Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього ступеня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Розробка рекомендацій щодо оптимізації процесів з інформаційної безпеки невеликих підприємств»

Виконавець: студентка IV курсу, групи КБ-42

_____ **Єлизавета АНДРУЩЕНКО**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник	Микола БРАЇЛОВСЬКИЙ.	

Нормоконтроль	Сергій ДАКОВ.	

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідуюча кафедри кібербезпеки
та захисту інформації
_____ Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-42** **Єлизавети Олексіївни Андрущенко**
(група) (прізвище ім'я по батькові)

Тема дипломної роботи Розробка рекомендацій щодо оптимізації процесів з інформаційної безпеки невеликих підприємств

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Класифікація загроз, методи захисту від інцидентів безпеки на підприємстві, алгоритм оцінки ризиків, модель порушника, модель загроз

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно проаналізувати літературу з теми дослідження, розглянути основні проблеми захисту інформації, дослідити основні методи та види захисту, ознайомитися з нормативно-правовою базою, дослідити модель загроз та модель порушника, розробити рекомендації щодо оптимізації процесів інформаційної безпеки підприємства.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблені рекомендації щодо оптимізації процесів забезпечення інформаційної безпеки, що використовуються на підприємствах

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2021 року

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ім'я, прізвище)

Завдання прийняла до виконання _____ Єлизавета АНДРУЩЕНКО
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.10.2021 – 23.01.2022	*виконано*
2	Аналіз літератури за тематикою	24.01.2022 – 13.02.2022	*виконано*
3	Аналіз шляхів виникнення загроз та їх класифікація	14.02.2022 – 27.02.2022	*виконано*
4	Дослідження систем інформаційної безпеки	28.02.2022 – 13.03.2022	*виконано*
5	Аналіз існуючих методів захисту на підприємстві	14.03.2022 – 27.03.2022	*виконано*
6	Формування моделей порушника та загроз	28.03.2022 – 17.04.2022	*виконано*
7	Формування рекомендацій щодо оптимізації процесів інформаційної безпеки на підприємстві	18.04.2022 – 22.05.2022	*виконано*
8	Оформлення пояснювальної записки	23.05.2022 – 29.05.2022	*виконано*
9	Підготовка до захисту дипломної роботи	30.05.2020 – 14.06.2022	*виконано*

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Єлизавета АНДРУЩЕНКО
(підпис) (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Загальний обсяг дипломної роботи на тему «Розробка рекомендацій щодо оптимізації процесів з інформаційної безпеки невеликих підприємств» становить 67 сторінки і складається зі вступу, основної частини, що містить 3 розділи, висновків і списку використаних джерел та додатків. Робота містить 13 рисунків, 8 таблиць в основній частині роботи та 1 таблицю в додатках. Список використаних джерел включає 21 джерело.

Метою даної випускної кваліфікаційної роботи є розробка рекомендацій щодо побудови ефективного центру забезпечення інформаційної та кібербезпеки підприємства.

Об'єктом дослідження кваліфікаційної роботи є процес забезпечення інформаційної та кібербезпеки підприємства.

Предметом дослідження роботи є рекомендації щодо побудови ефективного центру забезпечення інформаційної та кібербезпеки підприємства**.**

При написанні роботи **були використані методи** аналізу, дослідження, порівняння, статистики.

Практичне значення отриманих результатів: розроблені рішення можуть бути застосовані на об'єктах, що потребують підвищеного захисту, забезпечення безпеки інформації та впровадження ефективних центрів з забезпечення інформаційної безпеки підприємства.

Ключові слова: розробка рекомендацій, рекомендації, загроза, класифікація загроз, система інформаційної безпеки, оцінка ризиків, модель загроз, модель порушника, аналіз захищеності системи, інформаційна та кібербезпека, аналіз інфраструктури, оптимізація процесів.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

IDS	–	Intrusion Detection System
IP	–	Internet Protocol
VPN	–	Virtual Private Network
АРМ	–	Автоматизоване робоче місце
АС	–	Автоматизована система
БД	–	База даних
ЗУ	–	Закон України
ІБ	–	Інформаційна безпека
ІС	–	Інформаційна система
ІТ	–	Інформаційні технології
КІ	–	Конфіденційна інформація
ОС	–	Операційна система
ПД	–	Персональні дані
ПЗ	–	Програмне забезпечення
ПК	–	Персональний комп'ютер
СКУД	–	Система контролю та управління доступом
ТЗ	–	Технічний захист

ЗМІСТ

ВСТУП

Інформація — це предмет захисту усіх інформаційних систем підприємства. Основними відмінностями інформації як ресурсу є її нематеріальність, неможливість виміряти її параметри за допомогою приладів чи фізичних методів, а спосіб її зберігання та передачі виконується із використанням матеріальних носіїв. Отримати інформацію людина може лише за обставин, якщо вона занесена у один з матеріальних носіїв, будь то мозок людини, електромагнітні та звукові хвилі, машинні, паперові чи інші носії інформації.

Інформації притаманні визначені властивості. З боку інформаційної безпеки більш важливими є конфіденційність, доступність та цілісність. В цей же час значущою властивістю є цінність та важливість інформації саме для її власника.

Більша частина інформації усіх рівнів конфіденційності на сучасних підприємствах та організаціях підлягає збору, зберіганню, обробці та передачі в комп'ютерних системах. Кількість організацій, що зараз використовує централізовані системи, невпинно знижається, адже у сьогоденні більш затребуваними є розподілені комп'ютерні системи.

Вищезазначені комп'ютерні системи мають в своєму складі чимало різноманітних програмних продуктів та інформаційних систем. Кожен із них, як компонент цілої системи, через притаманну йому вразливість, може становити загрозу безпеці всієї комп'ютерної системи. Інформація передається в розподілених системах по каналам зв'язку, які часто не є власністю організації. Саме отримавши до нього доступ, зловмисник має змогу дістатися ресурсів організації.

Діяльність із захисту інформації в організаціях дозволяє запобігти здійсненню втрат через витік інформації, ненавмисних чи несанкціонованих дій. Вона ґрунтується на програмі інформаційної безпеки підприємства та створенні ефективних центрів, що працюють заради забезпечення інформаційної та кібернетичної безпеки. Програма інформаційної безпеки описує вимоги й

принципи систем, що захищають інформацію. До системи захисту включені правові норми, організаційні, технічні, програмні й криптографічні засоби, методи та механізми, що забезпечують інформаційну безпеку. Вся вказана діяльність спрямована на забезпечення критеріїв конфіденційності, цілісності й доступності одночасно.

Актуальність проблеми, що розглядається в рамках даної роботи, спричинена потребою в захисті інформації, створенні ефективних центрів забезпечення інформаційної та кібернетичної безпеки організації, розробці інженерних і організаційних заходів, що зможуть протистояти ймовірним загрозам та порушникам.

Створення ефективних центрів має на меті модернізацію політики безпеки, що наразі існує, та пояснюється пріоритетністю інформаційних відносин різного змісту в сучасних реаліях.

Мета даної випускної кваліфікаційної роботи — розробка рекомендацій **щодо побудови ефективного центру забезпечення інформаційної та кібербезпеки підприємства.**

При написанні роботи були встановлені **наступні задачі:**

1. Проаналізувати літературу з теми дослідження. Поглиблено розглянути основні проблеми захисту інформації на підприємствах та показати актуальність забезпечення інформаційної та кібербезпеки підприємства;

2. Охарактеризувати можливі методи і види захисту та нормативно-правову базу, на яку вони мають спиратися;

3. Розглянути модель загроз і порушника інформаційної та кібербезпеки підприємства;

4. На основі розробленої моделі загроз і порушника розробити рекомендації щодо побудови ефективного центру забезпечення інформаційної та кібербезпеки підприємства, а також навести приклад обладнання, яке можна використовувати для захисту інформації.

Об’єктом дослідження кваліфікаційної роботи є забезпечення інформаційної та кібербезпеки підприємства.

Предметом дослідження роботи є рекомендації щодо побудови ефективного **центру забезпечення інформаційної та кібербезпеки підприємства**.

Під час написання роботи були використані наступні методи: аналіз, порівняння, дослідження, статистика.

Наукова новизна отриманих результатів є в тім, що було отримано можливості подальшого розвиток рекомендацій щодо побудови ефективного **центру забезпечення інформаційної та кібербезпеки підприємства.**

Практичне значення результатів, що були отримані в ході роботи: розроблені рішення можуть застосовуватися на об’єктах, що потребують захисту й покращення процесів задля зменшення ризиків виникнення інцидентів безпеки.

РОЗДІЛ 1
ІСНУЮЧІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ НА ПІДПРИЄМСТВІ

1.1 Причини виникнення загроз та появи вразливостей системи захисту

Через зростаючу роль інформаційних ресурсів в житті суспільства сьогодення реальність загроз з боку їх безпеки проблема безпеки інформації потребує постійної уваги. Систематичність впливу на інформаційну безпеку, яка полягає у сукупності різноманітних обставин різної фізичної природи, що переслідує різні цілі й спричинює різні наслідки, призводить необхідності комплексного розгляду цієї проблеми.

Комерційна (підприємницька) діяльність тісно сполучена із різноманітною роботою з інформацією (отримання, накопичення, зберігання, обробка та використання різних інформаційних потоків). Проте підлягає захисту не всі дані, а лише цінна для підприємця інформація. При визначенні цінності отриманої ділової інформації, необхідно орієнтуватися на її користь, своєчасність, достовірність.

Заходи щодо збереження ділової таємниці підприємства повинні розроблятися відповідно до принципу усестороннього перекриття ймовірних шляхів витоку інформації та забезпечення однакової безпеки захисту всіх його носіїв інформації. Загроза секретності може бути зовнішньою та внутрішньою (рис.1.1).

Оцінюючи загрози інформаційній безпеці та обираючи пріоритети в системі захисту підприємств, слід застосовувати практику захисту інформації та безпеки діяльності різних організацій – державних і комерційних банків, великих фірм, промислових підприємств, а також враховувати наявний міжнародний досвід вирішення подібних проблем.

Поняття інформаційної безпеки можна розглядати як широко, так і вузько. Інформаційна безпека (у вузькому розумінні) є необхідною, але невід'ємною

частиною інших видів безпеки. Інформаційна безпека є частиною політичної, економічної, військової, соціальної та інших складових національної безпеки.

Рисунок 1.1 – Загрози збереження комерційної таємниці

Інформаційна безпека у галузі інформатизації закріплена на законодавчому рівні Законом України «Про Національну програму інформатизації»

За ним, інформаційна безпека забезпечується наступним:

1. Сукупністю нормативних документів, що стосуються усіх аспектів використання засобів обчислювальної техніки при обробці та зберіганні інформації із обмеженим доступом;

2. Набором державних стандартів на технічне обслуговування, документацію, застосування, сертифікаційне тестування ПЗ (програмного забезпечення) захисту інформації;

3. Банком інструментів, що можуть використовуватися задля діагностики, локалізації чи профілактики комп'ютерних вірусів, нових технологій захисту даних із застосуванням спектральних методів, надзвичайно надійних криптографічних методів в сфері захисту інформації та ін.

Щодо розповсюдження інформаційних впливів, діє наступне визначення: інформаційна безпека – це стан інформаційної (моральної, етичної, політичної, духовної чи інтелектуальної) зброї людей, суспільства чи держави в цілому, де жодна інформація не впливає на власника в негативному сенсі, не викликає руйнівні думки та дії, які можуть призвести до негативних наслідків, особливо на шляху до стабільного прогресивного розвитку.

Інформаційна безпека також розглядається, як «…єдність концептуальних, теоретичних і технологічних основ забезпечення на інформаційному рівні безпеки всіх сфер державної і суспільної діяльності (політичної, економічної, соціальної, воєнної, екологічної, духовної та ін.), а також сфер формування, обігу, накопичення і використання інформації (інформаційний простір, інформаційні ресурси, інформаційно-аналітичне забезпечення органів державного управління у всіх різновидах діяльності тощо)»

Для комерційних підприємств, найбільше підходить визначення в організаційно-управлінському плані дане поняття розглядається як «…стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій Загрози інформаційній безпеці можуть надходити з різних джерел та через різні мотиви, основними з яких є фінансова вигода або помста. У випадку фінансового інтересу загрозі підлягають

фінансові дані різного роду такі як загальні фінансові деталі бізнесу, дані клієнтів (наприклад, дані кредитних карток), конфіденційні персональні дані (електронні адреси співробітників та клієнтів, облікові дані для входу у внутрішні системи підприємства), бази даних клієнтів, IT-послуги (наприклад, можливість безпечно приймати онлайн-платежі), певна інтелектуальна власність, тощо. У випадку помсти, як мотивації, загрозі можуть підлягати всі ті самі елементи, що і при фінансовому інтересі, але кінцевою метою замість особистого збагачення виступає нанесення максимально можливих збитків підприємству. Найчастіше, до помсти вдаються колишні ображені працівники або партнери по бізнесу.

Окрім вказаного, інші мотиви можуть включати шпигунство, з метою отримання конкурентної переваги; хактивізм (внесення соціального або політичного контексту до діяльності підприємства) або інтелектуальний виклик (біле хакерство).

Також поняття інформаційної безпеки характеризує стан (власність) інформаційної безпеки людей та усього суспільства, природи перед можливими загрозами, якого можливо досягти завдяки системі заходів, що спрямовані на запобігання та виявлення можливих загроз.

Попередження загроз – це сукупність превентивних заходів задля забезпечення інформаційної безпеки, що попереджають можливість їх виникнення.

Для виявлення загроз необхідні наступні кроки:

1. Систематичний аналіз та контроль ймовірності виникнення реальних чи потенційних загроз та своєчасних заходів, спрямованих на їх попередження;

2. Локалізація злочинних дій, вжиття заходів по ліквідації загрози чи певних злочинних дій;

3. Ліквідація наслідків загроз інформаційній безпеці чи злочинів.

Головним об'єктом, на який впливають ці загрози, є інформація, яка обробляється автоматизованими системами установи. Основою автоматизованих систем (АС) є: системне програмне забезпечення, програмні оболонки, додатки загального призначення, інтегровані програмні пакети, текстові процесори та редактори. Системи управління БД грають окрему роль в системному програмному забезпеченні.

Інформація в АС може надходити з автоматизованого робочого місця (далі – АРМ) локальної мережі по внутрішнім і по зовнішніх каналах зв'язку, при цьому інформація може вводитися як з клавіатури, так і з зовнішніх носіїв інформації. Крім того, АС може використовувати інформаційні ресурси інших установ і організацій та ресурси глобальних телекомунікаційних мереж. До користувачів АС відносяться всі зареєстровані в ній особи (організації), наділені певними повноваженнями доступу. В рамках своїх повноважень користувач може здійснювати тільки дозволені йому дії з використанням загальносистемного і прикладного ПЗ.

До користувачів автоматизованих систем відносяться всі особи чи організації, що були зареєстровані в ній, які мають певні повноваження доступу. Користувач може виконувати лише ті дії, дозволені ним за допомогою системного та прикладного програмного забезпечення, тобто виключно в межах своїх повноважень.

Обробка інформації в автоматизованій системі проводиться в умовах контролю системних адміністраторів, а її захист контролюється адміністраторами безпеки.

1.2 Класифікація основних загроз на підприємстві

Загроза – комплекс чинників та обставин, які виникають під час взаємодії об’єкта безпеки з іншими об’єктами, та складових її компонентів стосовно один одного та здатних впливати на неї негативно. Він виступає як можливість вирішити певні протиріччя, що виникають під час взаємодії об’єкта безпеки з другими об'єктами чи компонентами об'єкта безпеки в стадії дисгармонії або при конфлікті, що завдає шкоди.

Сприймаючи інформаційну безпеку як стан безпеки інформаційного середовища людства, яке забезпечує її створення, застосування та покращення на користь громадян, організацій, доцільно визначати ймовірні загрози, їх джерела, способи їх реалізації та призначення, а також інші умови та дії, що порушують

безпеку. Звичайно, слід також розглянути заходи щодо захисту інформації від шахрайських дій, які завдають шкоди.

Між загрозою та небезпекою заподіяння шкоди завжди існують відносини заподіяння, які визначаються як спричинені суттю взаємодіючих об'єктів, елементами системи, взаємозв'язком між явищами, у яких одне явище, назване причиною, за наявності певних умови неминуче породжують інше явище — слідство.

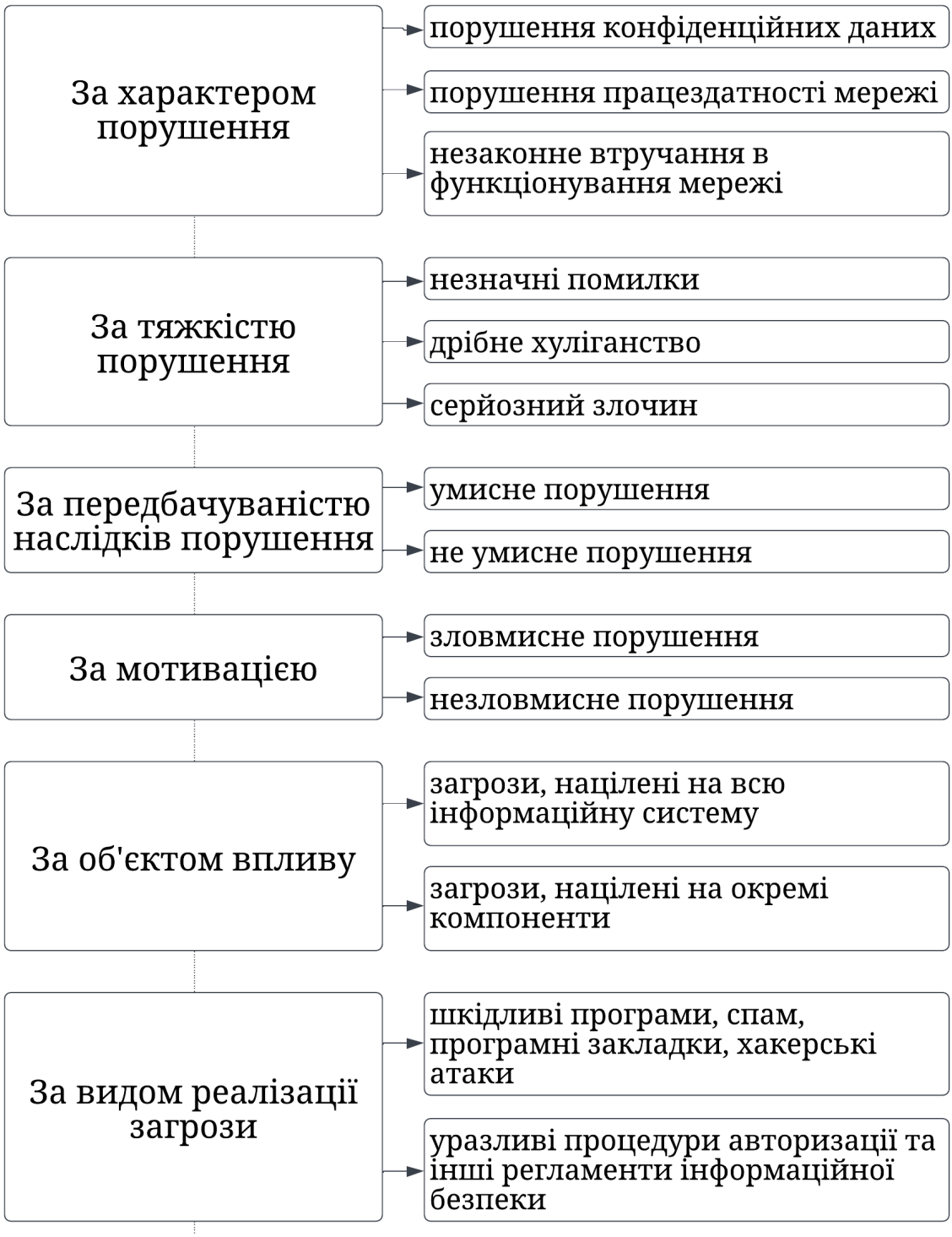
Загроза завжди створює небезпеку. Останню можна визначити як становище, в якому об’єкт безпеки обумовлений загрозою. Різниця між ними полягає в тому, що небезпека — це властивість об’єкта безпеки, а власне загроза являє собою властивість об'єкта взаємодії чи взаємодіючих елементів об'єкта безпеки, що виступають джерелом загроз. Загроза пов'язана як з небезпекою, так і з очікуваною у майбутньому від неї шкодою, тобто наслідками негативних змін, що потрібно подолати, щоб відновити необхідні умови. Ймовірна шкода визначає масштабі небезпеки.

Всі джерела загроз безпеці інформації організації розподіляються на антропогенні, техногенні та стихійні (рис.1.2).

Рисунок 1.2 – Джерела загроз безпеки інформації підприємства

«Загрози інформаційній безпеці - це можливі дії або події, які можуть вести до порушень ІБ. Види загроз інформаційній безпеці дуже різноманітні і мають безліч класифікацій» (рис.1.3)

Відповідно до вищезазначеної класифікації загроз за типом об’єкта впливу, загрози в подальшому розподіляються на спрямовані на фактичну інформацію, особовий склад об’єкта чи діяльність, що забезпечує інформаційну безпеку об’єкта. Під час детальнішого розгляду інформаційних загроз, вони також диференціюються на загрози в адресу носіїв конфіденційної інформації чи місця їх локації, канали передачі (системи обміну інформацією), а також інформацію, яка зберігається в електронній формі на будь-яких носіях інформації.


За характером порушення
порушення конфіденційних даних
порушення працездатності мережі
незаконне втручання в функціонування мережі
За тяжкістю порушення
незначні помилки
дрібне хуліганство
серйозний злочин
За передбачуваністю наслідків порушення
умисне порушення
не умисне порушення
За мотивацією
зловмисне порушення
незловмисне порушення
За об'єктом впливу
загрози, націлені на всю інформаційну систему
загрози, націлені на окремі компоненти
За видом реалізації загрози
шкідливі програми, спам, програмні закладки, хакерські атаки
уразливі процедури авторизації та інші регламенти інформаційної безпеки

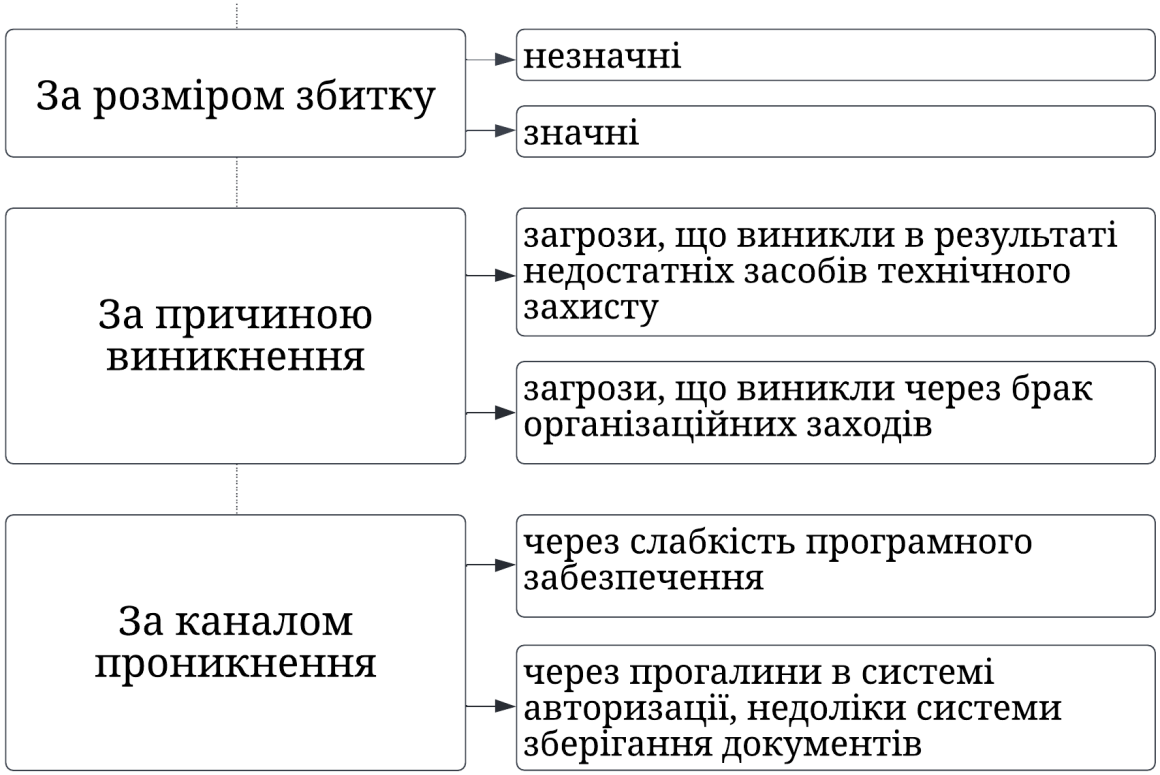


Рисунок 1.3 – Класифікація загроз інформаційної безпеки

Класифікація загроз за характером порушення — рис. 1.4.

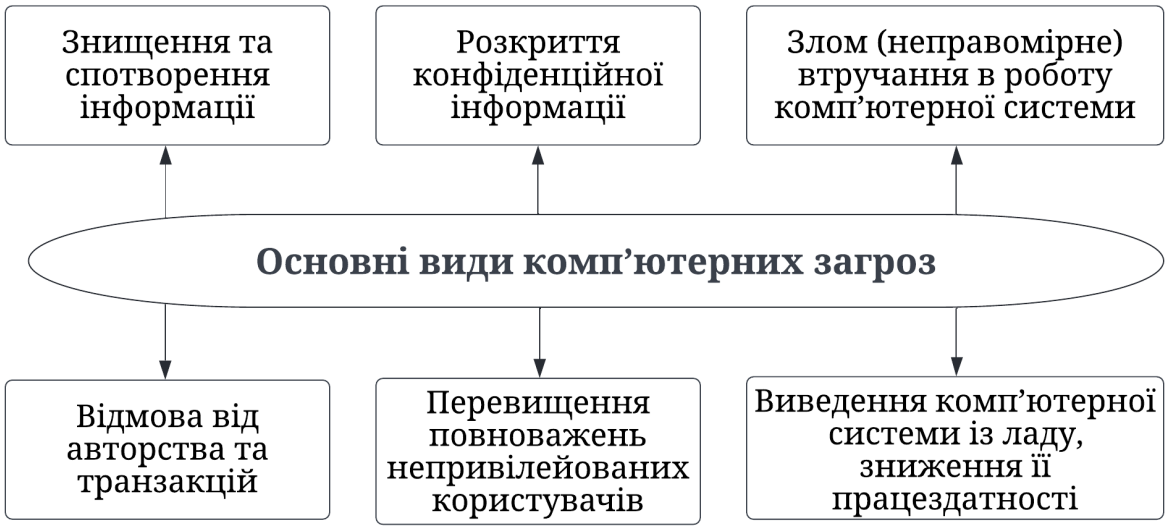


Рисунок 1.4 – Типи загроз інформаційної безпеки за характером порушення

Виходячи із зазначеного можна стверджувати: дія загроз інформаційній безпеці об'єкта направлено на створення можливих каналів витоку інформації, що захищається (передумов до її витоку) і безпосередньо на витік інформації.

Однією з ключових концепцій оцінки ефективності загрози інформаційній безпеці є пошкодження цього об’єкта (підприємства) внаслідок впливу загроз. По суті, будь-яка втрата, її визначення та оцінка мають чітку економічну основу. Пошкодження інформаційної безпеки об'єкта (підприємства) не є винятком.

З погляду економічного підходу, загальна втрата інформаційної безпеки підприємства складається з двох компонентів: прямої та непрямої шкоди. Пряма втрата інформаційної безпеки підприємства виникає внаслідок витоку конфіденційної інформації. Непрямі збитки – збитки, понесені підприємством через обмеження розповсюдження інформації у встановленому порядку, класифіковані як конфіденційні. Опис збитків, заподіяних підприємству внаслідок витоку конфіденційної інформації, ґрунтується на його кількісних та якісних показниках, які ґрунтуються на одному з принципів класифікованої інформації (класифікуючи її як конфіденційну) – принципі дії. Він полягає у встановленні (за допомогою експертних оцінок) доцільності класифікації конкретної інформації, а також ймовірних наслідків цих дій з урахуванням поставлених підприємством завдань та завдань.

Введення обмежень на розповсюдження інформації (у зв'язку з її класифікацією як конфіденційної) призводить як до позитивних, так і до негативних наслідків. Основними позитивними наслідками є запобігання можливої прямої втрати інформаційної безпеки підприємства через витік захищеної інформації.

Негативні наслідки пов'язані з наявністю (ймовірним збільшенням) непрямого збитку або витрат у вигляді витрат на захист інформації та вартості втрачених прибутків, які можуть бути отримані шляхом її відкритого розповсюдження.

1.3 Складові системи інформаційної безпеки підприємства

В теперішній час інформація — це вже не просто допоміжний ресурс виробництва і стала вирішальною складовою будь-якого бізнесу. Ефективне інформаційне забезпечення неможливо забезпечити в умовах відсутності інформаційної безпеки.

Певними науковцями під поняттям інформаційної безпеки вбачається загальна система безпеки підприємства чи тільки сам захист інформації. Варто також зазначити, що багатьма авторами термін «інформаційна безпека» ідентифікується як «комп'ютерна безпека» або «автоматизована безпека системи». Інформаційна безпека — це невіддільний компонент суцільної безпеки.

Методи та способи захисту елементів інформаційної системи зводяться до методів захисту даних, методів авторського захисту програм та даних у час їх розроблення. Основні з способів захисту даних проілюстровано на рис 1.5.

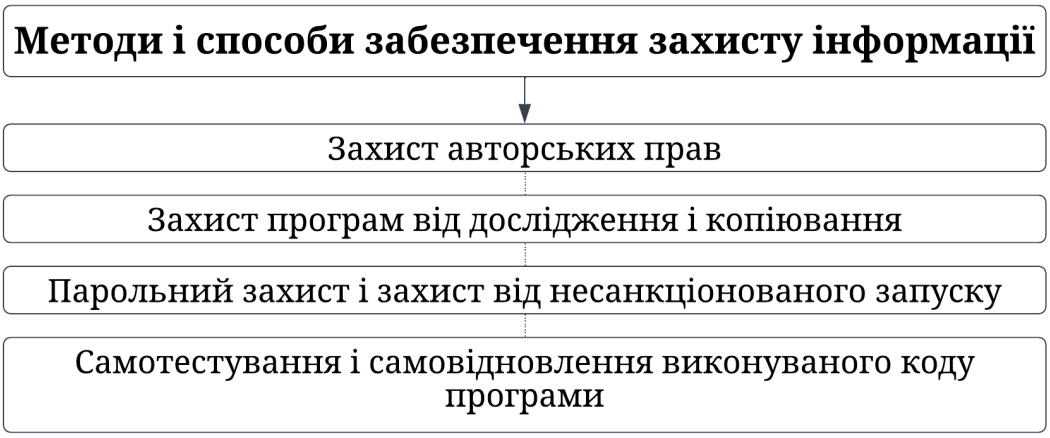


Рисунок 1.5 – Методи і способи забезпечення захисту інформації

Для захисту пароля та захисту запущених програм використовуються ідентифікація користувача та обмеження кількості запусків, або за датою початку, або за кількістю запусків. Для самостійного оновлення виконуваного програмного коду вводяться модулі діагностики характеристик виконуваного програмного коду: розмір файлу, контрольна сума, список контрольних точок тощо.

Крім того, існують алгоритми, які дозволяють відновити виконуваний код програми. До засобів тестування та відновлення належать усі відомі антивірусні засоби, так звані поліфаги та полі детектори.

На жаль, у більшості підприємств сьогодні відділ інформаційної безпеки відірваний від реалій бізнесу та пов'язаний виключно з інформаційними технологіями. Існує три основні сфери захисту інформації (рис. 1.6):

1. Організаційно-технічна база, яка створює оболонку навкруги об'єкта захисту – інформаційні ресурси, з певним ступенем достовірності виключає або

значно перешкоджає маніпулюванню інформацією в автоматизованій системі всупереч інтересам користувачів системи;

2. Правовий напрям — має на меті забезпечення імунітету, що заснований на загрозі використання репресивного інструменту всупереч інтересів користувачів системи. Він встановлює санкційний механізм проти правопорушника;

3. Економічний [78, с. 174].

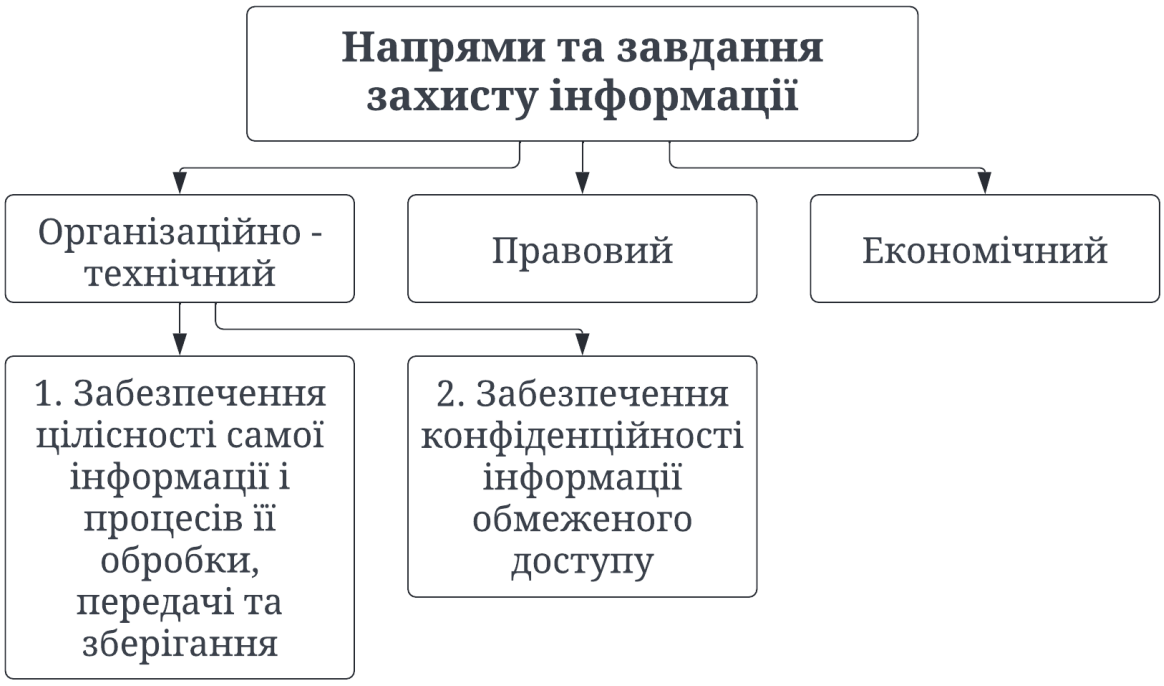


Рисунок 1.6 – Напрями та завдання захисту інформації

Організаційно-технічний напрям захисту являє собою більш реальний напрямок захисту інформації підприємства. Задля побудови та ефективного використання системи, що забезпечує інформаційну безпеки, необхідно виконати наступне:

1. Визначити вимоги щодо інформаційної безпеки, характерні для цього об'єкта безпеки;

2. Враховувати вимоги, що висуває національне та міжнародне законодавство;

3. Використовувати розроблені практики (стандарти, методики) побудови таких систем гарантування інформаційної безпеки;

4. Визначити відповідальні за впровадження та підтримку системи забезпечення інформаційної безпеки підрозділи;

5. Розподіляти відповідальність між підрозділами за виконання вимог, що висуває система забезпечення безпеки інформації;

6. Визначити основні положення, технічні й організаційні потреби, складові політики об'єкта безпеки, керуючись управлінням ризиками інформаційної безпеки;

7. Виконати вимоги політики інформаційної безпеки завдяки впровадженню відповідного програмного забезпечення та методів захисту інформації;

8. Впровадити систему управління інформаційною безпекою;

9. Впровадити використання системи управління для організації регулярного моніторингу результативності системи забезпечення інформаційної безпеки, а також, за необхідності, перегляду та коригування такої системи.

Під системою безпеки розуміється організований набір, до якого входять спеціальні органи, служби, інструменти, методи та заходи, які забезпечують захист найбільш важливих інтересів людини, підприємства та всієї держави від загроз — внутрішніх та зовнішніх (рис. 1.7).

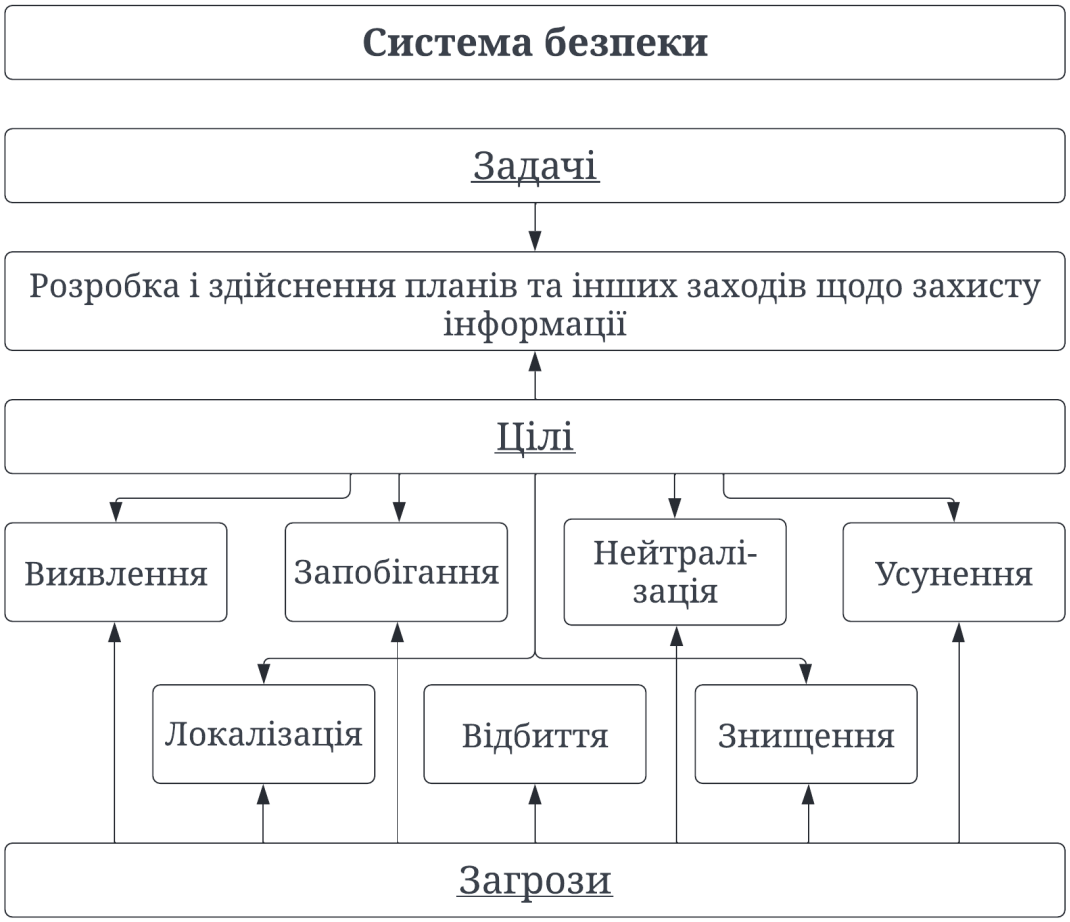


Рисунок 1.7 – Функціональна система інформаційної безпеки

За допомогою базової лінії та розроблених моделей з’являється змога виділити основні класи завдань захисту інформації:

1. Забезпечення непошкодженості даних, процесів обробки й конфіденційності інформації, тобто захист елементів обчислювального середовища;

2. Управління елементами робочого середовища – зовнішніми компонентами, цілісності внутрішніх компонентів та семантики даних.

На основі структури інформаційної безпеки, яка повинна складатися з економічної розвідки інформаційної безпеки, аналітичної та консультативної підтримки, система інформаційної безпеки включає:

1. Перевірку інформації;

2. Визначення важливості та рівня конфіденційності інформації;

3. Надання доступу та доступу до інформації;

4. Захист комерційної таємниці інформації [15, с. 142-147].

Враховуючи викладене, можна стверджувати, що система впровадження інформаційної безпеки базується на п'яти компонентах:

1. Технічний – його призначення полягає у забезпеченні захисту інформації й об’єктів підприємства, та виявленні фактів втрачання інформації, а також неправомірних дій співробітників або сторонніх для даного підприємства осіб при використання технічних засобів;

2. Організаційний – має забезпечити належну поведінку, користування персоналом товариства конфіденційною інформацією чи іншими об'єктами захисту суб'єкта господарювання;

3. Дозвільний – має розподіляти інформацію компанії на рівні секретності та визначати ступінь доступу до кожних із них;

4. Попереджувальний – існує задля попередження дезінформації, прийняття хибних управлінських рішень, а також максимальної ймовірності витоку секретної інформації;

5. Правовий – призначений для забезпечення правового захисту інтересів підприємства щодо безпеки інформації, а також закріплення прав підприємства на

комерційну таємницю в установчих документах, контрактах та інших нормативно-правових актах.

Оскільки в будь-якій системі всі елементи та підсистеми взаємопов'язані, більшість завдань, що стосуються захисту інформації, виконуються разом із основними та допоміжними підсистемами системи економічної безпеки підприємства.

Системи інформаційної безпеки, пропоновані науковцями та практиками, не повністю відображають завдання та функції, що в умовах сьогодення мають здійснятися задля захисту інформації, інформаційної та економічної безпеки загалом.

До завдань системи захисту інформації відносяться:

1. Організація спеціального обліку та контролю за важливими та секретними документами:

2. Виявлення, запобігання та блокування каналів витоку інформації;

3. Формування посадових інструкцій та положень для меморіалів, методичних вказівок щодо поводження з конфіденційною інформацією;

4. Захист інформації із застосуванням комп’ютерів, інших технічних засобів, що здатні здійснювати обробку та передачу даних;

5. Обґрунтування, організація використання технічних засобів, необхідних задля забезпечення зберігання інформації;

6. Захист в державних органах (у тому числі судових) інтересів підприємства, що стосуються питання комерційної таємниці;

7. Розробка нормативної документації про комерційну таємницю на підприємстві;

8. Вивчення правил інформаційної безпеки співробітниками.

Висновки за розділом 1

В розділі 1 даної дипломної роботи було розглянуто основні види загроз, основні причини виникнення загроз, мотиви, що збільшують ризик виникнення

загроз пов’язаних з людським фактором та складові систем захисту на які дані загрози можуть бути спрямовані.

Була наведена класифікація загроз за різними типами починаючи від причини виникнення і закінчуючи можливими наслідками та розміром збитку, було виконано опис основних видів комп’ютерних загроз.

Ототожнюючи теоретичну інформацію розглянуту в першому розділі, можливо дійти до висновку: статистично найчисленніша кількість загроз безпеці інформації пов’язана з можливістю витоку та знищення інформації різного рівня конфіденційності, а найбільшим ризиком виникнення загроз є людський фактор, що може спричинити інциденти безпеки як навмисно, так і випадково.

РОЗДІЛ 2
МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВІД ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

2.1. Принципи та види заходів забезпечення інформаційної безпеки

Існування суспільства та його інформаційна безпека забезпечується стабільним функціонуванням, живучестю, надійністю та готовністю інформаційно-телекомунікаційних мереж. Стрімкий технологічний прогрес поставив цілу низку вкрай важливих питань стосовно організації процесів обробки, зберігання, розповсюдження та захисту інформації в інформаційно-комунікаційних системах. Адже саме завдяки інформаційним технологіям та розвиненій інфраструктурі телекомунікацій й можливе чимало вдосконалень: покращення продуктивності виробництва, адміністративе та господарське управління, розширення інформаційної взаємодії через людей, поширення масової інформації, інтелектуалізація суспільства.

Таким чином, основними принципами забезпечення інформаційної безпеки є такі, що відображені на рис.2.1.

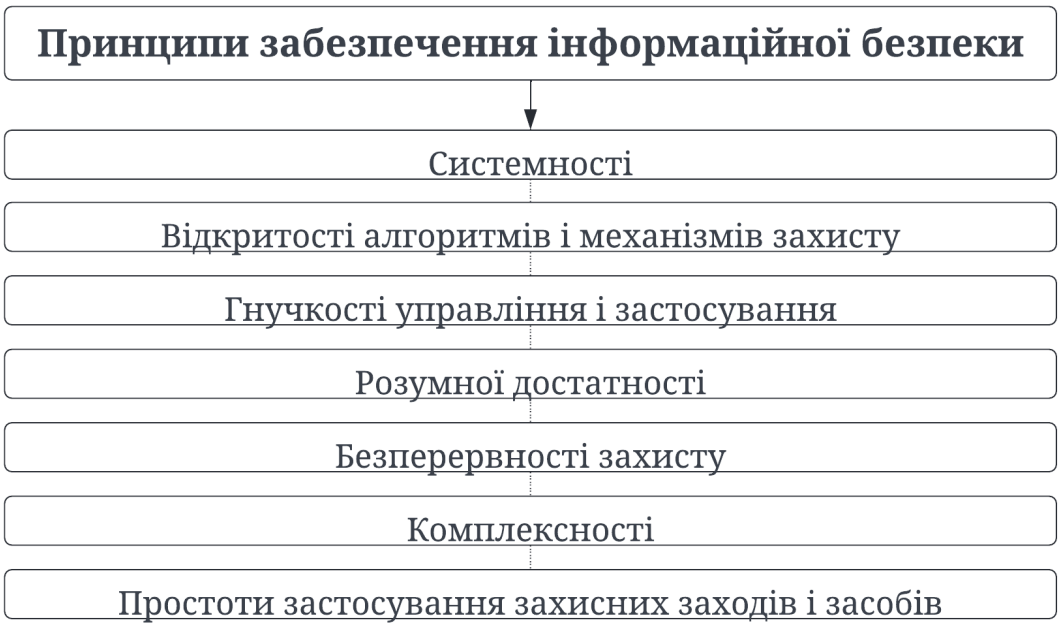


Рисунок 2.1 – Принципи забезпечення інформаційної безпеки

«Інформаційна безпека має важливе значення для того, щоб інформаційні технології могли відповідати очікуванням ділового світу, споживачів і урядів та щоб дійсно надавали всі ті потенційні вигоди, що їх забезпечують інформаційно-комунікаційні технології» (P.I., 2019).

Інформація, яка підлягає захисту, може бути представлена на різних технічних носіях. Його користувачами можуть бути люди з числа користувачів та сервісний персонал. Інформація може оброблятися в комп'ютерних системах, передаватися каналами зв'язку та відображатися різними пристроями. Вони можуть відрізнятися за вартістю. Об'єкти, підлягаючи охороні інформації, можуть охороняти не лише комп'ютери та канали зв'язку, але й приміщення, будівлі та прибудинкову територію. Кваліфікація порушників, а також методи та канали несанкціонованого доступу до інформації можуть суттєво відрізнятися.

За способами здійснення заходи забезпечення безпеки комп'ютерних систем мають свою класифікацію (рис.2.2).

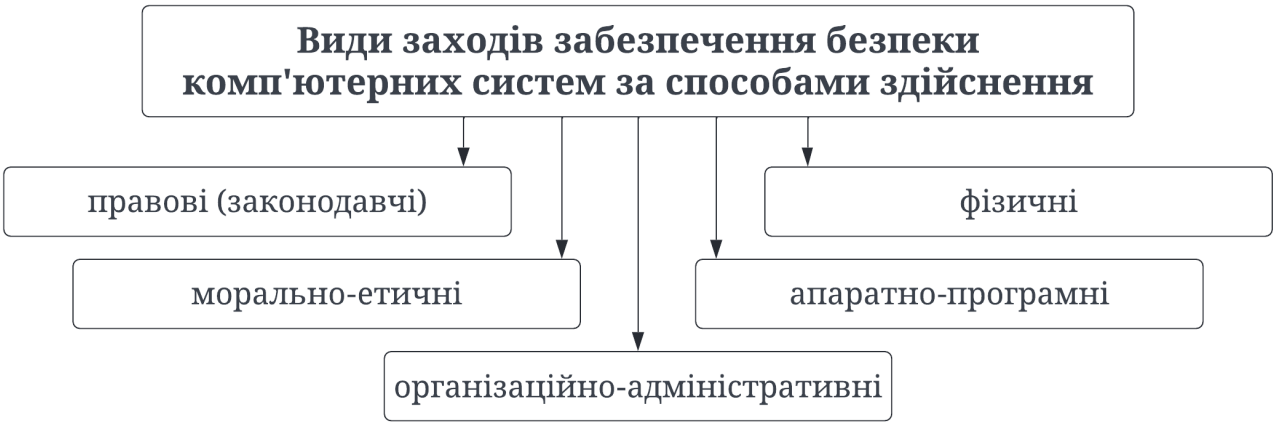


Рисунок 2.2 – Види заходів забезпечення безпеки комп'ютерних систем за способами здійснення

Морально-етичні протидії включають усі види поведінки, які традиційно були або розвиваються в суспільстві в міру поширення в країні інформаційно-телекомунікаційних систем. Ці норми є або неписаними (загальноприйняті норми чесності, патріотизму тощо) і викладені в деякому наборі правил чи приписів [55, с. 188].

Організаційно-адміністративні заходи захисту регулюють функціонування інформаційних систем; використання його ресурсів; діяльність персоналу інформаційної служби на підприємстві; порядок взаємодії користувача з системою, щоб зробити найбільш складним або неможливим реалізацію загроз безпеки [63, с. 44].

Фізичні заходи захисту включають різні механічні, електричні та електромеханічні пристрої чи споруди, що були спеціально розроблені з метою створення фізичних бар'єрів для можливих способів проникнення та доступу злочинців. До них відносяться пожежна сигналізація, турнікети, кодові замки, колючий дріт та інші перешкоди.

Заходи безпеки апаратного та програмного забезпечення включають різноманітні електронні пристрої та спеціальне програмне забезпечення, що реалізують такі методи безпеки самостійно чи в поєднанні з засобами іншого роду:

1. Ідентифікацію і аутентифікацію суб'єктів;
2. Розмежування доступу до даних інформаційної системи;
3. Контроль неушкодженості інформації;
4. Гарантування конфіденційності інформації;
5. Аудит подій інформаційної системи;
6. Зберігання інформації та складових інформаційної системи (резервування).

Захист інформації розуміється як сукупність організаційно-технічних заходів і законодавчих норм запобігання нанесення шкоди власнику інформації чи особам та системам, що її використовують. Під захистом інформації в ширшому розумінні розуміється сукупність організаційних, правових, технічних заходів щодо запобігання загрозам інформаційній безпеці та усуненню їх наслідків. Захист інформації за своєю суттю полягає в наступних процесах: виявлення, усунення чи нейтралізація джерел, причин та умов із негативним впливом на інформацію. Дані джерела загрожують інформаційній безпеці.

Мета та способи захисту інформації визначають її суть. Захист інформації ототожнюється із забезпеченням інформаційної безпеки як суцільної проблеми розвитку світової цивілізації, держав, спільності людей, особистості , існування

природи у безпеці. Запобігання можливим загрозам та протиправними діями може бути забезпечено різними способами, від створення клімату глибокого ставлення працівників до проблеми безпеки та захисту інформації до створення глибокої, чіткої системи захисту фізичними, апаратними, програмними та криптографічними засобами.

Попередження загрози можливе також шляхом отримання інформації про протиправні діяння, які готуються, заплановані крадіжки, підготовчі дії та інші елементи неправомірних діянь. Важливу роль у запобіганні загроз відіграє інформаційно-аналітична робота служби безпеки, заснована на ретельному аналізі криміногенного статусу та діяльності конкурентів та нападників.

Виявлення загрози – це дія щодо виявлення визначених загроз та їх джерел, які завдають певної чи всієї шкоди. Такі дії включають виявлення крадіжок, шахрайства, розголошення секретної чи персональної інформації або інцидентів незаконного доступу до осередків комерційної таємниці. Мета розкриття інформації – вжити заходів щодо збору, накопичення та обробки аналітичної інформації про можливу підготовку злочинних діянь злочинними структурами чи конкурентами на ринку виробництва та продажу товарів та продукції.

Локалізація (закінчення) загроз – направлені на усунення наявної загрози та конкретних злочинів дії. Наслідки спрямовані на відновлення стану, який передував виникненню загрози. Усі ці методи спрямовані на захист інформаційних ресурсів від неправомірного втручання та забезпечення:

1. Не допускання розголошення та витоку таємної інформації;
2. Заборона незаконного доступу до джерел інформації, що підлягає охороні;
3. Збереження цілісності та доступності інформації;
4. Конфіденційність інформації;
5. Захист авторських прав.

Загальними принципами захисту усіх типів захищеної інформації є:

1. Захист інформації організовується та проводиться власником інформації чи уповноваженими ним особами (юридичними чи фізичними);

2. Захищаючи інформацію, власник захищає свої права на інформацію (володіння, розпорядження), бажає захистити її від несанкціонованого вилучення та використання за рахунок своїх інтересів;

3. Захист інформації реалізується проведенням комплексу заходів, що накладає обмеження доступу до секретної інформації та створенням таких умов, що не допускають чи помітно ускладнюють незаконний доступ до таємних даних і їх носіїв.

Наразі безпеку інформаційних ресурсів можна забезпечити лише комплексною та багатокомпонентною системою захисту даних, що має бути сталою, надійною, плановою, цілеспрямованою та специфічною. Дана система має опиратися на систему типів особистої безпеки, що здатна реалізувати свою реалізацію як в повсякденних, так і критичних умовах та ситуаціях.

2.2 Нормативно-правова база регулювання заходів забезпечення безпеки інформації підприємства

Правова (законодавча) форма захисту конфіденційної інформації «…базується на використанні статей Конституції і законів держави, положень цивільного і кримінального кодексів та інших нормативно-правових документів в галузі інформатики, інформаційних відносин та захисту інформації. Вона регламентує права і обов’язки суб’єктів інформаційних відносин, правовий статус органів, технічних засобів і способів захисту інформації і є базою для створення морально-етичних норм в області захисту інформації» (В.В., 2002).

Захист інформації на законодавчому рівні визнаний як на міжнародному, так і на державному рівні. В першому випадку у формі міжнародних договорів, декларацій, угод, конвенцій, а у другому визначається, закріплюється та захищається відомчими та державними нормативно-правовими актами.

Система законів, нормативних, організаційних, адміністративних документів має забезпечувати максимально ефективний контроль за їх виконанням за допомогою роботи правоохоронних органів. Дана система може віднестися до

морально-етичних норм людської поведінки, що склалися традиційно чи розвиваються у зв’язку із актуальністю обчислювальних засобів у сучасному суспільстві.

Законодавчі акти, що захищають інформацію в Україні:

- Закон України (ЗУ) «Про інформацію»;
- ЗУ «Про захист персональних даних»;
- ЗУ «Про електронні довірчі послуги»;
- ЗУ «Про державну таємницю»;
- ЗУ «Про електронні документи та електронний документообіг»;
- ЗУ «Про Національну програму інформатизації»;
- ЗУ «Про захист інформації в інформаційно-комунікаційних системах»;
- Положення про порядок здійснення криптографічного захисту інформації в Україні;
- Стаття 31 Конституції України про «Право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції»;

Державну політику у галузі інформаційної безпеки за законом реалізує Держспецзв’язок України (Державна служба спеціального зв’язку та захисту інформації України).

Приведені вище закони розглянуті більш детально у таблиці у додатку А.

2.3 Показники захищеності системи та оцінка можливих ризиків

Для визначення актуальних загроз для підприємства необхідно знати показник вихідної захищеності. Під рівнем вихідної захищеності розуміється узагальнений показник, що залежить від технічних і експлуатаційних характеристик (Y1) [15].

В таблиці 2.1 представимо розрахунок показників вихідної захищеності підприємства. Виходячи з даних, отриманих в таблиці 2.1, всього 14% показників - високого рівня захищеності, 57% - середнього рівня захищеності, 28,6% - низького рівня захищеності.

Отже, система має середній рівень захищеності. Для середнього рівня захищеності, характерний числовий коефіцієнт -5 [15].

Таблиця 2.1

Показники вихідної захищеності

Технічні та експлуатаційні характеристики	Рівень захищеності		
	високий	середній	низький
За територіальною розгалуженістю:			
Локальна мережа, розгорнута в межах близько розташованих будівель	-	+	-
За наявністю з'єднання з мережами загального користування:			
Мережа, що має одноточковий вихід в мережу загального користування	-	+	-
За вбудованими операціями із записами баз персональних даних:			
Модифікація, передача	-	-	+
Щодо розмежування доступу до персональних даних:			
Доступ мають певні співробітники організації	-	+	-
За наявністю з'єднань з іншими базами:			
Використовується одна база, що належить організації	+	-	-
За рівнем узагальнення (знеособлення):			
Є інформація, що дозволяє ідентифікувати суб'єкта	-	-	+
За обсягом даних, які надаються стороннім користувачам без попередньої обробки:			
Система, що надає частину даних	-	+	-

Задля того, щоби визначити шляхи ймовірної втрати інформації, які були визначені при проведенні етапу обстеження, потрібно розробити окремий документ під назвою «Приватна модель загроз безпеки конфіденційної інформації (КІ) при їх обробці для систем».

В його складі міститься перелік усіх ймовірних загроз безпеки ІС (інформаційної системи), а також методи та засоби захисту даних, які дають змогу мінімізувати актуальність зазначених загроз до прийнятного рівня. Рівень актуальності розраховувався із урахування рівня вихідної уразливості та захищеності.

Загрози безпеці даних, які містить модель загроз, можна доповнювати новими під час їх виявлення.

Модель загроз утворюється на базі аналізу вірогідних загроз безпеки даних.

Приватну модель загроз приведено в формі таблиці 2.2.

Таблиця 2.2

Модель загроз ІС

Загрози	Актуальні заходи захисту	Вразливості	Імовірність реалізації
1.1 Фізична загроза (порушник має фізичний доступ)	Охоронна сигналізація та елементи фортифікації	-	Низька
1.2. Розголошення таємної інформації, яка збережена на серверах	Трудовий кодекс України, трудовий договір.	Людський фактор (необережність, помста, підкуп, шантаж, погрози)	Середня
1.3. Пошкодження чи знищення захищеної Інформації, що зберігається на серверах, при використанні спеціальних вірусів та ПЗ.	-	Людський фактор (необережність, помста, підкуп, шантаж, погрози) та несучасний антивірусний захист	Середня

Продовження таблиці 2.2

1.4. Копіювання захищених даних з сервера	Розподіленя прав доступу серед користувачів	Недотримання користувачами заходів інформаційної безпеки	Середня
1.5. Доступ здійснюється до серверів із мереж загального користування	Використовується міжмережевий екран, додатково провайдер забезпечує захист даних	Міжмережевий екран має застаріле ПЗ чи антивірусний захист	Середня
2.1. Порушник здійснює фізичний доступ до АРМ, копіює конфіденційну інформації	Використовуються елементи фортифікації, охоронна сигналізація, права доступу користувачів розмежовано	Користувачі знехтують заходи щодо забезпечення інформаційної безпеки	Середня
2.2. Розголошення захищеної інформації з АРМ	Трудовий кодекс та договір	Людський фактор (необережність, помста, підкуп, шантаж, погрози)	Середня
2.4. Доступ до АРМ з мереж загального користування	Працює міжмережевий екран та здійснюється додатковий захист з боку провайдера	Міжмережевий екран має застаріле ПЗ та антивірусний захист	Середня

Продовження таблиці 2.2

3.1. Фізичний доступ зловмисника до документів, носіїв інформації	Застосовуються елементи фортифікації, охоронна сигналізація.	Користувачі знехтують правилами інформаційної безпеки	Середня
3.2. Розголошення збереженої в документах таємної інформації, винесення даних поза кордони контрольованої зони	Трудовий кодекс та договір	Людський фактор (необережність, помста, підкуп, шантаж, погрози)	Середня
3.3. Несанкціоноване копіювання, роздрукування та розмноження секретних документів	Використовуються елементи фортифікації, охоронна сигналізація	Користувачі знехтують заходами по ІБ	Середня

Після створення приватної моделі загроз для ІС було виявлено потенційні загрози, чия ймовірність вище низької. Дані загрози вважаємо актуальними задля розробки політики безпеки [16].

Під час побудови моделі потенційних зловмисників можна поділити на зовнішніх та внутрішніх.

Зовнішні порушники для ІС —конкуруючі організації в першу чергу, а також ймовірні кримінальні чи терористичні організації, корупційні елементи, які мають відношення до органів влади [17,18].

Частіше за все діяльність перелічених злочинців має на меті здобуття пасивних носіїв конфіденційної інформації, вони орієнтовані на копіювання, пошкодження чи знищення носіїв захищених даних.

Дії зовнішніх правопорушників потенційно спрямовані власне на співробітників підприємства, та можуть проявлятися в формі здійснення загроз, спроб підкупу, що має на меті вилучення витребуваної інформації (комерційної таємниці) чи переманювання робітників компанії. Проте більш небезпечними є внутрішні порушники, адже в них є доступ до даних, що мають статус конфіденційних. Також їм відомо про застосовані на підприємстві методи захисту.

Виступати в ролі внутрішніх порушників можуть не тільки шахраї, але й чесні керівники та співробітники.

Також необхідно мати на увазі припущення, що деякі працівники можуть бути незадоволеними атмосферою в робочому колективі, розміром зарплатні чи умовами праці та мати завищене відчуття власної гідності.

В таблиці 2.3 представлена модель порушника:

Таблиця 2.3

Модель порушника

Порушник	Мотив дії	Потенційні можливості
Керівник	Власна вигода	Право доступу до конфіденційної інформації та її носіїв
Системний адміністратор, адміністратор безпеки	Образа, помста, користь, примус з боку сторонньої організації	
Співробітник		Право доступу до конфіденційної інформації, проте не мають доступу до відповідного обладнання
Підрядник		Інколи мають доступ до обладнання, де зберігається або обробляється секретна інформація.

Продовження таблиці 2.3

Колишній співробітник	Образа, користь, помста, примус сторонньою організацією	Доступ до обладнання, де зберігається або обробляється секретна інформація, залишається протягом часу між звільненням та закриттям доступу з боку адміністратора. Якщо звільняється адміністратор, необхідний контроль щодо позбавлення звільненого робітника адміністраторського доступу до даних
Терористичні, екстремістські угруповання	Власна вигода, примушення, помста	Примушення (підкуп, залякування) працівників, хакерські атаки (якщо є вихід в мережу Інтернет)
Кримінальні структури		
Організації-конкуренти		
Іноземні спецслужби		
Розробники, постачальники програмних, технічних та програмно-технічних засобів		Хакерські атаки (якщо є вихід в мережу Інтернет)

Відповідно до базової моделі загроз безпеки персональних даних (ПД), зовнішніми порушниками є: зовнішні суб'єкти, що здійснюють доступ до секретних даних, із застосуванням розроблених із злочинним наміром спеціальних вірусів, програм, алгоритмів, програмних закладок, що наносять шкоду.

Відповідно з базовою моделлю загроз безпеки персональних даних, внутрішніми порушниками є:

- 1 категорія: співробітники адміністративно-господарського відділу (співробітники, що відповідають за електробезпеку, за пожежну безпеку, охорона, прибиральники), які мають доступ до технічних засобів, але не мають доступ до ПД;
- 2 категорія: начальники, керівники, фахівці відділів, які мають доступ до ресурсів з робочого місця;
- 3 категорія: співробітники відомчих організацій, що мають віддалений доступ до ПД;
- 4-6 категорії: співробітники групи автоматизації, які мають повноваження адміністратора;
- 7 категорія: програмісти - розробники, що забезпечують супровід;
- 8 категорія: програмісти - розробники, особи, які забезпечують поставку, супровід і ремонт.

Внутрішніх порушників категорії 4-6 можна виключити з потенційних, так як при розгляді кандидатур на дані посади проводиться додатковий аналіз відповідності вимогам і надійності.

Внутрішній порушник з категорії 7 і категорії 8 також виключаються з потенційних порушників, так як організації-постачальники здійснюють поставку обладнання або ТЗ на підставі договору, що вже тягне за собою фінансові ризики.

Отже, актуальними внутрішніми порушниками залишаються порушники категорій 1,2,3 і зовнішній порушник.

Висновки за розділом 2

В другому розділі дипломної роботи було розглянуто основні заходи щодо забезпечення інформаційної безпеки, до яких відносять ряд правових, фізичних, морально-етичних, апаратно-програмних та організаційно-адміністративних заходів.

Наступним етапом було розглянуто нормативно-правову базу за допомогою якої регулюються основні вимоги до захисту інформації. Правовий захист може визначатись як на міжнародному рівні, так і на державному.

Одним із критичних моментів є оцінка ризиків, що проводиться на базі визначенні пріоритетів та вимог до захисту, бізнес-стратегії підприємства, оцінці захищеності поточної системи, формуванні моделі загроз та порушників, що є справедливими для визначених факторів. Лише на основі даного аналізу є можливим створення ефективних рекомендацій щодо покращення існуючих процесів та політик підприємства.

РОЗДІЛ 3
ФОРМУВАННЯ РЕКОМЕНДАЦІЙ ДЛЯ ОПТИМІЗАЦІЇ ПРОЦЕСІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА НЕВЕЛИКОМУ ПІДПРИЄМСТВІ

3.1 Способи проведення аналізу інфраструктури підприємства

На базисі розробленої моделі загроз і порушника сформуємо перелік організаційних рекомендації щодо побудови ефективного центру забезпечення ІБ. Для виконання даного завдання необхідно провести комплекс заходів, спрямованих на модернізацію політики безпеки.

1. Проаналізувати існуючий на даний момент стан інформаційної безпеки організації. Чи відповідає він функціональним вимогам безпеки, передбачених стандартом ISO / IEC 17799: 2005.

2. На основі отриманих результатів сформувати критично важливі загрози безпеки, які потребують негайного вирішення.

3. Шляхом розробки адміністративно-нормативних, а також технічних документів описати процедури і правила, виконання яких знизить або зведе до мінімуму загрози інформаційній безпеці [19].

4. Віддати пакет документів на вивчення керівнику. Також в якості профілактичних заходів провести консультацію з користувачами і інструктаж з адміністратором інформаційної системи.

Тепер розглянемо кожен пункт окремо:

1. Етап аналізу включає в себе:

- аудит інформаційної безпеки;
- аналіз стану локальної мережі;
- стан технічних засобів;
- стан фізичної захищеності;
- обізнаність співробітників компанії в області інформаційної безпеки.

Аудит інформаційної безпеки - це процес об'єктивних якісних і кількісних оцінок стану інформаційної системи організації відповідно до стандарту інформаційної безпеки, тобто аудит дозволяє виявити, чи відповідає рівень безпеки інформаційної інфраструктури компанії висунутим вимогам, чи забезпечуються необхідні параметри конфіденційності, цілісності і доступності ресурсів інформаційної системи.

Аудит включає в себе наступні кроки:

- інтерв'ювання персоналу;
- інвентаризація і обстеження комп'ютерів;
- аналіз захищеності інформаційної системи компанії.

На етапі аналізу стану локальної мережі потрібно, перш за все, визначити, чи є недоліки в структурі, вузлах, а також каналах зв'язку мережі. Пріоритетним є завдання забезпечення безперебійної роботи мережі, навіть в умовах порушення її цілісності. Після того, як проведений аудит інформаційної безпеки, і аналіз стану локальної мережі слід провести перевірку технічних засобів, а також фізичної захищеності. Необхідно провести консультації з співробітниками компанії. Далі переходимо до розробки документів на основі виявлених недоліків в області інформаційного захисту.

За результатами проведеного аналізу та аудиту була сформована політика ІБ, яка складалася з наступних організаційно-розпорядчих документів:

- Політика інформаційної безпеки організації. Це основний документ, що відображає політику в цілому, де дані загальні положення, розглянуті всі аспекти, необхідні для дотримання з метою підвищення рівня безпеки, дані посилання на посадові та інші інструкції з безпеки;
- Інструкція по регламентації роботи користувачів;
- Інструкція адміністратора локальної мережі;
- Інструкція адміністратора бази даних;
- Інструкція по роботі з ресурсами Інтернету;
- Інструкція з організації парольного захисту;

- Інструкція з організації антивірусного захисту.

2. Затвердження пакета документів політики безпеки і прийняття їх до виконання.

Після безпосереднього оформлення пакету документів, які формують політику інформаційної безпеки, необхідно їх затвердження або генеральним директором компанії, або протоколом засідання, на якому документи були розглянуті. Після чого слід провести ознайомлення співробітників з посадовими інструкціями, а також іншими документами, в яких позначені їх права і обов'язки.

Виділимо основні рекомендації і заходи щодо складових елементів мережі.

1. Необхідно розгорнути міжмережеві екрани в усіх офісах і підрозділах, де вони ще не розгорнуті, а також регулярно перевіряти їх роботу. Допускається організація локальних мереж без мережевого екрану, що підвищує ризик порушення безпеки даних.

2. Бажано розгорнути між мережеві екрани для конкретних серверних ресурсів усередині мережі і забезпечити фільтрацію трафіку для запобігання несанкціонованих підключень.

3. Необхідно виділити публічні ресурси і обмежити до неї доступ із загальної мережі. Для розглянутого підприємства цими ресурсами можуть служити поштовий і термінальний сервер, а також сервер IP-телефонії.

4. Необхідно встановити антивірусне програмне забезпечення на всі сервери і настільні комп'ютери підприємства. Також потрібно регулярно оновлювати сигнатури вірусів і налаштувати централізоване управління.

5. Рекомендується розглянути можливість розгортання багатофакторної перевірки автентифікації для VPN-з'єднань.

6. Необхідно забезпечити повну сегментацію мережі. Необхідно виділити в окремі VLAN-и схожі ресурси (серверні та інші), також доцільно використовувати сегментацію по підрозділах.

7. Необхідно розглянути можливість розгортання мережевих і вузлових систем виявлення вторгнень (IDS) для визначення і повідомлення про атаки в корпоративній мережі. Основна проблема полягає в тому, що такі системи, як

правило, дуже дорогі і вимагають більш детального опрацювання економічної доцільності їх застосування, співвідносячи вартість впровадження з можливими наслідками. Слід враховувати той факт, що для розгортання та аналізу отриманої інформації такої системи будуть потрібні додаткові компетенції.

8. Рекомендується проводити регулярну зміну паролів і використовувати стійкі алгоритми шифрування. Бажано розглянути можливість використання VPN і в бездротовій мережі.

9. Для адміністративних користувачів бажано розглянути можливість впровадження багатофакторної перевірки автентичності крім використання складного пароля.

10. Для віддалених користувачів мережі необхідно розглянути можливість впровадження багатофакторної перевірки автентичності крім використання складного пароля і надавати віддалений доступ тільки тим співробітникам, яким він справді необхідний.

11. Рекомендується регулярно проводити аудит віддалених користувачів на предмет актуальних оновлень своїх систем. На даний момент дана процедура може бути не регламентована.

12. Для створення безпечних робочих станцій рекомендується створити унікальний образ для кожного типу робочих станцій. Слід регулярно стежити за актуалізацією цих образів.

13. Необхідно розглянути можливість встановлення персональних міжмережевих екранів на робочі станції користувачів.

14. Рекомендується використовувати програмне забезпечення шифрування даних на диску для робочих станцій користувачів. Доцільно виділяти ряд найбільш критичних з боку безпеки робочих станцій і встановити там дане програмне забезпечення.

15. Рекомендується розглянути можливість відмови від використання систем віддаленого спостереження і контролю.

16. Необхідно забезпечити розміщення мережевого обладнання в закритих шафах / стійках. Для виконання цього пункту досить в місцях розміщення провести

монтаж закритих шаф з доступом тільки для IT-персоналу.

17. Рекомендується використовувати кошти забезпечення фізичної безпеки для персональних комп'ютерів. Для переносних комп'ютерів використовувати додаткові кабельні замки.

18. Для серверів, розташованих в серверній кімнаті також рекомендується використовувати шафи або стійки. Це дозволить зменшити ризик несанкціонованого використання.

Розглянемо рекомендації для додатків:

1. Рекомендується розгортати засоби балансування навантаження і кластеризації.

2. Бажано розглянути можливість зберігання резервних копій критично важливих додатків за межами корпоративного середовища і в вогнетривких корпусах.

3. Необхідно забезпечити укладання договорів на технічну підтримку додатків, розроблених сторонніми постачальниками.

4. Рекомендується регулярно надавати оновлення та виправлення для додатків, розроблених власними IT-фахівцями. У разі необхідності, доцільно залучити незалежну організацію для цих цілей.

5. Рекомендується розглянути можливість використання політики паролів і політики облікових записів для всіх додатків, що використовуються в корпоративній мережі.

6. Рекомендується розглянути можливість централізованого ведення журналів для всіх IT-систем підприємства і забезпечити запис усіх подій, а не тільки невдалих.

7. Рекомендується розробити і впровадити методології розробки систем безпеки програмного забезпечення для підвищення безпеки додатків.

8. Бажано використовувати алгоритм шифрування для особливо критичних даних.

Розглянемо рекомендації для протоколів

1. Необхідно розглянути можливість розгортання окремих робочих станцій

управління для адміністрування мережевих серверів і пристроїв з використанням захищеного протоколу. Робочі станції, що використовуються для управління, повинні бути особливо добре захищені. Повинні бути реалізовані надійні елементи управління паролями на основі функцій вузлової системи і додатки для управління.

2. Рекомендується задокументувати допустимі протоколи і служби, які можна використовувати в корпоративній мережі. Після цього необхідно виконати аудит мережевих пристроїв на предмет відповідності їх налаштувань задокументованим правилам.

3. Необхідно забезпечити ознайомлення всіх співробітників підприємства з наявними політиками безпеки і правильного використання ресурсів. Це можна зробити за допомогою розміщення їх на корпоративному WEB-порталі.

4. Рекомендується змінити існуючу політику безпеки таким чином, щоб вона враховувала юридичні, технічні та бізнес-вимоги.

5. Необхідно актуалізувати існуючі схеми мереж і заснувати політику регулярного їх поновлення в разі зміни топології. Доступ до схем повинен мати тільки обмежене коло IT-фахівців і фахівців з безпеки.

6. Рекомендується розробити процес документування і перевірки всіх оновлень конфігурацій перед розгортанням [20].

7. Необхідно забезпечити регулярну перевірку журналів реєстрації всіх систем підприємства.

8. Рекомендується задокументувати політики архівації та відновлення в корпоративній мережі.

Розглянемо рекомендації для персоналу:

1. Рекомендується використовувати модель призначення рівня важливості кожного компонента IT-інфраструктури. Це дозволяє застосовувати ресурси безпеки найбільш ефективно для тих систем, де вони більш потрібні.

2. Рекомендується використовувати сторонню організацію, яка заслуговую довіри для регулярних перевірок безпеки організації.

3. Необхідно спільно з відділом кадрів розробити офіційну політику звільнення співробітників. Найбільш важливим компонентом цієї політики є

гарантоване припинення дії фізичного доступу і привілеїв фахівця відділу IT для даного співробітника.

4. Необхідно створити групу (або виділити співробітника) щодо забезпечення інформаційної безпеки, яка буде контролювати будь-які зміни обчислювального середовища.

5. Рекомендується створити політику щодо повідомлення працівників про питання безпеки для своєчасного інформування про загрози в IT середовищі.

6. Необхідно розробити план навчання співробітників підприємства з питань безпеки.

Під безпекою інфраструктури мається на увазі те, яким чином повинна функціонувати мережа, які бізнес-процеси (внутрішні або зовнішні) вона повинна підтримувати, як створюються і розгортаються вузли і як організувати управління мережею і її обслуговування. Дієва безпека інфраструктури забезпечить значні поліпшення в областях мережевого захисту, реагування на події.

Створивши надійну і зрозумілу інфраструктуру і слідуючи їй, організація отримує можливість визначити області ризику і розробити способи його зниження. Оцінка передбачає перевірку процедур високого рівня, які організація може застосовувати для зниження загрози з боку інфраструктури, зосередившись на наступних областях безпеки, пов'язаних з інфраструктурою:

- Захист по периметру - Міжмережеві екрани, Антивірусні програми, Віддалений доступ, Сегментація;
- Перевірка автентичності - Політики паролів;
- Управління і контроль - Вузли керування, Файли журналів;
- Робоча станція - Конфігурація збірки.

Основні етапи впровадження політики інформаційної безпеки:

1. Регламентація роботи користувачів відділів. Інструкція по роботі з ресурсами інтернет

Припустимо, що був проведений аудит по роботі користувачів з локальною мережею і робочими станціями. Підвищена увага приділялася усвідомленню відповідальності кожного користувача перед неправильним розпорядженням

інформацією при роботі, неважливо в якому вигляді вона представлена (електронні інформаційні потоки, електронні носії, фізичні потоки або носії).

Був зроблений акцент на важливість проходження розробленої інструкції, яка обумовлена серйозними витратами в разі інцидентів, пов'язаних з порушенням інформаційної безпеки.

2. Посадова інструкція адміністратора локальної мережі.

Для підтримки працездатності локальної мережі, а також підтримки користувачів в разі виникнення будь-яких технічних проблем в організації існує адміністратор локальної мережі. Однак у своїй роботі адміністратор не приділяв належної уваги безпеці мережі. Для цього була затверджена посадова інструкція адміністратора локальної мережі, що входить в пакет документів політики безпеки. Також з адміністратором був проведений аудит з питань інструкції.

3. Посадова інструкція адміністратора бази даних.

Важливий елемент інформаційної системи організації є база даних. Однак вона ж і є джерелом підвищеної небезпеки в разі витоку інформації або неправильної експлуатації. Для цього була розроблена посадова інструкція адміністратора бази даних організації. У ній передбачені посадові обов'язки, права і відповідальність адміністратора бази даних

4. Реалізація антивірусного і парольного захисту.

Однією з найсильніших загроз інформаційній безпеці є всілякі віруси, «троянські коні», черви й інші шкідливі програми. У разі зараження збиток може бути вельми істотним: від крадіжки даних, логінів-паролів до фізичного псування устаткування. Тому політика безпеки в обов'язковому порядку повинна передбачати інструкції антивірусного захисту. Інструкції були складені і за допомогою адміністратора локальної мережі успішно реалізовані.

Те ж саме стосується і парольного захисту. В аудит про регламентацію роботи користувачів входила в розгляд організація парольного захисту. Особлива увага приділялася використанню надійних, якісних паролів, своєчасна зміна пароля (в разі підозри загрози) а також не фіксування паролів на паперових чи інших носіях.

5. Фізичні заходи захисту.

Фізичні заходи захисту призначені задля встановлення фізичних бар’єрів на ймовірних шляхах проникнення потенційних зловмисників до підприємства, компонентів АС (автоматизована система) і доступу до секретної інформації, а також технічних засобів відеоспостереження, зв'язку та охоронної сигналізації.

- Для розмежування доступу в приміщення, де розташовується серверне обладнання та інші критично важливі об'єкти АС, доцільно використовувати системи фізичного захисту, що дозволяють реєструвати і контролювати доступ виконавців і сторонніх осіб, засновані на таких методах ідентифікації і автентифікації (наприклад: магнітні та електронні карти з особистими даними , біометричні характеристики особистості користувачів і т.п.).
- Експлуатація АРМ (автоматизоване робоче місце) і серверів АС повинна проводитися в приміщеннях, що обладнані високоякісними автоматичними замками, сигналізаціями і постійно охороняються або контролюються. Також це виключає вірогідність неконтрольованого проникнення сторонніх та підвищує фізичну безпеку ресурсів (робочих місць, даних, реквізитів доступу тощо).
- Розташування та установлення АРМ, серверів має не допускати вірогідності візуального доступу до введеної чи виведеної інформації не маючими такі повноваження особами.
- Прибирання приміщень, в яких обробляється або зберігається інформація обмеженого доступу і / або службова інформація, має здійснюватися в присутності відповідального працівника. Це може бути черговий по підрозділу чи відповідальний за певне приміщення працівник, що повинен дотримуватися заходів, які виключають ймовірність отримання доступу сторонніми особами до конфіденційних ресурсів.
- В службових приміщеннях, де відбувається обробка та відображення на АРМ даних з обмеженим доступом, мають бути присутніми лише співробітники, які мають відповідний доступ. Прийом відвідувачів в цих робочих приміщеннях під час обробки таємної інформації забороняється.

- Дані приміщення забезпечуються спеціальним устаткуванням (сейфами, металевими шафами) задля безпечного зберігання важливих документів і машинних носіїв. Дані приміщення мають передбачати усі ситуації, що можуть загрожувати документам, та бути забезпеченими засобами знищення таємних паперів.
- В разі необхідності фізичні бар'єри мають розташовуватися від підлоги до стелі.
- Забороняється передавати стороннім людям будь-які дані щодо того, що відбувається у захищених зонах.
- Для забезпечення належного рівня безпеки та запобігання дій, які можуть зашкодити даним, поодинці, тобто без належного контролю, працювати з вкрай важливою інформацією чи її носіями, компонентами АС забороняється.
- Захищені зони мають бути фізично недоступними та час від часу перевірятися охороною в неробочий час.
- Персоналу, який відповідає за технічну підтримку сервісів, необхідно надавати доступ до захищених галузей лише в разі потреби та з дозволу керівництва.
- Забороняється використання фотографічної, звукозаписної і відео апаратури в захищених областях, за винятком санкціонованих випадків.
- Після завершення робочого дня приміщення, де є установлені захищені АРМ, мають здаватися під охорону — в цей час включається сигналізація та ставиться відмітка у журналі прийому / здачі службових приміщень.
- Виносити обладнання, дані і програми за межі підприємства без встановленого документального оформлення забороняється.

6. Правила користування робочим столом.

В разі аварії носії інформації, які були залишені на робочому столі, ризикують бути пошкодженими чи знищеними. До того ж це може зумовити витік конфіденційних даних. У зв'язку з цим були висунуті наступні рекомендації по використанню робочого столу:

- паперова документація та знімні носії в час, коли вони не використовуються, мають зберігатися у спеціальних шафах (особливо в неробочий

час). У разі неможливості зберігання і знімних носіїв, користувачі зобов'язані вжити всіх заходів щодо недопущення сторонніх осіб до службової інформації;

- персональні комп'ютери та комп'ютерні термінали мають бути захищеними блокуванням із ключем, паролями чи іншими засобами контролю в час, коли вони не застосовуються.

7. Джерела електроживлення.

Обладнання повинно бути захищене від збоїв в системі електропостачання з іншими проблемами в електромережі. Блок живлення повинен бути відповідним специфікаціям виробника обладнання. Слід враховувати необхідність використання резервного джерела живлення. Рекомендується мати джерело постійного живлення для обладнання, що підтримує критичні виробничі служби.

План на випадок надзвичайних ситуацій повинен включати заходи, які необхідно вжити після закінчення терміну дії джерел безперебійного живлення.

Усе обладнання, яке взаємодіє із джерелами безперебійного живлення, необхідно регулярно перевіряти за рекомендаціями виробника.

Силові кабелі та мережеві кабелі для передачі даних повинні бути захищені від розтину з метою перехоплення інформації та пошкодження. Щоб зменшити цей ризик, організація пропонує впровадити наступні захисні заходи:

- Силові та комунікаційні кабелі, що діють на підприємстві, повинні бути прокладені під землею (за можливості) або відповідно захищені іншими засобами;
- Слід розглянути заходи щодо захисту мережевих кабелів від несанкціонованого розкриття з метою перехоплення даних та від пошкодження, наприклад, шляхом використання екранів або прокладання цих ліній так, щоб вони не проходили через громадські місця.

8. Захист обладнання, використовуваного за межами підприємства.

Використання обладнання ІС, яке підтримує виробничі процеси поза підприємства, повинно бути санкціонованим керівництвом. Рівень захисту цього обладнання має дорівнювати рівню обладнання, яке розташовано на території компанії. Нижче викладені рекомендації:

- працівники не мають права продовжувати роботу вдома на ПК;

- забороняється лишати обладнання та носії інформації під час відсутності працівника в місцях загального користування без відповідного нагляду;
- мобільні комп'ютери варто перевозити разом із ручним багажем;
- такі комп'ютери також можуть бути викрадені, загублені чи піддатися спробам несанкціонованого доступу.
- слід завжди дотримуватися інструкції виробника щодо захисту обладнання, наприклад, захищати обладнання від впливу виражених електромагнітних полів [21].

3.2 Формування базового захисту для основних активів підприємства

Розглянемо розробку технічних рекомендацій для підприємства, яке потребує побудови ефективного центру з забезпечення інформаційної та кібербезпеки. Враховуючи визначення моделі загроз та правопорушника, а також те, що головні дані щодо системи можна отримати з ПК, доцільно розглянути впровадження СКУД (системи контролю та управління доступом) на прикладі об’єкта, який охороняється, та на який надходять усі дані.

На пості охорони, що розташовується біля входу, оформлюються всі пропуски робітників у офіс. Схема організації СКУД представлена нижче на рисунку 3.1.

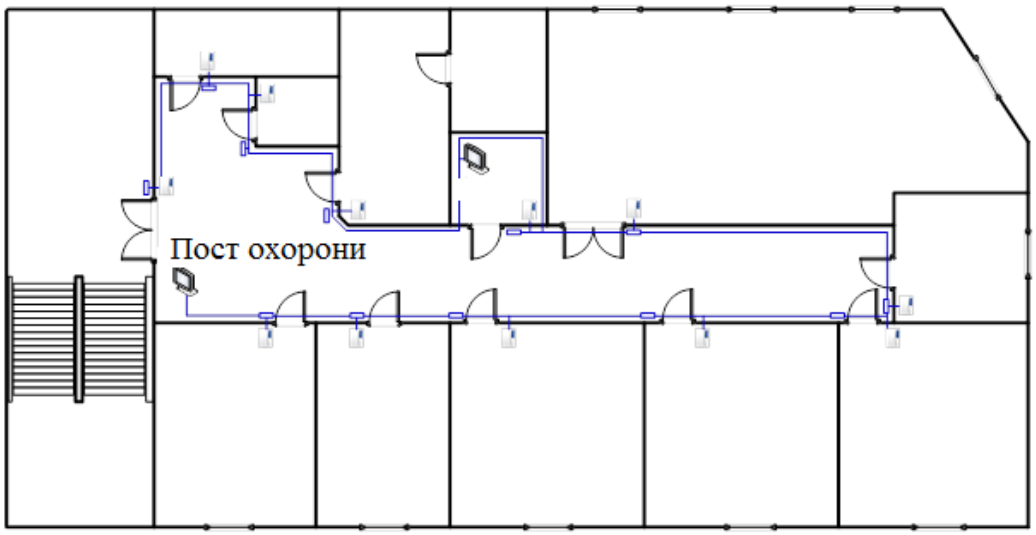


Рисунок 3.1 – Схема організації СКУД

Задля роботи апаратних пристроїв застосовується спеціальне ПЗ, завдяки якому реалізується управління контролем доступу.

Окрім того, задля більш ефективного контроля управління доступу доцільним є впровадження системи відеоспостереження. На рисунку 3.2 зображено план розташування камер відеоспостереження, що забезпечують повне охоплення площі усього об'єкта захисту та контроль над ним.

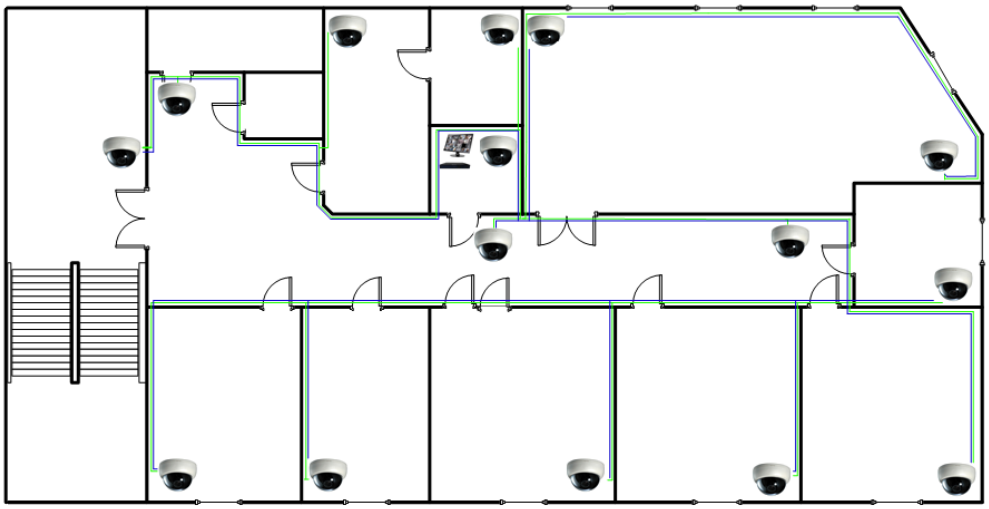


Рисунок 3.2 – Розроблена система відеоспостереження

Кабель буде прокладений за підвісною стелею. Спеціальний сервер для відеоспостереження буде розміщений на окремій телекомунікаційної стійці у серверній. Доступ до пристрою можливий лише при використанні паролю, що має лише керівних служби безпеки та системного адміністратора. Монітори відеонагляду будуть встановлені на пості охорони. Запис відеопотоку відбуватиметься цілодобово на спеціальне мережеве сховище.

Можлива модернізація мережу в зв’язку з впровадженням відеоспостереження представлена на рисунку 3.3.

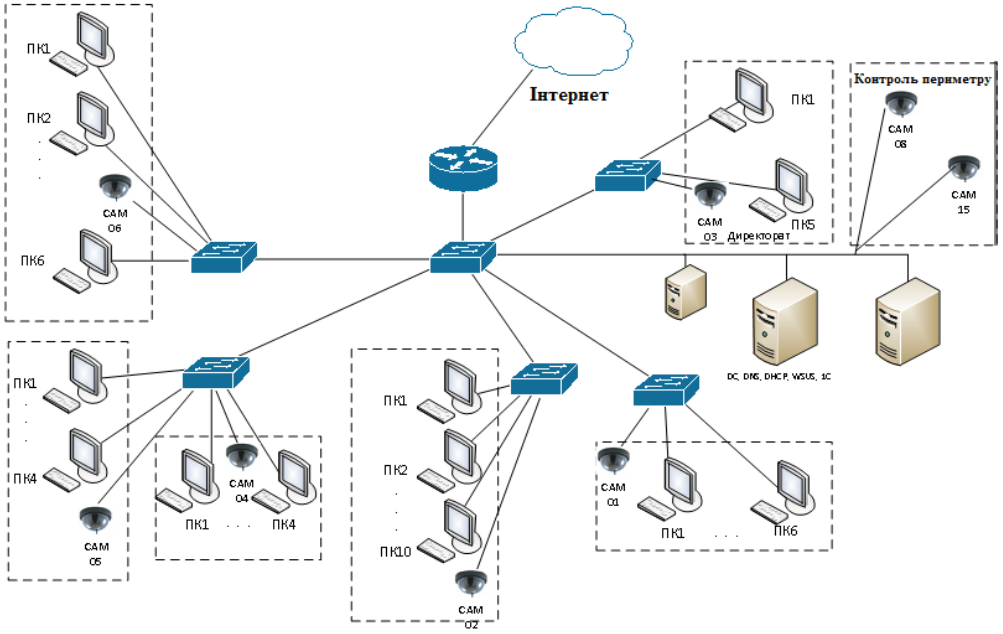


Рисунок 3.3 – Модернізована схема мережі

Узагальнюю чи, можна сказати, що пропонується застосовувати купольні камери відеоспостереження, так як вони дуже популярні для використання на об'єктах малого та середнього бізнесу.

У таблиці 3.1 перераховано голосні виробники даних камер. Камери з 1,3 Мпс віддається перевага, адже зараз камери з таким дозволом широко розповсюджені — вони мають великий кут огляду в базовій комплектації.

Таблиця 3.1

Вибір купольної камери

Марка	Кількість пікселів	Кут огляду	Вартість, грн.
ActiveCam AC-D8111IR2W	1,3 Мпс	74,7	2990
AHD MT-DW960IP	1,3 Мпс	80	3700
MDC-i8260VTD	1,3 Мпс	78	4800

Камери спостереження усі без виключень мають веб-сервер, що дозволяє встановлювати віддалений доступ. Дані камер підключаються із використанням кабелю витої пари. За даними таблиці 3.2 обираємо виробника AHD — цій камері притаманна функція максимального окуту огляду та середня вартість порівняно

до конкурентів. Камера мініатюрна та має ІЧ-підсвічування, завдяки чому вона здатна працювати без додаткового освітлення середовища. За гарантією виробника, ступінь захисту становить IP66. Використовуючи IP-відеореєстратор, вдасться зберігати відеопотік з камер спостереження.

Задля попередження виникнення ймовірних колізій під час роботи обладнання різноманітних виробників вирішено використовувати IP-відеореєстратор MATRIXM-16IPMC, що підтримує функцію хмарного сховища даних. Також обладнання дає змогу здійснювати відеоспостереження в реальному часі чи відтворювати певні дані із зовнішніх камер. Завдяки підтримці жорсткого диска до 6 Тб є можливість зберігати відео у форматі 1280x960 до тижня (7 діб).

Таблиця 3.2 відображує загальну вартість обладнання офісу системою відеоспостереження.

Таблиця 3.2

Кошторисна вартість на обладнання

Найменування	Ціна, грн.	кількість	Вартість, грн.
IP-камера	3700	15	55500
Відеореєстратор MATRIXM-16IPMC	7050	1	7050
Разом			62550
Невраховані витрати, %	10		6255
Всього			68805

Як підсумок, витрати на вищезазначене обладнання на об'єкті складатиме біля 68 805 грн.

Пропонується використати шлюз контролю доступу задля централізованого управління доступом — це дозволить зробити процес впровадження контекстного контролю доступу значно простіше.

Даний процес складається з чотирьох етапів:

1. Аналіз мережевої взаємодії — пристрої взаємодіють один з одним через шлюз контролю доступу, через що вказана задача стає зрозумілою.

2. Використання правил ревізії доступу — запити проміж пристроями зазнають фільтрації, що відповідає прийнятим правилам контролю доступу.

3. Оновлення контексту — виробляється на базі безпосереднього опитування пристроїв та отриманих раніше запитів. В якості частини контексту зберігаються журнали значень параметрів та виконаних операцій, адже вони ілюструють процес переходу до нового стану.

4. Оновлення правил контролю доступу — беручи за основу оновлений контекст і політику контекстної моделі здійснюється оновлення правил контролю доступу і їх реалізація, тобто приведення у дію.

На об'єкті пропонується застосовувати спеціальний міжмережевий екран, що аналізує проходження крізь нього потоку трафіку, в той же час реєструються події та тривожна сигналізація при виявленні загроз.

Характеристики основних мережевих екранів наведені в таблиці 3.3.

Таблиця 3.3

Порівняння мережевих екранів

Продукт	Тип	Платформа	Особливості
Solstice Firewall	Комплексний екран	SunOS, UNIX, Solaris	Здійснює політику безпеки: уся інформація без вказаного до неї дозволу відкидається. Під час роботи фільтри пакетів на шлюзах та серверах генерують записи щодо всіх подій, що активують механізми тривоги та потребують реакції адміністратора.
Black Hole	Екранує шлюз прикладного рівня	Різноманітні апаратні платформи	Механізм фільтрації пакетів не застосовує. Принцип дії: не дозволене — заборонено. Відбувається реєстрація усіх дій сервера, попередження щодо можливих порушень. Може

			застосовуватися в якості двонаправленого шлюзу.
Border Ware FirewallServer	Екранує шлюз прикладного рівня	UNIX, Windows, DOS	Захисна програма, яка забезпечує роботу під керуванням ОС та дає змогу фіксувати використовуваний протокол, час, адреси, спроби.
ALF (Application LayerFilter)	Екранує шлюз прикладного рівня	BSDI	Фільтрує IP-пакети за адресами, діапазонами портів, протоколами та інтерфейсами.
ANS Inter Lock Service	Екранує шлюз прикладного рівня	UNIX	Користується програмами-посередниками для служб FTR, Telnet, HTTR та підтримує шифрування з'єднання точка-точка, причому, як засоби автентифікації можуть використовуватися апаратні.
Brimstone	Комплексний екран	SunOS, BSDI на Intel, IRIX на INDY і Challenge	Аналізує з використанням часу, дати, адреси, порту тощо. Включає програми-посередники прикладного рівня для служб FTR, Telnet, X11, SMTP, Gopher, HTTP та інші. Підтримує основну частину пакетів апаратної автентифікації.
Centri	Екранує шлюз прикладного рівня	SunOS, BSDI, Solaris, HP-UX, AIX	Закрита мережа бачиться ззовні єдиним хостом, містить програми-посередники для служб: електронна пошта, протокол FTR тощо. Здійснює еєстрацію всіх дій сервера

			та виводить попередження в разі порушень.
CONNECT	Екранує шлюз прикладного рівня	UNIX	Є програмним продуктом, що забезпечує захист інформації від несанкціонованого доступу при з'єднанні закритою і відкритою мережами. Дозволяє реєструвати всі дії сервера і попереджати про можливі порушення.
Cyber Guard Firewall	Двонаправлений шлюз комплексного типу	Платформа RISC, OS UNIX	Використано комплексні рішення, що включають механізми захисту ОС UNIX і інтегровані мережеві засоби, призначені для RISC-комп'ютерів.
DigitalFirewall for UNIX	комплексний екран	DigitalAlpha	Представляє можливості екрануючого фільтра та шлюзу прикладного рівня.
Eagle Enterprise	Екранує шлюз прикладного рівня	Реалізація технології VirtualPrivateNetworking	Включає в себе програми-посередники прикладного рівня для служб FTR, HTTP, Telnet. Реєструє всі дії сервера і попереджає про порушення.
Firewall IRX Router	Екранує маршрутизатор	DOS, MS-Windows	Дозволяє проаналізувати мережі задля оптимізації мережевого трафіку, зв'язати локальну мережу безпечно
Firewall-1	Комплексний міжмережевий екран	Intel x86, SunSolaris.	Гарантує захист від хакерських атак типу address-spoofing (підробка адрес пакетів) та

			представляє поєднання засобів захисту мережевого та прикладного рівнів.
Firewall-1 / VPN-1	Комплексний міжмережевий екран	Intel x86, SunSolaris.	Є відкритим інтерфейсом програми OPSEC API та допомагає виявляти комп'ютерні віруси, сканувати URL, блокувати Java і ActiveX, підтримувати протокол SMTP та обробляти FTP, фільтрувати HTTP
Fortinet FG-60E	Міжмережевий екран	Різні апаратні платформи	Просте адміністрування, висока продуктивність централізоване управління, масштабованість мережі, поділ повноважень,

Обираємо Fortinet FG-60E в якості міжмережевого екрану.

Пристрої комплексної мережевої безпеки FortiGate-60E забезпечують захистом малі офіси, відділення й роздрібні мережі. Технологія FortiASIC System on a Chip 3 (SOC3), що є основою пристрою, забезпечує повний комплекс усіх захисних функцій для захищення програм і інформації.

Проста схема ліцензування за пристрій, вбудована консоль управління, багатий набір інтерфейсів, можливість віддаленого управління помітно скоротять вартість закупівлі, обслуговування і управління.

Можливості та переваги FortiGate-60E.

Повний функціонал безпеки – міжмережевий екран, система передбачення вторгнень, контроль додатків, VPN і веб-фільтрація – включені в ціну єдиної підписки Система ліцензування "за пристрій" гарантує те, що кількість користувачів обмежена лише продуктивністю системи, а це дає змогу економити на операційних витратах.

Проста установка та перший запуск завдяки FortiExplorer Автоматизоване оновлення підписок в режимі реального часу при використанні сервісів підписки FortiGuard.

Розглянемо також межах даного розділу існуюче антивірусне ПЗ, що пропонується для установки в корпоративних мережах. На рис 3.4 наводиться рейтинг антивірусного ПЗ станом на 10 лютого 2022 за версією AV-TEST Institute (німецький незалежний інститут досліджень в галузі IT безпеки, що проводить дослідження ринку більше ніж 15 років). В табл 3.4 приводиться порівняння цінових політик зазначеного ПЗ.

Рисунок 3.4 – Топ 10 антивірусів згідно рейтингу AV-TEST Institute

Таблиця 3.4

Цінові політики антивірусного ПЗ

Виробник	Продукт	Термін ліцензії	Ціна, $.
AhnLab	V3 Endpoint Security	1 рік / 20 ПК	500
Avast	Business Antivirus Pro Plus	1 рік / 20 ПК	410
Bitdefender	Endpoint Security 7.4	1 рік / 20 ПК	320
Eset	Endpoint Security 9.0	1 рік / 20 ПК	748
G Data	Endpoint Protection Business 15.1	1 рік / 20 ПК	760
Microsoft (for Windows users)	Defender Antivirus 4.18	1 рік / 20 ПК	Free
Symantec	Endpoint Security Complete 14.3	1 рік / 20 ПК	1870
Trellix	Endpoint Security 10.7	1 рік / 20 ПК	1638
Trend Micro	Apex One 14.0	1 рік / 20 ПК	560
With Secure	Elements Endpoint Protection 21 and 22	1 рік / 20 ПК	920

Зважаючи на рейтинги від інституту досліджень, популярність та рейтинг серед кристувачів, цінову політику найкращими варінтами антивірусного захисту виступають компанії Eset та Trend Micro. Наявність системи моніторингу — це ще один інструмент, що забезпечує мережеву безпеку. Моніторинг дає змогу системному адміністратору системи розумного міста відстежувати всередині локальної мережі рух пакетів.

На ринку послуг є безліч платних та безкоштовних продуктів. Проведемо порівняльний аналіз більш популярних продуктів. Основні системи моніторингу наведені в таблиці 3.5. Розглянемо виключно безкоштовні продукти моніторингу, оскільки купувати систему немає необхідності.

Таблиця 3.5

Порівняльний аналіз систем моніторингу

Система моніторингу	Переваги
Zabbix	• відмінна функціональність; • можливість масштабування; • зручна система оповіщень; • можливість намалювати карту мережі; • є агенти під windows; • можливість підключення скриптів.
Nagios	• стабільна і проста система; • великий набір плагінів; • моніторить тисячі хостів
Cacti	• зручний, сучасний веб інтерфейс; • красиві, інформативні графіки.
Monit	• існування процесу по PID; • ресурси займані процесом; • робота певного порту (TCP / UDP); • відповідь протоколу за певним портом (SMTP, SSH, HTTP тощо); • обсяг і вільний простір в файловій системі; • права доступу до файлу або каталогу. • комбінація методів перевірки; • сповіщення по email; • підтримує зовнішні скрипти; • має веб-інтерфейс.

Зупинимо свій вибір на Zabbix, адже він має простий інтерфейс та можливість оповіщення різними засобами. До того ж ця система має власний Web-інтерфейс, а це дозволяє проводити віддалений моніторинг.

Висновки за розділом 3

На базі першого та другого розділів було сформовано третій заключний розділ дипломної роботи в якому охарактеризовані способи проведення аналізу інфраструктури підприємства до яких входить комплекс заходів спрямованих на модернізацію політики безпеки, заходи щодо захисту складових елементів мережі, рекомендації щодо використання додатків та допустимих протоколів, описані рекомендації щодо інструктування та поводження персоналу. Як результат, було описано основні етапи впровадження подібних рекомендацій.

Окрім організаційно-адміністративних заходів захисту, було розроблено рекомендації, щодо програмно-апаратного та фізичного захисту, до якого входить впровадження системи керування та управління доступами, встановлення систем відеоспостереження, порівняльна характеристика при виборі міжмережевого екрану, антивіруса, системи моніторингу та огляд цінової політики при впроваджені подібних систем захисту.

ВИСНОВКИ

У результаті написання бакалаврської роботи були розроблені необхідні заходи щодо впровадження комплексної системи інформаційної безпеки підприємства, а також представлені рекомендації з побудови ефективних центрів з забезпечення кібербезпеки.

В результаті впровадження даної політики співробітники будуть проінструктовані належним чином. Крім цього, в роботі були розроблені комплексні заходи щодо підвищення захищеності комерційної інформації він несанкціонованого втручання.

В роботі була проведена оцінка загроз, в ході якої були виявлені і класифіковані всі актуальні загрози безпеці згідно моделі загроз. Було вирішено ряд актуальних завдань по організації політики безпеки.

Проведено підбір інженерно-технічних засобів, за підсумком якого був запропонований міжмережевий екран і антивірусне ПЗ.

Щодо впровадження інженерно-технічних засобів захисту, був зроблений вибір системи контролю доступу, а також обрана система відеоспостереження.

Для організації необхідного відеоспостереження пропонується використовувати IP-камери з відеореєстратором. Для здійснення моніторингу мережі локальної мережі використовується система моніторингу Zabbix.

В результаті написання роботи були виконані наступні задачі:

1. Розглянуто основні проблеми та показано актуальність забезпечення інформаційної та кібербезпеки підприємства;

2. Розглянуто можливі методи і види захисту та нормативно-правову базу, на яку вони спираються;

3. Розглянуто модель загроз і порушника інформаційної та кібербезпеки підприємства;

4. На основі розробленої моделі загроз і порушника розроблено рекомендації щодо побудови ефективного центру забезпечення інформаційної та кібербезпеки

підприємства, а також наведено приклад обладнання, яке можна використовувати для захисту інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби // Теоретичні та прикладні питання економіки : зб. наук. пр. Київ : Вид.- поліграф. центр «Київ. ун-т», 2019. – 256 с.

2. Закон України "Про інформацію" // ВВР. – 1992. – № 48. – Ст. 650. Вводиться в дію Постановою ВР від 02.10.92 №2658-12 // ВВР. – 1992. – №48. – Ст. 651 зі змінами № 1089-IX від 16.12.2020

3. Закон України "Про державну таємницю" // ВВР. – 1994. – № 16. – Ст. 93. Вводиться в дію Постановою ВР № 3856-XII від 21.01.94, ВВР, 1994, № 16, ст.94. Із змінами, внесеними згідно із Законами № 2107-IX від 03.03.2022.

4. Закон України "Про електронні документи та електронний документообіг" //ВВР. – 2003. – № 36. – Ст. 275. Із змінами, внесеними згідно із Законами № 1089-IX від 16.12.2020

5. Закон України " Про електронні довірчі послуги " // ВВР. – 2017. – № 45. – Ст. 400. Із змінами, внесеними згідно із Законами № 440-IX від 14.01.2020, ВВР, 2020 та № 1089-IX від 16.12.2020

6. Закон "Про Національну програму інформатизації" // ВВР. – 1998. - № 27-28. - ст.181. Із змінами, внесеними згідно із Законами № 1089-IX від 16.12.2020

7. Закон "Про захист персональних даних" // ВВР. – 2010. - № 34. - ст. 481. Із змінами, внесеними згідно із Законами № 4452-VI від 23.02.2012, ВВР, 2012, № 50, ст.564.

8. Закон "Про захист інформації в інформаційно-комунікаційних системах" // ВВР. – 1994. - №31 - ст.286. Із змінами, внесеними згідно із Законами № 1089-IX від 16.12.2020

9. Указ президента України "Про Положення про порядок здійснення криптографічного захисту інформації в Україні" // 22.05.1998, Л. Кучма № 505/98. Із змінами, внесеними згідно з Указами Президента // № 1019/98 (1019/98) від

15.09.98 // № 1229/99 (1229/99) від 27.09.99 // № 333/2008 (333/2008) від 11.04.2008 // № 693/2009 (693/2009) від 28.08.2009.

10. Конституція України. [Електронний ресурс] / Офіційний веб-сайт Верховної Ради України. - Режим доступу: http://portal.rada.gov.ua/.

11. Максимов Н.В. Технические средства информатизации/Н.В. Максимов, М.: Форум, 2013 – 608 с.

12. Ярочкин В.И. Информационная безопасность: учебник для студентов вузов. – М.: Академический проект; Гаудеамус, 2009. – 216 с.

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

14. Поляк-Брагинский А.В. Локальная сеть. Самое необходимое/А.В. Поляк-Брагинский, Спб.: БВХ-Петербург, 2011 – 576.

15. Кавун С. В. Інформаційна безпека : навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків : Вид. ХНЕУ, 2008. – 352 с.

16. Сердюк В.А. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий/В.А. Сердюк, М.: Высшая Школа Экономики (Государственный Университет), 2013 – 576 с.

17. Шевченко А. С. Метод оцінювання ризиків з урахуванням впливу механізмів захисту інформації на параметри безпроводових інформаційно-телекомунікаційних систем під час інформаційних операцій / А. С. Шевченко, О. В. Кокотов // Науково-практичний журнал «Безпека інформації». — 2014. — № 1. — С. 7–11.

18. Шевченко А. С. Модель загроз для відомчих безпроводових інформаційно-комунікаційних систем в умовах інформаційної боротьби при впливі комплексу навмисних атак порушника / А. С. Шевченко // Сучасний захист інформації. — 2011. — № 3. — С. 58–65.

19. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерних системах - К:"Корнійчук" 2000. – 256 с.

20. Кузнецов О.О. Захист інформації в інформаційних системах. / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. - Харків: Вид. ХНЕУ, 2011– 510 с.

21. Скотт Бармен. Разработка правил информационной безопасности. - К: Вильямс.2002. – 300 с.

ДОДАТОК А
ЗАКОНОДАВЧІ ДОКУМЕНТИ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

Закон України «Про інформацію» (ВВР, Закон України "Про інформацію" // ВВР. – 1992. – № 48. – Ст. 650. Вводиться в дію Постановою ВР від 02.10.92 №2658-12 // ВВР. – 1992. – №48. – Ст. 651., 1992);	Цей закон «…встановлює загальні правові підстави для отримання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації. Дія цього Закону поширюється на інформаційні відносини, що виникають у всіх сферах життя і діяльності суспільства та держави при отриманні, використанні, поширенні та зберіганні інформації. Законодавство України про інформацію складається з Конституції України, зазначеного Закону, законодавчих актів з окремих галузей, видів, форм і засобів інформації, ратифікованих Україною міжнародних договорів та угод, а також принципів і норм міжнародного права…» (ВВР, Закон України "Про інформацію" // ВВР. – 1992. – № 48. – Ст. 650. Вводиться в дію Постановою ВР від 02.10.92 №2658-12 // ВВР. – 1992. – №48. – Ст. 651., 1992)[2].
Закон України «Про державну таємницю» (ВВР, Закон України "Про	«…Під державною таємницею розглядається вид таємної інформації, що містить відомості у сфері оборони, економіки, науки і техніки, зовнішніх

державну таємницю" / Вводиться в дію Постановою ВР № 3856-XII від 21.01.94, № 16, ст.94. Із змінами, внесеними згідно із Законами № 1169-VII від 27.03.2014., 1994);	відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою. Відносини у сфері охорони державної таємниці регулюються Конституцією України, Законом України "Про інформацію", цим Законом, міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України та відповідними нормативно-правовими актами. Державну політику щодо державної таємниці як складову засад внутрішньої та зовнішньої політики визначає Верховна Рада України. Спеціально уповноваженим органом державної влади у сфері забезпечення охорони державної таємниці є Служба безпеки України…»(ВВР, Закон України "Про державну таємницю" / Вводиться в дію Постановою ВР № 3856-XII від 21.01.94, № 16, ст.94. Із змінами, внесеними згідно із Законами № 1169-VII від 27.03.2014., 1994) [3].
Закон України «Про захист персональних даних» (ВВР, Закон "Про захист персональних даних" // ВВР. – 2010. - № 34. - ст. 481. Із змінами, внесеними згідно із Законами № 4452-VI від 23.02.2012, ВВР, 2012, № 50,	Закон «…має важливе суспільно-політичне значення для держави, є свідченням позитивних демократичних зрушень у суспільстві, долученням до кращих правових здобутків людства. Він надає можливість законодавчо врегулювати конституційні положення щодо права кожного на захист конфіденційної інформації про особу. Дія цього Закону поширюється на відносини пов'язані

ст.564.);	із обробленням відомостей про певну фізичну особу в органах державної влади та органах місцевого самоврядування, організаціях, установах і підприємствах усіх форм власності, а також фізичними особами, які виконують професійні обов'язки приватно практикуючих адвоката, нотаріуса, лікаря тощо…» (ВВР, Закон "Про захист персональних даних" // ВВР. – 2010. - № 34. - ст. 481. Із змінами, внесеними згідно із Законами № 4452-VI від 23.02.2012, ВВР, 2012, № 50, ст.564.)[7].
Закон України «Про електронні документи та електронний документообіг» (Закон України "Про електронні документи та електронний документообіг" //ВВР. – 2003. – № 36. – Ст. 275. Із змінами, внесеними згідно із Законами № 2599-IV від 31.05.2005, ВВР, 2005, № 26, ст.349., 2003);	Закон «…встановлює основні організаційно-правові основи електронного документообігу та використання електронних документів. Дія цього Закону поширюється на відносини, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів. Кабінет Міністрів України та інші органи виконавчої влади в межах повноважень, визначених законом, реалізують державну політику електронного документообігу (ВВР, Закон України "Про електронні документи та електронний документообіг" //ВВР. – 2003. – № 36. – Ст. 275. Із змінами, внесеними згідно із Законами № 2599-IV від 31.05.2005, ВВР, 2005, № 26, ст.349., 2003)
Закон України «Про електронні довірчі послуги» (Закон України "Про електронні довірчі послуги"	Закон «…визначає правові та організаційні засади надання електронних довірчих послуг, у тому числі транскордонних, права та обов'язки суб'єктів правових відносин у сфері електронних

№ 45, ст.400 https://zakon.rada.gov.ua/laws/show/2155-19#Text);	довірчих послуг, порядок здійснення державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, а також правові та організаційні засади здійснення електронної ідентифікації…» (ВВР, Закон України "Про електронні довірчі послуги" № 45, ст.400 https://zakon.rada.gov.ua/laws/show/2155-19#Text, 2017)[5].
Закон України «Про Національну програму інформатизації»;	Закон розглядає основи Національної програми інформатизації (принципи її формування, впровадження, вдосконалення), що сама по собі також визначає алгоритм забезпечення інформаційних потреб у багатьох видах діяльності в галузях державного значення. «Головною метою Національної програми інформатизації є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави. (України)
Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (ВВР);	Даний закон «…регулює суспільні відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах з метою забезпечення дотримання права власності фізичних і юридичних осіб на інформацію та їх права доступу до неї, а також права власника інформації на її захист. Захист інформації в

	системі забезпечується запровадженням комплексної системи захисту інформації; дотриманням суб'єктами відносин, пов'язаних з обробкою інформації в системі, законодавства України та нормативних документів у сфері захисту інформації в системі; використанням засобів електронно-обчислювальної техніки, програмного забезпечення, телекомунікаційного обладнання, а також засобів захисту інформації у системі, які відповідають вимогам законодавства України щодо захисту інформації (наявність сертифіката, експертного висновку тощо)…» (ВВР, Закон "Про захист інформації в інформаційно-телекомунікаційних системах" // ВВР. – 1994. - №31 - ст.286. Із змінами, внесеними згідно із Законами N 879-VI (879-17) від 15.01.2009, ВВР, 2009, № 24, ст.296.)[8].
Положення про порядок здійснення криптографічного захисту інформації в Україні;	Це Положення «…визначає порядок здійснення криптографічного захисту інформації з обмеженим доступом, розголошення якої завдає (може завдати) шкоди державі, суспільству або особі…» (Про Положення про порядок здійснення криптографічного захисту інформації в Україні від 12.09.2009, 2009)
Стаття 31 Конституції України;	Згідно зі Статтею 31 Конституції України «Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під

	час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо…» (ВВР, Конституція України. [Електронний ресурс] / Офіційний веб-сайт Верховної Ради України. - Режим доступу: http://portal.rada.gov.ua/.)[10]. В цій статті проголошується, що посягання на приватну кореспонденції зазнавати не може ніхто (без офіційних підстав). Також тут конкретизуються головні види кореспонденції. Таємниця приватної кореспонденції людини належить до її особистих таємниць.