Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Калюжного Михайла Сергійовича*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ «eUnify»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Горєв В.М.			
розділів:				
спеціальний	ст. викл. Войцех С.І.			
економічний	доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	Конограй Н.О.			

Дніпро
2021

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____2021 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Калюжному Михайлу Сергійовичу* **академічної групи** *125-17-2*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації _____

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ «eUnify»*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 07.06.2021 № 317-С

Розділ	Зміст	Термін виконання
Розділ 1	У розділі розглянуто основні загрози для підприємств різних категорій та поставлено задачу підвищити рівень інформаційної захищеності ІТС компанії «eUnify».	07.05.2021-14.05.2021
Розділ 2	У розділі проведено обстеження ОІД, створено модель порушника та модель загроз, обрано методи та засоби захисту інформації.	17.05.2021-31.05.2021
Розділ 3	У розділі наведено економічне обґрунтування доцільності запровадження обраних методів та засобів захисту інформації.	01.06.2021-08.06.2021

Завдання видано _____ Горєв В.М.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 18.01.2021

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Калюжний М.С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 62 с., 6 рис., 15 табл., 4 додатків, 12 джерел.

Об’єкт дослідження: інформаційно-телекомунікаційна система товариства з обмеженою відповідальністю «eUnify».

Мета роботи: підвищення рівня захищеності інформації в інформаційно-телекомунікаційній системі ТОВ «eUnify».

Методи розробки: спостереження, порівняння, аналіз, опис, розрахунки.

В першому розділі кваліфікаційної роботи наводяться та аналізуються статистичні дані про стан інформаційної безпеки на підприємствах, також аналізується загальна тенденція кіберінцидентів за 2020 рік.

В другому розділі кваліфікаційної роботи проводиться обстеження ІТС компанії «eUnify». Під час обстеження розглядається: фізичне середовище, обчислювальна система, інформаційне середовище. Розробляється модель порушника та модель загроз. Базуючись на цьому, обрано методи та засоби захисту інформації для підвищення рівня захищеності інформації в ІТС.

В третьому розділі кваліфікаційної роботи розраховується економічна доцільність впровадження обраних методів та засобів захисту інформації в ІТС об’єкта інформаційної діяльності.

Практичне значення роботи полягає у дослідженні та поліпшенні рівня інформаційної захищеності ІТС ТОВ «eUnify».

Результати досліджень, виконаних у кваліфікаційній роботі, можуть бути використані для вдосконалення КСЗІ.

ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА

РЕФЕРАТ

Пояснительная записка: 62 с., 6 рис., 15 табл., 4 приложений, 12 источников.

Объект исследования: информационно-телекоммуникационная система общества с ограниченной ответственностью «eUnify».

Цель работы: Повышение уровня защищенности информации в информационно-телекоммуникационной системе ООО «eUnify».

Методы разработки: наблюдение, сравнение, анализ, описание, расчеты.

В первом разделе квалификационной работы приводятся и анализируются статистические данные о состоянии информационной безопасности на предприятиях, также анализируется общая тенденция киберинцидентов за 2020 год.

Во втором разделе квалификационной работы проводится обследование ИТС компании «eUnify». При обследовании рассматриваются: физическая среда, вычислительные системы, информационная среда. Разрабатывается модель нарушителя и модель угроз. Основываясь на этом - выбираются методы и средства защиты информации для повышения уровня защищенности информации в ИТС.

В третьем разделе квалификационной работы рассчитывается целесообразность внедрения выбранных методов и средств защиты информации в ИТС объекта информационной деятельности.

Практическое значение работы заключаєтся в исследовании и улучшении уровня информационной защищенности ИТС ООО «eUnify».

Результаты исследований, выполненных в квалификационной работе, могут быть использованы для совершенствования КСЗИ.

ИНФОРМАЦИОННО-ТЕЛЕКОМУНИКАЦИОННАЯ СИСТЕМА, ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ

ABSTRACT

Explanatory note: 62 pages, 6 drawings, 15 tables, 4 appendices, 12 sources.

Object of research: information and telecommunication system of the limited liability company "eUnify".

Purpose: to increase the level of information security in the information and telecommunications system of LLC "eUnify".

Development methods: observation, comparison, analysis, description, calculations.

The first section of the qualification work presents and analyzes statistical data on the state of information security in enterprises, as well as analyzes the general trend of cyber incidents in 2020.

In the second section of the qualification work, an ITS survey of the "eUnify" company is carried out. During the survey the following is considered: physical environment, computer systems, information environment. A model of the violator and a model of threats are being developed. Based on this - selected methods and means of information protection to increase the level of information security in ITS.

The third section of the qualification work calculates the feasibility of implementing the selected methods and means of information protection in the ITS of the object of information activities.

The practical significance of the work is to study and improve the level of information security of ITS LLC "eUnify".

The results of research performed in the qualification work can be used to improve the CISS.

INFORMATION AND TELECOMMUNICATIONS SYSTEM, OBJECT OF INFORMATION ACTIVITY, METHODS AND MEANS OF INFORMATION PROTECTION, THREAT MODEL, INTRUDER MODEL

СПИСОК УМОВНИХ СКОРОЧЕНЬ

КСЗІ – комплексна система захисту інформації;

ТОВ – товариство з обмеженою відповідальністю;

ПЗ – програмне забезпечення;

ІТС – інформаційно-телекомунікаційна система;

ДСТУ – державний стандарт України;

НД ТЗІ – нормативний документ в галузі технічного захисту інформації;

ОІД – об’єкт інформаційної діяльності;

ІТ – інформаційні технології;

КЗ – контрольована зона;

КПП – контрольно-пропускний пункт;

ПК – персональний комп’ютер;

АС – автоматизована система;

ОС – операційна система;

КЗЗ – комплекс засобів захисту;

КС – комп’ютерна система;

ШПЗ – шкідливе програмне забезпечення;

ІС – інформаційна система.

ЗМІСТ с.

ВСТУП

Потреба в захисті інформації в наш час існує не тільки у великих і середніх підприємств, а і у малих. Це зумовлено тим що втілювати різні інформаційні атаки стало простіше і дешевше. Поява нових загроз потребує постійного вдосконалення інформаційної захищеності підприємства, адже в іншому випадку при реалізації загрози інформації підприємство може зазнати значних збитків. На жаль в більшості випадків фінансові можливості малого підприємства не дозволяють йому скористатись послугами організацій, які забезпечують захист інформації підприємств, здійснюють виявлення та усунення загроз.

Малі підприємства є вразливими до інформаційних атак різних видів через такі причини:

- висока вартість засобів захисту інформації;
- необхідність у залученні спеціалістів у області захисту інформації;
- низький рівень обізнаності персоналу щодо методів і засобів забезпечення кібербезпеки.

Актуальність роботи обумовлена необхідністю підвищення рівня інформаційної захищеності ТОВ «eUnify».

Об’єктом кваліфікаційної роботи є товариство з обмеженою відповідальністю «eUnify», яке займається розробкою та підтримкою ПЗ.

Метою кваліфікаційної роботи є підвищення рівня інформаційної безпеки інформаційно-телекомунікаційної системи ТОВ «eUnify». Для цього необхідно вирішити наступні завдання:

- проаналізувати інформаційну систему ТОВ «eUnify» з точки зору інформаційної безпеки;
- проаналізувати об’єкти захисту;
- привести теоретичне обґрунтування рекомендованих засобів захисту інформації;
- дати оцінку економічній доцільності реалізації проєкту КСЗІ підприємства «eUnify».

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Успішний бізнес – завжди ціль, яку ставить перед собою будь-який підприємець. Такі цілі є причиною прогресу, що обумовлено ростом конкуренції на ринку та постійним вдосконаленням продукції. Успішний бізнес - це також вигода для споживачів, яка полягає в отриманні задоволення від володіння чи використання якісного продукту та ціль для послідовників, які надихаються ідеями для створення чи підвищення рівня власних сервісів. Але, що найважливіше, успішний бізнес є мішенню для конкурентів та зловмисників, мета яких збагатитись на чужому успіху.

Безліч компаній як мінімум один раз за рік зазнавали зовнішньої атаки або зіштовхувалися з внутрішніми інцидентами інформаційної безпеки. У світі безперервно створюється безліч нового шкідливого програмного забезпечення (ШПЗ). Чорний ринок вірусів та шкідливого програмного забезпечення досить великий і через це з кожним днем інформаційні небезпеки для підприємств зростають.

Зовнішніми загрозами для бізнесу є шкідливе ПЗ, DDoS-атаки, фішингові атаки, проникнення у мережу, втрата пристроїв зі збереженими паролями. Внутрішніми найпоширенішими загрозами є вразливе або неліцензійне ПЗ та витоки інформації через співробітників або з їх вини.

Збільшення обсягів клієнтських даних, що оброблюються і зростаюча роль інтелектуальної власності в успіху продукту призводять до виникнення нових форм викрадення інформації. Конкурентів цікавить інформація про внутрішні процеси у компанії, дані про співробітників, фінансова інформація, інтелектуальна власність, дані корпоративного банківського аккаунту.

Проблема забезпечення захисту інформації полягає у тому, що бізнес рідко використовує надійне антивірусне ПЗ чи спеціалізовані рішення щодо захисту інформації в інформаційно-телекомунікаційних системах (ІТС). Також великою проблемою є створення однакових або дуже схожих паролів для різних облікових

записів. Це означає що у тому випадку коли шахрай дізнається пароль від одного облікового запису, то він отримає доступ до всіх інших облікових записів.

Заголовки новин містять безліч повідомлень про випадки зломів інформаційних систем комерційних структур, витік даних, електронне шахрайство, порушення функціонування державних структур або критично важливих об'єктів інфраструктури, крадіжку інтелектуальної власності, витоки інформації, пов'язаної з національною безпекою тощо. Об'єктами інформаційних атак стають компанії різного рівня та масштабів.

Відповідно до досліджень міжнародної компанії Positive Technologies, що спеціалізується на розробці інноваційних рішень в сфері інформаційної безпеки, підсумки 2020 року в сфері кібербезпеки є такими [1]:

- кількість унікальних кіберінцидентів в 2020 році зросло на 51% в порівнянні з 2019 роком;
- росте значимість злому облікових записів (хакінга) в атаках на організації (рисунок 1.1). За результатами 2020 року ця частка складає 24% (на 10 відсотків більше, ніж в 2019 році). Відзначено зростання ринків з продажу доступів в компанії і підвищений інтерес до теми злому сайтів;
- атак з використанням шкідливого ПЗ з кожним роком стає все більше і більше. У 2020 році кількість таких атак збільшилася на 54% в порівнянні з 2019 роком;
- тренд 2020 року в атаках на організації – застосування програм шифрувальників, їх частка серед ШПЗ склала 45%. Оператори програм-вимагачів перейшли від масових атак до цілеспрямованого вибору жертв, збільшили суми викупу, відкрили нові сайти з продажу вкраденої інформації і почали використовувати DDoS-атаки для шантажу жертв.

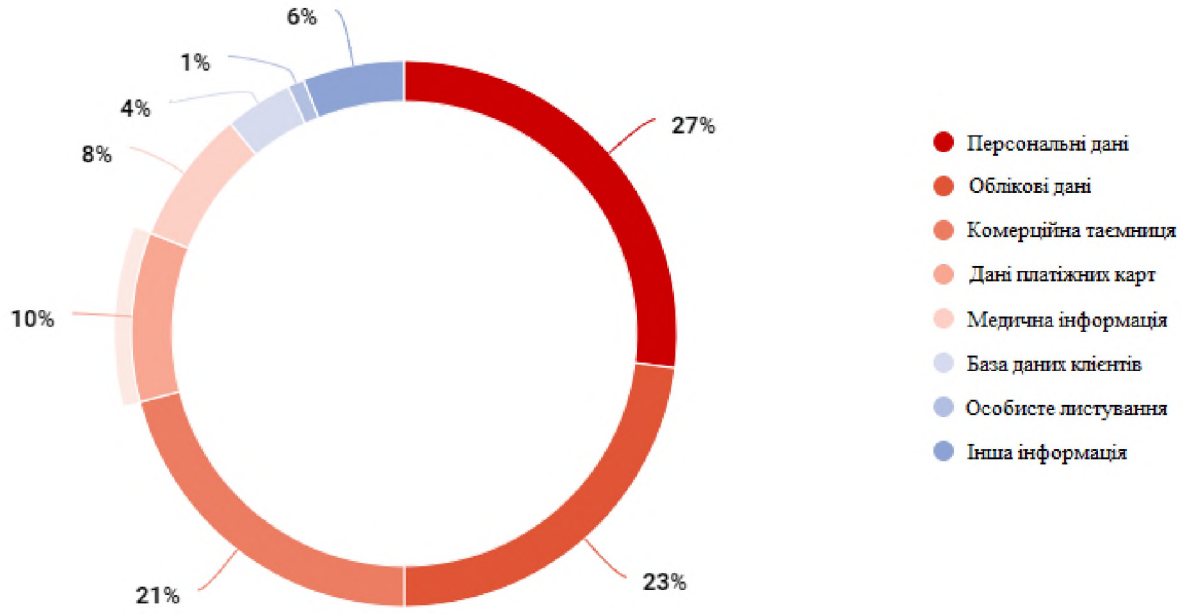


Рисунок 1.1 - Типи викрадених даних за 2020 рік

2020 рік відзначився атаками, пов'язаними з компрометацією ланцюжка поставок (supply chain attacks). Найбільш гучні інциденти сталися з компаніями Blackbaud і SolarWinds. В результаті цих атак компанія Blackbaud призначена відповідачем по 23 груповим позовам від постраждалих клієнтів, а акції компанії SolarWinds впали в ціні.

Виходячи з усього вищезгаданого, можна стверджувати, що кожному підприємству, яке має ІТС і бажає бути успішним, незалежно від його розміру та місця на ринку, необхідно мати комплексну систему захисту інформації (КСЗІ).

1.2 Нормативно-правове забезпечення щодо створення КСЗІ

Державні та недержавні установи, організації та підприємства відповідно до законодавства України зобов’язані захищати інформацію, яка містить державну таємницю. Стосовно власної службової (конфіденційної) інформації, то підприємства можуть захищати її на власний розсуд.

При створенні комплексної системи захисту інформації необхідно посилатись та використовувати такі нормативні документи та стандарти:

- НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»;
- НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»;
- ДСТУ 3396.1-96 «Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт»;
- НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»;
- НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі»;
- НД ТЗІ 3.6-001-2000 «Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу»;
- НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».

Дія цих нормативних документів поширюється тільки на ІТС в яких інформація оброблюється або зберігається автоматизованим способом.

1.3 Постановка задачі

На основі аналізу проблем у пункті 1.1, де було розглянуто основні загрози для підприємств різних категорій, виникає потреба у необхідності підвищення рівня захищеності інформації компанії «eUnify».

У вищезгаданих нормативних документах зазначено необхідність впровадження системи захисту інформації на об'єктах інформаційної діяльності, де циркулює відкрита інформація, що потребує захисту, та інформація з обмеженим доступом, якщо потребу у КСЗІ встановлює власник інформації [2].

Для підвищення рівня захищеності інформації в ІТС компанії «eUnify» необхідно [3]:

- провести обстеження фізичного середовища;
- провести обстеження обчислювальної системи;
- провести обстеження інформаційного середовища;
- розробити модель порушника;
- розробити модель загроз;
- обрати профіль захищеності;
- визначити методи та засоби захисту інформації.

1.4 Висновок

У розділі приведено актуальні причини та наслідки порушення безпеки інформації на підприємствах. Приведено перелік зовнішніх і внутрішніх загроз для підприємств. Враховуючи загальну тенденцію росту кіберінцидентів, прийнято рішення щодо необхідності підвищення рівня захищеності інформації в інформаційно-телекомунікаційній системі ТОВ «eUnify». В розділі визначені необхідні для цього кроки.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про компанію

Компанія «eUnify» займається розробкою та підтримкою програмного забезпечення. Організація веде свою діяльність з 2004 року, в 2010 році була інкорпорована. Офіс компанії знаходиться за адресою м. Дніпро вул. Акінфієва 18.

У компанії працюють кваліфіковані співробітники, завдяки зусиллям яких компанія розвивається. Перелік співробітників наведений в таблиці 2.1.

Таблиця 2.1 - Ідентифікація суб'єктів інформаційної системи

Посада	Відділ	Роль в ІС	Рівень кваліфікації
Старший програміст (Team Lead)	IT	Користувач	Високий
Сисистемний Адмін	IT	Адміністратор	Середній
Програміст (Middle developer)	IT	Користувач	Середній
Програміст (Middle developer)	IT	Користувач	Середній
Програміст (Middle developer)	IT	Користувач	Середній
Програміст (Junior developer)	IT	Користувач	Середній
Програміст (Junior developer)	IT	Користувач	Середній
Бухгалтер	Бухгалтерія	Користувач	Середній
Директор	-	-	Високий

2.2 Обстеження об’єкта інформаційної діяльності

Метою обстеження є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт [4].

Межі КЗ співпадають з межами ОІД. З північної сторони КЗ обмежена зовнішньою стіною будівлі, східна і південна стіни межують із офісними приміщеннями інших компаній.

Компанія займає приміщення на першому поверсі в офісному центрі (за адресою вул. Івана Акінфієва, 18), яке включає в себе одну кімнату (рисунок 2.2). Вхід на територію здійснюється через КПП який розміщений на вході до офісного центру.

Найбільшою цінністю компанії є інформація, яка зберігається на електронних носіях, а також технічне обладнання для розробки ПЗ: системні блоки (8 штук), монітори (8 штук). Із архітектурних засобів протидії несанкціонованому проникненню на об’єкт є дерев’яні двері з замком, захисні ролети на всіх вікнах.

На ОІД є система електроживлення яка виходить за межі КЗ і з’єднується з міською системою електроживлення. Об’єкт має вихід до інтернет мережі (рисунок 2.3), лінії якої виходять за межі об’єкта. Також є система опалення, трубопровід якої з’єднується з міською опалювальною системою (рисунок 2.4).

2.2.1 Обстеження фізичного середовища

Фізичне середовище:

- тип будівлі - громадська споруда;
- ситуаційний план (рисунок 2.1);
- трансформаторна підстанція (розміщена на вул. Івана Акінфієва, 18).

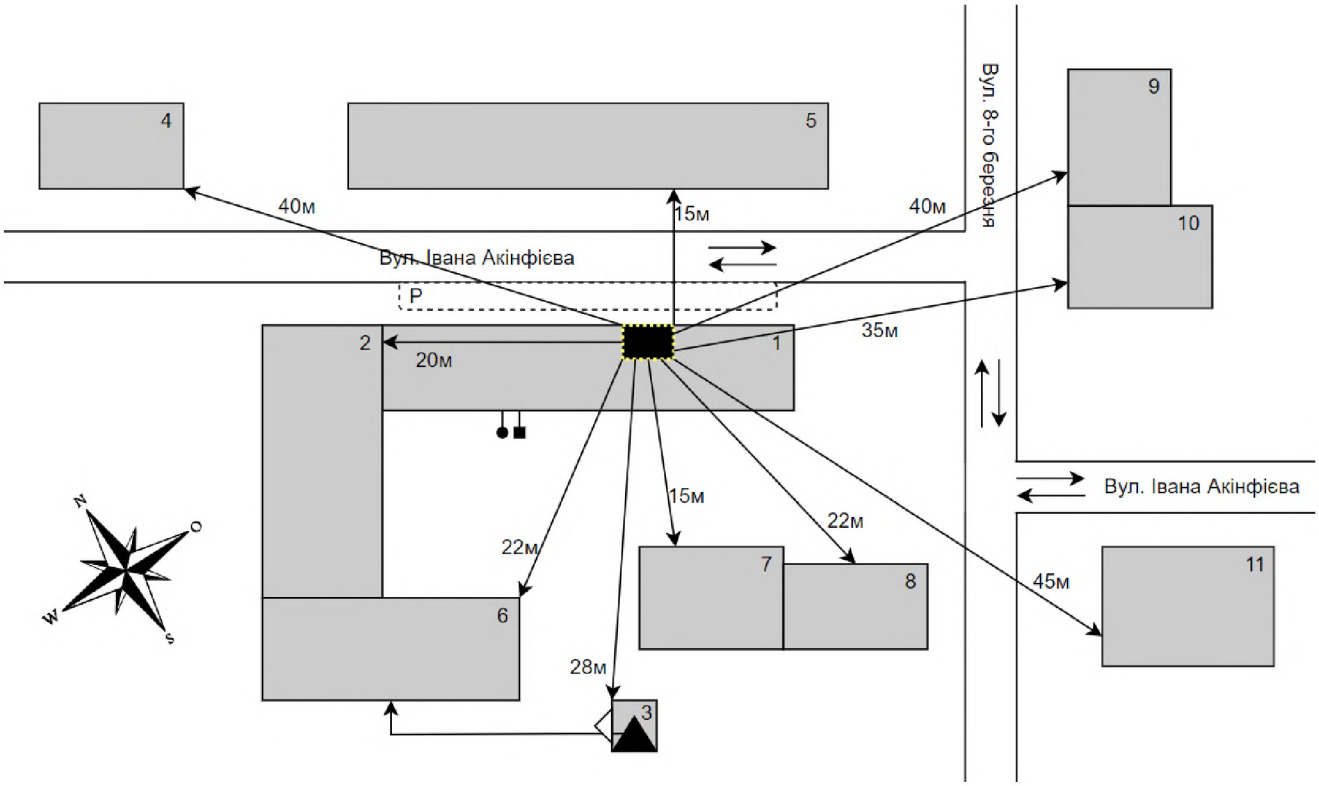
Архітектурно-будівельні особливості:

- площа - 42 м^2, розміри 9х5м, висота стелі 3м, поверх - перший;
- стеля (бетон, 150мм), підлога (бетон , 150мм), несуча стіна (цегла, 510мм), інші стіни (газобетон, 100мм), підвісна стеля (матеріал – мінерально-волокниста плита, товщиною 12мм);
- двері (одні, дерев'яні), вікна (3 пластикових вікна, розміри – 2.3м х 1.5м), вікна виходять в сторону вул. Івана Акінфієва, сектор прямої видимості – дев'ятиповерховий житловий будинок.

На рисунку ситуаційного плану відображено розташування ОІД відносно інших об'єктів місцевості, які перелічені і описані в таблиці 2.1.

Таблиця 2.1 - Будівлі, прилеглі до ОІД

Найменування	Кількість поверхів	Адреса	Відстань до ОІД, м
1. Офісна будівля	5	вул. Івана Акінфієва, 18а	-
2. Офісна будівля	7	вул. Івана Акінфієва, 18	20
3. Трансформаторна підстанція	1	вул. Івана Акінфієва, 18г	28
4. Житловий будинок	9	вул. Івана Акінфієва, 11	40
5. Житловий будинок	9	вул. Івана Акінфієва, 15	15
6. Офісна будівля	7	вул. Івана Акінфієва, 18б	22
7. Магазин	1	вул. Івана Акінфієва, 18в	15
8. Офісна будівля	3	вул. Івана Акінфієва, 18д	22
9. Житловий будинок	5	вул. 8-го Березня, 9б	40
10. Житловий будинок	6	вул. Івана Акінфієва, 17	35



Умовні позначення:

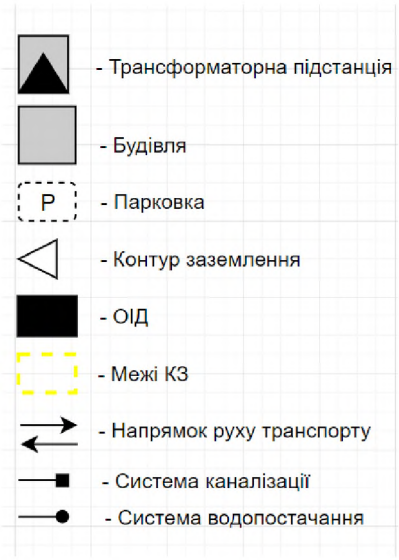
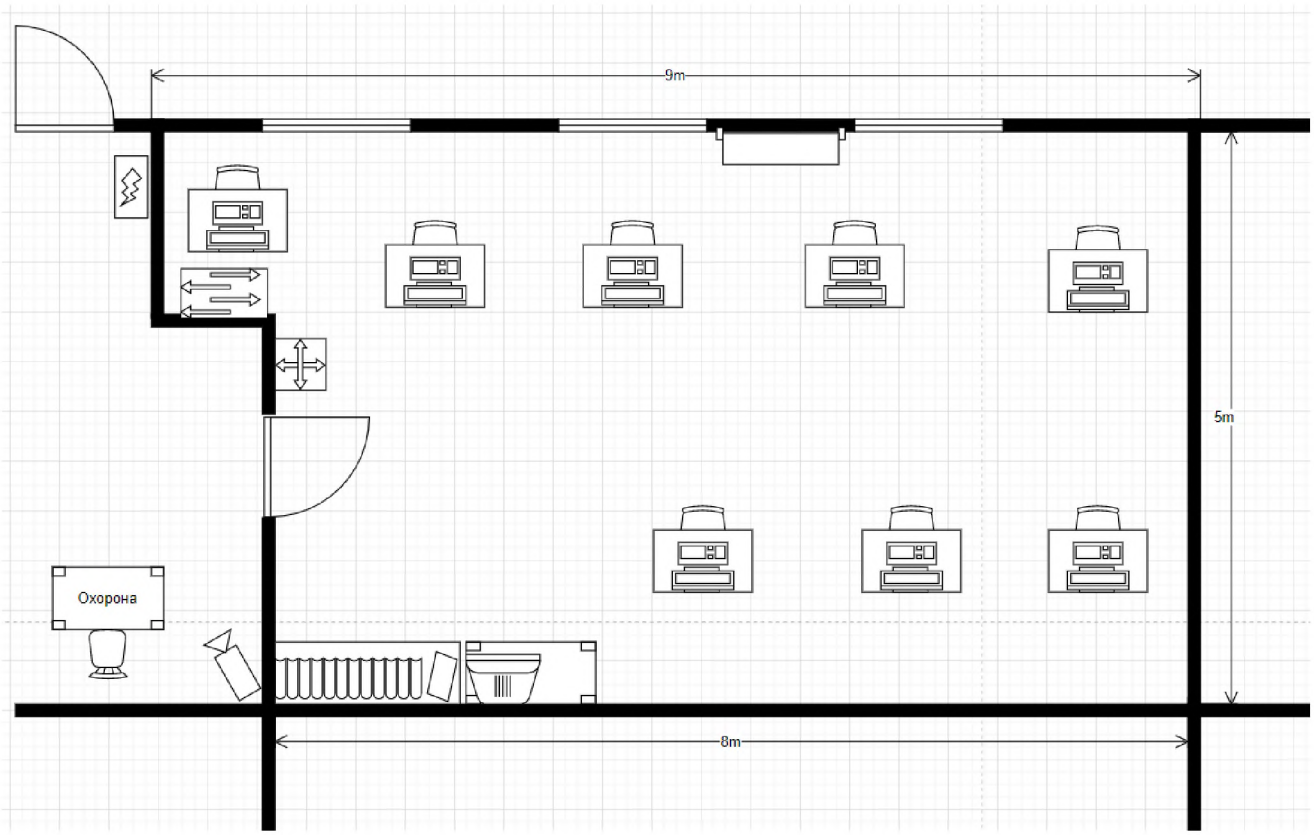


Рисунок 2.1 - Ситуаційний план



Умовні позначення:

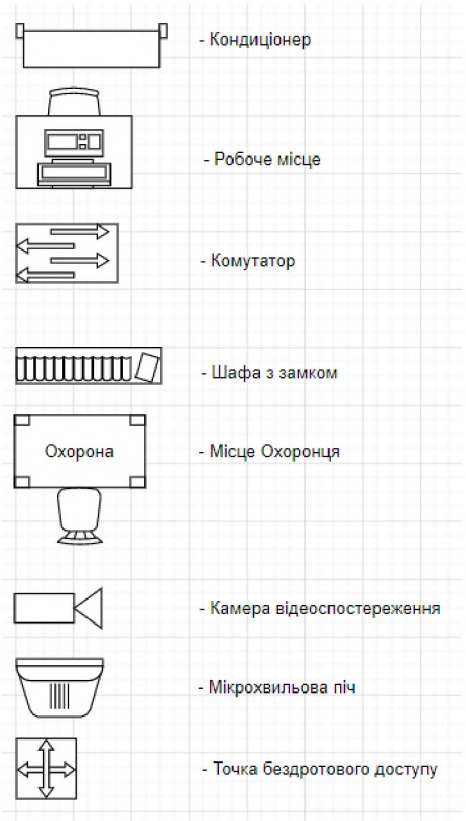
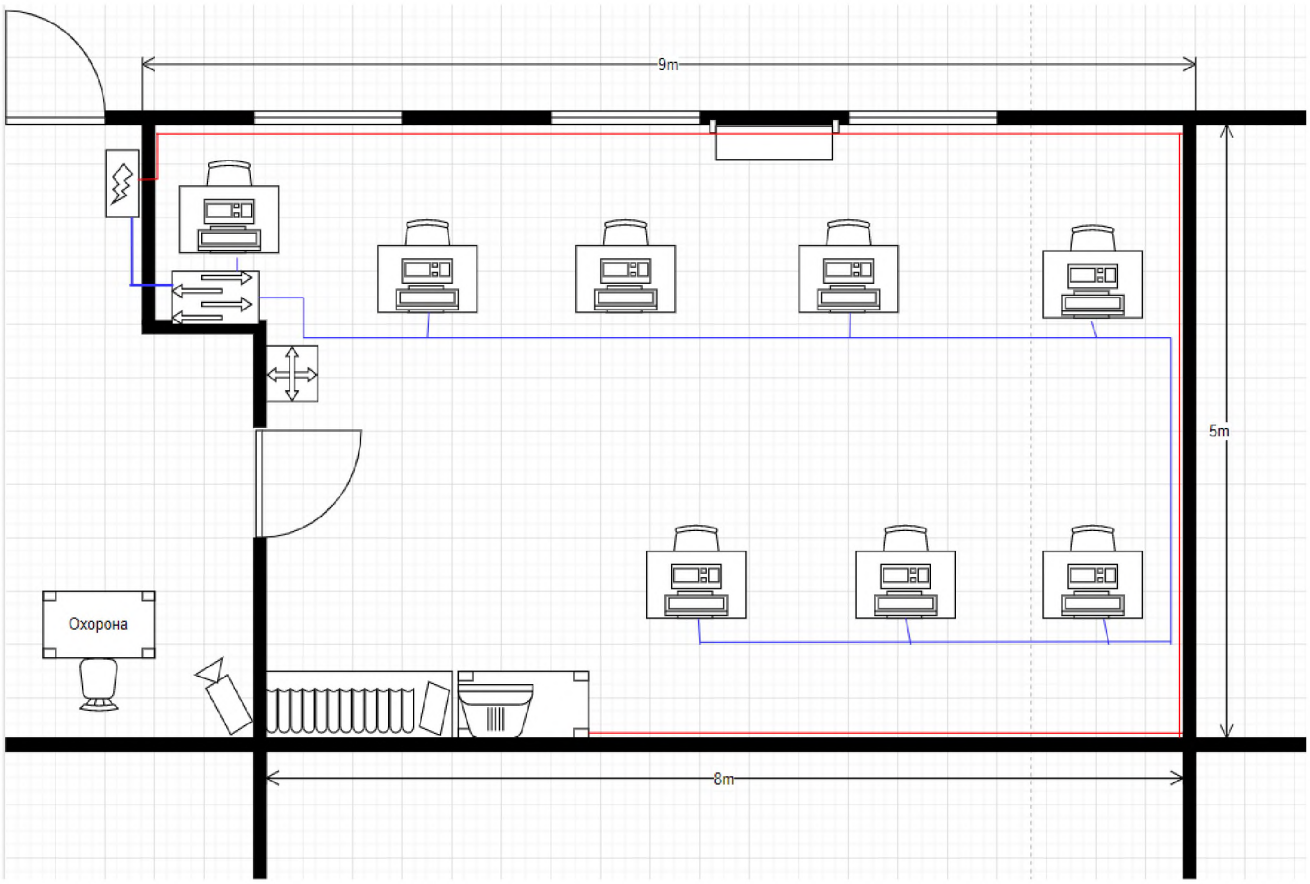


Рисунок 2.2 - Генеральний план приміщення



Умовні позначення:

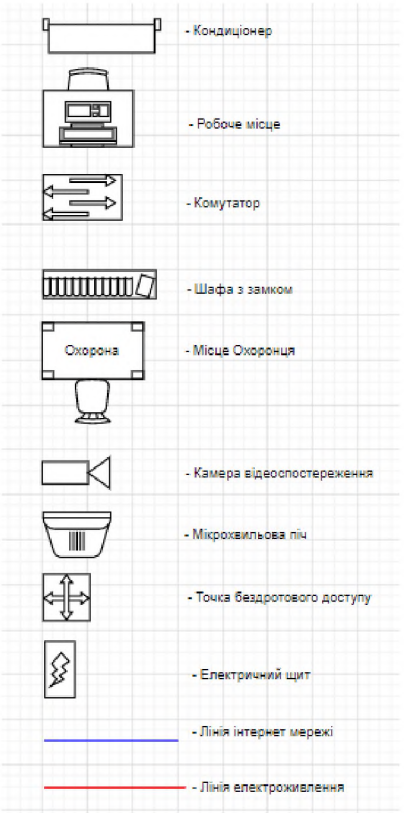
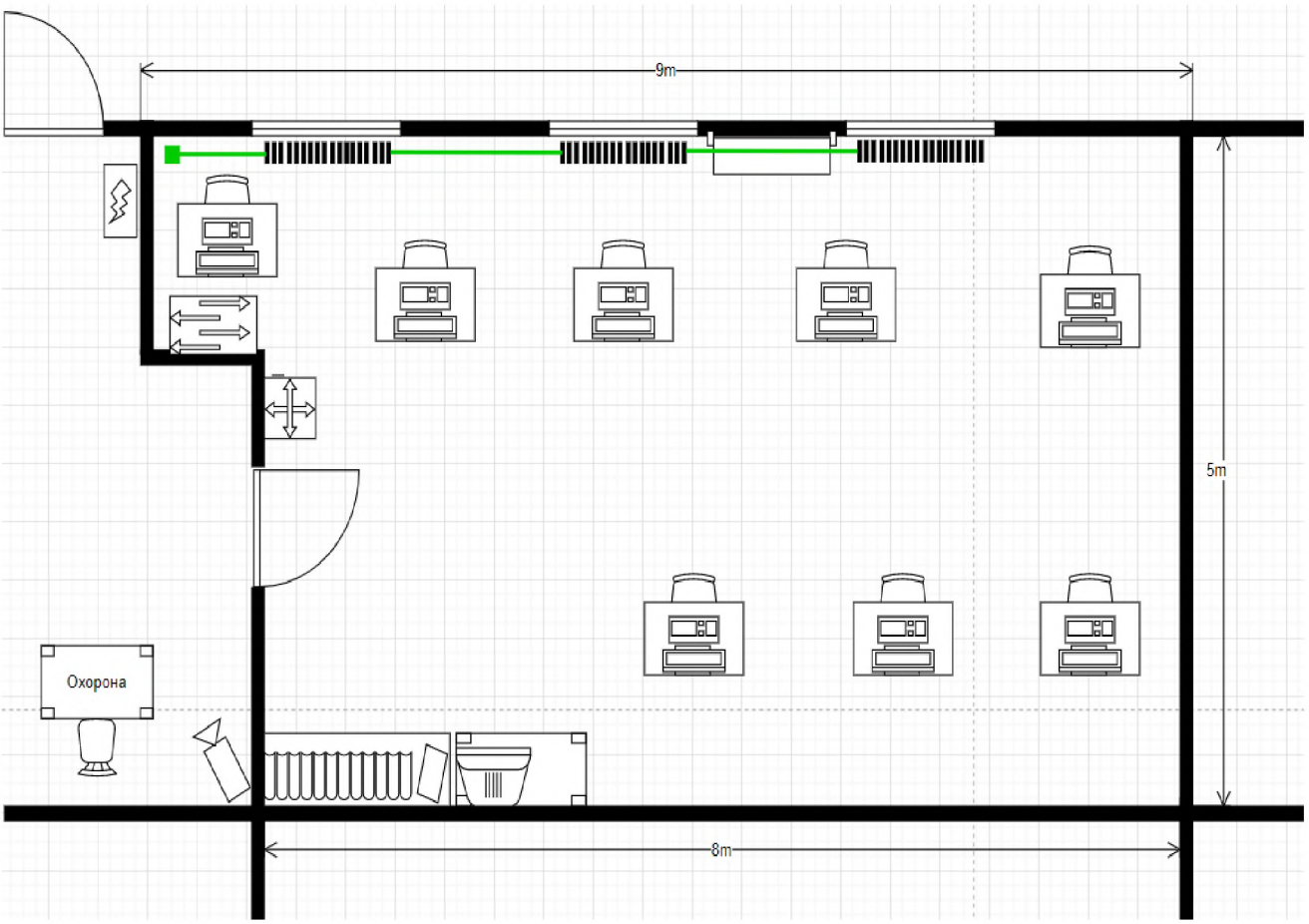


Рисунок 2.3 - Схема ліній систем електропостачання та комп’ютерної мережі



Умовні позначення:

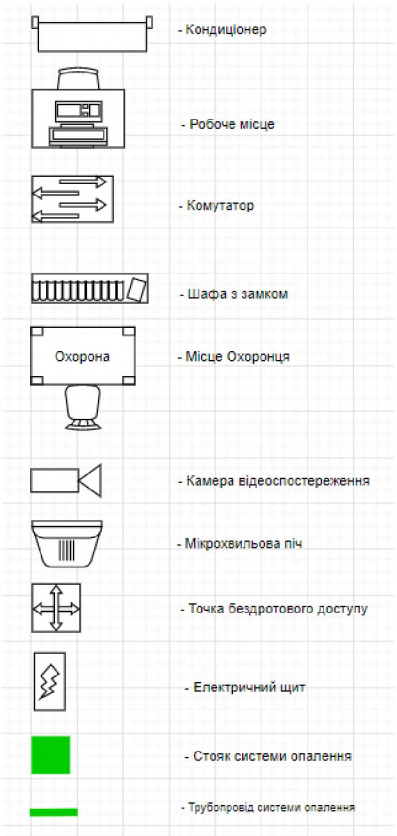


Рисунок 2.4 - Схема системи опалення приміщення

2.2.2 Обстеження обчислювальної системи

В мережі ОІД кожному комп'ютеру присвоєне унікальне ім'я, а в самій мережі передбачено дві ролі - адміністратори та користувачі. Одна особа має роль адміністратора, усі інші - користувачі.

Інформація, що містить комерційну таємницю, оброблюється на комп'ютерах перелічених в таблиці 2.2, за допомогою програмного забезпечення, що перелічене в таблиці 2.3. Для того, щоб запобігти несанкціонованому доступу до інформації, що зберігається і оброблюється на комп'ютерах, встановлені антивіруси, кожен обліковий запис захищений паролем.

Таблиця - 2.2 Перелік основних технічних засобів

Найменування	Специфікація	Ім'я в ІС	Серійний номер	Користувач
ПК	Монітор Philips 246E	PC1	UK01AK14039859	Team Lead
	Процесор Intel Core i5 6400 4 физ. ядра,		AK27E031041991	
	SAMSUNG DDR4 2666MHz 32 ГБ		S1104UA201EB510014002495	
	Материнська плата ASUS Prime B360M		MP2F2839210028	
	TOSHIBA 1ТБ HDD		1DAA471384	
ПК	Монітор Philips 246E	PC2	KD23OI11283251	Системний адміністратор
	Процесор Intel Core i5 6400 4 физ. ядра		DS81ES2863849	
	SAMSUNG DDR4 2666MHz 32 ГБ		K1902RF912DE311682894627	
	Материнська плата ASUS Prime B360M		FA92FF83112341	
	TOSHIBA 1ТБ HDD		1C2A343122	
ПК	Монітор Philips 246E	PC3	KA03EE0384727	Middle developer
	Процесор Intel Core i5 6400 4 физ. ядра		AF29KI25738011	

	SAMSUNG DDR4 2666MHz 32 ГБ		S1827SB371DS332720825891	
	Материнська плата ASUS Prime B360M		DS90FA9284782	
	TOSHIBA 1ТБ HDD		5F2C341075	

Продовження таблиці 2.2

ПК	Монітор Philips 246E	PC4	US12RD2132311	Middle developer
	Процесор Intel Core i5 6400 4 физ. ядра		AH04JR3323455	
	SAMSUNG DDR4 2666MHz 32 ГБ		E1D72TY130SS3242534701127	
	Материнська плата ASUS Prime B360M		AD87LK2176293	
	TOSHIBA 1ТБ HDD		9K1D348712	
ПК	Монітор Philips 246E	PC5	EK03LI18254029	Middle developer
	Процесор Intel Core i5 6400 4 физ. ядра		JD94SH99280184	
	SAMSUNG DDR4 2666MHz 32 ГБ		S4H39FR215YS212343916023	
	Материнська плата ASUS Prime B360M		GH27RD341241	
	TOSHIBA 1ТБ HDD		5C7F496352	
ПК	Монітор Philips 246E	PC6	FI82SD5498240	Бухгалтер
	Процесор Intel Core i5 6400 4 физ. ядра		AS26EF29634284	
	SAMSUNG DDR4 2666MHz 32 ГБ		S3F43GF301FT392017482512	
	Материнська плата ASUS Prime B360M		FH98KA260175	
	TOSHIBA 1ТБ HDD		7FD7204671	
ПК	Монітор SAMSUNG S24F350F	PC7	JF91FH730511	Junior developer

	Процесор Intel Core i3 8100 4 физ. ядра		UK76JF896301	
	SAMSUNG DDR4 2666MHz 32 ГБ		F3S10SH211SQ7255109 7012	
	Материнська плата ASROCK B365M Pro4-F		AK29FF02911	
	TOSHIBA 1ТБ HDD		1C8J920471	

Продовження таблиці 2.2

ПК	Монітор SAMSUNG S24F350F	PC8	UA72IF2340557	Junior developer
	Процесор Intel Core i3 8100 4 физ. ядра		HF28IF2053825	
	SAMSUNG DDR4 2666MHz 32 ГБ		Q1S81FG350DS3062953 2190	
	Материнська плата ASROCK B365M Pro4-F		SF20JG209173	
	TOSHIBA 1ТБ HDD		1F8F96193	
Принтер	CANON PIXMA TS704	PR	BF32453334562	Бухгалтер
Комутатор	TP-LINK TL-SG1024D	SW	SV0A2933212399	Системний адміністратор
Маршрутизатор	TP-LINK Archer C60	TP	LP28381D21232	Системний адміністратор

Таблиця - 2.3 Ідентифікація ПЗ

Найменування	Де встановлено	Термін дії ліцензії
Microsoft Windows 10 Pro	На всіх ПК	Безстрокова
Windows Defender		
Visual Studio Proffesional		
Google Chrome		
Microsoft Office		
SQL Server 2014 Management Studio		

2.2.3 Обстеження інформаційного середовища

На об’єкті інформаційної діяльності циркулює така інформація:

- інформація про клієнтів;
- бухгалтерські звіти;
- продукт діяльності компанії;
- інформація про діяльність компанії.

Інформація про клієнтів: дана інформація заповнюється на робочій станції PC6 за допомогою програмних продуктів: Microsoft Word, Microsoft Excel. Секретар може її друкувати.

Бухгалтерські звіти: ця інформація заповнюється на робочій станції PC6 за допомогою програмних продуктів: Microsoft Word, Microsoft Excel. Секретар може друкувати цю інформацію.

Продукт діяльності компанії: дана інформація оброблюється за допомогою Visual Studio Proffesional та SQL Server 2014 Management Studio. Тільки програмісти компанії мають доступ до цієї інформації у повному доступі і з усіма правами.

Інформація про діяльність компанії: дана інформація слугує для підтримки репутації компанії та приваблення нових клієнтів. Обробляється вона на робочій станції PC1.

На ОІД можна виділити такі інформаційні потоки (рисунок 2.5):

- обробка бухгалтерської документації;
- продукт діяльності компанії;
- інформація про клієнтів компанії;
- інформація про діяльність компанії;
- оновлення ПЗ.

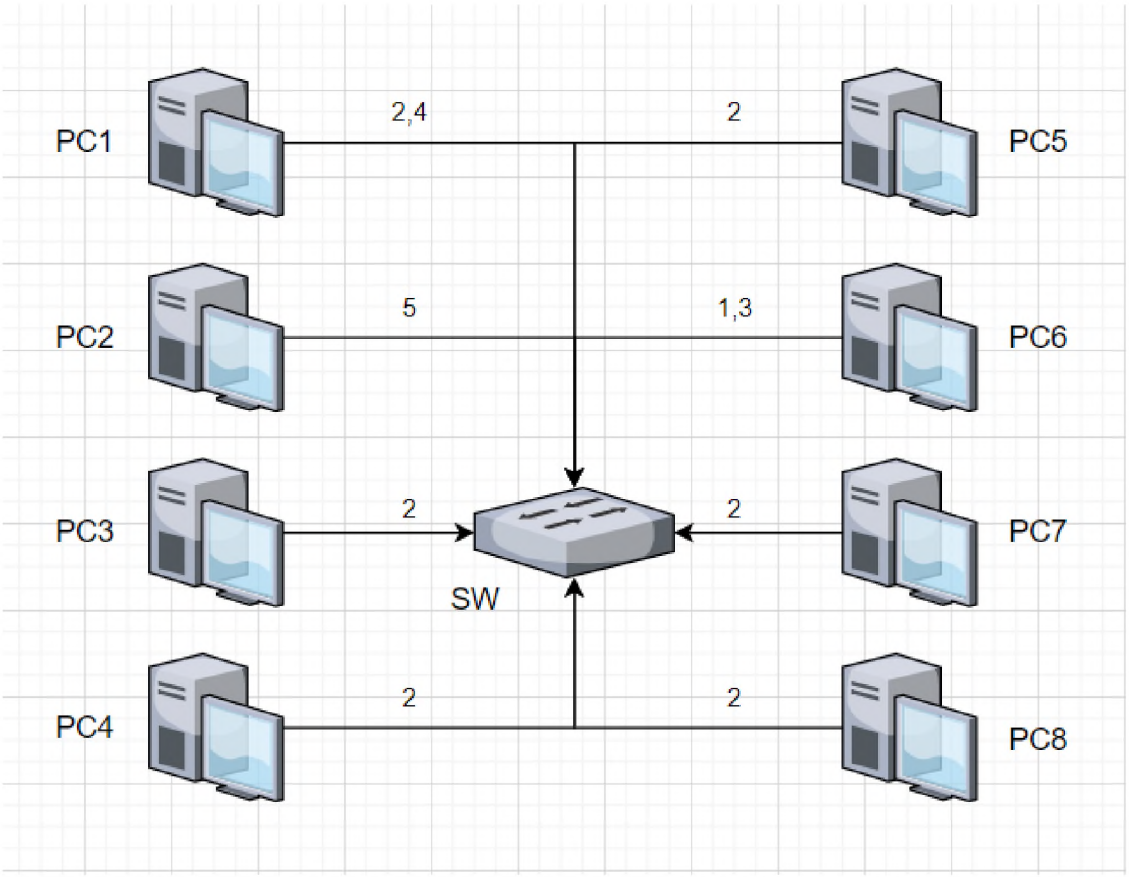


Рисунок 2.5 - Схема інформаційних потоків

Таблиця - 2.4 Середовище користувачів

Посада	Ім’я в ІТС	Роль в ІС	Рівень кваліфікації
Старший програміст (Team Lead)	PC1	Користувач	Високий
Сис. Адмін	PC2	Адміністратор	Середній
Програміст (Middle developer)	PC3	Користувач	Середній
Програміст (Middle developer)	PC4	Користувач	Середній
Програміст (Middle developer)	PC5	Користувач	Середній
Програміст (Junior developer)	PC7	Користувач	Середній
Програміст (Junior developer)	PC8	Користувач	Середній
Бухгалтер	PC6	Користувач	Середній

Таблиця - 2.5 Класифікація інформації, що обробляється в ІС

Вид інформації	Режим доступу	Рівень секретності [5]	Вид представлення в ІС	Підвищені вимоги (властивості)		
				К	Ц	Д
Бухгалтерські звіти	Обмежений доступ	Конфіденційна інформація	Паперовий, електронний	3	3	2
Інформація про діяльність компанії	Відкрита	–	Паперовий та електронний	1	3	3
Продукт діяльності компанії	Обмежений доступ	Комерційна таємниця	Електронний	4	4	3
Інформація про клієнтів	Обмежений доступ	Конфіденційна інформація	Електронний	4	3	3

Рівні конфіденційності:

К1 - рівень конфіденційності інформації, при якому можна знехтувати збитками у разі розкриття інформації особам, що не мають допуску до неї, або при якому інформація не є конфіденційною;

К2 - рівень конфіденційності інформації, при якому компанія зазнає незначних збитків у разі розкриття інформації особам, що не мають допуску до неї;

К3 - рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особами, що не мають допуску до неї;

К4 - рівень конфіденційності інформації, що може призвести до значних матеріальних втрат у разі розкриття інформації особам, що не мають допуску;

К5 - критичний рівень конфіденційності інформації, що може призвести до краху компанії у разі втрати конфіденційності інформації.

Рівні цілісності:

Ц1 - рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації;

Ц2 - рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;

Ц3 - рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;

Ц4 - рівень цілісності інформації, що може призвести до значних матеріальних втрат у разі втрати цілісності інформації;

Ц5 - критичний рівень цілісності інформації, що може призвести до краху компанії у разі втрати цілісності інформації.

Рівні доступності:

Д1 - рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;

Д2 - рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;

Д3 - рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;

Д4 - рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;

Д5 - критичний рівень доступності інформації, що може призвести до краху компанії у разі втрати доступності інформації.

Директор визначає вектор розвитку компанії та перевіряє якість виконаної роботи співробітниками. Права доступу директора описані в таблиці 2.6.

Програмісти є основною силою, завдяки якій компанія має прибутки, а також росте та розвивається. Вони займаються розробкою та підтримкою кінцевого продукту компанії і займають робочі станції PC1, PC3, PC4, PC5, PC7, PC8. Права доступу приведені в таблиці 2.6.

Бухгалтер складає звіти всіх витрат та прибутків підприємства. Здійснює контроль оплати праці усіх працівників компанії. Бухгалтер використовує робочу станцію PC6, всі права описані в таблиці 2.6.

Системний адміністратор відповідає за технічну складову компанії. Забезпечує роботу усієї техніки, комп'ютерної мережі та програмного забезпечення. До безпосередніх зобов'язань належать встановлення, оновлення та видалення ПЗ, необхідного для роботи підприємства. Системний адміністратор займає робочу станцію PC2, його права доступу приведені в таблиці 2.6.

Таблиця - 2.6 Права доступу

Посада	Доступ до інформації	Рівень доступу
Старший програміст (Team Lead)	Інформація про клієнтів	R
	Продукт діяльності компанії	R,W,M,D
	Інформація про діяльність компанії	R,M,W
Системний адміністратор	Інформація про діяльність компанії	R
	Оновлення ПЗ	R,M,W
Програміст (Middle developer)	Продукт діяльності компанії	R,W,M,D
	Інформація про діяльність компанії	R
Програміст (Junior developer)	Продукт діяльності компанії	R,W,M,D
	Інформація про діяльність компанії	R
Бухгалтер	Бухгалтерські звіти	R,W,M,P
	Інформація про клієнтів	
	Інформація про діяльність компанії	R
Директор	Інформація про діяльність компанії	R,D
	Інформація про клієнтів	R,W,M,D
	Бухгалтерські звіти	R,D
	Продукт діяльності компанії	R,D

Права доступу:

- R (Read) - читання;
- W (Write) - запис;
- M (Modification) - модифікація;
- D (Delete) - видалення;
- P (Print) - друк.

2.2.3 Модель порушника

Згідно НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», модель порушника (user violator model) - абстрактний формалізований або неформалізований опис порушника [6].

Модель порушника відображає його практичні та теоретичні можливості, апріорні знання, час і місце дії тощо. Порушники поділяються на дві основні групи: зовнішні та внутрішні (таблиця 2.7).

Слід зауважити, що всі злочини, зокрема і комп'ютерні, здійснюються людиною. Користувачі ІТС, з одного боку, є її складовою частиною, а з іншого - основною причиною і рушійною силою порушень і злочинів. Отже, питання безпеки ІТС фактично є питанням людських відносин та людської поведінки. Моделі порушників можна відобразити системою таблиць, для побудови якої використовуються усі можливі категорії, ознаки та характеристики порушників для більш точного їх аналізу, причому рівень загрози кожної з них оцінюється за 4-бальною шкалою [7].

Таблиця 2.7 - Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загроз
Внутрішні по відношенню до ІТС:		
ПВ1	Прибиральники	1
ПВ2	Сантехніки, електрики	1
ПВ3	Користувачі ІТС	2
ПВ4	Системний адміністратор	4
Зовнішні по відношенню до ІТС		
ПЗ1	Комунальні служби(енергопостачання, теплопостачання)	1
ПЗ2	Хакери	2
ПЗ3	Злочинці	2
ПЗ4	Агенти конкурентів	3

Усіх порушників можна класифікувати за такими ознаками:

- за рівнем кваліфікації та знань про ІТС (таблиця 2.9);
- за рівнем можливостей (таблиця 2.10);
- за часом дії (таблиця 2.11);
- за місцем дії (таблиця 2.12);
- за мотивами порушення (таблиця 2.8).

Таблиця 2.8 - Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М1	Помилка	1
М2	Корисливий інтерес	2
М3	Безвідповідальність	2

Таблиця 2.9 - Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К1	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К2	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К3	Низький рівень знань, вміння працювати з компонентами ІТС	1

Таблиця 2.10 - Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З1	Використання програмних засобів для модифікації або крадіжки інформації	4
З2	Підслуховування розмов, підглядання в монітор	1
З3	Злом облікових записів користувачів ІТС	3
З4	Крадіжка майна	2

Таблиця 2.11 - Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час повної бездіяльності	2
Ч2	Під час роботи компонентів ІТС	1
Ч3	Під час призупинення роботи компонентів ІТС з метою оновлення, вдосконалення	2

Таблиця 2.12 - Специфікація моделі порушника за місцем дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Д1	З робочих місць користувачів	2
Д2	В приміщенні ІТС	1
Д3	В будь-якому місці (знаючи паролі облікових записів)	3

На основі таблиць приведених вище побудовано загальну таблицю, модель внутрішніх і зовнішніх порушників (таблиця 2.13)

Таблиця 2.13 - Модель порушників

Посада	Категорія порушника	Мотив порушення	Можливості	Рівень обізнаності про ІТС	Час	Місце	Сума загроз
Прибиральники	ПВ1	М1	З2	К3	Ч2	Д2	6
	1	1	1	1	1	1	
Сантехніки, електрики	ПВ2	М1	32	К3	Ч1	Д2	7
	1	1	1	1	2	1	
Користувачі ІТС	ПВ3	М3	31	К1	Ч2	Д1	13
	2	2	4	2	1	2	
Системний адміністратор	ПВ4	М3	31	К2	Ч3	Д1	17
	4	2	4	3	2	2	
Хакери	ПЗ2	М2	33	К2	Ч2	Д3	14
	2	2	3	3	1	3	
Комунальні служби	ПЗ1	М1	34	К3	Ч1	Д2	7
	1	1	2	1	2	1	
Злочинці	ПЗ3	М2	34	К3	Ч1	Д2	9
	2	1	2	1	2	1	
Агенти конкурентів	ПЗ4	М2	З1	К2	Ч2	Д2	14
	3	2	4	3	1	1	

На основі аналізу результатів, наведених у таблиці 2.13, можна зробити висновки, що найбільшу небезпеку в ІТС представляє системний адміністратор, тому організація роботи цієї особи повинна бути найбільш контрольованою.

2.2.5 Модель загроз

Згідно НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», модель загроз (model of threats) — абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.

На підставі моделі порушника розробляється «Модель загроз для інформації в ІТС» (таблиця 2.14).

Модель загроз визначає:

- перелік можливих типів загроз, класифікований за результатом впливу на інформацію, тобто на порушення яких її властивостей вони спрямовані (конфіденційності, цілісності або доступності інформації);
- перелік можливих способів реалізації загроз певного типу (способів атак) відносно різних інформаційних об'єктів ІТС у різному стані класифікований, наприклад, за такими ознаками, як компонент обчислювальної системи ІТС або програмний засіб, уразливості яких експлуатуються порушником, причини виникнення відповідної уразливості тощо.

Загрози для інформації, що обробляється в ІТС, залежать від характеристик обчислювальної системи, апаратного складу, програмних засобів, фізичного середовища, персоналу, технологій обробки та інших чинників.

Таблиця 2.14 - Модель загроз для інформації в ІТС

Загрози	Вразливість	Порушення властивостей інформації	Рівень шкоди	Джерело
Вплив природних факторів				
Пожежа	Стихійне лихо	Ц, Д	Дуже Високий	Зовн.
Збої та відмови у роботі обладнання та тех. засобів АС, аварійне відключення живлення	Неідеальність техніки	Ц, Д	Середній	Зовн. Внутр.
Впливи природних завад(Грозові розряди, іскріння в електромережах і т.п.)	Природне явище	Ц, Д	Низький	Зовн.
Навмисні загрози				
Невиконання вимог до організаційних заходів захисту чинних в ІТС розпорядчих документів	Безвідповідальність персоналу ІТС	К, Ц, Д	Середній	Внутр.
Крадіжка технічного обладнання	Недостатня фізична захищеність приміщення	К, Ц,	Високий	Зовн.

Продовження таблиці 2.14

Перехоплення побічних сигналів	Відсутність КТЗІ на ОІД	К	Високий	Зовн.
Несанкціонована зміна повноважень працівників	Безвідповідальність персоналу ІТС	К	Середній	Внутр.
Промисловий шпіонаж	Недостатня перевірка кандидатів на посади в компанії	К, Ц	Високий	Зовн.
Несанкціоноване ознайомлення із документацією підприємства	Відсутність сейфа	К	Дуже високий	Зовн. Внутр.
Злом облікових записів	Використання хакерами недосконалостей ПЗ, яке використовується в ОІД, відсутність політики паролів	К, Ц, Д	Дуже високий	Зовн.
Випадкові загрози				
Пошкодження носіїв інформації або документації	Людський фактор	Ц, Д	Середній	Внутр.
Не збереження даних при роботі з ними	Відсутність забезпечення безперервного джерела живлення	Ц	Низький	Внутр.
Помилки програмного забезпечення	Недосконалість ПЗ	Ц, Д	Низький	Внутр.
Зараження системи вірусами	Використання неліцензованого ПЗ	К, Ц,	Дуже Високий	Зовн.
Помилка сис. адміністратора	Помилкові дії адміністратора(неправильне встановлення, налаштування або оновлення ПЗ або ОС)	К, Ц, Д	Високий	Внутр.
Неправомірне впровадження та використання заборонених політикою безпеки ПЗ	Відсутність контролюю встановлюваного ПЗ	К, Ц, Д	Середній	Внутр.

Найбільш актуальними загрозами для інформації в ІТС є:

- зараження системи вірусами;
- несанкціоноване ознайомлення із документацією підприємства;
- помилки системного адміністратора;
- злом облікових записів;
- крадіжка обладнання.

Якщо вищезгадані загрози будуть реалізовані, підприємство зазнає значних та небажаних збитків, тому вразливості, які можуть привести до реалізації цих загроз, рекомендується усунути в першу чергу.

2.3 Профіль захищеності

Згідно НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»:

Автоматизована система; АС (automated system) — організаційно-технічна система, що реалізує інформаційну технологію і об'єднує ОС, фізичне середовище, персонал і інформацію, яка обробляється.

Проаналізувавши основні характеристики ІТС підприємства «eUnify» відповідно до НД ТЗІ 2.5-004-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу», було встановлено що ІТС відповідає АС класу «3».

АС класу «3» - розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності. Істотна відміна від попереднього класу - необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки [8].

Обраний профіль захищеності:

3.КЦ.3 = { КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

КД-2. Базова довірча конфіденційність. Ця послуга надає можливість користувачу керувати потоками інформації від інших користувачів до захищеного

об’єкта, який належить його домену. Рівні цієї послуги ранжуються за повнотою захисту та вибірковістю керування. Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ має реалізовувати розмежування доступу на підставі атрибутів доступу захищеного об’єкта та користувача. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта або процесу, що належить його домену, визначити групу користувачів та/або конкретних користувачів, які мають право отримувати інформацію від захищеного об’єкта або процесу. Права доступу користувача повинні встановлюватись при його створенні [9].

КА-2. Базова адміністративна конфіденційність. Ця послуга дозволяє адміністратору керувати потоками інформації від захищених об’єктів до користувачів, і визначає множину об’єктів до яких вона відноситься. Рівні послуги ранжуються повнотою захисту та вибірковістю користувачів. Розмежування доступу здійснюється на підставі атрибутів доступу захищеного об’єкта і користувача. КЗЗ має надавати можливість адміністратору визначати користувачів та/або групи користувачів, які мають право одержувати інформацію від захищеного об’єкта або ініціювати процес.

КО-1. Повторне використання об’єктів. Ця послуга є реалізованою, якщо перед наданням користувачу або процесу в розділювальному об’єкті не залишається попередньої інформації та скасовуються попередні права доступу до об’єкта. Критерії не встановлюють, коли має бути виконане очищення об’єкта, тому можна виконувати його очистку як після звільнення об’єкта, так і перед його наступним використанням. Послуга повторне використання об’єктів дозволяє забезпечити захист від атак типу «збирання сміття».

КВ-2. Базова конфіденційність при обміні. Ця послуга забезпечує захист об’єктів від несанкціонованого ознайомлення з інформацією, яка в них зберігається, під час імпорту чи експорту їх незахищеними каналами. Рівні послуги ранжуються повнотою захисту та вибірковістю користувачів. Реалізація базової конфіденційності при обміні дає можливість керувати засобами імпорту

та експорту і забезпечує захист від помилок користувача, а також від витоку інформації при підключенні несанкціонованих користувачів.

ЦД-1. Мінімальна цілісність при обміні. Ця послуга надає можливість користувачу керувати потоками інформації від інших користувачів до захищеного об'єкта, який належить його домену. Рівні цієї послуги ранжуються за повнотою захисту та вибірковістю керування. На рівні мінімальної довірчої цілісності користувач домену, якому належить об'єкт, може обмежувати доступ до цього об'єкта з боку інших користувачів. Для такої системи можна побудувати часткову матрицю доступу користувачів до об'єктів.

ЦА-2. Базова адміністративна цілісність. Ця послуга дозволяє адміністратору керувати потоками інформації від захищених об'єктів до користувачів, і визначає множину об'єктів до яких вона відноситься. Рівні послуги ранжуються повнотою захисту та вибірковістю користувачів. Згідно з політикою адміністративної цілісності розмежування доступу здійснюється на підставі атрибутів доступу захищеного об'єкта і користувача. КЗЗ має надавати можливість адміністратору визначати користувачів та/або групи користувачів, які мають право одержувати інформацію від захищеного об'єкта або ініціювати процес.

ЦО-1. Обмежений відкат. Ця послуга дає можливість відмінити операцію або послідовність операцій і повернути об'єкт до його попереднього стану. Рівні цієї послуги ранжуються на підставі множини операцій, для яких передбачений відкат. Відкат повинен бути автоматизованою, завжди доступною функцією системи. Якщо в системі реалізована послуга відкату, то всі її використання повинні бути зафіксовані в журналі. Відміна операції не повинна приводити до видалення інформації про цю операцію в журналі.

ЦВ-2. Базова цілісність при обміні. Ця послуга забезпечує захист об'єктів від несанкціонованої модифікації інформацією, яка в них зберігається, під час імпорту чи експорту їх незахищеними каналами. Рівні послуги ранжуються повнотою захисту та вибірковістю користувачів. Базова цілісність при обміні дозволяє керувати засобами імпорту та експорту і

забезпечує захист від помилок користувача, а також від модифікації інформації при підключенні несанкціонованих користувачів.

НР-2. Захищений журнал. Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні цієї послуги ранжуються залежно від повноти та вибірковості контролю, складності аналізу даних із журналу реєстрації і можливості виявлення потенційних порушень. Журнал реєстрації має містити інформацію про місце, дату та час, тип і успішність чи неуспішність зареєстрованої події. Журнал реєстрації повинен містити інформацію для встановлення користувача, процесу та/або об'єкта, що мали відношення до кожної зареєстрованої події. КЗЗ має здійснювати реєстрацію подій, які мають безпосереднє відношення до безпеки. КЗЗ повинен забезпечити захист журналу реєстрації від несанкціонованого доступу або модифікації.

НИ-2. Одиночна ідентифікація і автентифікація. Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, який намагається отримати доступ до КС. Рівні даної послуги ранжуються в залежності від кількості задіяних механізмів автентифікації. Кожний користувач повинен бути однозначно ідентифікований в КЗЗ та мати атрибути якими він характеризується. Перш ніж користувачу буде дозволено виконувати дії, що контролюються КЗЗ, КЗЗ повинен автентифікувати користувача з використанням захищеного механізму. КЗЗ повинен забезпечити захист цілісності і конфіденційності даних автентифікації.

НК-1. Однонаправлений достовірний канал. Дана послуга дає гарантію, що безпосередньо користувач взаємодіє із КЗЗ і ніякі інші користувачі чи процеси не можуть втручатись. Рівні даної послуги ранжуються в залежності від надання можливості користувача або КЗЗ ініціювати захищений обмін. Політика достовірного каналу має визначати механізми, якими буде встановлено достовірний канал. Достовірний канал повинен бути використаний для ідентифікації і автентифікації користувача. Зв'язок з використанням даного каналу повинен ініціювати тільки користувач.

НО-2. Розподіл обов’язків адміністраторів. Дана послуга дозволяє зменшити збитки від помилкових або навмисних дій користувачів і обмежити авторитарність керування. Рівні даної послуги ранжуються на підставі вибірковості керування можливостями адміністраторів та користувачів.

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі звичайного користувача і адміністратора з притаманними їм функціями.

Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані до необхідних для виконання даної ролі.

НЦ-2. КЗЗ з гарантованою цілісністю. Дана послуга визначає, наскільки КЗЗ здатний захищати себе і гарантувати спроможність керувати захищеними об’єктами. Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що реалізовуються для реалізації розподілення доменів. КЗЗ повинен підтримувати власний домен задля захисту від зовнішніх впливів та несанкціонованої модифікації або втрати контролю. Мають бути описані обмеження, при дотримані яких буде гарантовано, що послуги безпеки доступні тільки через інтерфейс КЗЗ та всі запити на доступ до захищених об'єктів контролюються КЗЗ.

НТ-2. Самотестування при старті. Дана функція дозволяє перевірити КЗЗ і після цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжуються за можливістю виконання тестів у процесі запуску або штатної роботи. Політика самотестування повинна описувати властивості КС і реалізовані процедури, що можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ повинен бути здатен виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження при ініціалізації КЗЗ.

НВ-1. Автентифікація вузла. Дана послуга дозволяє КЗЗ ідентифікувати одне одного перш ніж почати взаємодію. Політика ідентифікації і автентифікація

при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ. КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ з використанням захищеного механізму. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

2.4 Вибір методів та засобів захисту інформації

При виборі методів та засобів захисту інформації в ІТС необхідно спиратись на актуальність вибраних методів чи засобів захисту, економічну доцільність, відповідність вразливостям, які присутні в ІТС, п. 17 Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27 вересня 1999 р. № 1229. «Перелік, призначений для використання суб'єктами системи технічного захисту інформації під час розроблення, модернізації та впровадження комплексів ТЗІ на об’єктах інформаційної діяльності та комплексних систем захисту інформації в автоматизованих системах».

За результатами аналізу загроз та вразливостей, приведених в таблиці 2.14, обрано методи та засоби, які необхідно впровадити в ІТС для збільшення рівня її інформаційної захищеності.

2.4.1 Антивірусний захист

ІТС потребує якісної системи антивірусного захисту в зв’язку з тим що реалізація загрози зараження системи вірусами може привести до порушення цілісності та конфіденційності інформації в ІТС та завдасть дуже високих збитків підприємству.

Політика впровадження антивірусного комплексу:

- антивірусне ПЗ повинне бути встановлене на всі робочі станції в ІТС;
- для антивірусного ПЗ повинен бути увімкнутий автозапуск при старті ОС;
- антивірусне ПЗ має своєчасно обновлюватись;

- ліцензія на використання антивірусного ПЗ має бути своєчасно продовжена;
- перед початком роботи користувач повинен переконатись, що антивірусне ПЗ увімкнено.

Проаналізувавши характеристики та властивості антивірусних ПЗ з переліку, який формує та ліцензує Держспецзв'язку, було обрано програмний комплекс антивірусного захисту «Avast Business Antivirus» версії 19.1.2360.0 виробництва компанії AVAST Software s.r.o. (Чеська республіка), виробництва ТОВ «Ідеалсофт», м. Київ, вул. Дегтярівська, буд. 53А. Програмний комплекс відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі «Програмний комплекс антивірусного захисту «Avast Business Antivirus» версії 19». Технічні вимоги щодо захисту інформації від несанкціонованого доступу, сукупність яких визначається функціональним профілем захищеності - {КА-2, ЦА-1, ЦО-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2}. Експертний висновок №936, дійсний з 27.03.2019 до 27.03.2022.

2.4.2 Політика паролів

Політика паролів - це набір правил, спрямованих на підвищення безпеки КС шляхом заохочення користувачів до використання надійних паролів і їх правильного використання.

Через те, що в ІТС існує загроза злому облікових записів, є необхідність впровадження політики паролів для всіх користувачів. Це може запобігти витоку інформації через злом облікових записів користувачів.

Вимоги до паролів користувачів:

- використання букв верхнього та нижнього регістру;
- включення однієї або декількох цифр;
- включення спеціальних символів, таких як @, #, $…;
- заборона слів, знайдених в чорному списку паролів;
- заборона слів, що містяться в особистій інформації користувача;

- заборона на використання назви компанії або абревіатури;
- заборона паролів, які збігаються з форматом дати, номерами машин, телефонними номерами, або іншими поширеними значеннями.

Політика паролів зобов'язує користувачів змінювати паролі кожні 180 днів. Заборонено використовувати попередні паролі, записувати паролі в текстових документах або на папері.

2.4.3 Курси підвищення кваліфікації адміністраторів

Через те, що існує загроза завдання шкоди ІТС через помилки адміністраторів, є необхідність підвищувати кваліфікацію адміністраторів. Курси підвищення кваліфікації допоможуть адміністратору детальніше розібратися в сфері адміністрування ІТС, отримати нові знання про забезпечення безпеки інформації в ІТС.

Для підвищення рівня обізнаності адміністраторів рекомендовано курси в Cisco Networking Academy.

2.4.4 Підвищення фізичної захищеності ОІД

У зв'язку з тим, що приміщення ОІД знаходиться на 1 поверсі, потенційні злочинці можуть проникнути на об'єкт через вікна. Для ліквідації цієї вразливості необхідно встановити металеві решітки на вікна, датчики розбиття скла та магнітоконтактні датчики на відкриття вікон.

Необхідно обрати датчик розбиття скла з технологією фазо-частотної селективності одержуваних сигналів. Це означає, що для спрацьовування датчика на звук розбитого скла сенсор повинен отримати два послідовних сигнали: спочатку - низькочастотний звук удару, після цього - безпосередньо звук розбитого скла. Дана логіка роботи сенсора дозволяє звести до мінімуму ймовірність помилкового спрацьовування датчика від звуків, близьких по частоті до дзвону скла. Відповідно до цього критерія було обрано датчик розбиття скла CROW GBD-2.

Через те, що рами вікон в приміщенні ОІД виготовлені з пластику необхідно обрати магнітоконтактний датчик розроблений спеціально для пластикових поверхонь. Через це обрано магнітоконтактний датчик СМК-1Э

Вхідні дерев'яні двері до приміщення ОІД необхідно замінити на двері DEVI-U із сертифікатом RC-3 (зломостійкості 3 класу).

2.5 Висновок

Провівши детальне обстеження інформаційно-телекомунікаційної системи компанії «eUnify», яке включало в себе: обстеження фізичного середовища ОІД, створення плану місцевості та генерального плану ОІД, обстеження інформаційного середовища ОІД, обстеження обчислювальної техніки на ОІД, створення моделі порушника, створення моделі загроз - було виявлено найактуальніші загрози для інформації яка циркулює на об'єкті інформаційної діяльності. При реалізації виявлених загроз підприємство може понести значні фінансові збитки через простій системи, втрату дорогого обладнання або через витік конфіденційної інформації, що завдасть удару по репутації підприємства. Враховуючи вразливості ІТС були запропоновані відповідні методи та засоби захисту інформації.

Очевидно що для підвищення рівня захищеності інформації необхідні фінансові ресурси. Тому у наступному розділі буде розраховано витрати на впровадження обраних методів і засобів захисту та на їх підтримку.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою даного розділу є техніко-економічне обґрунтування доцільності запровадження проектних рішень для підвищення інформаційної безпеки підприємства «eUnify».

3.1 Визначення витрат на впровадження нововведень

3.1.1 Визначення трудомісткості розробки та розрахунок витрат на створення вимог з інформаційної безпеки

Трудомісткість створення вимог з інформаційної безпеки визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації за умови роботи одного робітника:

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ годин} \quad (3.1)$$

де, $t_{тз}$ - тривалість складання технічного завдання на розробку проекту для підвищення рівня захищеності ІТС;

$t_{в}$ - тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ - тривалість процесу аналізу ризиків;

$t_{вз}$ - тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ - тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$ - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_{д}$ - тривалість документального оформлення проекту для підвищення рівня захищеності ІТС [11].

Згідно з формулою 3.1:

$t = 16 + 24 + 16 + 16 + 16 + 8 + 8 = 104$ години.

3.1.2 Розрахунок витрат на створення проекту для підвищення рівня захищеності інформації в ІТС підприємства «eUnify»

Витрати на створення вимог з інформаційної безпеки $К_{рв}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для опрацювання програми на персональному комп'ютері $З_{мч}$:

$$К_{рп} = З_{зп} + З_{мч}, \text{ грн.} \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{зп} = t \cdot З_{іб}, \text{ грн.}, \quad (3.3)$$

де, t – загальна тривалість створення вимог з інформаційної безпеки;

$З_{іб}$ – середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину. Відповідно до ресурсу Work.ua вона складає 50,42 грн. [10].

Згідно з формулою 3.3:

$З_{зп} = 104 \cdot 50,42 = 5243,68$ (грн).

Вартість машинного часу для розробки вимог на персональному комп'ютері визначається за формулою:

$$З_{мч} = t \cdot С_{мч}, \text{ грн.}, \quad (3.4)$$

де, t – трудомісткість розробки вимог з інформаційної безпеки на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу персональному комп'ютері, грн./година. Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = Р \cdot t_{нал} \cdot C_e + \frac{Н_а \cdot Ф_{зла}}{F_p} + \frac{К_{лпз} \cdot Н_{апз}}{F_p}, \text{ грн.,} \quad (3.5)$$

де, Р – встановлена потужність ПК, кВт;

$С_е$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$– залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40 – годинного робочого тижня $F_р$ = 1920).

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

$$Н_а = 1 - \sqrt[Т]{\frac{ЛВ}{ПВ}}, \text{ частки одиниці,} \quad (3.6)$$

де, ЛВ – ліквідаційна вартість;

ПВ – первісна вартість;

Т – строк експлуатації.

Згідно з формулою 3.6:

$$Н_а = 1 - \sqrt[5]{\frac{5000}{16000}} = 0{,}2,$$

$$Н_{апз} = 1 - \sqrt[3]{\frac{15000}{48060}} = 0{,}32.$$

Згідно з формулою 3.5:

$$С_{мч} = 0{,}3 \cdot 1 \cdot 1{,}68 + \frac{12000 \cdot 0{,}2}{1920} + \frac{48060 \cdot 0{,}32}{1920} = 9{,}76 \text{ грн,}$$

Згідно з формулою 3.4:

$З_{мч} = 104 \cdot 9{,}76 = 1015{,}04$ грн,

Згідно з формулою 3.4:

$К_{рп}$ = 5243,68 + 1015,04 = 6258,72 грн.

Визначена таким чином вартість розробки проекту для підвищення рівня захищеності ІТС $К_{рп}$ є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи інформаційної безпеки. Таким чином, капітальні (фіксовані) витрати на проектування та впровадження методів та засобів захисту інформації складають:

$$К = К_{рп} + К_{зпз} + К_{о} + К_{навч} + К_{н}, \text{ грн.}, \quad (3.7)$$

де, $К_{пр}$ – вартість розробки проекту інформаційної безпеки, грн;

$К_{зпз}$ – вартість закупівлі ліцензійного основного й додаткового програмного забезпечення, грн (Avast Business Antivirus – 1846,68);

$К_{о}$ – витрати на обладнання та інші матеріали(двері DEVI-U – 15800 грн., Магнітоконтактний датчик 3шт. СМК-1Э - 126 грн., Датчик розбиття скла CROW GBD-2 – 413 грн.);

$К_{навч}$ – витрати на підвищення кваліфікації системного адміністратора (курси у центрі підготовки ІТ спеціалістів actpro – 15000 грн.);

$К_{н}$ – витрати на встановлення та налагодження обладнання.

Згідно з формулою 3.7:

К = 6258,71 + 1846,68 + (15800 + 126 + 413) + 15000 + 2400 = 41844,40 грн.

3.2 Розрахунок експлуатаційних витрат

Експлуатаційні витрати - це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період, що виражені у грошовій формі.

За методикою Gartner Group до поточних (експлуатаційних) відносяться наступні витрати:

- вартість Upgrade-відновлення й модернізації системи ($С_{в}$);

- витрати на керування системою в цілому ($С_к$);
- витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$ - "активність користувача").

Річні експлуатаційні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \text{ грн.}, \quad (3.8)$$

Витрати на технічну підтримку та відновлення ($С_в$) розраховуються:

$С_в = К \cdot 0,21 = 41844,40 \cdot 0,21 = 8787,32$ грн.

Витрати викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) можна визначити за формулою:

$С_{ак} = К \cdot 0,46 = 41844,40 \cdot 0,46 = 19248,42$ грн.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_{тос}, \text{ грн.} \quad (3.9)$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів ($С_н$) - 15000 грн..

Річний фонд амортизаційних відрахувань ($С_а$):

$$С_а = \frac{15800}{5} + \frac{1846,68}{3} = 3775 \text{ грн.}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$С_з = З_{осн} + З_{дод} = (12\ 100 + 1000) \cdot 12 = 157200$ грн.

де, $З_{осн}$, $З_{дод}$ - основна і додаткова заробітна плата відповідно, грн на рік. Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$С_{ел} = 0,3 \cdot 1920 \cdot 1,68 = 967,68$ грн.

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$), визначаються у відсотках від вартості капітальних витрат (1-3%):

$С_{тос} = К \cdot 0,02 = 41844,40 \cdot 0,02 = 836,89$ грн.

Згідно з формулою 3.9:

$С_к = 15000 + 10461,10 + 157200 + 967,68 + 836,89 = 184465,67$ грн.

Отже розрахувавши всі складові річних експлуатаційних витрат на функціонування системи інформаційної безпеки, використовується формула 3.8:

С = 184 465,67 + 8787,32 + 19248,42 = 212501,41 грн.

3.3 Оцінка величини збитку

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (КСІБ):

- порушення конфіденційності ресурсів КСІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);
- порушення доступності ресурсів КСІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);
- порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);
- порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

Можна виділити й деякі універсальні форми нанесення збитку, наприклад, порушення конфіденційності, доступності, цілісності або автентичності ресурсу можна характеризувати як компрометацію ресурсу, тобто втрату довіри до нього користувачів (це може мати прямий збиток, зв'язаний, наприклад, з переустановленням програмного забезпечення або проведенням розслідування). Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки - 8 годин;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу - 7 годин;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі - 24 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.) - 15000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі - 22285 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.) - 1 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі - 7 осіб;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі – 17500000 грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин - 10000 грн;

I – число атакованих сегментів корпоративної мережі - 1;

N – середнє число атак на рік 1.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V \text{ , грн.,} \qquad (3.10)$$

де, $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн.;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн.;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн..

Оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі розраховуються:

$$П_п = \frac{\sum З_с}{F} \cdot t_п \text{ , грн.,} \quad (3.11)$$

де, F – місячний фонд робочого часу (176 год.)

Згідно з формулою 3.11:

$$П_п = \frac{22285 \cdot 7}{176} \cdot 8 = 7090{,}68 \text{ грн.}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч} \text{ , грн.,} \quad (3.12)$$

де, $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн.;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн..

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с}{F} \cdot t_{ви} \text{ , грн.} \quad (3.13)$$

Згідно з формулою 3.13:

$$П_{ви} = \frac{22285 \cdot 7}{176} \cdot 24 = 21272{,}04 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_о}{F} \cdot t_в \text{ , грн.} \quad (3.14)$$

Згідно з формулою 3.14:

$$П_{пв} = \frac{15000 \cdot 1}{176} \cdot 8 = 681{,}82 \text{ грн.}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі дорівнюють:

$П_в$ = 21272,04 + 681,82 + 10000 = 31 953,86 грн.

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із сердньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{F_г} \cdot (t_п + t_в + t_{ви}) \text{ , грн.} \quad (3.15)$$

Згідно з формулою 3.15:

$$V = \frac{17500000}{2080} \cdot (8 + 7 + 24) = 328125 \text{ грн.}$$

Згідно з формулою 3.10 упущена вигода від простою атакованого сегмента корпоративної мережі дорівнює:

U = 7090,68 + 31 953,86 + 328125 = 367169,54 грн.

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \sum i \cdot \sum n \cdot U \text{ , грн.} \quad (3.16)$$

Згідно з формулою 3.16:

В = 1 · 1 · 367169,54 грн.

3.4 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C, \text{ грн.}, \quad (3.17)$$

де, В – загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн.;

R – очікувана ймовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

С – щорічні витрати на експлуатацію системи інформаційної безпеки, грн.

Згідно з формулою 3.17:

Е = 367169,54 · 0,7 - 212501,41 = 44517,27 грн.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки. Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K}, \text{ частки одиниці.} \quad (3.18)$$

Згідно з формулою 3.18:

$$ROSI = \frac{44517,27}{41844,40} = 1,06.$$

Термін окупності капітальних інвестицій Т. показує, за скільки років загального ефекту від капітальні інвестиції окупляться за рахунок впровадження системи інформаційної безпеки і розраховується за формулою:

$$T = \frac{1}{ROSI}, \text{ грн.} \quad (3.19)$$

Згідно з формулою 3.19:

$$T = \frac{1}{1{,}06} = 0{,}94 \text{ роки.}$$

3.5 Висновок

На підставі розрахунків, проведених в економічній частині встановлено, що капітальні затрати на покращення захищеності інформаційно-телекомунікаційної системи складають приблизно 41844,40 грн, а ефект від впровадження системи інформаційної безпеки – близько 44517,27 грн. Розрахунок цих двох параметрів дав змогу знайти коефіцієнт повернення інвестицій (ROSI), який становить 1,06 і термін окупності капітальних інвестицій, який складає приблизно рік.

Отже, запровадження запропонованих методів та засобів захисту інформації є економічно доцільними.

ВИСНОВКИ

Інформаційний захист підприємств – це складний процес, але він є обов'язковою складовою успішного бізнесу. З настанням епохи Інтернету кожне підприємство піддається процесу діджиталізації та використовує в своїй роботі новітні технології. Сьогодні компаніям складніше, ніж коли-небудь чітко визначити критичні точки та вразливості у власній багатогранній інфраструктурі, це також зумовлено ростом і розвитком «темної сторони інтернету», де зловмисники почувають себе у безпеці та можуть вільно ділитись своїми ідеями та розробками шкідливого ПЗ.

Цілями зловмисників стають абсолютно різні за розмірами та сферами діяльності підприємства. Нажаль сучасний світ повен різних загроз для компаній, але заходи по їх запобіганню повинні обумовлюватись рівнем ризиків. Це необхідно для того щоб сконцентруватись на найбільш актуальних загрозах для конкретного підприємства та не витрачати час і гроші на усунення загроз які малоймовірні або не є актуальними.

Впровадження на підприємстві комплексної системи захисту інформації допоможе зекономити кошти шляхом усунення вразливостей та зменшення наслідків після реалізації тієї чи іншої загрози. Але це не одноразовий захід. КСЗІ потребує супроводження при експлуатації та постійної модернізації, для того щоб ефективно протистояти сучасним загрозам зовнішнього світу.

На прикладі компанії «eUnify» та її інформаційно-телекомунікаційної системи було проведено аналіз рівня інформаційної безпеки, запропоновано методи та заходи для підвищення рівня захищеності інформації та надано оцінку економічній доцільності їх запровадження [12].

ПЕРЕЛІК ПОСИЛАНЬ

1. Статистичні дані компанії Positive Technologies про стан кібербезпеки за 2020 рік URL: https://www.ptsecurity.com.

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

3. Комплексні системи захисту інформації: проектування, впровадження, супровід.: Гребенніков В.В. Збірник Лекцій – Ужгород 2013.

4. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999.

5. Закон України «Про інформацію» URL:https://zakon.rada.gov.ua/laws/show/2657-12#Text.

6. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999.

7. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999.

8. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999.

9. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999.

10. Work.ua. Ресурс для визначення середньої заробітної URL: www.work.ua.

11. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: Д. П. Пілова. Дніпро: Дніпро: НТУ «ДП» 2019.

12. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофеєв, О.В. Кручінін, Ю.А. Мілінчук -Дніпро: НТУ «ДП», 2020.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	5	
6	А4	Спеціальна частина	30	
7	А4	Економічний розділ	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1) Пояснювальна_записка_Калюжний.docx
2) Пояснювальна_записка_Калюжний.pdf
3) Презентація_Калюжний.pptx

ДОДАТОК В. Відгук керівника кваліфікаційної роботи

ДОДАТОК Г. Відгук керівника економічної частини

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)