Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему
Технологія забезпечення комплексної інформаційної безпеки приватного підприємства

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

КРМКБ.180132.22.01.20 ПЗ

Виконав: студент 2 курсу, група КБм-22-1 _____ Підпис Огородник М.К.

Керівник доц., к.т.н, доцент _____ Підпис Тітова В.Ю.

Нормоконтролер старший викладач _____ Підпис Мостовий С.В.

До захисту допускаю:
Зав. кафедри кібербезпеки, к.т.н., доц _____ Підпис Кльоц Ю.П.

15 грудня 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Освітній рівень Магістр

Галузь знань 12 Інформаційних технологій

Спеціальність 125 Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"30" 08 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Огороднику Максиму Костянтиновичу
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Технологія забезпечення комплексної інформаційної безпеки приватного підприємства

Керівник роботи Тітова Віра Юріївна
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання
кандидат технічних наук, доцент

Затверджена наказом № 30 ректора університету, додаток №25 від 15.08.2023

2. Строк подання студентом проєкту (роботи) на кафедру 15.11.2023

3. Вихідні дані до проекту (роботи)Дослідження і вдосконалення політики інформаційної безпеки об'єкта інформаційної діяльності, рекомендації щодо вдосконаленої політики безпеки

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Проаналізувати вразливості інформаційної безпеки підприємства. Дослідити наявні засоби захисту підприємства. Створити систему комплексного захисту підприємства. Розробити рекомендації щодо вдосконалення.. Висновки.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали і посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В. Старший викладач кафедри кібербезпеки		

7. Дата видачі завдання «01» вересня 2023р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір напряму дослідження і узгодження тематики КРМ з керівником	01.06.2023	
2	Ознайомлення з предметною областю; формулювання мети і задач дослідження; визначення об'єкта і предмета дослідження	04.09.2023	
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	18.09.2023	
4	Робота над розділом 2 – розробка моделей і методів для вирішення поставленої задачі	02.10.2023	
5	Робота над розділом 3 – розробка алгоритмів і технологій, їх аналіз	16.10.2023	
6	Робота над розділом 4 – апробація запропонованих рішень	06.11.2023	
7	Робота над науковою публікацією	10.11.2023	
8	Узгодження отриманих результатів, оформлення пояснювальної записки згідно вимог	15.11.2023	
9	Попередній захист роботи	17.11.2023	
10	Захист роботи на засіданні ЕК	12.12.2023	

Студент _____ М.К. Огородник
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ В.Ю. Тітова
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Технологія забезпечення комплексної інформаційної безпеки приватного підприємства

Автор роботи: Огородник Максим Костянтинович

Керівник роботи: к.т.н., доц. Тітова Віра Юріївна

Загальний обсяг роботи: 74 сторінок, 11 рисунків, 12 таблиць, 1 додаток, 50 посилань.

Ключові слова: захист інформації, політика інформаційної безпеки, об'єкт інформаційної діяльності.

Розроблено політику інформаційної безпеки підприємства. Проведено техніко-економічні характеристики, виявлено основні проблеми та завдання захисту інформації. Зроблено порівняльний аналіз методів та засобів захисту інформації. Зроблено вибір та обґрунтування методів захисту інформації в корпоративній мережі підприємства. Розроблено політику інформаційної безпеки, що пропонує засоби та методи захисту даних. Здійснено розрахунок ефективності від реалізації рекомендацій щодо підвищення рівня інформаційної безпеки. Обґрунтування запропонованої концепції щодо покращення інформаційного захисту даних та прийняття політики інформаційної безпеки.

05.12.2023

ANNOTATION

Theme of qualification work: The technology of providing complex information security of a private enterprise

Author of the work: Ohorodnyk Maksym Kostyantynovich

Mentor: Ph.D. Assoc. Titova Vira Yuriyivna

Total volume of work: 74 pages, 11 figures, 12 tables, 1 appendice, 50 links.

Keywords: information protection, corporate network, trust criterion.

The company's information security policy has been developed. Technical and economic characteristics were conducted, the main problems and tasks of information protection were identified. A comparative analysis of methods and means of information protection was made. The selection and justification of information protection methods in the enterprise's corporate network has been made. An information security policy has been developed, offering means and methods of data protection. The calculation of the effectiveness of the implementation of recommendations for increasing the level of information security was made. Justification of the proposed concept for improving information data protection and adopting an information security policy.

05.12.2023

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ 4
ВСТУП 5
1 ЗАГАЛЬНІ ПОЛОЖЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ 7
1.1 Поняття комплексної системи захисту інформації 7
1.2 Сутність та задачі комплексної системи захисту інформації 10
1.3 Функції і стандарт комплексної системи захисту інформації 13
1.4 Призначення комплексної системи захисту інформації 15
2 АНАЛІЗ СИСТЕМИ ЗАХИСТУ ДАНИХ НА ПРИВАТНОМУ ПІДПРИЄМСТВІ 18
2.1 Аналіз та оцінка захисту даних в активах приватного підприємства 18
2.2 Основні проблеми та завдання захисту інформації в підприємстві 20
2.3 Обґрунтування необхідності вдосконалення забезпечення інформаційної безпеки та захисту інформації на підприємстві 24
3 РОЗРОБКА ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 26
3.1 Політика інформаційної безпеки на підприємстві 26
3.2 Вдосконалення основних положень політики інформаційної безпеки підприємства 30
3.3 Розробка організаційних підходів із забезпечення політики інформаційної безпеки підприємства 33
3.4 Розробка програмно-апаратних засобів забезпечення політики інформаційної безпеки на підприємстві 34
3.5 Використання криптографічних методів захисту даних в рамках політики інформаційної безпеки підприємства 46
4 РОЗРОБКА ТЕХНІЧНОГО ЗАВДАННЯ ТА РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ РОЗРОБЛЕНОЇ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ 51
4.1 Рекомендації щодо змісту технічного завдання і пропозиції формування змісту 51

4.2 Організація комплексного підходу із захисту підприємства відповідно до політики підприємства 65
4.3 Обґрунтування економічної ефективності реалізації політики інформаційної безпеки 69
4.4 Аналіз показників економічної результативності проекту 73
ВИСНОВКИ 79
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ 81
ДОДАТОК А Копії наукових публікацій 88

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

КСЗІ – комплексна система захисту інформації

ІБ – інформаційна безпека

ЗІ – захист інформації

АЗ – апаратного забезпечення

ЛЗ – лінії зв’язку

НС – надзвичайних ситуацій

НСД – несанкціонований доступ

ОІД – об’єкт інформаційної діяльності

ОС – операційна система

ЕЦП – Електронний цифровий підпис

ІзОД - інформація з обмеженим доступом

ВСТУП

Актуальність дослідження. Стрімкий розвиток інформаційних технологій, розширення глобального інформаційного середовища, розповсюдження засобів обміну інформацією та широка комп'ютеризація всіх сфер життя роблять важливим вивчення питання безпеки інформаційної інфраструктури. Забезпечення ефективного захисту інформації також є життєво-важливим для організацій, де щодня обробляються великі обсяги інформації з різним рівнем конфіденційності. У багатьох випадках ця інформація є конфіденційною.

Тому зростає потреба в захисті інформації від незаконного використання та несанкціонованого доступу.

Сьогодні керівництво більшості організацій не має сумнівів у тому, що їм необхідно приділяти серйозну увагу інформаційній безпеці своєї організації. Використання сучасних інформаційних технологій відкриває широкий спектр можливостей для зловживань,

Використання сучасних інформаційних технологій підвищує потенціал для ряду зловживань, пов'язаних з використанням технологій обробки інформації.

Мета дослідження. Дослідити технологію забезпечення інформаційної безпеки приватного підприємства.

Вирішено завдання дослідження.

1) проаналізовано вразливості інформаційної безпеки підприємства;

2) досліджено наявні засоби захисту підприємства;

3) створено систему комплексного захисту підприємства;

4) розроблено рекомендації щодо вдосконалення.

Предмет дослідження. Засоби та прийоми забезпечення безпеки у системі інформації.

Об’єкт дослідження. Інформація, яка знаходиться на зберіганні, обробці та передаванні в телекомунікаційних системах і мережевому середовищі захисту від внутрішніх і зовнішніх втручань і потенційних небезпек, які можуть бути умисними, випадковими, природними або створеними штучно.

Методи дослідження. Для дослідження технології забезпечення комплексної інформаційної безпеки приватного підприємства розглядаються такі питання:

1) Основні аспекти системи повного захисту інформації

2) Аналіз структури і вдосконалення комплексної системи захисту ОІД

3) Поради з формулювання завдання на виконання робіт з розробки системи захисту об'єктів інформатизації.

Наукова новизна. Полягає у висновках які були отримані в ході дослідження а саме:

1) труднощі в області забезпечення безпеки

2) аспекти захисту

Практична цінність одержаних результатів.

Отримані нові наукові висновки в ході спільних досліджень, основою для розробки та вдосконалення інтегрованих систем інформаційної безпеки для типових цілей інформаційної діяльності. Ця система спрямована на захист від впливу зовнішніх і внутрішніх втручань та різних загроз, навмисних, випадкових, природних або штучних, з метою задоволення потреб державних, бізнес структур та спеціальних підрозділів.

Перелік публікацій за темою кваліфікаційної роботи

За темою роботи опублікована стаття “Розроблення політики інформаційної безпеки приватного підприємства“ у журналі Вісник ХНУ

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Поняття комплексної системи захисту інформації

Робота із захисту інформації в нашій країні триває інтенсивно і доволі тривалий час. Сформувався значний накопичений досвід. На теперішній день ніхто не думає, що для забезпечення безпеки достатньо вжити кілька організаційних заходів та автоматизувати кілька програмно-апаратних засобів у компанії. Основний напрямок, в якому слід шукати нові способи захисту інформації, - це не тільки побудова відповідних механізмів, але й комплексне використання всіх наявних інструментів безпеки та впровадження регулярних процесів, що здійснюються на всіх етапах життєвого циклу системи обробки інформації.

При цьому всі засоби, методи і заходи, що застосовуються для захисту інформації не тільки від зловмисників, не тільки від технічних аварійних ситуацій, але і від некомпетентних або погано підготовлених користувачів і персоналу, а також технічних ситуації позаштатного характеру.

Основними питаннями, які необхідно вирішити при впровадженні системи безпеки:

– З одного боку, забезпечення захисту ідентифікації інформації в системі, тобто запобігання випадковому або навмисному доступу неавторизованих осіб до інформації; розмежування доступу до системного обладнання та ресурсів для всіх користувачів, адміністраторів, обслуговуючого персоналу та персоналу з технічного обслуговування;

– з другої сторони, система безпеки не повинна створювати помітних перешкод під час роботи користувачів з ресурсами системи.

Проблема забезпечення очікуваного рівня захисту інформації є дуже складною і її вирішення вимагає не тільки застосування окремих науково-технічних і організаційних заходів та використання спеціальних засобів і методів,

а й створення комплексної системи організаційно-технічних заходів та використання спеціальних засобів і методів захисту інформації.

Системний концептуальний підхід до інформаційної безпеки сформульовано на основі теоретичних досліджень і практичної роботи в галузі інформаційної безпеки.

Як ключова частина системного концептуального підходу, систематичність означає:

– цільова систематизація, інформаційна безпека визнається ключовою частиною загальної концепції якості інформації;

– просторова системність, забезпечує взаємопов'язані рішення всіх проблем захисту у всіх компонентах підприємства;

– системність у часі, стосується безперервності діяльності з ЗІ, що здійснюється відповідно до плану;

– організаційна системність, стосується єдності організації та управління всіма роботами, пов'язаними з ЗІ.

Концептуалізація цього підходу означає розробку єдиної концепції як повного набору науково обґрунтованих думок, суджень і рішень, необхідних і достатніх для бажаної організації та надійності захисту інформації, а також означає цілеспрямовану організацію всіх робіт із захисту інформації.

Комплексний (системний) підхід до створення системи включає в себе: першочергове вивчення предмету системи, що впроваджується; оцінку загроз безпеці предмету; аналіз інструментів, які будуть використані для створення системи; оцінка економічної доцільності, вивчення самої системи, її характеристики, принципи роботи, можливості підвищення ефективності, взаємозв'язки між усіма внутрішніми та зовнішніми факторами; можливості додаткових змін у процесі побудови системи та організація всього процесу від початку до кінця.

Комплексний (системний) підхід - це принцип дослідження проектів, який аналізує всю систему, а не окремі її частини. Завдання полягає не в підвищенні ефективності окремих частин, а в оптимізації всієї системи. Це пов'язано з тим, що,

як показує практика, поліпшення одних параметрів часто спричинює до погіршення інших, тому необхідно намагатися збалансувати протиріччя між вимогами і характеристиками.

Комплексний (системний) підхід не рекомендує починати будувати систему, поки не будуть визначені наступні компоненти:

1. Вхідні елементи. Це елементи, з яких будується система. Вхідні елементи - це типи загроз безпеці, які можуть виникнути на конкретному об'єкті;

2. Ресурси. Це кошти, які забезпечують побудову та експлуатацію системи (наприклад, матеріальні витрати, енергоспоживання, допустимі габарити тощо). Зазвичай доцільно чітко визначити типи різних ресурсів та їх допустимі витрати як в процесі створення системи, так і під час експлуатації;

3. Навколишнє середовище. Необхідно пам'ятати, що реальна система завжди знаходиться у взаємодії з іншими системами і кожен об'єкт залежить від інших об'єктів. Дуже важливо встановити межі для областей інших систем, які не слідують за відповідальними особами підприємства і знаходяться поза зоною їх відповідальності.

Типовим прикладом важливості вирішення цієї проблеми є розподіл функцій по захисту інформації, що передається сигналами в кабельних лініях, що проходять по території різних об'єктів. Незалежно від того, як встановлені межі системи, взаємодія з навколишнім середовищем не можна ігнорувати, тому що, прийняті рішення по конкретних випадках можуть виявитися марними;

4. Мета і функція. Для кожної системи необхідно сформулювати мету, до якої вона (система) прагне.

Ця мета може бути визначена як її функція і призначення системи. Чим точніше і конкретніше вказано призначення і функціонал системи, тим швидше і точніше можна буде вибрати оптимальний варіант її конструкції. Наприклад, найбільш широко сформульованою метою забезпечення безпеки об'єктів є варіант створення глобальної системи захисту, яка прояснює, як забезпечити збереження інформації, що передається, наприклад, по каналах зв'язку в будівлі, значно звужуючи спектр можливих рішень. Слід зазначити, що глобальні цілі зазвичай

досягаються шляхом досягнення менш поширених місцевих цілей. Побудова такого "дерева цілей" значно спрощує, прискорює і здешевлює процес побудови системи.

5. Критерії ефективності. Завжди необхідно враховувати різні шляхи, що ведуть до досягнення цілей, особливо різні варіанти побудови системи, яка забезпечує конкретну мету функціональності. Оцінити, який метод краще, потрібен інструмент порівняння, який є критерієм ефективності.

Він повинен характеризувати якість виконання зазначених функцій; враховувати вартість ресурсів, необхідних для виконання його функціонального призначення; мати чіткий і однозначний зміст; бути поєднуваним з основними функціями системи і дозволяти проводити кількісну оцінку на всіх етапах побудови системи.

Отже, беручи до уваги різноманіття потенційних загроз інформації всередині підприємства, складність його структури і участь людини в технологічних процесах обробки інформації, мета захисту інформації може бути досягнута тільки шляхом створення СЗІ на основі комплексного підходу[3].

1.2 Сутність та задачі комплексної системи захисту інформації

Дехто стверджує, що питання інформаційної безпеки стосуються лише інформації, яка обробляється комп'ютерами. Це може бути пов'язано з тим, що комп'ютери, зокрема персональні комп'ютери, є "ядром" або центром зберігання інформації. Інформатизація стосується заходів із захисту інформації, яка, здається, є ширшим поняттям, ніж комп'ютери.

Насправді всі ці окремі "інформаційні об'єкти" знаходяться в межах однієї організації і являють собою єдиний набір компонентів, пов'язаних спільними цілями, завданнями, структурними зв'язками та технологіями обміну інформацією.

Сучасне підприємство - це складна система, що складається з безлічі різних компонентів, об'єднаних для досягнення мети, яка може змінюватися в процесі діяльності підприємства. Оскільки різноманітність і складність впливів внутрішніх

і зовнішніх факторів часто не піддається чіткій кількісній оцінці, ця складна система може набувати нових характеристик, не притаманних її складовим.

Такі системи характеризуються, перш за все, наявністю людини в кожній зі складових підсистем і віддаленістю цієї людини від об'єкта діяльності. Це пов'язано з тим, що сукупність компонентів, з яких складається інформаційний об'єкт, може бути цілісно представлена трьома групами систем:

1) люди (біосоціальні системи);

2) техніка (технологічні системи і приміщення, в яких вони розташовані);

3) інтелектуальні посередники між людьми і технікою, тобто програмне забезпечення (інтелектуальні системи).

Поєднання цих трьох груп утворює соціотехнічну систему. Ця ідея соціотехнічної системи є дуже загальною і може бути застосована до багатьох тем. Наш інтерес обмежується дослідженням безпеки систем, призначених для обробки отриманої інформації та видачі результатів.

Дивлячись на історію питання, можна умовно виділити три періоди розвитку інформаційної безпеки (ІБ):

1. Перший період - коли обробка інформації здійснювалася традиційними (ручними та паперовими) методами;

2. Другий період - коли для обробки інформації регулярно використовувалися електронно-обчислювальні машини першого покоління;

3. Третій період - коли використання електронно-обчислювальної техніки стало масовим і повсюдним (поява персональних комп'ютерів).

У 60-70-х роках 20 століття проблема захисту інформації вирішувалася дуже ефективно, в основному за рахунок впровадження організаційних заходів. До них належали заходи безпеки, охорона, сигналізація та найпростіші програмні засоби захисту інформації. Ефективність цих заходів забезпечувалася централізацією інформації в певних місцях (спеціальних сховищах, обчислювальних центрах), що допомагало забезпечувати захист відносно невеликими силами.

"Розподілення" інформації до місць зберігання та обробки погіршила ситуацію із захистом. Стали доступними дешеві персональні комп'ютери. Це

призвело до створення комп'ютерних мереж (локальних, глобальних, національних і транснаціональних), здатних використовувати різні канали зв'язку. Ці фактори сприяли створенню високоефективних систем розвідки та збору інформації. Вони також знайшли своє відображення в сучасному бізнесі.[3]

Сучасне підприємство являє собою складну систему, в рамках якої здійснюється захист інформації.

Розглянемо основні характеристики сучасних підприємств:

– Складна організаційна структура;

– Багатовимірні функції;

– Передове технічне оснащення;

– Широка кооперація;

– Потреба у більшому доступі до інформації;

– Зростання частки цифрових технологій обробки інформації;

– Збільшення частки автоматизованих процедур у загальному обсязі обробки даних;

– Важливість і відповідальність прийняття рішень в автоматизованому режимі на основі автоматизованої обробки інформації;

– Концентрація інформаційних ресурсів в автоматизованих системах;

– Широке розповсюдження компонентів автоматизованих систем;

– Накопичення великої кількості інформації на технічних носіях;

– Інтеграція інформації різного призначення і власності в єдину базу даних;

– Довгострокове зберігання великих обсягів інформації на машинних носіях;

– Прямий і одночасний доступ великої кількості користувачів різних категорій і організацій до ресурсів (у тому числі інформаційних) системи автоматизації;

– Централізований розподіл інформації між компонентами системи автоматизації, в тому числі віддаленими один від одного.

Як бачимо, поява індустрії обробки інформації, з одного боку, створила об’єктивні передумови для підвищення продуктивності праці та рівня життя

людини, а з іншого – створила багато складних і масштабних проблем. Одним із них є забезпечення збереження та встановленого статусу інформації, яка циркулює та обробляється на підприємствах та в організаціях.

1.3 Функції і нормативні документи комплексної системи захисту інформації

Закони та норми України вимагають захист інформації, що належить державі, а також інформації з обмеженим доступом, вимоги щодо захисту якої встановлені законом, у тому числі персональні дані.

Комплексна система захисту інформації (КСЗІ) – це організаційні (обов'язкові) та технічні (при необхідності) заходи для захисту інформації від розголошення, витоку та несанкціонованого доступу.

Рисунок 1.1 – Функції КСЗІ

Створення КСЗІ в Автоматизованій Системі або Інформаційно-Телекомунікаційній Системі (далі – АС, ІТС, «цільовий об'єкт») здійснюється згідно з НД ТЗІ 3.7-003-05 "Порядок проведення робіт зі створення комплексної

системи захисту інформації в інформаційно-телекомунікаційній системі” на підставі технічного завдання, розробленого відповідно до вимог НД ТЗІ 3.7-001-99 “Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі”.[1]

Стандарт ISO/IEC 27001 — міжнародний стандарт в галузі IT, назва якого «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги». Мовою оригіналу англ. «Information technology — Security techniques — Information security management systems — Requirements».

ISO / IEC 27001 встановлює вимоги до створення, впровадження, підтримки та постійного поліпшення системи менеджменту інформаційної безпеки в контексті організації. Він також включає в себе вимоги до оцінки і обробки ризиків інформаційної безпеки з урахуванням потреб організації. Вимоги, викладені в ISO / IEC 27001 є загальними і призначені для застосування всіма організаціями, незалежно від їх типу, розміру і характеру.

Входить в групу стандартів ISO 27000 — СУІБ та тісно пов'язаний із стандартом ISO/IEC 27002.[2]

1.4 Призначення комплексної системи захисту інформації

Основною метою створення СЗІ є забезпечення надійності інформації. Система інформаційної безпеки - це організована сукупність об'єктів і суб'єктів інформаційної безпеки, організована сукупність методів і засобів захисту, що використовуються, а також вжитих заходів захисту. При цьому компоненти системи захисту інформації, з одного боку, є невід'ємною частиною системи, а з іншого - регулюють систему, реалізуючи захисні заходи.

Систему можна визначити як сукупність взаємопов'язаних елементів, метою СЗІ є інтеграція всіх компонентів захисту в єдине ціле, де кожен компонент виконує свої функції і в той же час дозволяє іншим компонентам виконувати свої функції та логічно і технічно пов'язаний з ними. Система повинна бути інтегрована в єдину систему.

Надійність захисту інформації прямо пропорційна системному підходу. Якщо окремі компоненти не узгоджуються між собою, ризик порушення безпеки зростає.

По-перше, необхідність комплексного рішення полягає в об'єднанні локальних КСЗІ в єдине ціле, водночас вони повинні функціонувати як єдиний "пучок". Наприклад, до локальних КСЗІ можна віднести такі види захисту інформації (правові, організаційні та технічні).

По-друге, потреба в інтегрованих рішеннях випливає з призначення самої системи. Система повинна логічно і технічно об'єднувати всі компоненти захисту. Однак вона не вирішує питання цілісності цих компонентів і не враховує всі елементи, які можуть гарантувати або впливати на якість захисту.

Наприклад, система може охоплювати багато об'єктів захисту, не всі з яких можуть бути включені до неї. Таким чином, якість і надійність захисту залежить не тільки від типу компонентів системи, але й від їхньої повноти, за умови, що всі фактори та умови, які впливають на захист, враховані. Цілісність усіх компонентів системи захисту на основі аналізу цих факторів та умов є другою метою комплексності.

При цьому слід враховувати всі параметри вразливості інформації, потенційні загрози її безпеці, охоплювати всі необхідні цілі захисту, використовувати всі можливі види захисту, методи, інструменти та людські ресурси, необхідні для захисту, і все це повинно базуватися на цілях і завданнях. Робити це відповідно до цілей і завдань захисту від інцидентів.

По-третє, система може забезпечити безпеку всієї інформації за будь-яких обставин лише за умови комплексного підходу до її захисту. Це означає, що всі носії інформації повинні бути захищені в усіх місцях, де інформація збирається, зберігається, передається та використовується, і в усіх формах функціонування системи обробки інформації.

Навпаки, складність не усуває, а натомість забезпечує спеціалізований підхід до захисту інформації, який залежить від складу її носіїв інформації, пов'язані з нею види таємниці, ступінь її конфіденційності, засоби її зберігання та обробки, форми

та умови її розголошення, канали та способи отримання несанкціонованого доступу до інформації.

Тому важливість комплексного підходу до захисту інформації полягає в наступному:

– Інтеграція локальних систем захисту;

– Забезпечення цілісності всіх компонентів системи захисту;

– Забезпечення комплексності захисту інформації.

Виходячи з цього, можна дати наступне визначення:

“Комплексна система захисту інформації - це система, яка повністю і всебічно охоплює всі елементи, процеси і засоби для забезпечення безпеки всієї інформації, що захищається.”

2 АНАЛІЗ СИСТЕМИ ЗАХИСТУ ДАНИХ НА ПРИВАТНОМУ ПІДПРИЄМСТВІ

2.1. Аналіз та оцінка захисту даних в активах приватного підприємства

В результаті дослідження сфер діяльності організації можна виділити наступні інформаційні активи:

– інформація/дані (в т.ч. секретна документація генпланів міських комунікацій, проектна документація організацій, особисті дані клієнтів тощо);

– апаратні засоби (комп'ютери, сховища даних, оргтехніка);

– програмне забезпечення, включаючи прикладні програми;

– документи у паперовому вигляді (у т.ч. договори, скани генпланів, виписки з державних реєстрів тощо);

– конфіденційність та довіра при наданні послуг.

Усі активи компанії можна розглянути з позиції цінності та розташувати їх у порядку зростання:

– прикладне програмне забезпечення;

– системне програмне забезпечення;

– особисті відомості про працівників;

– особисті дані клієнта;

– проектна документація, плани комунікацій;

– стратегічного призначення;

– проектна документація, одержана від замовника;

– проектна документація, розроблена організацією;

Таким чином, у компанії виявлено безліч активів, пов'язаних із інформаційними даними. Відповідно для них можуть бути виділені такі вразливості:

– дії зловмисників;

– вихід із ладу апаратного забезпечення (АЗ);

– нестача ресурсів АЗ;

– конструктивні недоліки програмного забезпечення (ПЗ);

– вихід з ладу ПЗ;

– нестача ресурсів ПЗ;

– викрадення під час передачі по лініях зв'язку (ЛЗ);

– підміна під час передачі по ЛЗ;

– відмова в обслужувані ЛЗ;

– помилки користувача;

– розголошення конфіденційної інформації;

– недбале ставлення до інформаційної безпеки;

– саботаж;

– виникнення НС;

– обставини непереборної сили.

Загрози безпеки підприємства можуть мати природний чи людський чинник, загрози можуть виникнути як випадково, і навмисно. Для підприємства необхідно і вкрай важливо не пропустити жодної загрози інформаційній безпеці, оскільки можливі збитки можуть бути дуже значними, але й акцентувати увагу на незначних загрозах не треба, тому що може бути задіяно дуже багато коштів, а шкоди підприємству може бути не завдано.

Після того як виявлено можливе джерело загрози та сектор, схильний до загрози (об'єкт загрози), треба визначити можливість і розміри здійснення загрози. Для цього необхідно врахувати аналітичні дані, такі як:

частоту виникнення небезпеки;

– мета загрози, використовувані ресурси та можливості здійснення

– тієї чи іншої загрози;

– наскільки привабливим є ресурс, на який впливає загроза;

– наскільки можливі виникнення випадкових загроз, що з географічним чинником, реалізацією яких може бути природна чи техногенна катастрофа.

Для проведення аналітики щодо загрози, що виникла, необхідно скористатися статистичними даними, якщо такі є.

Статистичні дані дозволять визначити, як часто виникає загроза і на що націлена, яких збитків може завдати.

По даному пункту можна дійти невтішного висновку що з цієї компанії є вразливі інформаційні активи, які потрібно захищати. А для більш правильного вибудовування політики інформаційної безпеки необхідно визначити основні проблеми та завдання захисту інформації на підприємстві.

2.2 Основні проблеми та завдання захисту інформації в підприємстві

У компанії під час роботи з великим обсягом конфіденційних даних стоїть першочергове завдання організації захисту, тобто, визначення заходів, спрямованих на створення, забезпечення та - підтримку інформаційної безпеки. Об'єкт захисту інформації є інформацією або інформаційним процесом, який вимагає забезпечення захисту від несанкціонованого доступу, порушення цілісності та структурованості даних.

Мета захисту інформації - це отримання результатів від запобігання збиткам, зумовленим витоком або несанкціонованим впливом на інформацію. Ефективність захисту інформації дозволяє визначити рівень відповідності результатів використовуваної системи захисту даних до поставлених цілей. Виділяють такі основні види захисту інформації:

1. Захист інформації від витоків – це заходи, створені задля безпеку і цілісність конфіденційних даних, що використовуються в внутрішньому та зовнішньому документообігу підприємства.

2. Захист даних від розголошень – це заходи, направлення на запобігання необережним, умисним діям співробітників чи інших осіб, які оголосили конфіденційну інформацію, що може призвести до подальшу передачу даних.

3. Захист даних від несанкціонованого доступу (НСД) – це заходи, спрямовані на заборону доступу до комп'ютерної мережі за рахунок застосування комплексу інженерно-технічних, програмних та організаційних засобів.

Крім того, необхідно розробити систему захисту даних, що включає сукупність технічних, програмних, криптографічних та організаційних засобів, що дозволяють забезпечити безпеку мережі в будь-якій момент часу від випадкового чи навмисного впливу, а також несанкціонованого використання.

Безпека даних – це стан захищеності даних, при якому забезпечені цілісність, конфіденційність та доступність. Інформаційна безпека є однією з головних проблем сучасного суспільства та обумовлена збільшенням значущості інформації в основних бізнес процесах.

Проблеми захисту інформації в даний час пов'язані з дестабілізуючим впливом зовнішніх та внутрішніх загроз, що виникають у компанії та впливають на її функціонування. У свою чергу, поняття проблема безпеки даних взаємопов'язане із поняттям загроза безпеці. Це призвело до того, що в діяльності підприємств все більше виникає проблем, які негативно впливають на систему управління, а також технологічну підтримку в питаннях зберігання та обробки даних. Тому методи та інструменти для забезпечення комплексної системи захисту на підприємстві мають виконувати моніторинг загроз на рівні інформаційного, апаратного та програмного забезпечення. Розвиток комп'ютерних технологій, апаратного та програмного забезпечення розширило коло проблем захисту інформаційних потоків, що циркулюють у комп'ютерних мережах від несанкціонованого доступу. Основною проблемою є необхідність забезпечення необхідного рівня захисту, при якому необхідно враховувати, що інформація, що передається через комп'ютерну мережу, може бути отримана зловмисником і передана каналами зв'язку.

Проблеми інформаційної безпеки поділяють на три основні види:

– перехоплення даних, пов'язане з порушенням конфіденційності інформації;

– модифікація або зміна даних, пов'язаних із зміною вихідного повідомлення або повної його заміни з наступним пересиланням адресату;

– порушення авторства інформації, тобто передача інформації не від імені автора, а від імені зловмисника.

Для того, щоб здійснити перехоплення конфіденційної інформації, зловмисником використовуються віруси, кейлоггери, троянські програми, шкідливе та шпигунське програмне забезпечення. Проблеми захисту мережі пов'язані з тим, що не кожна антивірусна програма може своєчасно виявити загрози, що виникли в мережі, і це створює можливість для зловмисника використовувати мережу для досягнення поставлених цілей. Однак можливість перехоплення інформації не завжди створює можливість отримання доступу до захищених даних, з наступною модифікацією. Як приклад перехоплення інформації може виступати мережевий аналіз трафіку в мережі. У разі зловмисник отримує інформацію про мережі підприємства, але можливість спотворювати цю інформацію немає. Проблеми безпеки даних пов'язані з розвитком глобальної мережі Інтернет, яка користується популярністю серед різних категорій користувачів.

Посилення глобалізації, а водночас і інформатизації створює можливості для зловмисника з будь-якої точки світу створювати загрози безпеці для комп'ютерної мережі.

До основних завдань інформаційної безпеки даних відносяться:

– забезпечення конфіденційності, цілісності та структурованості інформації;

– організація своєчасного виявлення та запобігання зовнішнім та внутрішніх загроз;

– запровадження організаційних, інженерно-технічних, апаратно-програмних методів, що дозволяють посилити захист даних;

– розробка та вдосконалення політики безпеки з урахування сучасних тенденцій розвитку апаратного та програмного забезпечення.

Для підприємств завдання забезпечення захисту даних є одними з першочергових, оскільки, виступаючи як об'єкт постійного уваги зловмисників. Отже, інформаційна безпека спрямована на забезпечення достатнього та необхідного рівня захисту інформації, що багато в чому визначається платіжними,

інформаційними та іншими процесами. Збої, що виникають у роботі інформаційної структури підприємства можуть завдати значних збитків у галузі отримання інформації для забезпечення стабільності основних бізнес-процесів.

Тому інформаційна безпека постійно контролюється, вживаються заходи для управління ризиками, розробляються документи, які є основною стандартизацією управління захистом інформації. Особливого значення при забезпеченні інформаційної безпеки приділяється формальним методам захисту інформації, в основі яких знаходиться стандартизація. Головною метою стандартизації є підвищення довіри, виконання необхідних заходів щодо захисту інформації від загроз і використання методів зниження ризиків.

Для забезпечення захисту даних підприємства повинні виконувати такі завдання:

– забезпечувати високий рівень організації та функціонування підрозділів у галузі інформаційної безпеки підприємства;

– здійснювати корекцію у сфері функціонування системи захисту даних;

– розробляти плани з управління ризиками порушення інформаційної безпеки та забезпечуватися високий рівень організації впровадження даних планів у основні бізнес-процеси підприємства;

– коригувати внутрішній документообіг у сфері захисту даних;

– приймати управлінські рішення у сфері вдосконалення системи захисту даних, а також розробляти та організовувати програми навчання співробітників, заходи щодо підвищення обізнаності працівників підприємства у галузі захисту даних;

– здійснювати постійний моніторинг виявлення загроз та удосконалюватись заходи щодо їх ліквідації;

– впроваджувати сучасні методи захисту даних, проводити внутрішній та зовнішній аудит інформаційної безпеки;

– приймати рішення у сфері вдосконалення політики безпеки підприємства, коригуватися концепція та стратегія в галузі інформаційної безпеки.

Таким чином, було визначено основні завдання, які будуть покладено в основу організації системи інформаційної безпеки та захисту даних у аналізованої компанії.

2.3 Обґрунтування необхідності удосконалення забезпечення інформаційної безпеки та захисту інформації на підприємстві

При загальному аналізі можливих загроз підприємству можна дійти невтішного висновку про те, що поточний стан інформаційної безпеки організації перебуває у задовільному стані і потребує певного вдосконалення.

Таким чином, у рамках розробки комплексної інформаційної безпеки було ухвалено рішення вести розробку у трьох напрямках.

1. Розробка адміністративних методів забезпечення інформаційної безпеки.
2. Розробка програмно-апаратних методів інформаційної безпеки.
3. Розробки інженерно-технічних методів інформаційної безпеки.

Перший напрямок - регламентація робочого графіку компанії, запровадження регламенту перебування сторонніх осіб на території компанії та запровадження регламенту на робочих місцях співробітників.

Розробка даного напряму організації стратегії інформаційної безпеки узгоджено з керівником організації. Контроль за впровадженням методології покладається на співробітників підрозділів та служби безпеки.

Особлива увага приділяється розвитку другого напрямку:

- централізованої установки антивірусного програмного забезпечення;
- організацію міжмережевого екрану;
- організацію засобів розподілу інтернет-трафіку;
- організацію засобів централізованої авторизації користувача;
- заборона використання зовнішніх накопичувачів;
- організацію обміну інформацій між комп'ютерами;
- організацію розподілу доступу;
- оновлення програмного забезпечення до актуальних стабільних версій;

– організацію резервного копіювання даних.

Виконання інструкцій, щодо даного напряму буде покладено на IT персонал організації.

Розробка інженерно-технічних засобів передбачає використання засобів інженерно-технічного характеру:

– використання датчиків руху;

– впровадження відеокамер спостереження;

– використання «тривожних кнопок».

Виконання цих рекомендацій буде покладено на підрядні організації та організації, що займаються приватною охоронною діяльністю. Контроль за виконанням заходів проводитиме директор організації та завгосп офісного центру (не є співробітником компанії).

За підсумками розробка всіх трьох напрямів зводиться до єдиних вимог:

1. Усунути можливі загрози інформаційній безпеці усередині підприємства.

2. Усунути можливі загрози у віртуальному просторі глобальної мережі.

3. Усунути можливі загрози вільного проходу на підприємство та доступу до інформації.

Для більш ретельного вивчення інформації з цього питання необхідно розглянути основні положення політики інформаційної безпеки підприємства, спираючись на вимоги, яких необхідно досягти.

3 РОЗРОБКА ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Політика інформаційної безпеки на підприємстві

Політика інформаційної безпеки підприємства представлена комплексом документів, що дозволяють відобразити вимоги щодо забезпечення захисту даних та основні напрямки підприємства щодо забезпечення безпеки. Під час створення політики безпеки можна виділити три основні рівні: верхній, середній та нижній.

Верхній рівень політики безпеки даних організації дозволяє:

– сформулювати та демонструвати ставлення адміністрації

– підприємства до системи захисту інформації та відобразити основні цілі та завдання у цій галузі;

– розробити індивідуальні політики безпеки, інструкції та правила, за допомогою яких регулюються окремі питання;

– інформувати співробітників організації про основні завдання та пріоритети у сфері інформаційної безпеки.

Політика інформаційної безпеки середнього рівня служить для відображення відносин та вимог підприємства до:

– використання інформаційних систем;

– телекомунікаційних та інформаційних технологій, методів та підходів до обробки інформації;

– учасникам процесів обробки інформації, від яких залежить забезпечення захисту інформації на підприємстві.

Нижній рівень політики безпеки слугує для опису певних процедур та документів для забезпечення інформаційної безпеки на підприємстві.

Етапи розробки політики безпеки в організації включають:

– виконання оцінки особистого ставлення до загроз безпеці з боку власників та співробітників підприємства;

– проведення аналізу потенційно важливих інформаційних активів підприємства;

– виявлення існуючих загроз безпеці підприємства з наступною оцінкою ризиків.

При створенні політики безпеки всіх рівнів потрібно дотримуватися того, що розроблена політика безпеки на нижньому рівні повинна відповідати безпеці, наведеній на верхньому рівні. При цьому в тексті політики безпеки мають бути наведені правила, які не мають подвійного змісту і він має бути достатньо зрозумілим для працівників підприємства. Важливе значення для захисту інформації у компанії має політика безпеки, представлена у вигляді логічно та семантично пов'язаних, формованих та аналізованих структур даних, що використовуються для захисту інформації на всіх рівнях функціонування підприємства.

Розглянемо основні складові інформаційної політики безпеки підприємства Під захистом у разі передбачається використання наведених у безпековій політиці підприємства організаційних заходів захисту інформації. За допомогою політики інформаційної безпеки на підприємствах виконують зовнішній і внутрішній аудит захисту даних, результати якого використовуються для визначення рівня ефективності, використовуваних методів та засобів захисту. У свою чергу покращення виступає у вигляді підстроювання заходів політики безпеки з використанням отриманих результатів проведення тестування та моніторингу.

Політика безпеки у процесі функціонування підприємства має постійно оновлюватись. При цьому внесені зміни підлягають постійному порівнянню з тими методами та засобами, що вже використовуються. Основні складові політики інформаційної безпеки підприємства можна у вигляді схеми, наведеної на рисунку 3.1.

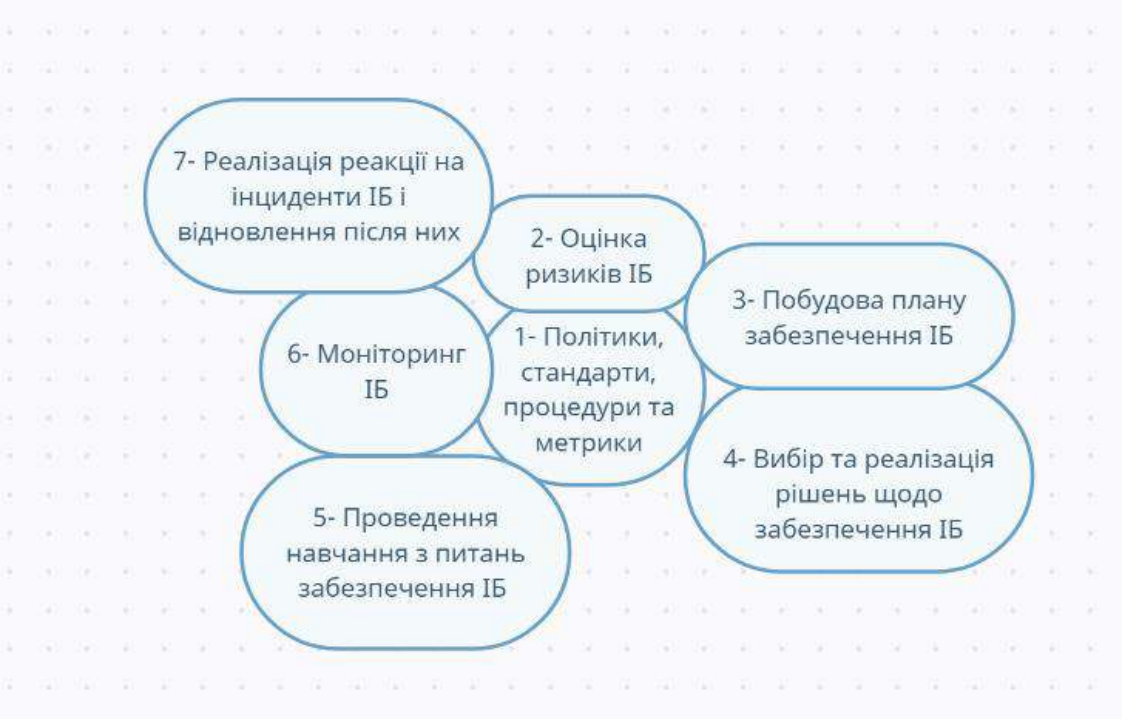

Рисунок 3.1 – Основні складові інформаційної політики безпеки підприємства

Як видно з рисунку 3.1 у політиці інформаційної безпеки відображаються взаємопов'язані етапи організації інформаційної безпеки підприємства, які представлені процедурами, що дозволяють систематизувати та ефективно вирішувати поставлені завдання для того, щоб досягти необхідного рівня захисту даних.

На першому етапі необхідно визначити межі, в рамках яких функціонуватиме політика інформаційної безпеки підприємства, поставити критерії для оцінки результатів.

На етапі аналізу ризиків інформаційної безпеки описується склад та визначаються пріоритети обраних засобів захисту з розподілом їх за ступенем важливості для підприємства, ідентифікуються вразливості активів підприємства та визначатиметься шкода. Результати аналізу ризиків інформаційної безпеки підприємства будуть застосовуватись у вигляді основи для планування роботи системи інформаційної безпеки, вибору найефективнішої стратегії та тактики. Для підвищення ефективності політики безпеки застосовуються такі прийоми як

групове визначення об'єктів безпеки, непряме визначення з використанням вірних атрибутів та мандатне керування доступом.

Багато підприємств використовують глобальну та локальну безпекову політику, засновані на принципах управління безпекою інформації. Глобальна політика інформаційної безпеки спрямована на забезпечення захисту інформації на рівні бізнес-процесів компанії, а локальна політика формується лише на рівні захисту даних підприємства.

У глобальній політиці підприємства представлені правила безпеки, що описують можливу взаємодію між об'єктами, для яких потрібне забезпечення захисту інформації. У загальному вигляді глобальну політику безпеки можна як структури наведеної рисунку 3.2.

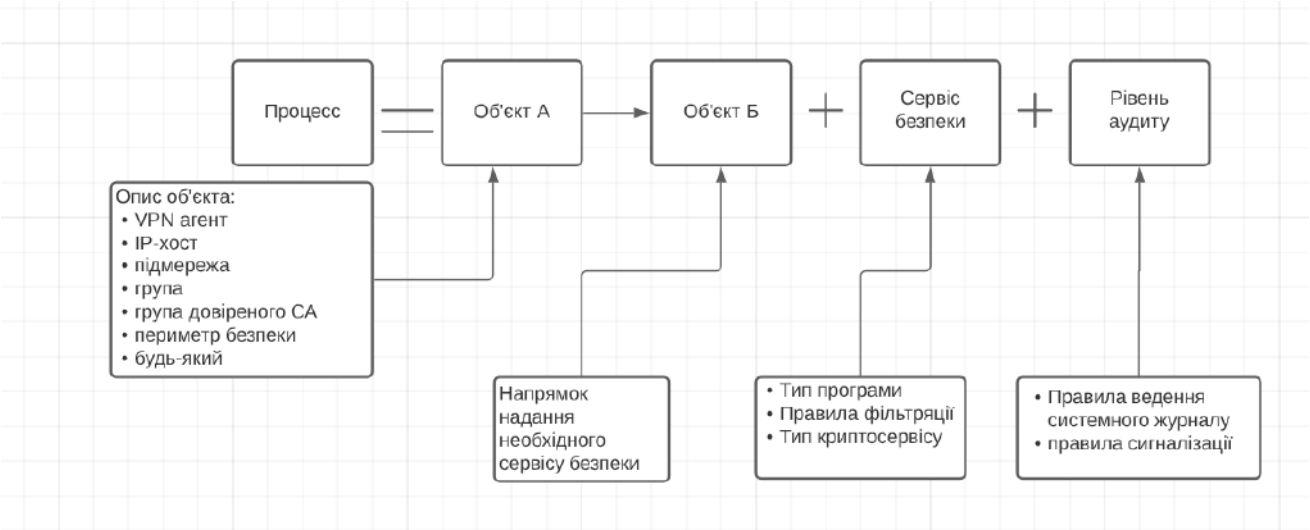

Рисунок 3.2 – Загальна структура глобальної безпекової політики підприємства

За рахунок використання наведеної на рисунку 3.2 глобальної політики для забезпечення захисту інформації виконують правила автентифікації об'єктів, обмін ключами, ведуть запис результатів безпеки в спеціальний журнал та облік ризиків безпеки даних. Як об'єкти для глобальної безпекової політики виступають окремі робочі станції та підмережі, що включають до свого складу структурні підрозділи підприємства.

У глобальній безпековій політиці компанії правила функціонально розбиваються на такі групи:

– правила VPN, які реалізовані за допомогою протоколів IPSec. Як агент виконання цих правил виступає драйвер VPN, встановлений в стеках клієнтських пристроїв або шлюзах безпеки;

– правила пакетної фільтрації, що дозволяють забезпечити фільтрацію пакетів типів stateless та stateful;

– проксі - правила, з включенням антивірусного захисту, які відповідають за фільтрацію трафіку, що передається через прикладні протоколи. В даному випадку як виконавчий агент виступає проксі-агент;

– правила авторизованого доступу із застосуванням правил одноразового входу, що дозволяють забезпечити роботу користувачів за паролями. Ці правила виконуються агентами різних рівнів від VPN-драйвера до проксі-агентів. Як агенти виконання таких правил захисту інформації виступають системи авторизації;

– правила, що відповідають за протоколювання подій, уразливостей у системі захисту інформації. У компанії політика ведення журналів подій виконується агентом протоколювання, а як виконавці виступає повністю вся інформаційна система. За допомогою локальної політики безпеки підприємства виконується налаштування засобів захисту інформації та реплікуються налаштування для вузлів з виконанням їх подальшого коригування. Загалом у локальній безпековій політиці підприємства розміщені правила за допомогою яких регламентуються з'єднання, змінюються настройки мережевих пристроїв.

3.2 Вдосконалення основних положень політики інформаційної безпеки підприємства

До цього моменту на об'єкті проводилася цілеспрямована розробка та впровадження політики інформаційної безпеки. Використання методів інформаційної безпеки було нерегулярним і обмежувалося встановленням

безкоштовного антивірусного програмного забезпечення та фізичного захисту (Замикання приміщень на ніч). Дана недбалість з боку інформаційно-технічного персоналу не привела до інцидентів, що становили загрозу для діяльності організації. Тому було ухвалено рішення про необхідність вдосконалення комплексної інформаційної політики безпеки.

Нижче буде розглянуто існуючий захист інформаційної безпеки з погляду:

– програмне забезпечення;

– технічного забезпечення.

Результати обстеження об'єкта щодо наявності інформаційної безпеки внесено до таблиці 3.1.

Таблиця 3.1 - Аналіз виконання основних задач із забезпечення захисту інформації

Основні завдачі щодо захисту безпеки інформації	Стан реалізації
1	2
Забезпечувати безпеку діяльності та захищати інформацію, що становить комерційну таємницю.	Задовільне
Організація робіт з правового, організаційного та інженерного (фізичного, апаратного, програмного та математичного) захисту комерційної таємниці.	Задовільне
Формування особливої роботи з документами, що унеможливлює сторонній прийом інформації, що становить комерційну таємницю.	Задовільне
Запобігання необґрунтованому допуску та відкритому доступу до відомостям та роботам, що становлять комерційну таємницю;	Задовільне
Виявлення та обмеження ймовірних каналів витоку інформації з обмеженим доступом, в екстремальних ситуаціях (нещасні випадки, пожежі і т. д.), в ході повсякденної виробничої діяльності;	Проводилося

Кінець таблиці 3.1

1	2
Забезпечення режиму безпеки під час здійснення таких видів діяльності, як різноманітних конференцій, перемовин, зборів та інші заходів, яке пов’язане з комерційною співпрацею на національному рівні;	Не проводилося

З таблиці 3.1 видно, що становище компанії стосовно стандартам захисту залишається задовільним. Дані, вказані в таблиці, показують, що обраний напрямок розробки інформаційної безпеки є актуальним.

Таким чином, можна зробити висновок, що компанія потребує вдосконалення політики інформаційної безпеки та обрані рішення є актуальними на даному підприємстві.

У третьому розділі дано визначення основним термінам та поняттям, пов'язаним з політикою захисту інформації, дано опис підприємства, проведено порівняльний аналіз системи безпеки, отримані наступні авторські висновки:

– основною проблемою є необхідність забезпечення необхідного рівня захисту, при якому необхідно враховувати, що інформація, що передається по комп'ютерній мережі, може бути отримана зловмисником та передана каналами зв'язку;

– головною метою стандартизації є підвищення довіри, рівня стабільності роботи мережі, виконання необхідних заходів щодо захисту інформації від загроз і впровадження методів для зниження ризиків;

– також необхідно розробити документи, які становитимуть основу політики інформаційної безпеки.

Отримані результати та сформульовані висновки дозволяють перейти до розгляду матеріалу третього розділу, присвяченого опису та визначення класифікації основних загроз інформаційній безпеці.

3.3 Розробка організаційних підходів із забезпечення політики інформаційної безпеки підприємства

При побудові інформаційної безпеки підприємства використовуються міжнародні стандарти інформаційної безпеки ISO 17799. Управління безпекою відповідно до ISO 17799 ISO (Міжнародна організація стандартів) є міжнародним органом із встановлення стандартів, який складається з представників національних органів стандартизації кожної країни. ISO встановлює світові промислові та комерційні стандарти.[4]

Стандарт ISO 17799 — це стандарт системи управління інформаційною безпекою, який було вдосконалено та впроваджено для використання компаніями для захисту їхніх даних або інформації. За допомогою стандарту ISO 17799 ми зможемо вимірювати, чи система інформаційної безпеки, яку ми впровадили, є ефективною та забезпечує гарантії безпеки для споживачів. До введення ISO 17799, у 1995 році, Британський інститут стандартів (BSI) запустив перший у світі стандарт з управління інформацією, а саме «B 7799», частина перша: Кодекс практики управління безпекою інформації, який базується на базовій інфраструктурі B 7799 Потім 1 грудня 2000 року був опублікований новий стандарт ISO 17799 з управління інформацією. Використання стандарту ISO 17799 передбачає наступне:

– Документи політики інформаційної безпеки;

– Відповідає за інформаційну безпеку;

– Освітні та навчальні програми з інформаційної безпеки існують для всіх користувачів;

– Розробити систему звітності про події безпеки;

– Ознайомлення з методами боротьби з вірусами;

– Розробити план безперервності бізнесу;

– Контроль копіювання пропрієтарного програмного забезпечення;

– Супровідний лист організаційних архівів для дотримання потреб захисту даних;

– Встановити процедури для дотримання політики безпеки.

Між тим, політика контролю або контролю відповідно до стандарту ISO 17799 включає: політики безпеки, організацію безпеки, класифікацію та контроль активів, безпеку персоналу, фізичну безпеку та контроль навколишнього середовища, розвиток та управління комп'ютерною мережею, системи контролю доступу, обслуговування системи, безперервність бізнесу планування та відповідність. . Щоб мінімізувати ризик загроз безпеці, які завдають шкоди бізнесу, ці проблеми потрібно вирішувати за допомогою превентивних дій без необхідності чекати в надзвичайних ситуаціях, щоб вжити заходів безпеки. Щоб бути проактивним щодо потреб безпеки, архітектура безпеки включає три основні елементи: Політика компанії полягає в участі керівництва в розподілі ресурсів і стратегічному баченні та глобальних проблемах у безпеці, індивідуальній поведінці (навчання співробітників і наявність комунікаційного процесу).

3.4 Розробка програмно-апаратних засобів забезпечення політики інформаційної безпеки на підприємстві

Програмно-апаратний комплекс (ПАК) представляє собою інтегровану систему, яка включає в себе як апаратне, так і програмне забезпечення для вирішення конкретної задачі або набору завдань. У контексті інформаційної безпеки підприємства програмно-апаратний комплекс може бути спроектований для забезпечення комплексного захисту інформації та інфраструктури.

Програмний комплекс на цьому підприємстві включає такі компоненти: операційна система Windows 7, 8 антивірус Avast Antivirus. Захист паролем у програмному комплексі відповідає звичайним порогам доступу для користувачів Windows, дані передаються в Інтернет без використання безпечної технології підключення VPN. Для розширеного функціонування комплексу на сервері необхідно зробити: налаштувати між мережевого екрану, встановлення поштового сервера і проксі-сервера.

Апаратний комплекс підприємства представлений наступним чином:

– D-Link DUB-1341 4xUSB3.0;

– принтери HP Laser 107a;

– сканери Canon LiDE 300.

Програмний та апаратний комплекс є одним робочим комплексом, що називається надалі програмно-апаратний комплекс.

Таблиця 3.2 – Проведені заходи щодо посилення безпеки мережі підприємства.

Об'єкт	Заходи
Сервер	Оновлення ОС Оновлення антивірусу Встановлення між мережевого екрану Встановлення проксі-сервера Встановлення поштового сервера
Робочі станції	Оновлення ОС Оновлення антивірусу Встановлення парольних захистів
З'єднання	Використання безпечного підключення до Інтернету

Комплексна політика інформаційної безпеки включаючи техніку та технології забезпечення комп'ютерної безпеки вважається елементом профілактики комп'ютерних злочинів. Захистом інженерних технологій прийнято вважати сукупність заходів, технічних засобів та заходів щодо забезпечення інформаційної безпеки.

Для перешкоджання інструментам технічної розвідки, компанії використовують методи шифрування, апаратної, прошивки, фізичної та забезпечення захисту інформації.

Фізичні методи захисту інформації стосуються захисту приміщень компанії, місць з робочими станціями, а також комп’ютерного обладнання та носіїв. Апаратні методи захисту означає апаратне обладнання як окремих технічних засобів, комп'ютерної техніки, які використовуються захисту цих систем. Таким чином, змінюється структура інженерно-технічного комплексу інформаційної безпеки та захисту інформації підприємства, зображена рисунку 3.3

Рисунок 3.3 – Структура інженерно-технічного комплексу

За допомогою інженерно-технічного комплексу на підприємстві ми обмежуємо доступ до мережі та проводимо розмежування доступу до бази даних. Щоб запобігти копіюванню даних на зовнішні носії, потрібно запечатати корпус на всіх особистих робочих місцях та демонтаж засобів підключення зовнішніх носіїв. Для цього, в з метою забезпечення інформаційної безпеки комп'ютерної мережі було проведено такі заходи (див. табл. 3.3).

Таблиця 3.3 – Здійснені заходи посилення інформаційного захисту

Об'єкт	Заходи
Сервер	Засоби для обмеження фізичного доступу
1	2

Кінець таблиці 4.1

1	2
Вузли мережі	Засоби для обмеження фізичного доступу
Комп’ютери	Герметизація корпусу за допомогою спеціального замикаючого пристрою. Демонтаж інструментів для підключення зовнішніх носіїв.

Необхідними для представлення комплексу інженерно-технічних засобів є такі задачі:

– попереджувати проникнення зловмисників у ресурси, щоб знищити, вкрасти чи змінити;

– захист носіїв інформації від знищення внаслідок дії сил природи і перш за все вогню та води при його гасінні;

– запобігання витоку інформації з різних технічних каналів.

Забезпечення ефективного інженерного та технічного захисту інформації, треба вирішити:

– що у цій організації, будівлі, приміщенні підлягає захисту;

– яким загрозам наражається інформація, що захищається з боку зловмисників та їх технічних засобів;

– які методи та інструменти краще використовувати для гарантій безпеки інформації з урахуванням як масштабів загрози, так і затрат на її запобігання;

– як влаштувати та реалізувати технічний захист інформації в організації.

Для організації було виділено такі об'єкти інженерно-технічного захисту, які були розділені за класами захисту:

1. Об'єкти першого (найвищого класу) захисту. До даних об'єктів захисту були віднесені всі носії інформації, знищення чи розкрадання яких призведе до зупинення діяльності фірми, несення великих фінансових втрат, виникнення конфліктів із законом тощо.

2. Об'єкти другого класу захисту. До цих об'єктів було віднесено об'єкти, знищення чи розкрадання яких спричинить ускладнення у роботі компанії, викликати тимчасові простої.

3. Об'єкти третього класу захисту, до даних об'єктів були віднесені об'єкти, знищення чи розкрадання яких незначно позначиться чи ніяк не вплинути на діяльність фірми.

Дані за важливістю об'єктів, що захищаються, зведені в таблицю 3.4

Таблиця 3.4 Розподіл по важливості об'єктів, що захищаються

№ п/п	Клас	Найменування об'єкта
1	1	Комп'ютер керівника
2	1	Комп'ютер гол. бухгалтера
3	1	Документи керівника
4	1	Документи гол. бухгалтера
5	1	Сервери
6	2	Документи бухгалтерії
7	2	Інші документи
8	3	Комп'ютер системного адміністратора
9	3	Комп'ютери бухгалтерії
10	3	Комп'ютер відділу кадрів
11	3	Інші носії інформації

Для охорони вирішено було задіяти такі інженерно-технічні методи для забезпечення інформаційної безпеки:

1) вдосконалення наявної системи відеоспостереження;

2) встановлення детекторів руху;

Дані кошти дозволяють скоротити ризик втрати, як інформації, і цінного майна, внаслідок спроби навмисного викрадення інформаційних носіїв чи матеріальних цінностей або за виникненні займання. Оскільки придбання, установка і обслуговування обходяться компаніям дорого, було вирішено відмовитися від використання засобів запобігання прослуховування та інших засобів шпигунства.

Для забезпечення безпеки інформації були визначені 3 класи об'єктів, необхідних для захисту, в якості переліку заходів і дій, необхідно усунути проблеми безпеки в корпоративних системах. Однак від засобів захисту було вирішено відмовитися від прослуховування та інших засобів захисту від шпигунства.

Реалізація розроблених заходів інформаційної безпеки з застосуванням конкретних засобів описано у таблиці 3.5.

Таблиця 3.5-Реалізація розроблених заходів інформаційної безпеки.

Об'єкт	Захід	Суть проведення
1	2	3
Сервер	Оновлення ПЗ	Встановлення останніх оновлень серверних операційних систем для усунення вразливостей захисту, налаштування автоматичних оновлень.
Сервер	Оновлення антивірусу	Встановлення сучасної ліцензійної антивірусної NOD 32 з налаштуванням постійних оновлень антивірусних баз.
Сервер	Встановлення між мережевого екрану	Встановлення між мережевого екрану Microsoft ISA Server
Сервер	Встановлення проксі-сервера	Встановлення між мережевого екрану Microsoft ISA Server
Сервер	Встановлення поштового сервера	Встановлення поштового сервера Microsoft Exchange
Робоча станція	Оновлення ОС	Для машин з Windows XP та Windows 7 зміна ОС на Windows 10, налаштування автоматичних оновлень.

Кінець таблиці 3.5

1	2	3
Робоча станція	Використання парольних захистів	Заклад груп користувачів у Microsoft Active Directory з подальшою генерацією індивідуальних паролів та настроюванням групових політик.
З'єднання	Використання захищеного Інтернет-з'єднання для обміну інформацією з головним офісом	Для безпечного обміну даними з головним офісом було використано захищене VPN з'єднання з локальною мережею основного офісу захищене 128 бітним шифруванням трафіку

Таким чином, використання розроблених заходів безпеки дозволить організувати політику інформаційної безпеки, а також скоригувати структуру апаратно-програмного комплексу, що реалізується.

Структура програмного складу комплексу наведено в рисунку 3.4.

У структуру оновленого пакету програмного забезпечення було включено:

1) сервер 1С: працює на ОС Windows 7, на ньому розташовується база програми 1С Підприємство 8.1; антивірус, встановлений на даному сервері NOD 32. Доступ поширюється через службу каталогів Active Directory.

2) сервер IBM – працює на ОС Windows 7, на ньому розміщується файл-сервер, а також Firewall. Підключення до інтернету здійснюється через брандмауер, а інформація з робочих станцій із прикладних програм надходить на файловий сервер.;

3) На комп’ютерах одного типу встановлена ОС Windows 7, на них установлена: програма 1С підприємство (клієнт), Microsoft Office 2016, а також браузер Internet Explorer 11, антивірус NOD 32;

4) .На комп'ютерах другого типу встановлена ОС Windows 8, на них установлена програма 1С підприємство (клієнт), Microsoft Office 2016, а також браузер Internet Explorer 11, антивірус NOD 32.

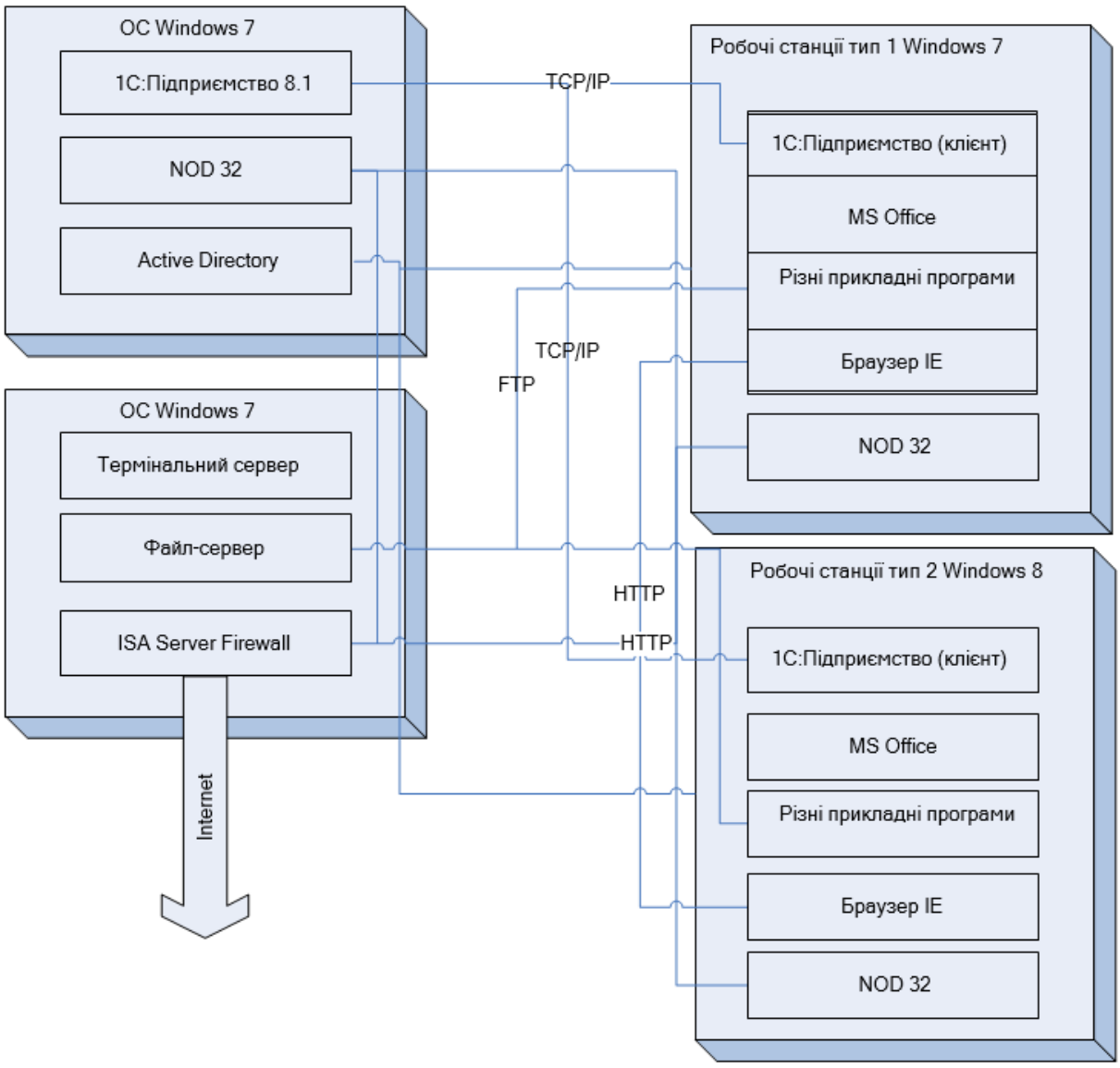

Рисунок 3.4 – Структура оновленого програмного комплексу

Для реалізації розроблених заходів та створення захищеного інтернету, а також для обмеження доступу до сервера вузлів мережі та робочих станцій необхідно вжити заходів щодо реалізації розроблених заходів обмеження доступу. Реалізація розроблених заходів щодо обмеження доступу та засоби контролю доступу до ресурсу описана в таблиці 3.6.

Таблиця 3.6 Реалізація розроблених заходів щодо обмеження доступу

Об'єкт	Захід	Суть проведення
Сервер	Обмеження фізичного доступу	Обладнання приміщення для розміщення серверів. Обладнання даного приміщення дверима, що замикаються, і системами сигналізації.
Вузли мережі	Обмеження фізичного доступу	Розташування мережних кабелів у спеціальних каналах для унеможливлення вільного доступу. Розташування важливого мережевого обладнання на території серверної або в спеціальних коробах, що замикаються.
Робочі станції	Опломбування корпусів та використанням спеціальних замикаючих пристроїв	Опломбування корпусів всієї комп'ютерної техніки з метою своєчасного виявлення спроб несанкціонованого застосування чи вилучення пристроїв. Застосування замикаючих пристроїв на корпусах, де таке передбачено конструкцією корпусу.

Реалізація інженерно-технічного захисту інформації представлена наступними завданнями:

– встановлення камер відеоспостереження;

– встановлення детекторів руху;

Встановлення камер відеоспостереження в офісі продемонстровано наступним планом (див. рис. 3.5).

В даному випадку в офісі компанії було встановлено 3 відеокамери Hikvision DS-2CD1321-I(F) (2.8 мм) та 2 панорамні відеокамери Speed Dome Covi Security AHD-7001-PTZ, у місцях потенційного входу відвідувачів:

– камера № 1 встановлена біля кімнати охорони, в її поле потрапляють всі люди які заходять до керівника;

– камера №2 встановлена так, що в її огляд потрапляють люди, що потрапляють у приміщення бухгалтерії;

– камера №3 встановлена так, що в поле її огляду потрапляють усі люди, що входять у кабінет системного адміністратора і у відділ кадрів;

– камера №4 фіксує всіх людей, які заходять через вхідні двері та кабінет головного бухгалтера;

– камера №5 встановлена у кімнаті Серверної, в її поле потрапляє двері та вікно приміщення.

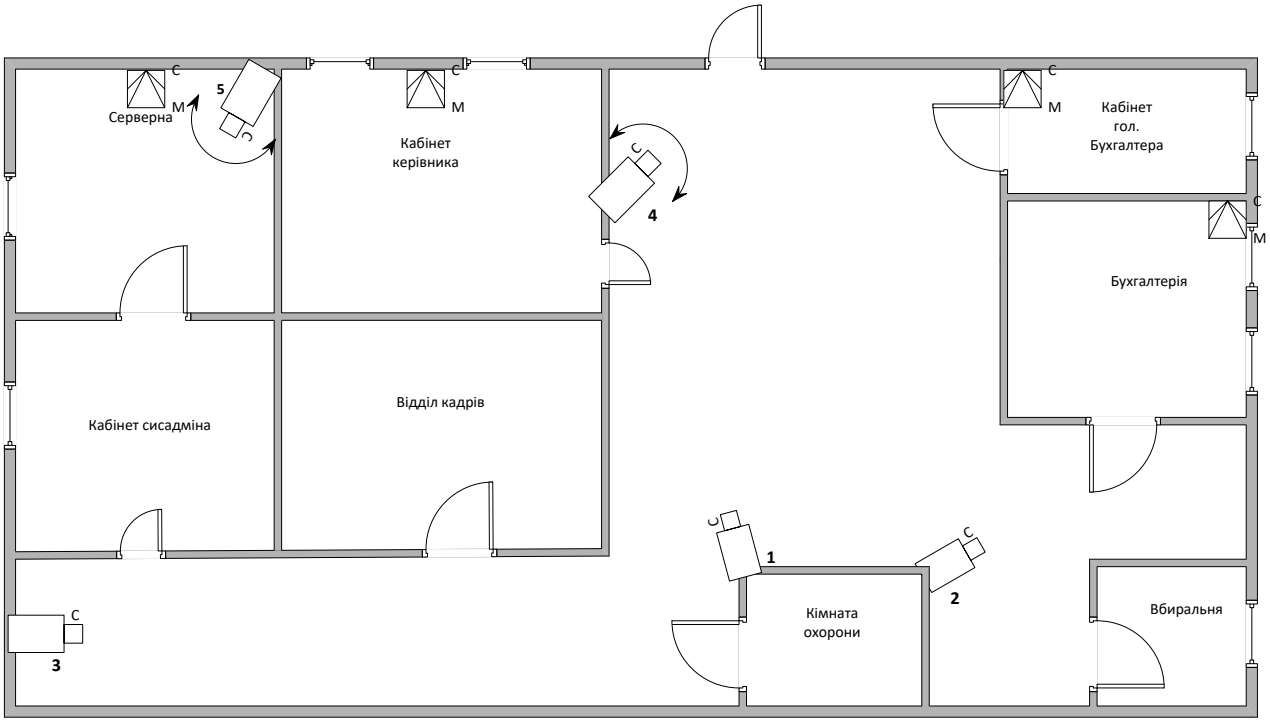

Рисунок 3.5 - План встановлення відеокамер

Таким чином, камери фіксують обличчя кожної людини, яка входить на підприємство. Відеодані з камер виводяться на монітор охорони та записуються на спеціальний носій інформації з періодичністю перезапису 14 днів.

Для захисту офісу в нічний час від проникнення зловмисників через двері та вікна в офісі було встановлено 4 детекторів руху наступних місцях:

– відділ кадрів;

– кабінет головного бухгалтера; бухгалтерія;

– серверна;

– кабінет керівника.

Були вибрані детектори IS215T (Ademco) (див. рис. 3.5) з такими технічними характеристиками:

– зона виявлення 12 х.12 м із контролем «під собою»;

– діаграма спрямованості типу "широкий кут";

– два рівні чутливості;

– висока стійкість до дії білого світла понад 6000 лк;

– діапазон робочих температур -10 ° С - +55 ° С;

– масштаб 87 х 62 х 40 мм.

Всі запропоновані засоби захисту інформації є актуальними та необхідними для підприємства.

3.5 Використання криптографічних методів захисту даних в рамках політики інформаційної безпеки підприємства

Криптографія є науковим напрямом, що дозволяє досліджувати методи забезпечення конфіденційності, цілісності інформації, аутентифікації, а також неможливість відмови від авторства.

Криптографія поділяється на два напрямки:

– шифрування інформації, пов'язане з оборотним перетворенням даних для того, щоб своєчасно встановити неавторизованих користувачів і дотримуватися конфіденційності даних, що передаються;

– створення алгоритмів електронного цифрового підпису.

Електронний цифровий підпис (ЕЦП) - це тип електронного підпису, який отримується в результаті криптографічного перетворення електронного набору даних, прикріпленого або логічно пов'язаного до цього набору, який може перевірити його цілісність для ідентифікації підписувача. Електронний цифровий підпис застосовується за допомогою приватного ключа та перевіряється за допомогою відкритого ключа. [5].

Електронний підпис як спосіб встановлення особи яка підписувала електронний документ, дає змогу достовірно визначити джерело інформації основу

інформації, що міститься у документі. Таким чином ЕЦП є також надійним способом розділення відповідальності за інформацію яка знаходиться уу документі, особливо за неправдиву інформацію.

Першим кроком є хешування електронного документа, яке безпосередньо пов'язане з процедурою генерації ЕЦП.

Мета хешування - "стиснути" вихідний бітовий рядок довільної довжини в повідомлення фіксованої довжини з певної кількості бітів, тобто створити хеш-образ вихідного повідомлення. Зауважимо, що в той час як традиційне архівування може відтворити оригінальне повідомлення в повному обсязі, це неможливо з хеш-образом.

Процедура створення хеш-образу повинна відповідати наступним вимогам[8]:

– Хеш-образ повинен мати однакову, чітко визначену довжину для будь-якого розміру вихідного тексту (зазвичай 128 біт і більше);

– Процедура хешування повинна бути незворотною, тобто з хеш-образу не можна відновити повний текст;

– Два тексти з незначними відмінностями (особливо якщо хоча б один символ був змінений або видалений) повинні мати різні хеш-образи;

– Необхідно виключити можливість випадкового створення ідентичних хеш-образів для різних документів, які вже створені або будуть створені в майбутньому.

Наступним кроком є безпосереднє створення ЕЦП. У найпростішому випадку це робиться шляхом шифрування лише хеш-образу, у більш критичних випадках - шляхом шифрування додаткової інформації (наприклад, ідентифікаторів відправника та отримувача, фіксації часу накладання ЕЦП тощо). (наприклад, фіксація часу виникнення ЕЦП).

Криптосистеми поділяються на:

1) симетричні системи, засновані на використанні одного і того ж ключа захисту даних в операціях шифрування та дешифрування даних

2) асиметричні системи, в яких ключ шифрування відрізняється від ключа розшифрування. При цьому навіть отримавши інформацію про відкритий ключ, зловмисник не зможе визначити секретний ключ.

Методи, що дозволяють здійснити ефективне шифрування та дешифрування даних наведено на рисунку 3.6.

Рисунок 3.6 – Методи, що дозволяють здійснити ефективне шифрування та дешифрування даних.

На рисунку 3.6 ми можемо простежити, як відбувається шифрування повідомлення та дешифрування. Тут зображені всі стадії проходження шифрування повідомлення в обох варіантах шифрування повідомлення. Маючи вихідне повідомлення за допомогою спеціального ПЗ, ми генеруємо ключ шифрування для повідомлення, після чого програма генерує відкритий ключ одержувача, потім повідомлення зашифровується. При дешифруванні даного повідомлення одержувач за допомогою відкритого ключа через ПЗ формує секретний ключ одержувача, після чого програма розшифровує повідомлення. Але найефективнішим є метод асиметричного шифрування.

Серед переваг криптографічних методів захисту слід відзначити високий рівень захисту даних, економічність у реалізації та ефективність у швидкодії.

Недоліком криптографічних методів захисту є складність у реалізації, що потребує залучення фахівців із криптографії для забезпечення необхідного рівня захисту даних.

У третьому розділі випускної кваліфікаційної роботи наведено характеристику організаційних, програмно-апаратних, криптографічних методів та засобів захисту та на підставі цього отримано такі авторські висновки:

– організаційні заходи забезпечення інформаційної політики безпеки підприємства регламентують документально використання заходів інформаційного захисту, що регламентує роботу усієї політики інформаційної безпеки;

– апаратні та програмні засоби забезпечення інформаційної безпеки в будівельній компанії дуже ефективні в комплексі, що дає найбільший захист даних і більше відповідає необхідним нормам політики інформаційної безпеки;

– в даний час серед криптографічних методів та засобів, використовуваних на підприємства найбільш ефективними є криптографічний метод захисту створення цифрового або електронного підпису.

Отримані результати та сформульовані висновки дозволяють перейти до розгляду матеріалу четвертого розділу, присвяченого розробці та впровадженню рекомендацій для розробленої політики інформаційної безпеки.

4 РОЗРОБКА ТЕХНІЧНОГО ЗАВДАННЯ ТА РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ РОЗРОБЛЕНОЇ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

4.1 Рекомендації щодо змісту технічного завдання і пропозиції формування змісту

Робота з підготовки робочих інструкцій проводиться після дослідження та моделювання загроз інформації в об'єкті інформаційної діяльності (ОІД). Технічне завдання (ТЗ) на встановлення систем захисту в ОІД може включати наступні розділи та підрозділи:

Загальна інформація:

- коротка характеристика об'єкта інформаційної діяльності;
- причини для виконання робіт;
- мета робіт та основні завдання;
- замовник;
- виконавці робіт;
- терміни завершення робіт.

2) Попередні дані про роботи.

3) Технічні вимоги до захисних комплексів:

- загальні вимоги;
- вимоги до стійкості до зовнішніх факторів;
- вимоги до експлуатаційної безпеки;
- вимоги до метрологічної підтримки;
- вимоги щодо забезпечення захисту державної таємниці;
- вимоги до технічного забезпечення при виконанні завдань;
- вимоги до забезпечення безпеки під час виконання завдань;
- інші вимоги;

4) Вимоги до документації.

5) Етапи виконання робіт і процедури їх приймання.

Залежно від складності, призначення та особливостей комплексу ТЗІ розділи та підрозділи можуть уточнюватися, додаватися нові, вилучатися або об'єднуватися.

У розділі "Загальна інформація" зазначаються найменування, призначення та місцезнаходження ОІД (інженерно-технічної споруди, дільниці або декількох споруд), де здійснюється виробнича діяльність, пов'язана з адміністративною, фінансово-господарською, науково-технічною та іншою інформацією з обмеженим доступом (ІзОД).

Метою дослідження є розробка та впровадження системи захисту, на ІОД дослідження включає в себе:

– проведення обстеження обладнання;

– вибір та обґрунтування технічних рішень (заходів) із захисту інформації;

– підготовку проектно-кошторисної документації;

– реалізація заходів та приймання робіт по системі захисту;

– атестація комплексу захисту.

Виконавці - це установи, організації та підприємства, які мають відповідні документи на проведення своєї діяльності в області ТЗІ, дозволи на провадження діяльності, пов'язаної з державною таємницею, відповідні виробничі ліцензії та дозволи на виконання проектних, будівельних та монтажних робіт.

Виконавцями є організації, установи та компанії, які отримали необхідні ліцензії на провадження господарської діяльності у сфері технічної та інтелектуальної власності, пов’язаної з інформацією із обмеженим доступом, мають ліцензії на виробництво та дозволи на встановлення, а також спеціалізуються на сфері технічної та інтелектуальної власності.

Основні відомості для створення та впровадження комплексного захисту включають у себе:

1) Матеріали, які використовуються в ОІД:

– перелік технологічних процесів, задіяних в ІзОД та інших технологічних процесах;

– види ІзОД, що підлягають технічному захисту (мовна ІзОД, інформація, оброблена технічними засобами) та грифи обмеження доступу;

– дані, що стосуються планів фундаменту та планів на випадок надзвичайних ситуацій;

– дані про будівельні та конструктивні дані; дані про плани опалення, вентиляції, електропостачання та інших систем життєзабезпечення, внутрішніх елементів, комунікацій (у тому числі тих, що знаходяться за межами контрольованої території (КТ));

2) Витяги з інструкцій з експлуатації технічних засобів для обробки ІзОД.

3) Витяги із затвердженої моделі загроз для ІзОД. Сюди входять дані про можливі місця розташування технічних засобів розвідки (стаціонарних або автоматизованих), які можуть бути використані для організації довготривалого перехоплення оброблюваної, а також мінімальна відстань від технічних засобів обробки ІзОД до кордону контрольованої території (КТ), наприклад, можливі технічні шляхи витоку ІзОД.

4) План або опис затвердженої КЗ.

У розділі "Загальні вимоги" можна вказати наступну інформацію:

1) Розроблення (проектування) засобів захисту здійснюється з урахуванням вимог основних нормативних актів та нормативних документів з ТЗІ та відповідно до класифікації об'єктів, на яких обробляються ТЗІ технічними засобами, та інших об'єктів, порядок функціонування яких визначено нормативними документами з ТЗІ.

2) Щоб досягти необхідного рівня, технічні рішення для технічних специфікацій повинні бути реалізовані з мінімальними витратами для захисту інформації.

3) При розробці комплексів захисту слід керуватися наступним:

– засоби захисту інформації, захищені пристрої, ТЗІ на телефонних та інших дротових лініях зв'язку та інші пасивні засоби захисту інформації;

– засоби активного захисту інформації (генератори віброакустичних завад, генератори просторових акустичних завад, генератори електромагнітних завад, лінійні генератори електромагнітних завад).

– засоби захисту використовуються за наявності сертифіката або відповідного експертного висновку про те, що вони відповідають вимогам нормативних документів з питань захисту інформації.

– імпортне обладнання може використовуватися лише за умови відсутності аналогічного продукту в країні, наявності відповідного техніко-економічного обґрунтування, його сертифікації або отримання похвального відгуку від спеціаліста;

4) Захисний комплекс має гарантувати інформаційний захист, беручи до уваги існуючих інформаційних систем та функціонування закладів підтриманого проживання.(Необхідно вказати конкретні системи):

– спеціалізовані системи зв'язку;

– автоматизовані системи;

– системи відкритого (міжміського та місцевого) телефонного зв'язку;

– мережі радіомовлення;

– системи кабельного телебачення;

– системи охоронної та пожежної сигналізації;

– системи електропостачання підприємства; освітлення та заземлення підприємства;

– системи опалення, вентиляції та кондиціонування повітря;

– інші системи життєзабезпечення та комунікації (за необхідності).

5) Контури заземлення повинні бути в межах КЗ.

6) Для запобігання витоку інформації з оптичного каналу слід унеможливити візуальний доступ до ОІД.

7) Для запобігання витоку звукової інформації акустичними та віброакустичними каналами необхідно покращити звукоізоляцію архітектурно-будівельних елементів та, за необхідності, забезпечити використання пристроїв акустичного шумозаглушення.

8) За необхідності слід передбачити використання пристроїв шумозаглушення для запобігання витоку звукової інформації з акустичного каналу лазера (за винятком встановлення оптичних дисплеїв).

9) Конструкція дверей (тамбурів), вікон та інших конструкцій, що оточують будівлю, повинна забезпечувати виключення можливості випадкового прослуховування джерел звуку (без використання технічних засобів інформації).

10) Захист джерела звуку від витоку через шляхи вторинних електромагнітних випромінювань та наведень.

11) Видалити або заземлити всі комунікації або металеві конструкції, які не використовуються або мають невідоме призначення для забезпечення функціонування ОІД.

12) Передбачити в ОІД спеціальні ніші для встановлення обладнання ТЗІ.

13) Під час виконання робіт на ОІД (будівництво, монтаж, пусконалагоджувальні роботи, встановлення транспортних засобів технічного призначення, обладнання життєзабезпечення, оргтехніки, елементів інтер'єру та меблів) та під час експлуатації вживатимуться організаційні та технічні заходи для унеможливлення встановлення закладних пристроїв для несанкціонованого зняття інформації.

14) Вказати заходи відносно взаємозв’язків з іншими системами забезпечення інформації об'єкта.

15) Атестація комплексу захисту повинна бути проведена відповідно до вимог нормативних документів з ТЗІ.

Розділ "Вимоги до стійкості до зовнішніх впливів":

Комплекси захисту повинні бути здатні працювати в наступних умовах:

- Температура навколишнього середовища 10 - 40°С.
- Вологість 45 - 85 % (при 35°С);
- Атмосферний тиск 86 - 106 кПа;
- Інші вимоги.

Розділ "Вимоги безпеки експлуатації".

Обладнання та компоненти системи захисту повинні бути спроектовані відповідно до вимог чинних в Україні нормативних документів для забезпечення безпеки обслуговуючого персоналу.

Розділ "Вимоги до метрологічної підтримки":

Методики виконання вимірювань повинні відповідати нормативним документам національних стандартів України. Засоби вимірювальної техніки, що використовуються в роботі з ТЗІ, повинні бути повірені відповідною метрологічною службою.

Розділ "Вимоги щодо забезпечення охорони державної таємниці":

Необхідно дотримуватися забезпечення режиму під час виконання роботи потрібно опиратися на вимоги Закону України" Про захист державної таємниці " та інших юридично-законодавчих актів України, що стосуються захисту державної таємниці.

Розділ "Вимоги до технічної допомоги у виконанні робіт":

Роботи виконуються підрядником з використанням власних матеріалів та технічної бази, необхідних для виконання робіт.

"Вимоги до безпеки під час виконання робіт":

Підрядник несе повну відповідальність за дотримання вимог безпеки, охорони праці та пожежної безпеки під час виконання робіт.

Структура технічної документації.

– проектна документація на вбудовані конструкції для монтажу мереж електропостачання для ТЗІ, телекомунікаційного обладнання, комп'ютерних мереж, телекомунікаційних систем, основного і допоміжного технічного обладнання та електроосвітлення, тощо;

– плани розміщення обладнання захисту;

– генеральні та монтажні схеми комплексу захисту;

– рекомендації щодо пасивних заходів із запобігання технічному проникненню;

– документація щодо систем інженерно-технічного забезпечення об'єктів та технічних засобів, включаючи вимоги до ТЗІ;

– будівельні та конструктивні частини, розробка (узгодження) інженерно-технічного забезпечення та питання, викладені в загальному коментарі "Заходи з ТЗІ";

– кошторис на реалізацію захисних установок;

– порядок встановлення та монтажу систем захисту; та

– програму та методику приймальних (сертифікаційних) випробувань систем захисту;

– технічна та експлуатаційна інструкції на систему захисту; технічний паспорт на систему захисту; паспорт на приміщення ОІД.

– вимоги до підготовки документації можуть визначатися та уточнюватися за погодженням між замовником та виконавцем робіт.

Цей розділ повинен містити етапи виконання робіт, строк виконання робіт, процедури приймання та, за необхідності, наступні процедури, узгоджені з етапами будівництва комплексу захисту, визначеними чинними нормативними документами з ТЗІ, а саме: технічна документація, авторський нагляд, контроль за виконанням будівельно-монтажних та пусконалагоджувальних робіт (можливе посилання на програму виконання робіт).

Інформація може бути загальнодоступною або доступною лише для обмеженого кола осіб. Захист інформаційних систем є актуальним лише тоді, коли не передбачається оприлюднення існуючих файлів. Інформаційні системи мають різні рівні безпеки. Завдання полягає в тому, щоб розрізняти різні рівні загроз і різні рівні захисту в залежності від загрози.

Розрізняють такі рівні захисту:

– Законодавчий (нормативно-правовий) ;

– Адміністративний (організаційні, обов'язкові та інші заходи, що вживаються керівництвом установи по відношенню до інформаційної системи, що захищається);

– Процедурний (заходи безпеки, орієнтовані на людину);

– Програмно-технічні (інженерно-технічні, апаратні та програмні засоби).

Законодавчий рівень

Для правового захисту підприємств, установ та організацій необхідно законодавчо відкоригувати правовідносини між державою та підприємством щодо правомірності використання засобів захисту інформації та між підприємством та його персоналом щодо обов'язку дотримання процедур захисту інформаційних ресурсів.

Керівництво для впровадження цього рівня захисту надають наступні закони та юридично-законодавчі акти:

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР.

– Стаття 4. Доступ до інформації в системі

– Стаття 8. Умови обробки інформації в системі

– Стаття 9. Забезпечення захисту інформації в системі

– Стаття 11. Відповідальність за порушення законодавства про захист інформації в системах

– НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі;

– Державний стандарт України Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96.

– Конституція України;

– Закон України «Про інформацію» від 02.10.1992 № 2657-XII.

Адміністративний рівень

На адміністративному віні режим інформаційної безпеки в системі забезпечується політикою безпеки організації, яка визначає цілі інформаційної безпеки та шляхи їх досягнення. На цьому рівні витік інформації може відбуватися через персонал. Тому для забезпечення безпеки на цьому рівні рекомендуються наступні підходи:

– Спеціалізований відбір працівників;

– Проведення тренінгів з техніки безпеки;

– Надання додаткових пільг персоналу (наприклад, премії, відпустки, заохочення) ;

– Управління та нагляд.

Процедурний рівень

На процедурному рівні режим інформаційної безпеки в системі забезпечується шляхом розробки та впровадження заходів фізичного захисту, а також частини інструкцій персоналу, присвячених інформаційній безпеці. На процедурному рівні вживають заходів, які реалізують люди. У цьому контексті процедурні заходи можна розділити на наступні групи:

– кадрове управління;

– безпековий контроль;

– підтримка ефективності працівників;

– дії при виявленні порушення безпеки;

– планування реанімаційних робіт.

Програмно-технічний рівень

Інформаційна безпека забезпечується на програмному та апаратному рівнях з використанням перевірених і затверджених рішень та стандартизованого набору контрзаходів, таких як резервне копіювання, антивірусний та парольний захист, брандмауери, шифрування даних тощо.

Програмний та апаратний рівні можна розділити на підрівні:

– Інженерно-технічний захист;

– Апаратний захист;

– Програмний захист.

Витік інформації - це навмисне або необережне розголошення конфіденційної інформації іншим особам.

Типи витоку інформації:

– Підслуховування в приміщенні;

– Прослуховування телефонних ліній;

– Перехоплення комп'ютерних даних;

– Таємна фото-або відеозйомка;

– Візуальне спостереження;

– Підкуп співробітників;

– Підкуп родичів співробітників;

– Прийом паразитних електромагнітних випромінювань.

Акустичний моніторинг приміщення може бути реалізований за допомогою:

– Мікрофони та виведення сигналу через кабель;

– Звукозаписуючий пристрій;

– Стетоскоп;

– Радіомікрофони;

– Телефонна лінія;

– Лазерний збір даних через віконне скло.

Прослуховування телефонних ліній

Телефонні лінії використовуються не тільки для прослуховування телефонних розмов, але й для прослуховування в офісі (телефонна трубка на слухавці). Для цього використовується мікрофонний ефект, такі системи, як високочастотне застосування, телемоніторинг і телефонні навушники. Деякі системи можна використовувати для прослуховування з-за кордону, якщо в приміщенні є телефонний кабель.

Перехоплення комп'ютерних даних

Інформація може бути викрадена з комп'ютера наступними способами:

– хакерами;

– прихованих камер;

– спеціалізовані радіоприймачі, які приймають інтерференційне випромінювання від комп'ютерів (зазвичай моніторів) і виявляють корисну інформацію.

Паразитні випромінювання

Електромагнітні поля, що утворюються внаслідок витоку електромагнітної енергії через щілини в екрані обладнання або його вузлах (елементах) чи від передавальної антени.

Принципова схема поведінкової моделі уявного злочинця

Порушник - це людина, яка випадково або через незнання, зловмисно чи ні, використовуючи різні можливості, способи і засоби, навмисно намагається здійснити дії, що призводять або можуть призвести до порушення характеристик інформації, визначених в політиці безпеки.

Модель порушника відображає фактичні та потенційні можливості порушника, його знання, можливий час і місце дій тощо.

До можливих внутрішніх зловмисників відносяться:

– Кінцеві користувачі (оператори системи), персонал (перший рівень);

– Особи, які обслуговують технічні засоби (третій рівень);

– Співробітники відділів розробки та супроводу програмного забезпечення (четвертий рівень);

– Працівники служби автоматизованих систем та безпеки (перший рівень);

– Керівники різних рівнів управління (перший рівень).

Можливі зовнішні зловмисники (сторонні особи):

– Технічний персонал, що управляє будівлею (первинний рівень);

– Клієнти (первинний рівень);

– Представники конкуруючих компаній (вторинний рівень);

– Відвідувачі, присутні за різними причини (другий рівень).

Правопорушники класифікуються відповідно до рівня можливостей, що надаються звичайними інструментами КС.

Існує чотири рівні цих компетенцій. Класифікація є ієрархічною, і кожен рівень містить функціональні компетенції попереднього рівня:

Перший рівень визначає найнижчий можливий рівень взаємодії з КС і полягає у здатності виконувати конкретні завдання (програми), що виконують задані функції обробки інформації;

Другий рівень визначається здатністю створювати та виконувати власні програми з новими функціями обробки інформації;

Третій рівень визначається здатністю керувати функціями КС, тобто її впливом на базове програмне забезпечення системи та конфігурацію і налаштування обладнання;

Четвертий рівень визначається сукупністю компетенцій тих, хто бере участь у проектуванні, впровадженні та ремонті апаратних компонентів КС.

Порушники можуть отримати несанкціонований доступ до інформації під час роботи автоматизованої системи або в періоди, коли автоматизована система не працює, або під час поєднання робочого та неробочого часу.

На спеціалізованих об'єктах КСЗІ передбачає, враховує та розробляє всі чотири рівні порушників.

Захист інформації - це сукупність методів і заходів, спрямованих на забезпечення цілісності, конфіденційності та доступності інформації в умовах впливу загроз природного або техногенного характеру, реалізація яких може завдати шкоди власникам і користувачам інформації.

Для боротьби із загрозами системи безпеки використовують різні інструменти та методи.

– Виявлення;
– Спотворення;
– Проштовхування;
– Локалізація;
– Профілактика;
– Деактивація;
– Попередження.

Основні принципи реалізації програмно-технічних засобів:

Основне завдання засобу забезпечення безпеки полягає в поділі об'єктів КС в області управління, перевірці всіх запитів на доступ до об'єкта і перевірці запиту і його валідації та/або підтвердження достовірності. Реалізація механізму може бути абсолютно різною. Наприклад, Програмне або апаратне забезпечення,

криптографічні перетворення та різні способи перевірки облікових даних. Це може бути використано для реалізації функцій безпеки. Вибір методів і механізмів найчастіше залишається за розробником. Єдиною вимогою є те, що функція захисту реалізована відповідно до заявленої політикою безпеки і гарантійними вимогами. Засоби захисту шифруванням можуть використовуватися для реалізації певних служб. Криптографічні перетворення можуть використовуватися безпосередньо для захисту певної інформації (наприклад, для реалізації служби конфіденційності) або для підтримки реалізації служби (наприклад, для реалізації служби ідентифікації та аутентифікації).

Технічне оснащення об’єкта засобами охоронної сигналізації

Перша межа блокує будівельну конструкцію навколо об'єкта (віконні та дверні прорізи, люки, вентиляційні канали, теплові входи, некапітальні стіни та інші елементи будинку, до яких можуть бути доступні несанкціоновані вторгнення).

Друга межа блокує внутрішній об'єм і простір будівлі.

Третя межа захищає цінність місцевих предметів та матеріалів. За бажанням замовника в приміщеннях можуть бути встановлені додаткові засоби так званої охоронної та пожежної сигналізації.

Система телеспостереження і контролю доступу на об'єкті може бути встановлена в якості додаткової лінії захисту.

На об'єкті встановлена тривожна кнопка для екстрених викликів мобільної групи реагування. Група служб мобільної безпеки спочатку реагує на його активацію. Тривожна кнопка встановлюється таємно, необхідно виключити фактори, які ви випадково натиснули під час установки. Передача тривожних повідомлень здійснюється через герметизуючі пристрої по окремих телефонних лініях, прямих лініях зв'язку, відповідним телефонним лініям, глобальним мережам Інтернету або бездротовим каналам.

Рисунок 4.1. Захисний прилад для аналогових телефонних ліній МП-1А

Прилад МП-1а призначений для запобігання витоку інформації з абонентської лінії аналогової АТС в режимі очікування виклику. Використовується як пасивний, так і активний засіб захисту одночасно. Пристрій включає в себе генератор шуму, введення шумових сигналів в нелінійні схеми і абонентські лінії, а також низькорівневий блок придушення сигналів, що забезпечує ослаблення низькорівневих сигналів. Захист інформації від витоків за допомогою методів активного впливу телефонних дзвінків на абонентські лінії і в режимі очікування виклику.

Рисунок 4.2 IP відеокамера Hikvision DS-2CD1321-I(F)

Рисунок 4.3 Детектор руху IS215T (Ademco)

Детектор руху IS215T (Ademco) призначений для спостереження за пересуванням людини в приміщенні, що охороняється. Принцип роботи датчика заснований на інфрачервоному (ІЧ) випромінюванні.

Щоб підвищити ступінь інформаційної безпеки, необхідно:

– Обмежувати можливість несанкціонованого виведення і друку інформації Користувачем на зовнішні носії (лазерний привід CD-RW, USB-накопичувач);

– Обмежувати кількість або виключити використання локальних принтерів і призначте особу, відповідальну за друк документа на мережевому принтері;

– Виключити доступ користувачів до ресурсів інших користувачів як для запису, так і для читання;

– Обмін інформацією між користувачами відбувається через спільні ресурси на сервері.

4.2 Організація комплексного підходу із захисту підприємства відповідно до політики підприємства

Електронні та електронно-механічні пристрої, що входять до складу технічних засобів охорони, є апаратними засобами забезпечення інформаційної безпеки.

Апаратні засоби, що працюють разом із програмними засобами або самостійно, виконують завдання необхідні побудови інформаційної безпеки.

Електронні та електронно-механічні пристрої є апаратними засобами забезпечення інформаційної безпеки. а не інженерно-технічними засобами, якщо вони обов'язково входять до складу технічних засобів політики інформаційної безпеки.

Апаратними засобами політики інформаційної безпеки є:

– пристрої введення біометричних даних розпізнавання;

– устрою ідентифікації співробітника;

– пристрої кодування інформації;

– електронні замки та блокатори, що не дають безконтрольно

– включати робочі станції.

До допоміжних засобів захисту інформації відносяться:

– засоби знищення магнітних носіїв та інформації на них;

– засоби сигналізації, що попереджають про несанкціоновані дії користувачів.

До програмних засобів захисту відносяться програми, що входять до складу програмного забезпечення, необхідного для захисту даних. До цих засобів захисту можна віднести:

– програми розпізнавання користувачів;

– програми визначення зони доступу до ресурсу;

– програми криптографічного захисту інформації;

– програмне забезпечення: баз даних, комп'ютерних засобів;

– програми, що захищають інформацію від незаконного доступу та

– копіювання.

Ідентифікація користувачів у політиці інформаційної безпеки розуміється як 100% визначення індивідуального та унікального імені користувача, а автентифікація служить для того, щоб визначити 100% належність користувача представленого імені.

Як приклад програм, що допомагають у захисті інформації, можуть виступати:

– програми видалення інформації, що залишилася (у тимчасових файли, оперативна пам'ять і т.д.);

– аудиторські програми подій, які описують погрози, журнали реєстрації подій, які можуть статися представлятися як доказ погроз;

– програми, що створюють можливі події, за яких здійснюється імітація роботи з порушником;

– програми тестування безпеки.

Для захисту локальної обчислювальної мережі необхідно поділити користувачів на групи з відповідними правами:

1. Administrator – адміністратори мережі (створення та керування політиками інформаційної безпеки, глобальні налаштування мережі тощо).

2. Manager – облікові записи для щоденного обслуговування інформаційного та комп'ютерного обладнання.

3. User – стандартний обліковий запис користувача (працівника підприємства) з обмеженими правами.

4. Security – обмежений вчений запис (Ті, хто не є працівниками організації, потребують доступу).

Для підтвердження особи юзера потрібно ActiveDirectory з використанням мережної операційної системи, де для кожного користувача має бути створений унікальний запис, і кожен запис був включений до відповідного класу. Внаслідок цього відбувається розмежування доступу (табл. 4.1)

Таблиця 4.1 – Групи користувачів та їх права

Дії	Security	User	Manager	Administrator
1	2	3	4	5
Створення та зміни груп користувачів	Ні	Ні	Ні	Так
Зміна налаштувань мережі	Ні	Ні	Ні	Так

Продовження таблиці 4.1

1	2	3	4	5
Підключення до мережі нових робочих станцій	Ні	Ні	Ні	Так
Зміна налаштувань серверів	Ні	Ні	Ні	Так
Зміна прав доступу до каталогів та резервних копіям	Ні	Ні	Ні	Так
Встановлення додатків	Ні	Ні	Так	Так
Доступ в Інтернет	Ні		Так	Так
Обсяг передачі даних за місяць	0	100	1000	1000
Доступ до завантаження файлів	Ні	Ні	Так	Так
Запис у системі	Виключно в «Мої документи»	"Мої документи", «Робочий стіл», «Для всіх», «Мережева»	Любий каталог на внутрішньому ПК	Любий каталог на будь-якому ПК в мережі
Підключення зовнішніх флеш дисків, зовнішніх дисків.	Ні	Ні	Так	Так
Підключення CD/DVD-ROM, гнучкий-диск	Ні	Ні	Так	Так
Використання ICQ	Ні	Так	Так	Так

Кінець таблиці 4.1

1	2	3	4	5
Доступ до FTP	Ні	Ні	Ні	Так
Доступ до POP3	Ні	Так	Так	Так
Доступ до SMTP	Ні	Так	Так	Так
Доступ до SSL	Ні	Так	Так	Так
Доступ до SOCKS	Ні	Ні	Ні	Так

Для зниження вразливості програмних засобів було вирішено оцінити рівень підготовки операційних систем.

Для цього було вжито наступних заходів:

1. Здійснено заміну застарілих операційних систем на нові операційні системи;

2. Там, де заміна операційних систем недоцільна, зроблено оновлення існуючих операційних систем шляхом встановлення сервіс - паків останніх версій.

Для підвищення якості антивірусного захисту було ухвалено рішення впровадити досконаліший антивірус. Контроль інтернет-трафіку здійснюватиметься за допомогою проксі-сервера, який одночасно служитиме і фаєрволом.

Можна зробити висновок, що окремо програмний комплекс та апаратний комплекс мало ефективні, тому необхідно два ці важелі захисту використовувати разом, тим самим отримавши програмно-апаратний комплекс.

4.3 Обґрунтування економічної ефективності реалізації політики інформаційної безпеки

Вихідною посилкою економічної ефективності є очевидне припущення: з одного боку, у разі порушення захищеності інформації завдається певні збитки, з іншого - забезпечення захисту інформації пов'язані з витрачанням коштів.

Без сумніву, що найбільш раціональним варіантом витрати на безпеку інформації, загальні витрати на забезпечення безпеки інформації.

Зрозуміло, що фінансова результативність заходів із захисту даних може залежати від розміру або об'єму заподіяних збитків або величину зниження ризику для інформаційних активів організації.

Оскільки оптимальне вирішення питання щодо розумного рівня витрат на захист стосується того, щоб відповідати рівню очікуваних збитків при порушенні безпеки, достатньо визначити лише ступінь втрат при порушенні захищеності. Одним із методів визначення для визначення рівня витрат можна використання такої емпіричної залежності, яка визначає очікувані втрати (ризики) від конкретної загрози інформації:

$$Ri = 10^{Si+Vi-4} \quad (1)$$

де Si – коефіцієнт, що вказує на ймовірність виникнення конкретної загрози;

Vi - коефіцієнт, що визначає розмір потенційних збитків за її виникнення. Si та Vi , наведені в таблиці 4.2.

Таблиця 4.2 – Значення коефіцієнтів Si та Vi

Очікувана (можлива) частота появи загрози	Передбачуване значення Si
1	2
Майже ніколи	0
1 раз на 1000 років	1
1 раз на 100 років	2
1 раз на 10 років	3
1 раз на 1 рік	4
1 раз на місяць (приблизно 10 разів на рік)	5
1-2 рази на тиждень (приблизно 100 разів на рік)	6
3 рази на день (1000 разів на рік)	7

Кінець таблиці 4.2

1	2
Значення можливих збитків при прояві загрози, грн.	Ймовірне значення Vi
1	2
30	0
300	1
3000	2
30000	3
300000	4
3000000	5
3000000	6
300000000	7

Сумарна вартість втрат визначається формулою:

$$R = \frac{N}{i=1} Ri, \qquad (2)$$

де N – кількість загроз інформаційним активам, визначених у п.1.2.3.

При обчислюванні загального показника бажано вважати, що потенційні загрози можуть бути реалізовані незалежно один від одного.

Тобто, якщо цілісність інформації порушена в результаті дій порушника, її вміст йому невідомо (конфіденційність не порушена), і авторизованому користувачеві не дозволяється її використовувати. (див. таблицю 4.3) .

Таблиця 4.3 Розмір втрат (ризиків) для ключових інформаційних активів перед впровадженням/оновленням захисту інформації

Актив	Загроза	Величина втрат (тис. грн.)
1	2	3
Проектна документація, розроблена організацією	конфіденційності	100
Проектна документація, розроблена організацією	цілісності	500

Продовження таблиці 4.3

1	2	3
Проектна документація, розроблена організацією	доступності	20
Проектна документація, отримана від замовника	конфіденційності	100
Проектна документація, отримана від замовника	цілісності	100
Проектна документація, отримана від замовника	доступності	20
Проектна документація, плани комунікацій у т.ч. стратегічного призначення	конфіденційності	500
Проектна документація, плани комунікацій у т.ч. стратегічного призначення	цілісності	100
Проектна документація, плани комунікацій у т.ч. стратегічного призначення	доступності	20
Особисті дані клієнта	конфіденційності	300
Особисті дані клієнта	цілісності	20
Особисті дані клієнта	доступності	20
Особисті відомості про співробітників	конфіденційності	100
Особисті відомості про співробітників	цілісності	10
Особисті відомості про співробітників	доступності	10
Системне програмне забезпечення	конфіденційності	0
Системне програмне забезпечення	цілісності	100
Системне програмне забезпечення	доступності	100

Кінець таблиці 4.3

1	2	3
Прикладне програмне забезпечення (в т.ч. САПР, CMS, ERP, CRM тощо)	конфіденційності	0
Прикладне програмне забезпечення (в т.ч. САПР, CMS, ERP, CRM тощо)	цілісності	100
Прикладне програмне забезпечення (в т.ч. САПР, CMS, ERP, CRM тощо)	доступності	100
Сумарна величина втрат		2320

Після проведення розрахунків та побудови таблиці 4.3 ми визначилися з ризиком фінансових втрат для підприємства, яка може становити приблизно 2 320 000 гривень. З цього можна дійти невтішного висновку, що з підприємства це буде дуже істотною втратою. Для поняття наскільки ефективна зароблена політика інформаційної безпеки необхідно розрахувати показники економічної ефективності проекту.

4.4 Аналіз показників економічної результативності проекту

Ризик для власників інформації залежить від ступеня технічного захисту інформації, що обумовлюється ресурсами системи. Ресурси можуть бути оцінені через кількість залучених працівників, що беруть участь у захисті інформації, інженерних споруд і технічних засобів, що використовуються для захисту, сум, що підлягають сплаті за працю, будівництво, розробку і придбання людьми технічних засобів, їх експлуатацію та інших витрат. Грошова оцінка є найбільш загальною формою представлення ресурсу. Ресурс, відведений на захист інформації, може бути як одноразовим, так і сталим.

Одноразовий ресурс витрачається на закупівлю, встановлення та налагодження дорогого обладнання.

Сталий ресурс - на оплату праці працівників служби безпеки та підтримання певного рівня безпеки, насамперед шляхом експлуатації технічних засобів та контролю ефективності захисту.

Таким чином, для визначення економічної ефективності захисту інформації підприємства необхідні така інформація (відомості):

– ресурси витрачені на створення або покращення системи, та підтримку її у працездатному стані ;

– величини втрат (ризиків), обумовлених загрозами інформаційним активам після впровадження/модернізації захисту інформації.

Сутність та розмір незмінного резерву, який виділяється на забезпечення безпеки інформації у таблиці 4.4

Таблиця 4.4 - Сутність та розмір незмінного резерву, який виділяється на забезпечення безпеки інформації

Організаційні дії				
№ п\ п	Дії, що виконуються	Погодинна зарплата фахівця (грн.)	Трудомісткість операції (чол.год.)	Вартість, всього (тис. грн.)
1.	Проведення тренінгів, інструктажів.	0,3	10	3
Загальні витрати на впровадження організаційних заходів				3
Заходи інженерно-технічного захисту				
№ п\ п	Перелік ресурсів для витрат та інвентаризації	Ціна за одиницю (тис.грн.)	Кількість (одиниць)	Вартість, всього (тис.грн.)
2.	Оновлення ПЗ	15	1	15
3.	Обслуговування відеоспостереження	0,3	10	3
4.	Обслуговування детекторів руху	0,3	10	3
5.	Обслуговування протипожежної системи	0,3	20	6
Фінансові витрати на захист інженерно-технічних заходів				27

.

Таким чином, для розробки інформаційної безпеки потрібно 355 640 грн., а для щорічної підтримки – 30 000 грн.

Для розрахунку необхідно отримати прогнозовані дані про величину втрат (ризиків) для критичних інформаційних ресурсів після впровадження/модернізації захисту інформації. Результати формуються за наслідками експертного опитування (див. таблицю 4.5).

Таблиця 4.5 - Розмір можливих втрат (ризиків) для ключових інформаційних активів після реалізації/модифікації інформаційної безпеки.

Актив	Загроза	Величина втрат (тис. грн.)
1	2	3
Проектна документація, розроблена організацією	конфіденційності	10
Проектна документація, розроблена організацією	цілісності	50
Проектна документація, розроблена організацією	доступності	2
Проектна документація, отримана від замовника	конфіденційності	10
Проектна документація, отримана від замовника	цілісності	10
Проектна документація, отримана від замовника	доступності	2
Проектна документація, плани комунікацій у т.ч. стратегічного призначення	конфіденційності	50
Проектна документація, плани комунікацій у т.ч. стратегічного призначення	цілісності	10
Проектна документація, плани комунікацій у т.ч. стратегічного призначення	доступності	2
Особисті дані клієнта	конфіденційності	30
Особисті дані клієнта	цілісності	2

Кінець таблиці 4.5

1	2	3
Особисті дані клієнта	доступності	2
Особисті відомості про співробітників	конфіденційності	10
Особисті відомості про співробітників	цілісності	1
Особисті відомості про співробітників	доступності	1
Системне програмне забезпечення	конфіденційності	0
Системне програмне забезпечення	цілісності	10
Системне програмне забезпечення	доступності	10
Прикладне програмне забезпечення (в т.ч. САПР, CMS, ERP, CRM тощо)	конфіденційності	0
Прикладне програмне забезпечення (в т.ч. САПР, CMS, ERP, CRM тощо)	цілісності	10
Прикладне програмне забезпечення (в т.ч. САПР, CMS, ERP, CRM тощо)	доступності	10
Сумарна величина втрат		232

Оцінка змін в розмірах можливих у період 2 роки (див. таблицю 4.6)

Таблиця 4.6 - Оцінка змін в розмірах можливих втрат

	1 кв	2 кв	3 кв	1 рік	1кв	2 кв	3 кв	2 рік
До реалізації СЗІ	580	1160	1740	2320	2900	3480	4060	4640
Після реалізації СЗІ	58	116	174	232	290	348	406	464
Зниження втрат	522	1044	1566	2088	2610	3132	3654	4176

Після прийняття необхідних припущень щодо стабільності частоти виникнення загроз, а також враховуючи стабільний ступень надійності створеного захисту інформації можна визначити термін окупності ($T_{ок}$). Це виконується аналітичним способом, з використанням наведеної нижче формули:

$$T_{ок} = \frac{R_{\Sigma}}{(R_{ср} - R_{прогн})} \quad (3)$$

та графічним, як це представлено на рисунку 4.4.

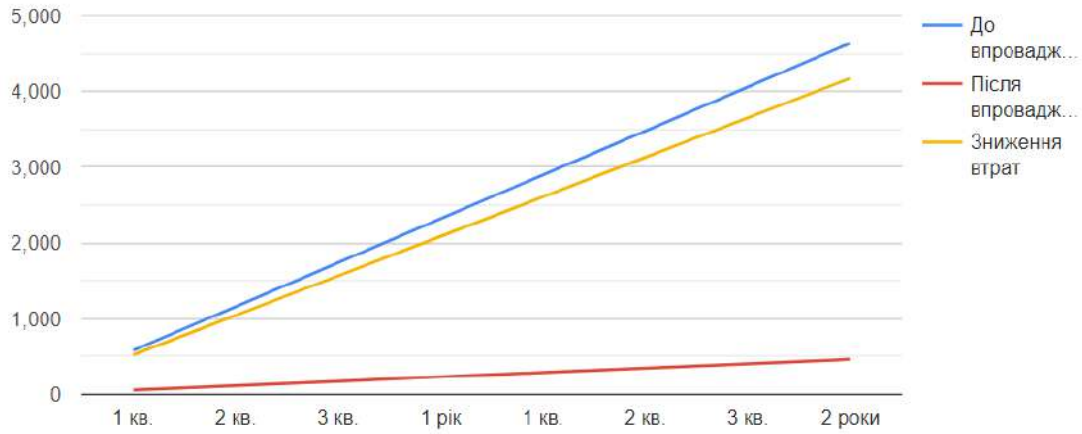

Рисунок 4.4 - Графічне представлення терміну повернення інвестицій

Отже, економічні обчислення свідчать про ефективність впровадження цілісного комплексу. Згідно з розрахунками, окупність інформаційної безпеки відбудеться ще в першому кварталі її використання. Що для підприємства є мінімальним фінансовим навантаженням.

У цьому розділі зроблено розрахунки, з них ми можемо побачити, що прогнозовані збитки є досить вагомими для підприємства, а одноразові витрати на реалізацію політики інформаційної безпеки менші, ніж передбачувані фінансові збитки. Це свідчить про те, що впровадження стратегії інформаційної безпеки сприятиме захисту інформації, що стане ефективним заходом для уникнення

можливих фінансових втрат для компанії від потенційних загроз. Через два роки стратегія інформаційної безпеки, реалізована в організації, забезпечить захист на суму близько 4 млн гривень. Отже, можна зазначити, що створена стратегія інформаційної безпеки виявляється дуже результативною.

ВИСНОВКИ

В процесі виконання випускної кваліфікаційної роботи була розроблена і вдосконалена політика інформаційної безпеки підприємства.

На основі аналізу основних положень теорії інформації було встановлено, що для створення політики захисту інформаційної безпеки необхідно розробити цілий ряд документів та інструкцій, спрямованих на захист інформації. І ні в якому разі не можна зупинятися на одному методі захисту інформації, захист даних буде під загрозою. Захист даних повинен бути комплексним. Інтегрована стратегія інформаційної безпеки охоплює створення, виробництво та встановлення технічних засобів захисту, а також регулярні перевірки використовуваного інформаційного обладнання. У сучасний період багато підприємств займаються процесом атестації систем інформатизації на предмет відповідності вимогам їх інформаційної безпеки.

Одне із напрямків розвитку сучасних підприємств - інформатизація. Використання сучасних інформаційних технологій дозволяє істотно підвищити ефективність виробничих і управлінських процесів. Але разом із застосуванням цих технологій виникає проблема забезпечення комплексного захисту інформації, яка може бути віднесена до конфіденційної. В межах даної роботи на підприємстві була створена система комплексного захисту інформації. Реалізація цього проекту передбачає наступні кроки:

– виявлення дефектів існуючої системи захисту інформації на підприємстві;

– визначення категорій потенційних загроз, що можуть виникнути внаслідок існуючих недоліків у системі захисту інформаційних систем підприємства;

– вибір підходів та засобів урегулювання наявних труднощів.

В якості вирішення був розроблений набір заходів, що включає в себе:

– управлінських заходів, які контролюють можливості неправомірного витоку інформації внаслідок впливу фактору людини;

– технічних рішень, що дозволили зменшити ймовірність виникнення ризику атак на інформаційні канали із зовнішнього середовища або із застосуванням різних пристроїв зберігання інформації;

– інженерно-технічних рішень, які дозволяють запобігти порчі або викрадання різних сховищ інформації, звести до мінімуму ризик виникнення атак на інформаційні канали із зовнішнього середовища або з застосуванням різних пристроїв зберігання інформації, або завдяки їх в результаті різних форс - мажорних обставин.

На основі аналізу основних методів і засобів інформації було встановлено, що організаційно-правові методи захисту і засоби захисту інформації повинні бути спрямовані на протидію загрозам інформаційної безпеки, знижувати ризики і ефективно обробляти інциденти з тривалою метою забезпечення достатнього рівня захисту даних.

Інженерно-технічні методи захисту інформації, засновані на захисті інформації на контрольованій території, всередині приміщень, мережі, програмному забезпеченні та наявності бази даних.

Апаратно-програмні методи, спрямовані на забезпечення безпеки мережі в мережі, рівні користувача, в тому числі і на рівень додатків.

В даний час серед криптографічних методів і засобів, використовуваних на підприємстві, найбільш ефективним є криптографічний метод створення цифрової або електронної підписи.

На підставі виконаного аналізу найбільш ефективними методами і засобами захисту інформації є комплекс мір як інженерно-технічних методів і засобів, що дозволяють забезпечити комплексний захист даних на підприємствах, так і апаратно-програмних, і криптографічних.

Політика інформаційної безпеки досліджена і вдосконалена. Оцінка ефективності запропонованих заходів показала їхню доцільність впровадження в організації.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Закон України «Про інформацію».

2. Закон України «Про захист інформації в інформаційно телекомунікаційних системах».

3. Parengkuan, Bierhoff, Kenny Tatauhe, and Fanny Worotijan. "Analysis of Information Security Management Systems at University." International Journal of Information Technology and Education 1.1 (2021): 43-50.

4. Сарапіна, Альона Ярославівна. "Метод захисту даних з використанням електронного цифрового підпису." (2021).

5. Tank, Margo HK, Sara E. Emley, and R. David Whitaker. "A brief guide to using electronic signatures in securities transactions." Practical Compliance & Risk Management for the Securities Industry (2013): 23-34.

6. ISO/IEC 27001 [Електронний ресурс] // Вікіпедія вільна енциклопедія. – 2023. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/ISO/IEC_27001

7. Електронний цифровий підпис [Електронний ресурс] // Вікіпедія вільна енциклопедія. – 2023. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D0%B9_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D0%B9_%D0%BF%D1%96%D0%B4%D0%BF%D0%B8%D1%81

8. National Security Strategy of the United States of America. — Washington, DC : White House, 2010, May. – 52 p.

9. Global trends 2025: The National Intelligence Council’s. 2025 Project [Електронний ресурс]. – Режим доступу : http://www.dni.gov

10. Internal security strategy for The European Union «Towards a European Security Model» [Електронний ресурс]. – Режим доступу : http://www.register.consilium.europa.eu

11. Міжнародна інформаційна безпека: сучасні виклики та загрози / [Є. А. Макаренко, М. А. Ожеван, М. М. Рижков та ін.]. – К. : Центр Вільної преси, 2006. – 916 с

12. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. [Електронний ресурс] / Г. Я. Аніловська. – Режим доступу : http://www.nbuv.eov.ua/

13. Державний стандарт України Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96.

14. Галузевий стандарт України: Інформаційні технології. Методи захисту. Система управління інформаційною безпекою (Вимоги Iso/Iec 27001:2005, Mod) [Електронний ресурс] / НБУ – Режим доступу : http://auditagency.com.ua

15. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України : лист НБУ від 03.03.2011 № 24-112/365 [Електронний ресурс] / НБУ – Режим доступу : http://zakon4.rada.gov.ua

16. Колєснік, М. О. "Розробка політики безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства “Оберіг-сервіс”." (2019).

17. Грищук Д. В. Аналіз та вибір програмного та технічного забезпечення для створення системи захисту на основі NGFW : дис. – ТНТУ, 2022.

18. Комплексна система захисту інформації [Електронний ресурс] - Режим доступу : https://www.h-x.technology/ua/services/kszi-implementation-ua

19. Комплексні системи захисту інформації / Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. // Навчальний посібник Вінницького національного технічного університету, 2018. – 119 с

20. Архипова Є.О. Особливості застосування електронного цифрового підпису // Матеріали Всеукр. наук.-практ.конф. «В.М.Глушков – піонер кібернетики» (2014 р., м. Київ). – К.: Політехніка, 2014. – 266 с. – С.188-190.

21. Dunn Cavelty, Myriam, and Andreas Wenger. "Cyber security meets security politics: Complex technology, fragmented politics, and networked science." Contemporary Security Policy 41.1 (2020): 5-32.

22. Kweon, Eunkyung, et al. "The utility of information security training and education on cybersecurity incidents: An empirical evidence." Information Systems Frontiers 23 (2021): 361-373.

23. Mishra, Alok, et al. "Cybersecurity enterprises policies: A comparative study." Sensors 22.2 (2022): 538.

24. Aldawood, Hussain, and Geoffrey Skinner. "Contemporary cyber security social engineering solutions, measures, policies, tools and applications: A critical appraisal." International Journal of Security (IJS) 10.1 (2019): 1.

25. Al-Turkistani, Hilalah F., Samar Aldobaian, and Rabia Latif. "Enterprise architecture frameworks assessment: Capabilities, cyber security and resiliency review." 2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA). IEEE, 2021.

26. Paananen, Hanna, Michael Lapke, and Mikko Siponen. "State of the art in information security policy development." Computers & Security 88 (2020): 101608.

27. Alias, Rose Alinda. "Information security policy compliance: Systematic literature review." Procedia Computer Science 161 (2019): 1216-1224.

28. Saura, Jose Ramon, Domingo Ribeiro-Soriano, and Daniel Palacios-Marqués. "From user-generated data to data-driven innovation: A research agenda to understand user privacy in digital markets." International Journal of Information Management 60 (2021): 102331.

29. Hamill, J. Todd, Richard F. Deckro, and Jack M. Kloeber. "Evaluating information assurance strategies." Handbook of Scholarly Publications from the Air Force Institute of Technology (AFIT), Volume 1, 2000-2020. CRC Press, 2022. 3-32.

30. Zeebaree, S. R., et al. "Security approaches for integrated enterprise systems performance: A Review." Int. J. Sci. Technol. Res 8.12 (2019): 2485-2489.

31. Balanovskaya, A. V., A. V. Volkodaeva, and A. Yu Smol'kova. "Innovative Solutions for Ensuring Information Security of Modern Enterprises." Current Achievements, Challenges and Digital Chances of Knowledge Based Economy (2021): 753-762.

32. Yildirim, Ebru Yeniman, et al. "Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey." International Journal of Information Management 31.4 (2011): 360-365.

33. Limba, Tadas, et al. "Cyber security management model for critical infrastructure." Entrepreneurship and sustainability issues. Vilnius: Entrepreneurship and Sustainability Center, 2017, vol. 4, no. 4. (2017).

34. Cavelty, Myriam Dunn. "Cyber-security and private actors." Routledge handbook of private security studies (2015): 89-99.

35. Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing." 2012 international conference on computer science and electronics engineering. Vol. 1. IEEE, 2012.

36. Blume, Peter. "Data Protection in the Private Sector." Scandinavian Studies in Law, Vo (2004).

37. Liu, Yi, et al. "Privacy-preserving traffic flow prediction: A federated learning approach." IEEE Internet of Things Journal 7.8 (2020): 7751-7763.

38. Howard, Patrick D. "The security policy life cycle: functions and responsibilities." Information security management handbook. Auerbach Publications, 2019. 297-312.

39. Ghelani, Diptiben. "Cyber security, cyber threats, implications and future perspectives: A Review." Authorea Preprints (2022).

40. Malatji, Masike, Sune Von Solms, and Annlizé Marnewick. "Socio-technical systems cybersecurity framework." Information & Computer Security 27.2 (2019): 233-272.

41. Ključnikov, Aleksandr, Ladislav Mura, and David Sklenár. "Information security management in SMEs: factors of success." Entrepreneurship and Sustainability Issues 6.4 (2019): 2081.

42. Srinivas, Jangirala, Ashok Kumar Das, and Neeraj Kumar. "Government regulations in cyber security: Framework, standards and recommendations." Future generation computer systems 92 (2019): 178-188.

43. Stallings, William. Information privacy engineering and privacy by design: Understanding privacy threats, technology, and regulations based on standards and best practices. Addison-Wesley Professional, 2019.

44. Szczepaniuk, Edyta Karolina, et al. "Information security assessment in public administration." Computers & Security 90 (2020): 101709.

45. Humayun, Mamoona, et al. "Cyber security threats and vulnerabilities: a systematic mapping study." Arabian Journal for Science and Engineering 45 (2020): 3171-3189.

46. Ghelani, Diptiben, Tan Kian Hua, and Surendra Kumar Reddy Koduru. "Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking." Authorea Preprints (2022).

47. Trang, Simon, and Benedikt Brendel. "A meta-analysis of deterrence theory in information security policy compliance research." Information Systems Frontiers 21 (2019): 1265-1284.

48. Rostami, Elham, Fredrik Karlsson, and Shang Gao. "Requirements for computerized tools to design information security policies." computers & security 99 (2020): 102063.

49. Rostami, Elham, Fredrik Karlsson, and Shang Gao. "Policy components–a conceptual model for modularizing and tailoring of information security policies." Information & Computer Security (2023).

50. Tariq, Maham. A Technique for Compliance Identification for Information Security Policy Documents. Diss. CAPITAL UNIVERSITY, 2021.

ДОДАТОК А

Копії наукових публікацій

УДК 004.056.53
DOI:

ТІТОВА ВІРА
Хмельницький національний університет
ORCID ID: 0000-0001-8668-4834
e-mail: titovav@khmnu.edu.ua
КЛЬОЦ ЮРІЙ
Хмельницький національний університет
ORCID ID: 0000-0002-3914-0989
e-mail: klots@khmnu.edu.ua
МОСТОВИЙ СЕРГІЙ
Хмельницький національний університет
ORCID ID: 0000-0002-9505-3206
e-mail: serhii.mostovyi@khmnu.edu.ua
ОГОРОДНИК МАКСИМ
Хмельницький національний університет
e-mail: maks737271@gmail.com

РОЗРОБЛЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИВАТНОГО ПІДПРИЄМСТВА

У даній роботі представлено методику формування політики інформаційної безпеки у приватному секторі. Проведено аналіз систем даних, представлено їх техніко-економічні характеристики та визначено основні проблеми та завдання захисту інформації. Проведено порівняльний аналіз методів та засобів захисту інформації на аналогічних об'єктах інформаційної діяльності. Вибрано та продемонстровано методи захисту інформації в корпоративній мережі компанії за допомогою адміністративних заходів із запобігання загрозам інформаційної безпеки.

Ключові слова: політика інформаційної безпеки, методи та засоби захисту інформації.

VIRA TITOVA, YURII KLOTS, SERHII MOSTOVYI, MAKSYM OHORODNYK
Khmelnitskyi National University

DEVELOPING THE INFORMATION SECURITY POLICY OF A PRIVATE ENTERPRISE

Based on the analysis of the main provisions of the information protection theory, it was established that in order to create an information security policy, it is necessary to develop a number of documents and instructions aimed at information protection. And in no case should stop at one method of information protection, otherwise data protection will be at risk. Data protection must be comprehensive. The comprehensive policy of information security covers the development, production and installation of technical means of protection, as well as regular inspections of the information equipment used. The development of this policy is as follows: identification of deficiencies in the

company's current information protection; identification of types of threats that may arise as a result of deficiencies in the protection of information systems of the enterprise; selection of methods and ways of solving existing problems.

As a solution, a set of measures was developed, which consists of administrative decisions that regulate the possibility of information leakage due to the influence of the human factor. Based on the analysis of the main methods and means of information protection, it was established that organizational and legal methods and means of information protection should be aimed at countering threats to information security, reducing risks and effectively handling incidents in order to ensure a sufficient level of data protection for a long time. The evaluation of the effectiveness of the proposed measures through economic substantiation proved their feasibility of implementation in the organization.

Keywords: information security policy, methods and means of information protection.

Постановка проблеми

Поява нових інформаційних технологій та розвиток потужних комп'ютерних систем для зберігання та обробки інформації підвищили вимоги до рівня захисту інформації та визначили необхідність розробки ефективних механізмів захисту інформації, сумісних із сучасними архітектурами зберігання даних.

Забезпечення захисту інформації на підприємстві – це безперервний процес, що включає контроль зовнішнього і внутрішнього середовища підприємства, організацію та проведення заходів щодо підтримки стабільного функціонування локальної мережі та обчислювальної техніки, а також використання сучасних методів, що дозволяють мінімізувати втрати від витоку інформації. Для захисту інформації, як у мережі, так і на виробництві, компаніям необхідно сформувати певні правила та норми, що регламентують поведінку співробітників для забезпечення безпеки, а також описати технічні та програмні засоби захисту інформації. На це й спрямовано розроблення політики безпеки.

Огляд існуючих рішень

Політика інформаційної безпеки компанії зазвичай виражається в серії документів, що відображають вимоги до захисту даних і основні напрямки діяльності компанії щодо безпеки [1]. Існує три основні рівні розробки політики безпеки: верхній, середній і нижній [2].

На верхньому рівні політики безпеки даних організації необхідно: сформулювати та продемонструвати ставлення адміністрації підприємства до системи захисту інформації та відобразити основні цілі та завдання в цій галузі; розробити індивідуальні політики безпеки, інструкції та правила, за допомогою яких регулюються окремі питання; інформувати співробітників організації про основні завдання та пріоритети в галузі інформаційної безпеки.

Політика інформаційної безпеки середнього рівня використовується для відображення корпоративних підходів і вимог, таких як: використання інформаційних систем; телекомунікаційних та інформаційних технологій, методів і підходів до обробки інформації; учасників процесів обробки інформації, від яких залежить забезпечення захисту інформації на підприємстві.

Нижній рівень політики безпеки використовується для опису конкретних процедур і документів для забезпечення інформаційної безпеки на підприємстві.

Етапи розроблення політики безпеки в організації включають: виконання оцінки особистого ставлення до загроз безпеці з боку власників і співробітників підприємства; проведення аналізу потенційно важливих інформаційних активів підприємства; виявлення існуючих загроз безпеки підприємства з подальшою оцінкою ризиків.

Розглянемо основні елементи політики інформаційної безпеки підприємства [3-5]. Захист передбачає використання організаційних засобів захисту, визначених політикою безпеки підприємства. На першому етапі необхідно визначити межі, в яких функціонуватиме політика інформаційної безпеки компанії та встановити критерії оцінки її результатів.

На етапі аналізу ризиків інформації визначають пріоритети обраних засобів захисту з розподілом їх за

ступенем важливості на підприємстві, ідентифікують уразливість активів підприємства та визначають збитки. Результати аналізу ризиків інформаційної безпеки підприємства будуть застосовуватися у вигляді основи для планування роботи системи інформаційної безпеки, вибору найефективнішої стратегії та тактики. Для підвищення ефективності політики безпеки застосовуються такі прийоми, як групове визначення з використанням атрибутів та мандатне керування доступом.

Багато підприємств використовують глобальні та локальні політики безпеки, засновані на принципах управління інформаційною безпекою. Глобальні політики інформаційної безпеки спрямовані на забезпечення захисту інформації на рівні бізнес-процесів підприємства, тоді як локальні політики формуються на рівні захисту даних підприємства [4-6].

Глобальна політика підприємства являє собою правила безпеки, що описують можливі взаємодії між об'єктами, які потребують захисту інформації. Локальні політики безпеки підприємства використовуються для налаштування засобів захисту інформації, реплікації налаштувань вузлів і подальших коригувань. Зазвичай, локальні політики безпеки підприємства містять правила, які регулюють з'єднання і змінюють конфігурацію мережних пристроїв.

Формулювання цілей статті

Отже, на основі проведеного огляду можна зробити висновок, що для розроблення політики безпеки приватного підприємства необхідно вирішити такі завдання: оцінити поточний стан інформаційної безпеки підприємства; виявити порушення в захисті інформаційної безпеки, а також виявлення найімовірніших загроз інформації; розробити пропозиції щодо реалізації адміністративних заходів із запобігання загрозам інформаційної безпеки.

Виклад основного матеріалу

Для захисту даних приватного підприємства необхідно користувачів розділити на групи з відповідними правами:

- administrator – адміністратори мережі (створення та управління політиками інформаційної безпеки, глобальні налаштування мережі тощо);
- engineer – облікові записи для повсякденного обслуговування інформаційно-обчислювальної техніки;
- worker – обліковий запис стандартного користувача (співробітника організації) з обмеженими правами;
- guest – обмежений обліковий запис (у разі необхідності доступу не співробітників організації).

Для ідентифікації користувача потрібен унікальний запис кожного користувача, який включено до відповідної групи. Тим самим здійснюється розмежування доступу (табл. 1).

Таблиця 1

Групи користувачів та їхні права

Дії	Guest	Worker	Engineer	Administrator
Створення та зміни груп користувачів	Ні	Ні	Ні	Так
Зміна налаштувань мережі	Ні	Ні	Ні	Так
Підключення до мережі нових робочих станцій	Ні	Ні	Ні	Так
Зміна налаштувань серверів	Ні	Ні	Ні	Так
Зміна прав доступу	Ні	Ні	Ні	Так
Встановлення додатків та ПЗ	Ні	Ні	Так	Так
Доступ до Інтернету	Ні	Так	Так	Так
Доступ до корпоративної електронної пошти	Ні	Так	Так	Так

Доступ до корпоративного чату	Ні	Так	Так	Так
Можливість завантажувати файли	Ні	Ні	Так	Так
Запис файлів	"Мої документи"	"Мої документи", "Робочий стіл"	Будь-яка папка на робочому ПК	Будь-який ПК мережі
Підключення флеш-дисків, зовнішніх дисків.	Ні	Ні	Так	Так

Відправною точкою для визначення економічної ефективності запропонованого підходу є очевидне припущення: з одного боку, порушення інформаційної безпеки завдає певної шкоди; з іншого боку, забезпечення інформаційної безпеки коштує дорого. Загальна очікувана вартість захисту може бути виражена як сума вартості захисту та збитків від порушення. Очевидно, що оптимальним рішенням є розподіл коштів на захист інформації таким чином, щоб мінімізувати загальну вартість захисту [7].

Також зрозуміло, що економічна ефективність заходів з інформаційної безпеки визначається розміром відверненого збитку або розміром зниження ризиків для інформаційних активів організації.

Достатньо визначити лише рівень збитків, оскільки оптимальне рішення проблеми доцільного рівня витрат на захист полягає в тому, що цей рівень дорівнює рівню збитків, які очікуються в разі порушення безпеки. Як одна з методик визначення рівня витрат можливе використання такої емпіричної залежності очікуваних втрат (ризиків) R від і-ї загрози інформації [8-9]:

$$R_i = 10^{Ti+Li-4}, \quad (1)$$

де T_i – коефіцієнт, що характеризує можливу частоту виникнення відповідної загрози; L_i – коефіцієнт, що характеризує значення можливого збитку в разі її виникнення.

Сумарна вартість втрат визначається формулою:

$$R = \sum_{i=1}^{N} R_i , \quad (2)$$

де N – кількість можливих загроз інформаційним активам.

При розрахунку сумарного показника рекомендується виходити з того, що загрози конфіденційності, цілісності та доступності здійснюються порушником незалежно. Іншими словами, припускається, що цілісність інформації порушена діями порушника, але її зміст залишається невідомим порушнику (конфіденційність не порушена), а авторизовані користувачі все ще мають доступ до активу, хоча й у спотвореному вигляді.

Для прикладу розглянемо інформаційні активи приватної компанії (табл. 2). Розрахунки показують, що ризик економічних втрат для цієї компанії становить приблизно 1 080 000 гривень. З цього можна зробити висновок, що це дуже значні втрати для підприємства. Для того, щоб зрозуміти, наскільки ефективною є розроблена політика інформаційної безпеки, необхідно розрахувати показники економічної ефективності проєкту.

Таблиця 2

Величини втрат (ризиків) для інформаційних ресурсів до впровадження розробленої політики безпеки

Інформаційний актив	Загроза	Величина втрат (тис. грн.)
Проєктна документація, розроблена організацією	конфіденційності	100
	цілісності	500
	доступності	20
Особисті дані клієнта	конфіденційності	300
	цілісності	20
	доступності	20
Особисті відомості про співробітників	конфіденційності	100

	цілісності	10
	доступності	10
Сумарна величина втрат		**1 080**

Для проведення розрахунків необхідно отримати дані про передбачуваний розмір втрат (ризику) ключових інформаційних ресурсів після впровадження/модернізації інформаційної безпеки. Результати базуються на висновках експертних досліджень (див. табл. 3).

Таблиця 3

Величини втрат (ризиків) для інформаційних ресурсів після впровадження розробленої політики безпеки

Інформаційний актив	Загроза	Величина втрат (тис. грн.)
Проєктна документація, розроблена організацією	конфіденційності	10
	цілісності	50
	доступності	2
Особисті дані клієнта	конфіденційності	30
	цілісності	2
	доступності	2
Особисті відомості про співробітників	конфіденційності	10
	цілісності	1
	доступності	1
Сумарна величина втрат		**108**

Отже, можна зробити висновки, що впровадження розробленої політики безпеки дозволяє знизити можливі збитки в 10 разів, тобто витрати політики безпеки окупляться вже в першому кварталі. І це є зовсім невеликим навантаження на фінансову систему організації.

Висновки

Аналіз основних положень теорії інформаційної безпеки показує, що для створення політики інформаційної безпеки необхідно розробити низку документів та інструкцій з метою захисту інформації. Крім того, захист інформації не повинен обмежуватися лише одним методом захисту інформації. Захист даних повинен бути комплексним. Комплексна політика захисту інформації поширюється на розробку, виготовлення та встановлення технічних засобів захисту, а також на регулярну перевірку інформаційного обладнання, що використовується.

Розробка такої політики включає в себе виявлення поточних недоліків інформаційної безпеки підприємства, визначення типів загроз, які можуть виникнути через недоліки в захисті інформаційних систем підприємства, а також вибір шляхів і засобів для вирішення існуючих проблем.

В якості рішення автори розробили комплекс заходів, що складається з адміністративних рішень, які регламентують можливість витоку інформації через вплив людського фактору. На основі аналізу основних методів та заходів захисту інформації встановлено, що організаційно-правові методи та заходи захисту інформації повинні бути спрямовані на протидію загрозам інформаційній безпеці, зниження ризиків, ефективне реагування на інциденти та забезпечення достатнього рівня захисту даних протягом тривалого часу.

Ефективність запропонованих заходів оцінено за допомогою економічного обґрунтування, що свідчить про їх доцільність в організації.

Література

1. Основи інформаційної безпеки: навчальний посібник/ В.А. Лужецький, А.Д. Кожухівський, О.П. Войтович. Вінниця: ВНТУ, 2013. 221 с.

2. ДСТУ ISO/IEC 27005:2019. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки/ Нац. стандарт України. Вид. офіц [Чинний від 2019-11-01]. Київ: ДП «УкрНДНЦ», 2019. 76

с.

3. Формування моделі політики інформаційної безпеки на основі концепцій “глибинного захисту/ Д.В. Дячков// Підприємництво і торгівля. 2019. № 25. С. 116-121.

4. Політика інформаційної безпеки в системах інформаційно-аналітичного забезпечення підтримки прийняття організаційних рішень / С.М. Чуруброва // Проблеми програмування. 2016. № 4. С. 97-103.

5. Розробка політики інформаційної безпеки комп’ютерного контролю знань/ Н. Кухарська// Вісник Львівського державного університету безпеки життєдіяльності. 2017. №16. С.34-39.

6. Політика інформаційної безпеки об’єкта/ Ю. Хохлачова// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2012 р. Вип. 2 (24). С. 23-29.

7. Оцінювання ефективності рішень в системах захисту інформації/ В. Ю. Тітова, О. С. Андрощук, В. С. Орленко, І. М. Шевчук, В. С. Даценко // Вісник Хмельницького національного університету. Технічні науки. 2020. № 5. С. 307–310.

8. Комерційна діяльність. Навч. посібник/ Л.Г. Филевич, Л.О. Попова, О.М. Прядко, Т.Л. Мітяєва, Л.А. Прибилович. Харків: ХДУХТ, 2014. 225 с.

9. Інформаційна політика в системі забезпечення фінансової безпеки держави/ А.Д. Глушко, В.В. Пантась, С.Р. Бабенко// «Ефективна економіка». 2022. №2.

References

1. Osnovy informatsiinoi bezpeky : navchalnyi posibnyk/ V.A. Luzhetskyi, A.D. Kozhukhivskyi, O.P. Voitovych. Vinnytsia: VNTU, 2013. 221 s.

2. DSTU ISO/IEC 27005:2019. Informatsiini tekhnolohii. Metody zakhystu. Upravlinnia ryzykamy informatsiinoi bezpeky / Nats. standart Ukrainy. Vyd. ofits [Chynnyi vid 2019-11-01]. Kyiv: DP «UkrNDNTs», 2019. 76 s.

3. Formuvannia modeli polityky informatsiinoi bezpeky na osnovi kontseptsii “hlybynnoho zakhystu/ D.V. Diachkov// Pidpryiemnytstvo i torhivlia. 2019. № 25. S. 116-121.

4. Polityka informatsiinoi bezpeky v systemakh informatsiino-analitychnoho zabezpechennia pidtrymky pryiniattia orhanizatsiinykh rishen / Churubrova S. M. // Problemy prohramuvannia. 2016. № 4. S. 97-103.

5. Rozrobka polityky informatsiinoi bezpeky kompiuternoho kontroliu znan/ N. Kukharska// Visnyk Lvivskoho derzhavnoho universytetu bezpeky zhyttiediialnosti. 2017. №16. S.34-39.

6. Polityka informatsiinoi bezpeky obiekta/ Yu. Khokhlachova// Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini. 2012 r. Vyp. 2 (24). S. 23-29.

7. Otsiniuvannia efektyvnosti rishen v systemakh zakhystu informatsii/ V. Yu. Titova, O. S. Androshchuk, V. S. Orlenko, I. M. Shevchuk, V. S. Datsenko // Herald of Khmelnytskyi National University. Technical sciences. 2020. № 5. S. 307–310.

8. Komertsiina diialnist. Navch. posibnyk/ L.H. Fylevych, L.O. Popova, O.M. Priadko, T.L. Mitiaieva, L.A. Prybylovych. Kharkiv: KhDUKhT, 2014. 225 s.

9. Informatsiina polityka v systemi zabezpechennia finansovoi bezpeky derzhavy/ A.D. Hlushko, V.V. Pantas, S.R. Babenko// «Efektyvna ekonomika». 2022. №2.

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Огородник Максим Костянтинович
ПІБ здобувача вищої освіти

Студента ФІТ, 2 курсу, групи КБм-22-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

05.12.2023
дата

підпис

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015985534

Дата перевірки:
08.12.2023 19:53:52 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
08.12.2023 19:58:33 EET

ID користувача:
100008300

Назва документа: **Огородник на плагіат 2023**

Кількість сторінок: 82 **Кількість слів:** 12930 **Кількість символів:** 108364 **Розмір файлу:** 1.55 MB **ID файлу:** 1015666330

15.8%
Схожість

Найбільша схожість: 6.37% з Інтернет-джерелом (http://dspace.nuft.edu.ua/jspui/bitstream/123456789/34926/1/Syniak%.

15.7% Джерела з Інтернету 597 ..... Сторінка 84

0.97% Джерела з Бібліотеки 46 ..... Сторінка 87

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи 2

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 4%**

	Документ		Сумарний збіг по Базі Даних	
ID: 122220 Назва: Технологія забезпечення комплексної інформаційної безпеки приватного підприємства Додано в БД: 2023-12-08 Автора: Огородник М.К. Керівники: Тітова В.Ю, Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	83448	1272	1565 (2%)	29 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Технологія забезпечення комплексної інформаційної безпеки приватного підприємства

Автор: Огородник Максим Костянтинович
Спеціальність: 125 – Кібербезпека
Освітня програма: освітньо-професійна
Науковий керівник: Тітова Віра Юріївна, к.т.н, доцент
Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 84,2%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99,9%.

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки. Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 15,8%, з яких 6.37% є збігами з одним джерелом, зумовленими наявністю типових фразеологічних виразів предметної області, а також формулюваннями, які утворюють загальновживані фрази.

Керівник роботи _____ В.Ю. Тітова

Гарант ОП _____ В.Ю. Тітова

Завідувач кафедри кібербезпеки _____ Ю. П. Кльоц

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Студент Огородник Максим Костянтинович

Тема Технологія забезпечення комплексної інформаційної безпеки приватного підприємства

Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека*»
Освітня програма «Кібербезпека»

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень - ; кількість сторінок записки 74

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі запропоновано технологію комплексного захисту інформації на приватному підприємстві, для цього було проаналізовано вразливості інформаційної безпеки досліджуваного підприємства, розглянуто наявні засоби захисту підприємства, створено систему комплексного захисту підприємства, розроблено рекомендації щодо вдосконалення та проведено оцінку економічної ефективності запропонованих рішень.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, чітко визначено об'єкт, предмет та методи дослідження, сформульована актуальність; визначені задачі, які необхідно вирішити для досягнення поставленої мети, практична цінність отриманих результатів, їхня новизна та наведені відомості про публікації. У першому розділі проаналізовано і досліджено загальні положення комплексної системи захисту інформації. У другому розділі проаналізовано та проведено оцінку захисту даних в активах приватного підприємства, визначено основні проблеми та завдання захисту інформації на підприємстві, обґрунтовано необхідність вдосконалення системи інформаційної безпеки та захисту інформації на підприємстві. У третьому розділі реалізовано розроблено політику інформаційної безпеки на підприємстві, вдосконалено організаційні підходи до забезпечення інформаційної безпеки підприємства, запропоновано перелік програмно-апаратних та криптографічних засобів. Четвертий розділ присвячений розробці технічного завдання та рекомендацій щодо впровадження розробленої політики інформаційної безпеки на підприємстві та оцінюванню економічної ефективності запропонованих рішень.

4. Позитивні сторони роботи полягають у тому, що наукові та практичні результати, отримані в роботі, складають підґрунтя для розроблення та вдосконалення комплексної системи інформаційної безпеки типового об'єкту інформаційної діяльності від впливу внутрішніх і зовнішніх втручань та загроз навмисного, випадкового, природного або штучного характеру для забезпечення потреб державних і комерційних структур, а також підрозділів спеціального призначення

5. Негативні сторони роботи у роботі не наведено порівняльний аналіз типових рішень комплексної інформаційної безпеки типового об'єкту інформаційної діяльності з запропонованими автором рішеннями

6. Оцінка графічного оформлення та пояснювальної записки роботи Оформлення всіх матеріалів кваліфікаційної роботи є якісним, здійснене з дотриман-ням актуальних стандартів та інституційних положень ХНУ. Пояснювальна записка ві-дповідає нормам щодо її оформлення як за структурою, так і за представленням і фор-матуванням матеріалу

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, доктор технічних наук, професор Мартинюк Валерій Володимирович.

« 8 » грудня 2023 року _____ (підпис)