієнтовна вартість реалізації проекту системи аналізу ризиків інформаційно безпеки становитиме – 22000 грн.

Отже, реалізація запропонованих заходів наддасть можливість поліпшити систему захисту на підприємстві; врахувати засоби захисту, які необхідно тримати на постійному контролі для відстеження можливого впливу актуальних загроз на активи організації.

Список використаної літератури

1. Goel, S., Chen, V. Information security risk assessment – a matrix-based approach. University at Albany. – SUNY. – 2005.

2. ISO/IEC 27035. Information technology. Security techniques. Information security incedent management. – 2011. – 78 p.

3. Y.1291: An architectural framework for support of Quality of Service in packet networks. – [Електронний ресурс]. – Режим доступу: http://www.itu.int/rec/ T-REC-Y.1291/en.

4. Y.1541: Network performance objectives for IP-based services. – [Електронний ресурс]. – Режим доступу: http://www.itu.int/rec/T-REC-Y.1541/en.

5. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій / Г.Я. Аніловська. [Електронний ресурс]. – Доступний з http://nbuv.gov.ua/portal/chem_biol/nvnltu/18_9/270_Anilowska_18_9.pdf.

6. Белов В.М. Методика оценки рисков информационной безопасности на предприятиях малого бизнеса / В.М. Белов, П.В. Плетнев // Доклады ТУСУРа. 2012. – № 1. – С. 83–86.

7. Бєгун А.В. Інформаційна безпека / А.В. Бєгун. – К. : Вид-во КНЕУ, 2008. – 280 с.

8. Борисов М.А. Основы программно-аппаратной защиты информации / М.А. Борисов, И.В. Заводцев, И.В. Чижов. – М .: Либроком, 2012.

9. Газизов А.Р. Концепция организационного построения защищенной информационной системы торгового предприятия / А.Р. Газизов // Вестник АГТУ. Сер. Управление, вычислительная техника и информатика. – 2018. – №2. – С. 110-115.

10. Галатенко В.А. Стандарты информационной безопасности / В.А.

Галатенко. – М.: Интернет-университет информационных технологий, 2006.

11. Гриджук Г.С. Систематизація методів інформаційної безпеки підприємства / Г.С. Гриджук. [Електронний ресурс]. – Доступний з http://www.nbuv.gov.ua/portal/natural/Vntu/2009_19_1/pdf/64.pdf.

12. Грицюк Ю.І. Особливості реалізації принципу розумної діагностики функціонування комплексної системи захисту інформації на підприємстві / Ю.І. Грицюк // Науковий вісник НЛТУ України. – 2015. – Вип. 25 (4) – С. 313–324.

13. Гуцу С.Ф. Правові основи інформаційної діяльності : навч. посіб. / С.Ф. Гуцу. – Х. : Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009. – 48 с.

14. Гуцу С.Ф. Правові основи інформаційної діяльності: навчальний посібник / С.Ф. Гуцу. – Х.: Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009. – 48с.

15. Дячков Д.В. Технологія забезпечення інформаційної безпеки підприємства / Д.В. Дячков, А.В. Паскаль, В.В. Кіт // Економічний форум. – 2018. – № 4. – С. 157–162. – Режим доступу: http://nbuv.gov.ua/UJRN/ecfor_2018_4_26.

16. Дячков Д.В. Формування моделі інформаційної безпеки / Д.В. Дячков [Електронний ресурс] – Режим доступу : http://dspace.pdaa.edu.ua:8080/bitstream/123456789/341/1/Diachkov%20_article%202017%20%283%29.pdf.

17. Євтушевська О.А. Інформаційна безпека як елемент підвищення ефективності комплексного контролю підприємств водного транспорту / О.А. Євтушевська // Зовнішня торгівля: економіка, фінанси, право. – 2015. - № 5–6 (82–83). – С. 157–162. – Режим доступу : http://zt.knute.edu.ua/files/2015/5-6%20(82-83)/18.pdf.

18. Жора Виктор. Комплексные системы защиты информации: быть или не быть? / Виктор Жора. [Электронный ресурс]. – Режим доступна : http://infosafe.ua/articles/article-6.html.

19. Забара І.М. Міжнародна інформаційна безпека в міжнародному

праві: до питання визначення / І.М. Забара // Український часопис міжнародного права. – 2012. – № 4. – С. 63-69.

20. Информатика : учебник / под ред. В. В. Трофимова. — М. : Издательство Юрайт ; ИД Юрайт, 2011. – 911 с.

21. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1 / С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с.

22. Кашпрук Н Міжнародна інформаційна безпека як актуальна проблема сучасності. – [Електронний ресурс]. – Режим доступу: http://naub.org.ua/?p=1050.

23. Кипарисов Г.Н. Обеспечение информационной безопасности в МБОУ СОШ №121 городского округа Самара / Г. Н. Кипарисов, О. Р. Загидуллина, О. Г. Корганова // Материалы X Всероссийской научно-технической конференции [Актуальные проблемы информационной безопасности. Теория и практика использования программно-аппаратных средств] (21-22 марта 2017 г., Самара) / Отв. редакторы А.И. Никонов, В.П. Свиридов. – Самара, Самар. гос. техн. ун-т, 2017. – С.23-25.

24. Конев И.Р. Информационная безопасность предприятия / И. Р. Конев, А. В. Беляев. – СПб. : БХВ-Петербург, 2003. – 747 с.

25. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: Монографія / Б.А. Кормич. – Одеса: Юридична література, 2003. – 472 с.

26. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. На здобуття наук. ступеня докт. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Б.А. Кормич ; Нац. ун-т внутр. справ. – Х., 2004. – 42 с.

27. Корнюшин П.Н. Информационная безопасность / П.Н. Корнюшин, С.С. Костерин. – Владивосток: ТИДОТ ДВГУ, 2003. – 154 с.

28. Крамаренко А.В. Удосконалення процесу підготовки та

прийняття управлінських рішень / А.В. Крамаренко, І.А. Алєксєєнко, М.О. Долинський // Східна Європа: економіка, бізнес управління. – 2019. – Вип. 2 (19). – С. 157–163. – Режим доступу : https://chmnu.edu.ua/wp-content/uploads/2019/07/Kramarenko-A.V.-Alyeksyeyenko-I.A.-Dolinskij-M.O..pdf.

29. Кропивка О.Г. Інформаційна безпека підприємства / О.Г. Кропивка // Економіка сьогодні: проблеми, моделювання та управління : матеріали X Всеукраїнської науково-практичної Інтернет - конференції (19–20 листопада 2020 року, м. Полтава). – Полтава : ПУЕТ, 2020. – Режим доступу : http://www.economicstoday2020.ukrbb.net/viewtopic.php?f=16&t=95.

30. Курилов, Ф. М. Моделирование систем защиты информации. Приложение теории графов / М. Ф. Курилов // Технические науки: теория и практика: материалы III Междунар. науч. конф. – Чита: Издательство Молодой ученый, 2016. – С. 6–9.

31. Литвиненко О.В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії): автореф. дис. на здобуття наук. ступеня канд. політ. наук: спец. 23.00.04. / О.В. Литвиненко. – К., 1997. – 18 с.

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

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

34. Мельников В.П. Информационная безопасность / В.П. Мельников, С.А. Клейменов, А.М. Петраков. – М.: Академия, 2012.

35. Нестеров А.К. Информационная безопасность предприятия: [Электронный ресурс]. – Режим доступа : http://odiplom.ru/lab/informacionnaya-bezopasnost-predpriyatiya.html.

36. Ольшанська О.В. Основні положення інформаційної безпеки та її

стан в сучасних умовах розвитку в Україні / О.В. Ольшанська // ВІСНИК КНУТД Економіка та управління підприємствами. – № 2 (85). – 2015. – С. 62–68. – Режим доступу : https://knutd.edu.ua/publications/pdf/Visnyk/2015-2/62-68.pdf.

37. Офіційний сайт компанії Нова Пошта в Україні URL: https://novaposhta.ua. (дата звернення: 20.04.2020).

38. Петраков А.В. Основы практической защиты информации : учеб. пособ. – М. : Изд-во "Радио и Связь", 2012. – 384 с.

39. Петров В.А. Информационная безопасность. Защита информации от несанкционирован- ного доступа в автоматизированных системах : учебн. пособ. / В.А. Петров, А.С. Пискарев, А.В. Шеин. – М. : Изд-во МИФИ, 2005. – 396 с.

40. Політична наука в Україні: стан і перспективи: матеріали всеукраїнської наукової конференції (Львів, 10-11 травня 2007 року) /Укл. Поліщук М., Скочиляс Л., Угрин Л. – Львів, ЦПД, 2008. – 308 с.

41. Попова М.С. Применение теории графов при выявлении потенциальных угроз безопасности информации / М.С. Попова, А.П. Карпов // Проблемы современной науки и образования. – 2016. – № 35 (77).

42. Потий А.В. Формальная модель процесса защиты информации / А.В. Потий // Радіоелектрон. і комп'ют. системи. – 2006. – №5. – С. 128-133.

43. Родичев А.Ю. Системная модель защиты информации информационных систем распределенного типа / А.Ю. Родичев, Ю.А. Родичев // Вестник СамГУ. Естественнонаучная серия. – 2003. – Второй спец. выпуск. – С. 15–20.

44. Саати Т.Л. Принятие решений при зависимостях и обратных связях: аналитические сети / пер. с англ. – Москва : ЛКИ, 2008. 360 с.

45. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки [Електронний ресурс]. – Режим доступу: http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.

46. Сороківська О.А. Інформаційна безпека підприємства : нові

загрози та перспективи / О.А. Сороківська, В.Л. Гевко // Вісник Хмельницького національного університету. – 2010. – № 2, т. 2. – С. 32–35.

47. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2 010_2_2/032-035.pdf.

48. Тацюра М.Ю. Проблемні аспекти стандартизації у галузі інформаційної безпеки підприємства // Матеріали Другої наук.-практ. конф. «Сталий розвиток та екологічна безпека суспільства в економічних трансформаціях» 23-24 вересня 2010 р., м. Бахчисарай, НДІ сталого розвитку та природокористування, РВПС України НАН України, Кримський інститут КНЕУ ім. Вадима Гетьмана / М.Ю. Тацюра. – Сімферополь: Фенікс, 2010. – С. 451–453.

49. Ткаченко В. Современные подходы к оценке рисков информационных технологий / В. Ткаченко, В. Сысоев // [Електронний ресурс]. – Режим доступу: https://studylib.ru/doc/2576904/sovremennye-podhody-k-ocenke-riskov-informacionnyh.

50. Фурашев В.М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки / В.М. Фурашев // Інформація і право: науковий журнал. – К.: НДЦПІ НАПрН України, 2012. – № 1(4). – С.46– 56.

51. Харченко Л.С. Інформаційна безпека України: Глосарій / Л.С. Харченко, В.А. Ліпкан, О.В. Логінов. – К.: Текст, 2004. – 136 с.

52. Цимбалюк В.С. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті / В.С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2004. – №8. – С.30–33.

53. Черевко О.В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту / О. В. Черевко. // Ефективна економіка. – 2014. – № 5. – Режим доступу: http://nbuv.gov.ua/UJRN/efek_2014_5_103.

54. Черемных С.В. Структурный анализ систем. IDEF-технологии / С.В. Черемных, И О.Семенов, В.С. Ручкин. – Финансы и статистика, 2003. — 208 с.

55. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: [учеб. пособ.] – М.: ИД «ФОРУМ»: ИНФРА-М, 2011. – 416 с.

Додатки