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

студентки *Білової Юлії Олексіївни*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи Дніпровського офісу ТОВ «Oxgaming»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	професор Кагадій Т.С.			
розділів:				
спеціальний	ст.викл. Кручінін О.В.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент	Дятченко О.В.			

Нормоконтролер	ст.викл. Тимофєєв Д.С.			

Дніпро
2021

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
д.т.н., проф. Корнієнко В.І.
« » 2021 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студентці ***Біловій Юлії Олексіївні*** **академічної групи** ***125-17-2***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***
спеціалізації[1]
за освітньо-професійною програмою ***Кібербезпека***

на тему ***Комплексна система захисту інформації інформаційно-телекомунікаційної системи Дніпровського офісу ТОВ «Oxgaming»***

Затверджую наказом ректора НТУ «Дніпровська політехніка» від *07.06.2021р.* №*317-С*

Розділ	Зміст	Термін виконання
Розділ 1	*Стан питання. Постановка задачі. Обстеження ІТС та аналіз стану захищеності інформаційно-телекомунікаційної системи приватного підприємства ТОВ «Oxgaming».*	19.04.2021-30.04.2021
Розділ 2	*Розробка комплексної системи захисту інформації.*	03.05.2021-21.05.2021
Розділ 3	*Техніко-економічне обґрунтування доцільності запровадження запропонованих в роботі рішень.*	24.05.2021-09.06.2021

Завдання видано _____ *Кагадій Т.С.*
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: *11.01.2021р.*

Дата подання до екзаменаційної комісії: *10.06.2021р.*

Прийнято до виконання _____ *Білова Ю.О.*
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 86 ст., 6 рис., 13 табл., 6 додатків, 12 джерел.

Об'єкт розробки: комплексна система захисту інформації інформаційно-телекомунікаційної системи Дніпровського офісу ТОВ «Oxgaming».

Мета: забезпечення необхідного рівня захищеності інформації інформаційно-телекомунікаційної системи Дніпровського офісу ТОВ «Oxgaming».

У першому розділі кваліфікаційної роботи описуються загальні відомості про підприємство, підстави для створення КСЗІ, нормативно-правову базу, види інформації та доступ до неї. Також наявна інформація про виконані обстеження інформаційної системи, фізичного середовища, середовища користувачів. Надаються дані про виявлені загрози та вразливості, сформована модель порушника..

У другому розділ представлений профіль захищеності, проектні рішення щодо забезпечення інформаційної безпеки, а також розроблені положення щодо захисту інформації на підприємстві.

Третій розділ – економічна частина, у якій були зроблені розрахунки фінансових витрат на запровадження комплексної системи захисту інформації, а також, щорічну підтримку. На підставі представлених розрахунків було доведено економічну доцільність введення в експлуатацію комплексної системи захисту інформації, що була розроблена у другій частині.

Практичне значення проекту полягає у забезпеченні необхідного рівня інформаційної безпеки приватного підприємства ТОВ «Oxgaming».

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ВРАЗЛИВОСТІ, ПРОФІЛЬ ЗАХИЩЕНОСТІ, НОРМАТИВНО-ПРАВОВА БАЗА.

РЕФЕРАТ

Пояснительная записка: 86 ст., 6 рис., 13 табл., 6 приложений, 12 источников.

Объект разработки: комплексная система защиты информации информационно-телекоммуникационной системы Днепровского офиса ООО «Oxgaming».

Цель: обеспечение необходимого уровня защищенности информации инф.-телекоммуникационной системы Днепровского офиса ООО «Oxgaming».

В первом разделе квалификационной работы описываются общие сведения о предприятии, основаниях для создания КСЗІ, нормативно-правовой базе, видах информации и доступе к ней. Также имеющаяся информация о выполненных обследованиях информационной системы, физической среды, среды пользователей. Предоставляются данные о выявленных угрозах и уязвимости, сформированная модель нарушителя.

Во втором раздел представленный профиль защищенности, проектные решения относительно обеспечения информационной безопасности, а также разработанные положения относительно защиты информации на предприятии.

Третий раздел - экономическая часть, в которой были сделанные расчеты финансовых расходов на ввод комплексной системы защиты информации, а также, ежегодную поддержку. На основании представленных расчетов была доказана экономическая целесообразность введения в эксплуатацию комплексной системы защиты информации, которая была разработана во второй части.

Практическое значение проекта заключается в обеспечении необходимого уровня информационной безопасности прчастного предприятия ООО «Oxgaming».

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УЯЗВИМОСТИ, ПРОФИЛЬ ЗАЩИЩЕННОСТИ, НОРМАТИВНО-ПРАВОВАЯ БАЗА.

ABSTRACT

Explanatory note: 86 p., 6 fig., 13 tables, 6 applications, 12 sources.

Object of development: integrated information protection system of information-telecommunication system of "Oxgaming" LLC.

Objective: to ensure the necessary level of information security of information and telecommunications system of the Dnipro office of "Oxgaming" LLC.

The first section of the qualification work describes the general information about the company, the basis for the creation of the CPPI, regulatory framework, types of information and access to it. Also available information about the performed examinations of the information system, the physical environment, the environment of users. The data on the identified threats and vulnerabilities are provided, as well as a model of an intruder.

The second section presents a security profile, design solutions for information security, and developed provisions for the protection of information in the enterprise.

The third section - the economic part, in which calculations were made of the financial costs for the introduction of an integrated information security system, as well as annual support. On the basis of the presented calculations the economic expediency of introduction of the complex information protection system was proved, which was developed in the second part.

The practical value of the project is to ensure the necessary level of information security of a private enterprise LLC "Oxgaming".

INTEGRATED INFORMATION SECURITY SYSTEM, THREAT MODEL, INTRUDER MODEL, INFORMATION SECURITY, VULNERABILITIES, SECURITY PROFILE, REGULATORY FRAMEWORK.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ДСТУ – державний стандарт України;

ЗУ – закон України;

ІБ – інформаційна безпека;

ІТС – інформаційно-телекомунікаційна система;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

НД ТЗІ – нормативний документ в галузі технічний захист інформації.

НСД – несанкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ПЕОМ – персональна електронно-обчислювальна машина;

ПЗ – програмне забезпечення;

ПБ – політика безпеки;

ТОВ – товариство з обмеженою відповідальністю;

БФП – багато-функціональний пристрій;

БД – база даних

ПК – персональний комп’ютер;

АРМ – автоматизоване робоче місце;

АС – автоматизована система;

РС – робоча станція;

ФС – файловий сервер;

ІзОД – інформація з обмеженим доступом;

ОС – операційна система.

CRM – Customer Relationship Management (система керування користувачами)

HR – Human Resources (менеджер з управління персоналом)

BA – Business Analyst (бізнес аналітик)

ЗМІСТ

ВСТУП

У сучасному світі людство має безліч можливостей для створення різних проектів та онлайн-платформ, які при правильному підході можна розвивати до масштабів великих підприємств.

Але у той час, коли компанія розвивається найбільш стрімко, і коли фінансові витрати на утримання й розвиток збільшуються, більшість людей допускають одну й ту саму помилку. Вони усю енергію та фінанси вкладають в розширення штату, нове устаткування, розкрутку підприємства, забуваючи про те, що також необхідно на даному етапі.

Забезпечити безпеку інформації на підприємстві. На жаль, з такою проблемою стикаються навіть ті компанії, які доволі довго на ринку.

Адже із стрімким розвитком рівня інформатизації, в інформаційно-телекомунікаційній системі (ІТС) циркулює інформація, розголошення якої призведе до значних збитків власнику інформації або особі, якої стосується інформація. Тому, на сьогоднішній день, питання створення заходів захисту інформації підприємств та держави є актуальним.

Тож для забезпечення безпеки інформації під час її обробки в ІТС створюється комплексна система захисту інформації (КСЗІ), що запобігає витоку тих чи інших видів інформації, а також політика безпеки, що регламентує порядок захисту інформації.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ. ОБСТЕЖЕННЯ ІТС ТА АНАЛІЗ СТАНУ ЗАХИЩЕНОСТІ

1.1 Стан питання

На етапі стрімкого розвитку компанії, у ній починає циркулювати важлива інформація, і якщо буде порушена її цілісність або конфіденційність, то компанія понесе дуже значні фінансові збитки.

Для захисту різних видів інформації розробляється комплексна система захисту інформації та політика безпеки інформації.

Метою роботи є аналіз підприємства, його інформаційної системи, виявлення в ній потенційних загроз і вразливостей, побудова комплексної системи захисту інформації (КСЗІ) для обраного підприємств. А також, техніко-економічне обґрунтування доцільності впровадження КСЗІ та розроблених політик безпеки.

1.2 Теоретичні відомості

1.2.1 Аналіз нормативно-правової бази забезпечення захисту інформації в автоматизованих системах

Закон України «Про інформацію» трактує поняття «інформація» в наступному вигляді: «під інформацією розуміється документовані або публічно оголошені відомості про події та явища, які відбуваються в суспільстві, державі та навколишньому середовищу».

У свою чергу, захист інформації в АС - діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків в результаті реалізації загроз.

Таким чином, ІТС являє собою складну систему, яку доцільно розділяти на окремі блоки (модулі) для полегшення її подальшого проектування. В результаті

цього, кожен модуль буде незалежний від інших, а в комплексі вони становитимуть цілісну систему захисту.

1.2.2 Поняття інформації. Види інформації. Порядок доступу

Основою основ та одним з початкових етапів перед створенням КСЗІ є усвідомлення того, що ж все-таки називають інформацією та які види інформації бувають.

Відповідно до закону України «Про інформацію», інформацією є будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Існує багато класифікацій інформації, але щодо порядку доступу, інформацію поділяють на інформацію з відкритим доступом, та інформацію з обмеженим доступом. [1]

Щодо інформації з обмеженим доступом, можна виділити 3 її вида – конфіденційна, таємна і службова. У рамках кваліфікаційної роботи та обраного підприємства, увага приділяється саме конфіденційній інформації. [1]

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації.

Порядок доступу інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством. У випадках, передбачених

законом, доступ до інформації в системі може здійснюватися без дозволу її володільця в порядку, встановленому законом. [3]

1.2.3 Об’єкт інформаційної діяльності

Згідно з нормативним документом системи технічного захисту «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці» [2], об'єкт інформаційної діяльності - інженерно-технічна споруда (приміщення), транспортний засіб, де здійснюється озвучення та/або обробка технічними засобами інформації з обмеженим доступом.

- Об'єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься інформація з обмеженим доступом, що не становить державної таємниці, підлягають обов'язковому категоріюванню.
- Категоріювання може бути первинним, черговим або позачерговим.
- Категоріювання здійснюється для визначення необхідного (зі встановлених нормативно-правовими актами та нормативними документами системи технічного захисту інформації рівнів) рівня захисту інформації, що обробляється технічними засобами та/або озвучується на об'єкті.
- Відповідальність за своєчасність категоріювання та правильність встановлення категорії об'єкта покладається на керівника установи - власника (розпорядника, користувача) об'єкта.
- Об'єктами категоріювання є об'єкти інформаційної діяльності, в тому числі об'єкти ЕОТ.
- Категоріювання здійснюється за ознакою: ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на ОІД.

- Об'єктам, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, встановлюється четверта (IV) категорія.
- За рішенням розпорядників (користувачів) інформації або за рішенням власників (розпорядників, користувачів) об'єктів, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, об'єктам може встановлюватися III категорія.
- Об'єкти, яким встановлено відповідну категорію, вносяться до Переліку категоризованих об'єктів, який ведеться власником (розпорядником, користувачем) об'єктів інформаційної діяльності.

1.2 4 Підстави створення КСЗІ

Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов’язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд. [6] Вихідні дані для обґрунтування необхідності створення КСЗІ у загальному випадку одержуються за результатами:

- аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;

- визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;
- оцінки можливих переваг (фінансово-економічних, соціальних, тощо)
- експлуатації ІТС у разі створення КСЗІ.

Обґрунтування необхідності створення КСЗІ на підприємстві:

На підприємстві циркулює інформація – персональні дані користувачів. Згідно з Законом України «Про захист персональних даних», кожна людина має право на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Вимоги цього закону є підставою для створення КСЗІ на підприємстві.

Крім того, компанія має ще інформацію з обмеженим доступом, яка, відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» та згідно з [4], повинна оброблятися в системі із застосуванням комплексної системи захисту інформації або СУІБ.

Також існує економічна доцільність створення КСЗІ — комерційна таємниця, оскільки інформація, що циркулює на підприємстві, та продукт, що створюється на підприємстві може втратити свою позицію на ринку, якщо вихідний код та база даних будуть перехоплені конкурентами.

На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ.

1.2.5 Процес створення КСЗІ.

Процес створення КСЗІ складається з декількох етапів.

1. Процес обстеження ОІД. Складається з опису підприємства, середовища функціонування ІТС. Виявлення в ІТС елементів, що можуть так чи інакше вплинути на безпеку інформації в цілому.
2. Процес аналізу загроз та побудови моделі порушника. Відповідно до [5] загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС.

Загрози для інформації, що обробляється в АС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись у моделі загроз.

1.3 Постановка задачі

Проаналізувавши вищезазначені пункти, задля доцільної розробки КСЗІ підприємства виконати обстеження об’єкта інформаційної діяльності, проаналізувати загрози та вразливості, виявити їх джерела.

Обрати та обґрунтувати вибір профіля захищеності.

Техніко-економічно обґрунтувати доцільність впровадження розроблених політик безпеки.

1.4 Обстеження об’єкту інформаційної діяльності

1.4.1 Загальні відомості

Об’єктом інформаційної діяльності є Дніпровський офіс Ізраїльської компанії ТОВ «Oxgaming».

ТОВ «Oxgaming» - це приватне підприємство, що займається розробкою платформ для онлайн-ігор як і власний продукт компанії, так і на продаж.

За формою власності ТОВ «Oxgaming» - комерційна організація, що була зареєстрована 16.10.2017 як товариство з обмеженою відповідальністю.

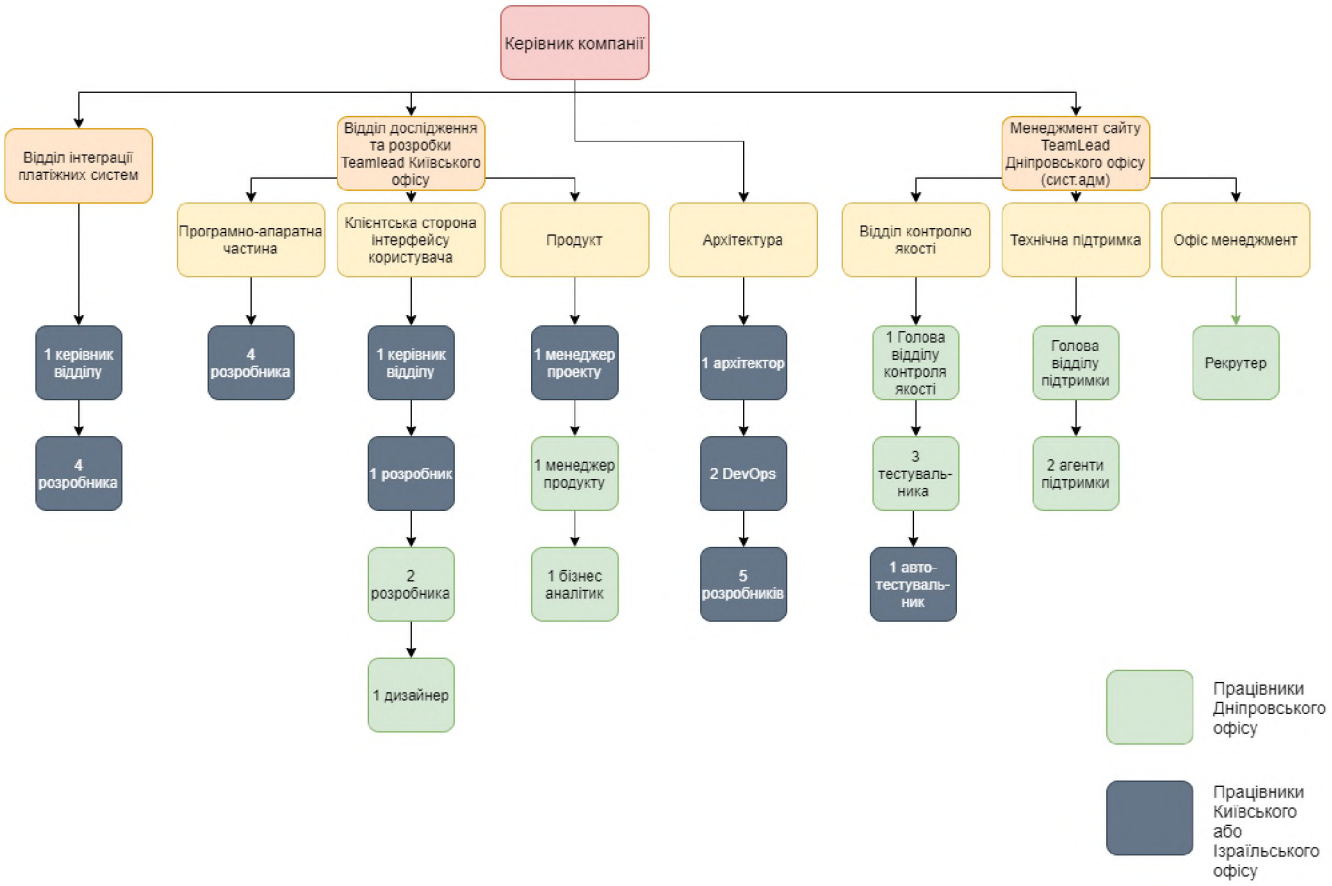

Рисунок 1.1 Організаційна структура компанії

Основні види діяльності на підприємстві:

1. Розробка власних веб-сайтів для онлайн-ігор
2. Розробка власної CPM системи для управління користувачами.
3. Розробка веб-сайтів для онлайн-ігор на замовлення.
4. Розробка CPM систем для управління користувачами на замовлення.
5. Моніторинг активності користувачів на сайті та прибутковості.
6. Робота відділу для боротьби з шахраями на веб-сайтах.
7. Підтримка користувачів.
8. Технічна підтримка.

З цих видів діяльності у Дніпровському офісі функціонують пункти №1,2,3,4,5,7.

Працює 5 днів на тиждень. З понеділка по п'ятницю з 9:00 до 03:00 ночі.

Штат працівників: TeamLead (1), Front-end розробник (2), HR менеджер (1), QA engineers (3), QA Lead(1), Support Lead (1), агент підтримки (2), Product Manager (1), BA(1).

1.4 Обстеження середовищ функціонування ІТС

1.4.1 Фізичне середовище

Об'єкт інформаційної діяльності (ОІД) знаходиться за адресою вул. Писаржевського 2, м.Дніпро, 49005

ОІД знаходиться в житловій дев'ятиповерховій будівлі на 7 поверсі. Контрольована зона обмежується стінами будівлі з північно-західної та південно-східної сторони, з південно-західної, північно-східної, зверху та знизу – стінами між іншими приміщеннями. Режим КЗ не відрізняється в робочий і неробочий час. У робочий та неробочий час до офісу ОІД доступ мають усі працівники лише за наявністю ключа. У робочий час режим КЗ також забезпечується персоналом на

підставі інструкцій з режиму роботи компанії. Дані про прилеглі споруди та дороги наведені у таблицях №1 та №2 відповідно.

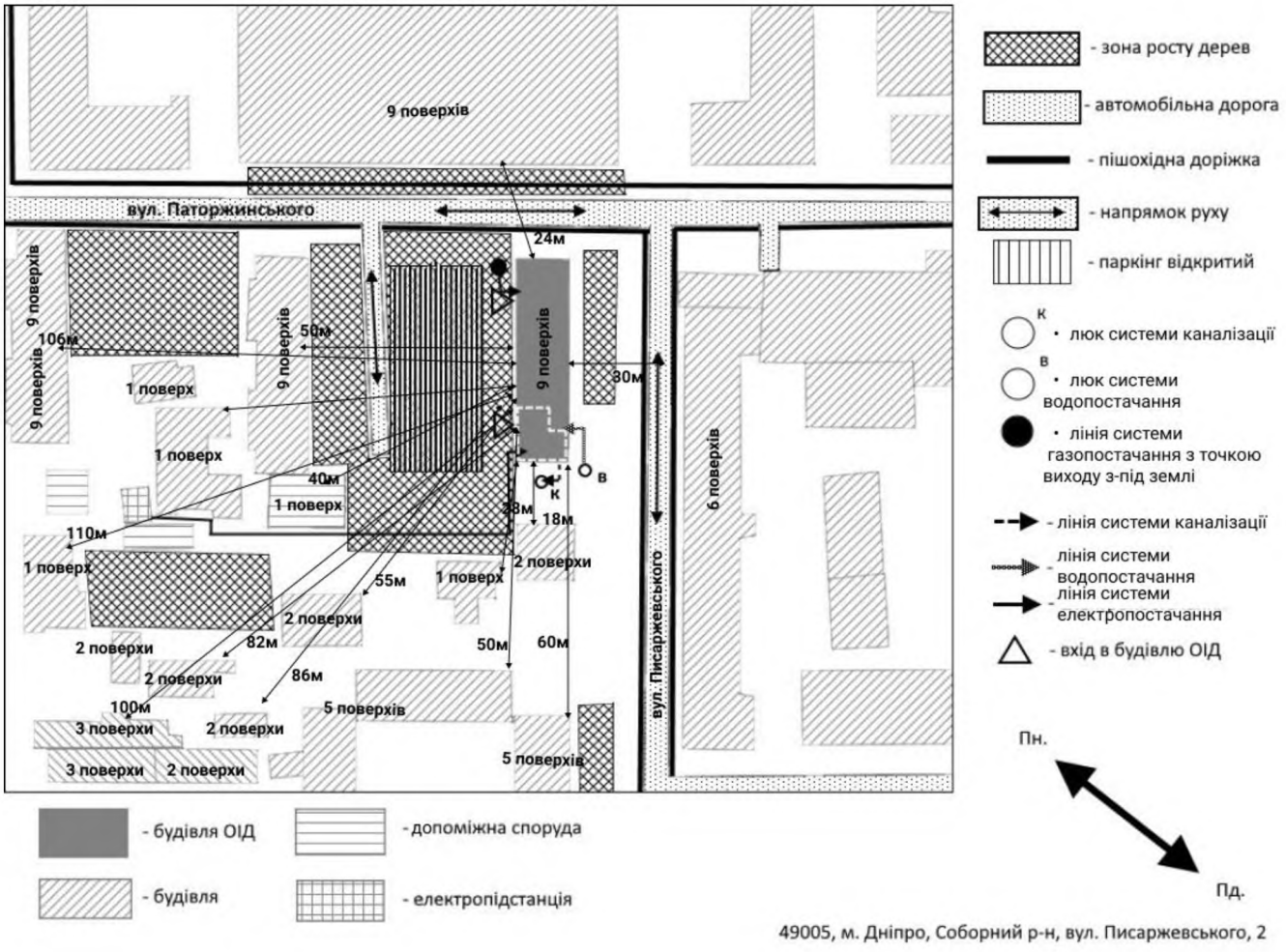

Рисунок 1.2 Ситуаційний план

Таблиця 1.1 - Перелік прилеглих споруд

№ п/п	Найменування	Кількість поверхів	Адреса	Відстань до ОІД	Розташування
1	Малоповерховий житловий будинок	2	вул. Писаржевського, 6	20м	Південно-західна сторона
2	Приватний будинок	1	вул. Писаржевського, 6Б	30м	Південно-західна сторона
3	Гараж	1	вул. вул. Писаржевського, 6	40м	Південно-західна сторона
4	Малоповерховий житловий будинок	2	вул. Писаржевського, 6А	55м	Західна сторона
5	Житловий будинок	5	вул. Писаржевського 8А	60м	Південно-західна сторона
6	Житловий будинок	5	вул. Писаржевського 8	65м	Південно-західна сторона
7	Господарський корпус	1	Вул. Паторжинського, 3	40м	Північно-західна сторона
8	Електропідстанція	123	7-й Зарічний мкр-н.	45м	Північно західна сторона

Продовження таблиці 1.1

№ п/п	Найменування	Кількість поверхів	Адреса	Відстань до ОІД	Розташування
9	Житловий будинок+приватна школа	9	вул. Паторжинського, 3	60м	Північно західна сторона
10	Відділ державної виконавчої служби Дніпропетровського міського управління юстиції	9	Вул. Писаржевського, 1а	25м	Північна сторона
11	Державний хіміко-технологічний університет (їдальня)	6	пр.Гагаріна, 8	35м	Східна сторона

Таблиця 1.2 - Перелік прилеглих доріг та паркінгів

№ п/п	Найменування	Ширина проїздн. частини	Інтенсивність руху	Відстань	Паркування
1	Під'їзна дорога до будівлі ОІД	4м	Рух інтенсивний	65м	Ні
2	Паркінг біля входу до будівлі ОІД	-	-	0м	Так
3	Паркінг напроти будівлі ОІД	-	-	40м	Так
4	Пішохідна доріжка до ОІД	3м	Рух не інтенсивний	65м	-

Опис ситуаційного плану:

Перед будівлею знаходиться Відділ державної виконавчої служби Дніпропетровського міського управління юстиції, праворуч через дорогу – Державний хіміко-технологічний університет, ліворуч – дитячий майданчик та житловий будинок. Позаду будівлі ОІД – житловий будинок.

Південна сторона офісу має два подвійних металопластикових вікна (1500 х 900 мм) з захисними ролетами та 2 метало-пластикові двері (1500 х 2500 мм), що ведуть на балкон. Південно-західна сторона має 1 подвійне металопластикове вікно (2100 х 1500 мм) з захисними ролетами.

Західна сторона має два подвійних металопластикових вікна (1500 х 900 мм) з захисними ролетами та 1 метало-пластикові двері (1500 х 2500 мм мм), що ведуть на балкон.

Стіни будівлі зроблені з залізобетонних панелей. Фундамент – стрічковий з бетонних блоків, дах – покритий руберойдом. Територія навколо будівлі вкрита асфальтом. Зовнішні стіни будівлі – залізобетонні. Товщина стін –200мм (панель 180мм та штукатурка).

Система електропостачання підключена до трансформаторної підстанції №5, яка має сторонніх споживачів і має вихід за межі КЗ.

Система опалення підключена до міської системи опалення та має вихід за межі КЗ. Системи каналізації та водопостачання підключені до міської системи, має вихід за межі КЗ.

Комунікації є підземними і входять до будинку через технічне приміщення, розташоване на 0-ому поверсі.

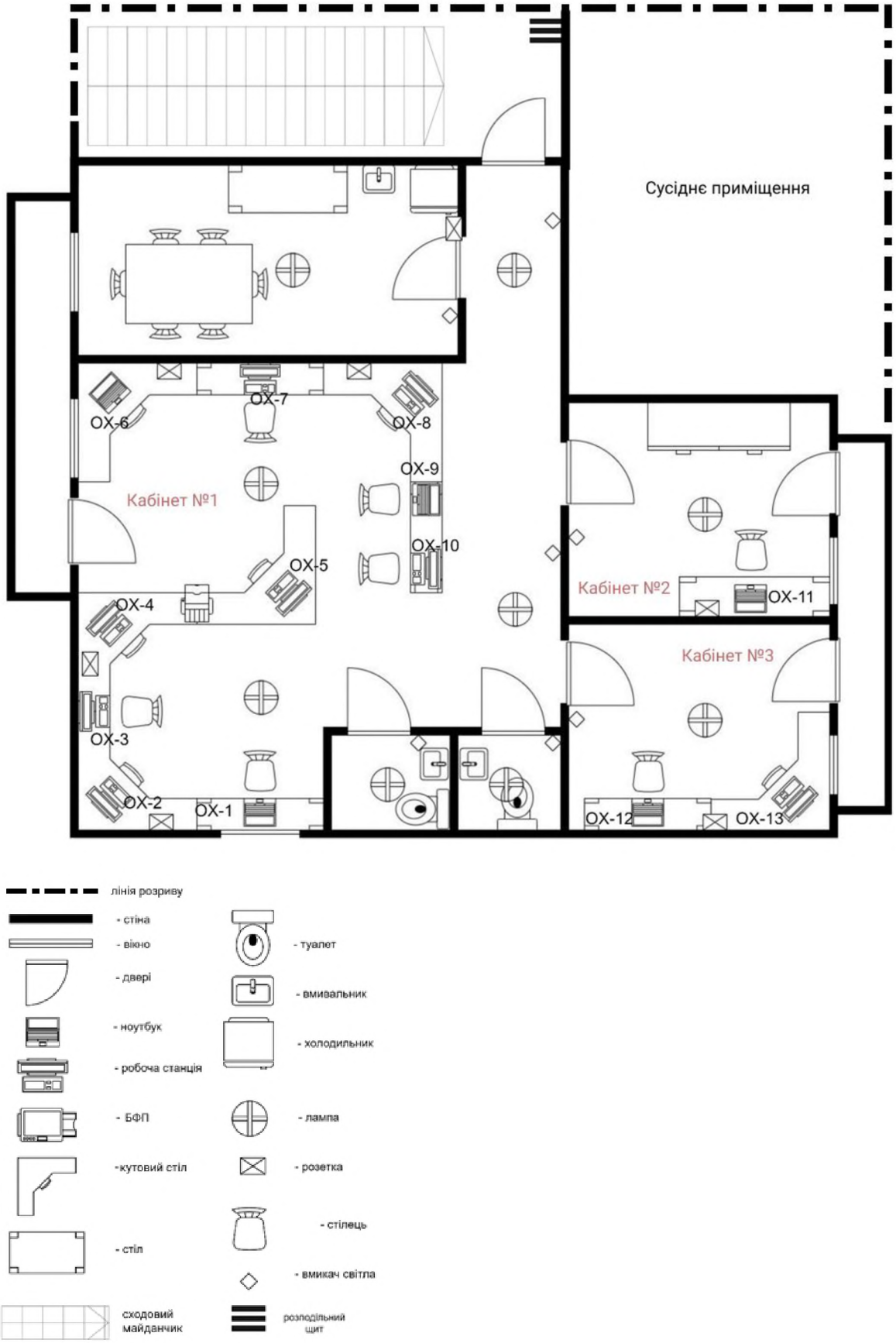

Рисунок 1.3 Генеральний план

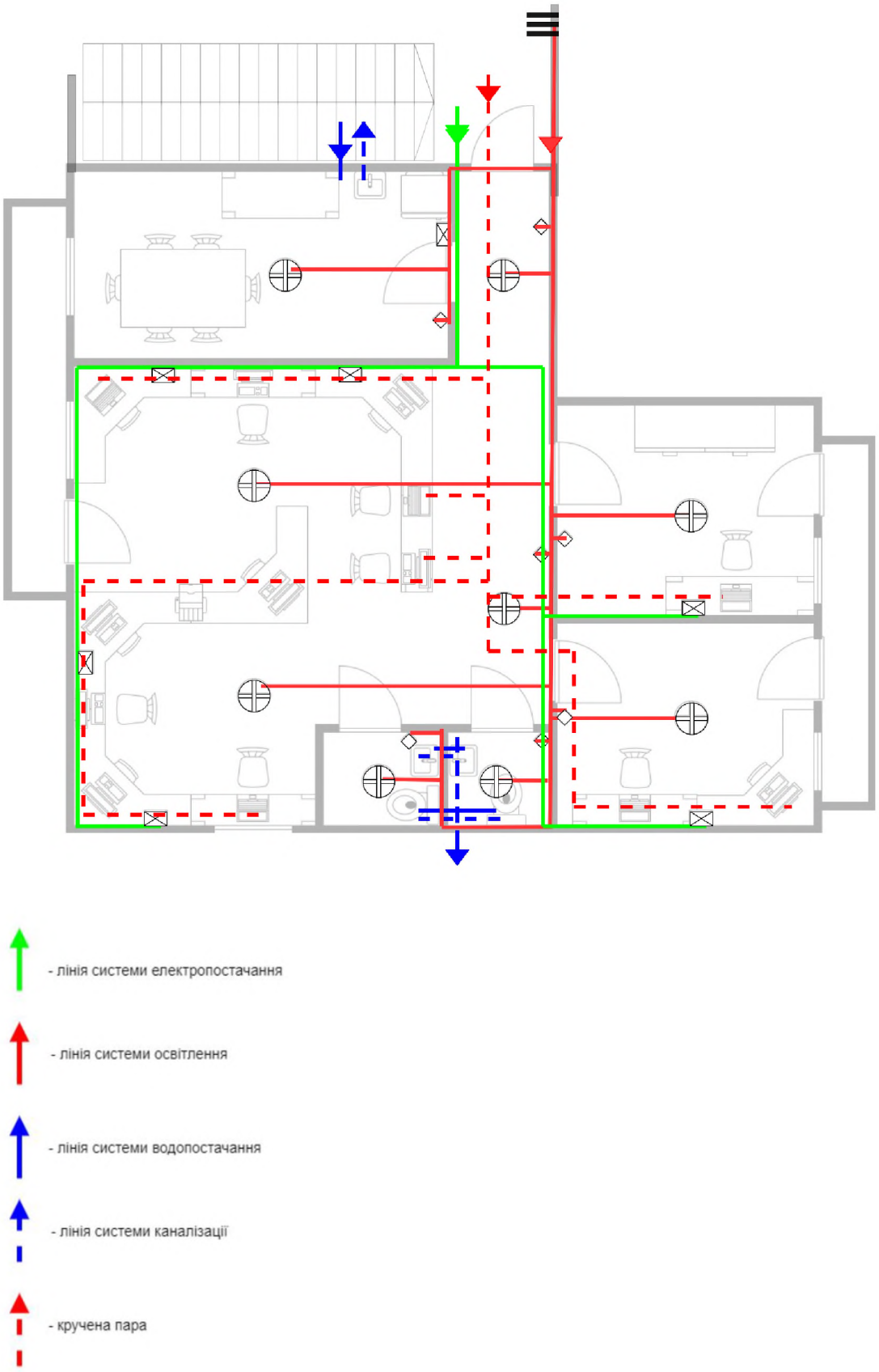

Рисунок 1.4 План комунікацій

Опис генерального плану:

Внутрішні стіни - залізобетонні. Товщина – 170мм – панель 140мм и штукатурка).

Вхідні двері подвійні – 1- металеві з подвійним замком шириною 800 мм та висотою 2000 мм, 2 – дерев'яні з 1 замком.

Замки – врізні зі сталі, закриваються вбудованим циліндром під ключ з перфорацією.

Міжкімнатні двері -МДФ зі скляними вставками.

Офіс має висоту 2.5м (від підлоги до стелі). Стеля – підвісна, з конструкцією кріплення Армстронг. Підлога – плитка.

Система електропостачання підключена до трансформаторної підстанції №3, яка має сторонніх споживачів і знаходиться за межами КЗ – щиток на поверсі, звідки вертикальними комунікаціями веде до підвального приміщення.

Системи каналізації та водопостачання підключені до міської системи. Знаходяться за межами КЗ. Інтернет проведено за допомоги крученої пари від обладнання провайдеру «Фрегат».

1.4.2. Обчислювальна система:

ІТС являє собою мережу з топологією типу «зірка» з виходом в Інтернет, побудовану з використанням одного маршрутизатору та одного комутатору. ІТС являє собою багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності, а також має доступ до мережі Інтернет, який забезпечується ВАТ «Фрегат». Відноситься до класу «3».

Обчислювальна система у складі:

1. 5 ноутбуків під керуванням Microsoft Windows 10 Professional (білд 1909);
2. 8 ПК під керуванням Microsoft Windows 10 Professional (білд 1909);
3. мережеве обладнання:
   - один маршрутизатор Mikrotik hAP ac під керуванням RouterOS 6.46;
   - один комутатор (некерований) TP-Link TL-SF1016;
4. один БФП HP OfficeJet Pro 9013;
5. системне ПЗ (Microsoft Windows 10 Pro 1909)
6. прикладне ПЗ (Microsoft Office, Mozilla Firefox 69.0, 7-Zip).
7. спеціалізоване ПЗ (ESET Endpoint Antivirus 7.1, TeamViewer, MySQL Workbench 8.08.18, PhpStorm 2020.1.04.

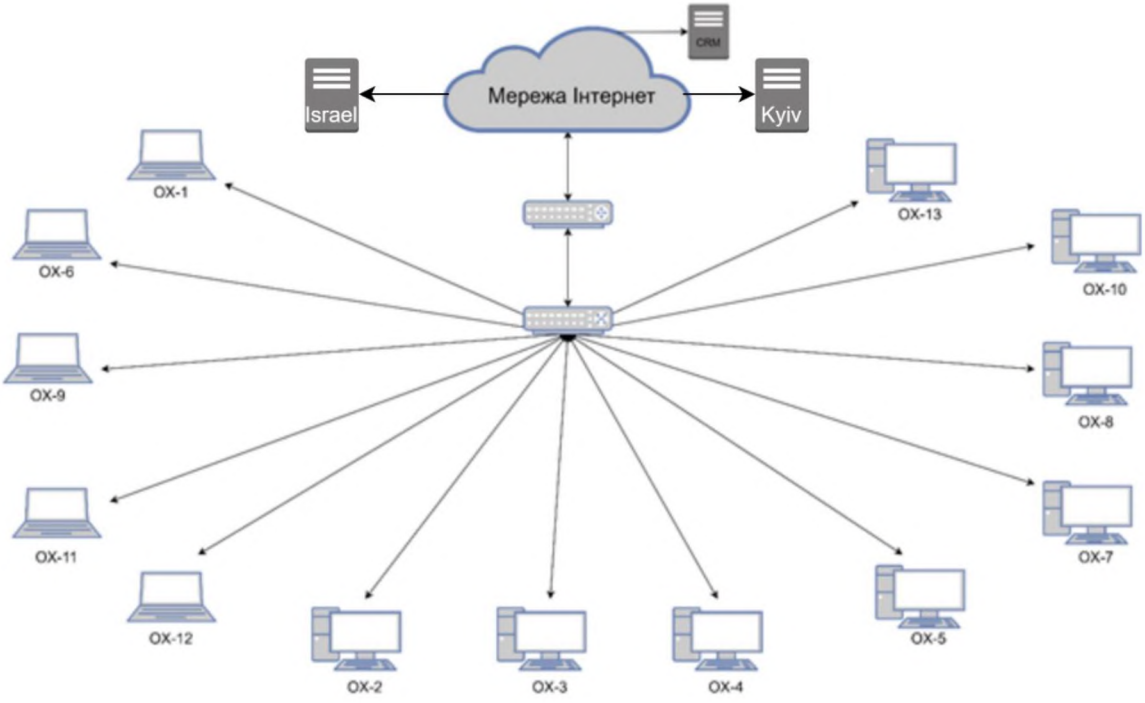

Рисунок 1.5 Схема ІТС

Апаратне забезпечення ІТС:

Таблиця 1.3 - Основні технічні засоби

№	Тип	Модель	Характеристики	Серійний та інвентаризаційний номери	Приміщення	Відстань до КЗ
1	Ноутбук (Ім’я в системі ОХ-1)	HP 250 G7	Процесор Intel Celeron N4000; RAM 4ГБ; Твердотілий накопичувач HP 8PE63AA120ГБ (UUID 47ba2efc-2db1-11e0-88f8-806e6f6e6963)	Ноутбук: R302N15, 370001 SSD накопичувач: 5QE0RCHD, -	Кабінет №1 На столі	1м

Продовження таблиці 1.3

№	Тип	Модель	Характеристики	Серійний та інвентаризаційний номери	Приміщення	Відстань до КЗ
2	Ноутбук (Ім’я в системі ОХ-6)	HP 250 G7	Процесор Intel Celeron N4000; RAM 4ГБ; Твердотілий накопичувач HP 8PE63AA 120ГБ (UUID 41ed5jsn-2kl8-51i9-11z5-624y5t5e9261)	Ноутбук: R411U34, 370006 SSD накопичувач: 7WE5KFDE, -	Кабінет №1 На столі	1.5м
3	Ноутбук (Ім’я в системі ОХ-9)	HP 250 G7	Процесор Intel Celeron N4000; RAM 4ГБ; Твердотілий накопичувач HP 8PE63AA 120ГБ (UUID 97gh5sfh-8f41-83d4-12s7-086d2a9r1045)	Ноутбук: R087F12, 370009 SSD накопичувач: 4DE2QWIU, -	Кабінет №1 На столі	1м

Продовження таблиці 1.3

№	Тип	Модель	Характеристики	Серійний та інвентаризаційний номери	Приміщення	Відстань до КЗ
4	Персональний комп'ютер (Ім'я в системі ОХ-2)	Everest Home&Office 1003	Процесор Intel Celeron J1900; RAM 4ГБ; Твердотілий накопичувач 120ГБ	Системний блок: SN29340, 370002 SSD накопичувач: 7TU92TYG,	Кабінет №1 На столі	1м
5	Персональний комп'ютер (Ім'я в системі ОХ-3)	Everest Home&Office 1003	Процесор Intel Celeron J1900; RAM 4ГБ; Твердотілий накопичувач 120ГБ (UUID 76sd4rty-r3e5-t6g8t435)	Системний блок: TP41937, 370003 SSD накопичувач: 3RE16IAH,	Кабінет №1 На столі	1м
6	Персональний комп'ютер (Ім'я в системі ОХ-4)	Everest Home&Office 1003	Процесор Intel Celeron J1900; RAM 4ГБ; Твердотілий накопичувач 120ГБ	Сист. блок: RR86234, 370004 SSD накопичувач 8RT12ERF	Кабінет №1 На столі	1.5м

Продовження таблиці 1.3

№	Тип	Модель	Характеристики	Серійний та інвентаризаційний номери	Приміщення	Відстань до КЗ
7	Персональний комп'ютер (Ім'я в системі ОХ-5)	Everest Home&Office 1003	Процесор Intel Celeron J1900; RAM 4ГБ; Твердотілий накопичувач 120ГБ (UUID 15fg4yef-s9k2-f2a7y258)	Системний блок: RG19362, 370005 SSD накопичувач: 7RF34ARG, -	Кабінет №1 На столі	2м
8	Персональний комп'ютер (Ім'я в системі ОХ-7)	Everest Home&Office 1003	Процесор Intel Celeron J1900; RAM 4ГБ; Твердотілий накопичувач Everest 120ГБ	Системний блок: TF71528, 370007 SSD накопичувач: 5RD82LFE	Кабінет №1 На столі	2м
9	ПК (Ім'я в системі ОХ-8)	Everest Home&Office 1003	Процесор Intel Celeron J1900; RAM 4ГБ; Твердотілий накопичувач Everest 120ГБ	Системний блок: ST10365, 370008	Кабінет №1 На столі	1.5м

Продовження таблиці 1.3

№	Тип	Модель	Характеристики	Серійний та інвентаризаційний номери	Приміщення	Відстань до КЗ
10	Персональний комп'ютер (Ім'я в системі ОХ-10)	Everest Home&Office 1003	Процесор Intel Celeron J1900; RAM 4ГБ; Твердотілий накопичувач Everest120ГБ (UUID 45dg3edc-g4h6-f3d6h709)	Системний блок: FD72510, 370010 SSD накопичувач: 6GF34KHT, -	Кабінет №1 На столі	2м
11	Ноутбук (Ім'я в системі ОХ-11)	HP 250 G7	Процесор Intel Celeron N4000; RAM 4ГБ; Твердотілий накопичувач HP 8PE63AA 120ГБ (UUID ab45rd7d-2c2d-44tv1mk7)	Ноутбук: R302N23, 370011 SSD накопичувач: U43G2VN, -	Кабінет №2 На столі	2м

Продовження таблиці 1.3

№	Тип	Модель	Характеристики	Серійний та інвентаризаційний номери	Приміщення	Відстань до КЗ
12	Ноутбук (Ім’я в системі ОХ-12)	HP 250 G7	Процесор Intel Celeron N4000; RAM 4ГБ; Твердотілий накопичувач HP 8PE63AA 120ГБ (UUID ab45rd7d-2c2d-44tv1mk7)	Ноутбук: R319N11, 370012 SSD накопичувач: U43G2VN, -	Кабінет №3 На столі	2м
13	Багатофункціональний пристрій	HP OfficeJet Pro 9013	Має підключення до локальної мережі	14Y7BC8M, 370074	Кабінет №1 На столі	2м
14	Персональний комп’ютер (Ім’я в системі ОХ-13)	Everest Home&Office 1003	Процесор Intel Celeron J1900; RAM 4ГБ; Твердотілий накопичувач Everest 120ГБ HP 8PE63AA	Системний блок: SN37589, 370052 SSD накопичувач: W45GB2C2,	Кабінет №3 На столі	1м

Таблиця 1.4 - Допоміжні технічні засоби

№	Тип	Модель	Характеристики	Серійний та інвентаризаційний номери	Приміщення	Відстань до КЗ
1	Світлодіодна лампа (9 шт)	Maxus LED R50	5W 4100K 200-240V 50Hz 500Lm 65mA Цоколь E14 Кут розсіювання 140 50000годин	B61839752	Їдальня	0.1м
				B72816387	Кабінет №1	0.1м
				B26387982	Кабінет №1	0.1м
				B62729861	Кабінет №1	0.1м
				B62918627	Кабінет №1	0.1м
				B51729836	Туалет 1	0.1м
				B28293270	Туалет2	0.1м
				B16623801	Кабінет №2	0.1м
				B19792973	Кабінет №3	0.1м
2	Миша комп'ютерна бездротова(13шт)	Logitech M185 Wireless Grey	Джерело живлення – 1xAA Тип датчику – jптичний Сумісність –	131D27-001532	Кабінет №1 На столі	1м
				135D55-013665	Кабінет №1 На столі	1м

			Mac OS, Microsoft Windows	105D23-917283	Кабінет №1 На столі	2м
				145D93-712649	Кабінет №1 На столі	1м
				128D24-087263	Кабінет №1 На столі	1м
				176D21-973478	Кабінет №1 На столі	1.5м
				125D44-574342	Кабінет №1 На столі	3м
				144D16-021267	Кабінет №1 На столі	2м
				114D99-923023	Кабінет №1 На столі	3.5м
				139D12-238238	Кабінет №1 На столі	2м
				198D98-137181	Кабінет №2 На столі	2м
				115D78-	Кабінет	1.5м

				089897	№3 На столі	
				166D23-293788	Кабінет №3 На столі	1м

Таблиця 1.5 - Програмне забезпечення

Тип	Найменування	Описання	Ліцензія	Термін дії	Встановлено на
Системне	Операційна система Microsoft Windows 10 Pro 1909 (білд 18363.476)		Пропрієтарна, OLP	-	ОХ-1 - 13
	Драйвери	Набір драйверів для пристроїв, які підключені до комп'ютера (графічна плата, принтер, тощо)	Пропрієтарна	-	ОХ-1 - 13

Продовження таблиці 1.5

Тип	Найменування	Описання	Ліцензія	Термін дії	Встановлено на
Прикладне	Microsoft Office 365 Business	Пакет офісних програм	Пропрієтарна, OLP	1 рік	ОХ-1 – 13
	7-Zip	Універсальний архіватор	GNU Lesser General Public License	-	ОХ-1 - 13
	Mozilla Firefox 69.0	Веб-браузер	Mozilla Public License v2, GNU GPL, GNU LGPL	-	ОХ-1 - 13
Спеціалізоване	PhpStorm 2020.1.04	Комерційне крос-платформове інтегроване середовище розробки для PHP	Пропрієтарна	1 рік	ОХ-1 – 13 (6)
	MySQL Workbench 8.08.18	Інструмент для візуального проектування баз даних	Пропрієтарна	-	ОХ-1 – 13 (6)

	TeamViewer	ПЗ для віддаленого доступу до системи	Пропрієтарна	1 рік	ОХ-1 - 13
	ESET Endpoint Antivirus 7.1	Антивірусне ПЗ	Пропрієтарна	3 роки	ОХ-1 - 13

Персональні комп'ютери, ноутбуки та БФП під'єднані до комутатору за допомоги крученої пари. Пристрої в мережі не об'єднані ані в робочу групу, ані в домен.

Кожен користувач ІТС має право відправити документ на друк до БФП.

БФП використовується тільки для друку.

Використання зовнішніх носіїв інформації не заборонене та не регулюється.

Адміністрування системи виконує системний адміністратор (що є Team Lead`ом офісу) за допомоги ПЗ для віддаленого доступу TeamViewer.

Доступ до CRM проходить з використанням незахищеного протоколу HTTP.

Сервера CRM і віддаленого репозиторію – на базі CentOS Linux 8, знаходяться за межами Дніпровського офісу.

Комунікації між віддаленими офісами налагоджено з використанням протоколів електронної пошти IMAP/SMTP без шифрування каналу зв'язку.

1.4.3 Інформаційне середовище

Інформація зберігається на електронних та паперових носіях.

Таблиця 1.6 - Інформація, що циркулює на підприємстві:

№	Інформація	Режим доступу	Правовий режим	Працівники, що мають доступ	Місце зберігання
1	Організаційно-розпорядча	З обмеженим доступом	Конфіденційна інформація	HR, TeamLead	ПК TeamLead'а, ПК HR`а
2	Фінансова звітність	З обмеженим доступом	Конфіденційна інформація	HR, TeamLead	ПК TeamLead'а, ПК HR`а
3	Інформація про працівників	З обмеженим доступом	Конфіденційна інформація	Всі працівники підприємства	ПК HR`а
4	Інформація про користувачів	З обмеженим доступом	Конфіденційна інформація	Всі працівники підприємства	Віддалений доступ, CRM, DB
5	Інформація про партнерів	З обмеженим доступом	Конфіденційна інформація	TeamLead, Support Lead, PM	ПК PM'а

Продовження таблиці 1.6

№	Інформація	Режим доступу	Правовий режим	Працівники, що мають доступ	Місце зберігання
6	Вихідний код	З обмеженим доступом (інформаційний запит)	Конфіденційна інформація	Team Lead, Product Manager, BA, розробники	Віддалений доступ
7	Аналітична інформація	З обмеженим доступом (інформаційний запит)	Конфіденційна інформація	Team Lead, Product Manager, BA	Віддалений доступ, Yandex Metrics
8	Моніторинг активності користувачів та прибутковості	З обмеженим доступом (інформаційний запит)	Конфіденційна інформація	Team Lead, Product Manager, BA	Віддалений доступ, Grafana
9	Поточні та заплановані задачі	З обмеженим доступом	Конфіденційна інформація	Всі працівники підприємства	Kanban дошка у онлайн-системі Jira
10	Технічна документація	З обмеженим доступом	Конфіденційна інформація	Всі працівники підприємства	Віддалений доступ, Confluence
11	Технологічна інформація	З обмеженим доступом	Конфіденційна інформація	Team Lead	ПК Team Lead’а

Технологія обробки інформації:

Організаційно-розпорядча інформація зберігається на ПК TeamLead'а та ПК HR`а. Створюється TeamLead'ом та керівництвом у Ізраїльському офісі. Серед працівників поширюється за необхідністю через електронну пошту та тим працівникам, яких стосується.

Фінансова звітність зберігається на ПК TeamLead'а та ПК HR`а. Створюється та редагується TeamLead'ом та HR`ом. Відсилається HR`ом електронним листом до керівництва у Ізраїльському офісі.

Інформація про працівників зберігається на ПК HR`а (в електронному виді). Створюється та публікується HR`ом.

Інформація про користувачів зберігається в базі даних та в онлайн CRM. Додається автоматично при реєстрації користувача.

Інформація про партнерів зберігається на ПК PM'а. Створюється керівництвом у Ізраїльському офісі.

Вихідний код зберігається і віддаленому репозиторії Php Storm, куди мають доступ користувачі з паролем від нього. Створюється розробниками, будь-який працівник інший може надати аргументований інформаційний запит до системного адміністратора (TeamLead) і отримати доступ до демо репозитрорію, але не до продакшену.

Аналітична інформація зберігається у єдиному аккаунті Yandex Metric, до якого мають доступ Team Lead, Product Manager, BA. Додається інформація бізнес аналітиком. Будь-який працівник інший може надати аргументований інформаційний запит і отримати доступ.

Моніторинг активності користувачів та прибутковості являє собою графіки та діаграми стосовно депозитів і реєстрацій на веб-сайті, що реалізовані за допомогою системи візуалізації даних Grafana, до якого мають доступ Team Lead,

Product Manager, BA. Додається інформація бізнес аналітиком. Будь-який працівник інший може надати аргументований інформаційний запит і отримати доступ.

Поточні та заплановані задачі відображаються на дошці в онлайн системі керування проектами Jira, до якої мають доступ усі працівники, у кожного свій окремий аккаунт, але доступ не розмежований належним чином, і усі працівники можуть продивлятися усі задачі, і створювати власні.

Технічна документація знаходиться в онлайн доступі для всіх працівників організації, в онлайн системі зберігання та написання корпоративної документації Confluence, у кожного свій окремий аккаунт, доступ так само не розмежований належним чином, і усі працівники можуть продивлятися усі статті в системі, навіть ті, що не є необхідними для них за сферою діяльності.

Технологічна інформація (паролі, реєстр, конфігурація мережевого обладнання) знаходиться на ПК Team Lead`a, і доступ до неї має лише він, оскільки власноруч роздає доступ до деяких програмних продуктів працівникам компанії.

1.4.4 Середовище користувачів

Таблиця 1.7 - Посадові обов'язки працівників

№	Посада	Кіль кість	Посадові обов'язки	Роль в ІТС	Рівень кваліфікації
1	TeamLead	1	Контроль робочих процесів, створення організаційно-розпорядчої інформації, управління командою	Системний адміністратор, Користувач	Високий

Продовження таблиці 1.7

№	Посада	Кіль кість	Посадові обов'язки	Роль в ІТС	Рівень кваліфікації
2	Front-end розробник	2	Написання frontend частини коду для веб-сайта.	Користувач 1	Високий
3	HR менеджер	1	Пошук нових кандидатів, проводження співбесід, фінансова звітність, організація дозвілля та тімбілдингу.	Користувач 2	Низький
4	QA engineer	3	Контроль якості продукту, що випускається	Користувач 3	Середній
5	QA Lead	1	Контроль якості продукту, що випускається, управління QA командою.	Користувач 3	Середній
6	Support Lead	1	Швидке реагування на виникаючі пробеми, комунікація з провайдерами, управління командою тех. підтримки.	Користувач 4	Середній
7	Агенти підтримки	2	Швидке реагування на виникаючі пробеми, сповіщення про це розробників, відповідь на запити	Користувач 5	Середній

Продовження таблиці 1.7

№	Посада	Кіль кість	Посадові обов'язки	Роль в ІТС	Рівень кваліфікації
8	BA	1	Аналітика проекту на основі статистичних даних, поміч у створенні бізнес вимог	Користувач 6	Високий
9	Product Manager	1	Поліпшення продукту, комунікація із замовниками, аналіз продукту і ринку, написання бізнес вимог.	Користувач 7	Високий

Таблиця 1.8 - Фрагмент матриці розмежування доступу

Посада	1	2	3	4	5	6	7	8	9	10	11
TeamLead	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ
Front-end розробник	ЧЗ	-	ЧЗ	ЧРЗ	-	ЧРЗВ	-	-	ЧРЗВ	ЧРЗВ	-
HR менеджер	ЧРЗВ	ЧРЗ	ЧРЗВ	ЧЗ	-	-	-	-	ЧРЗВ	ЧРЗВ	-
QA engineer	ЧЗ	-	ЧЗ	ЧРЗ	-	-	-	-	ЧРЗВ	ЧРЗВ	-
QA Lead	ЧЗ	-	ЧЗ	ЧРЗ	-	-	-	-	ЧРЗВ	ЧРЗВ	-
Support Lead	ЧЗ	-	ЧЗ	ЧРЗВ	ЧЗ	-	-	-	ЧРЗВ	ЧРЗВ	-

Продовження таблиці 1.8

Посада	1	2	3	4	5	6	7	8	9	10	11
Агенти підтримки	ЧЗ	-	ЧЗ	ЧРЗВ	-	-	-	-	ЧРЗВ	ЧРЗВ	-
BA	ЧЗ	ЧЗ	ЧЗ	ЧРЗВ	-	Ч	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	-
Product Manager	ЧЗ	ЧЗ	ЧЗ	ЧРЗВ	ЧРЗ	Ч	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	-

де Ч – читання, Р – редагування, З – зберігання, В – видалення. Цифрами від 1 до 10 позначено інформацію згідно до таблиці «Інформація, що циркулює на підприємстві».

Також кожен користувач може друкувати інформацію, до якої він має доступ.

Встановлення та запуск програм також дозволено кожному користувачеві.

1.4.4 Модель порушника

Таблиця 1.9 - Модель порушника [9]

Посада	Мотив	Кваліфікація	Можливості	Час дії	Місце дії	Сума загроз
Внутрішні порушники						
TeamLead	М3	К3	З2	Ч4	Д5	16
Front-end розробник	М1	К3	З2	Ч3	Д5	14
HR менеджер	М1	К1	З1	Ч3	Д4	10

Продовження таблиці 1.9

Посада	Мотив	Кваліфікація	Можливості	Час дії	Місце дії	Сума загроз
QA engineer	М1	К2	З1	Ч3	Д4	11
QA Lead	М2	К2	З2	Ч3	Д4	13
Support Lead	М2	К2	З2	Ч3	Д4	13
Агенти підтримки	М1	К2	З1	Ч3	Д4	11
BA	М3	К3	З2	Ч3	Д5	16
Product Manager	М3	К3	З2	Ч3	Д5	16
Зовнішні порушники						
Представники сторонніх організацій (компанії що створюють також онлайн платформи для ігор)	М3	К3	З1	Ч3	Д1	11
Користувачі	М3	К1	З1	Ч3	Д1	9
Хакери	М3	К4	З4	Ч3	Д1	15

Специфікація моделі порушника за мотивами здійснення порушень:

- М1 – Безвідповідальність.
- М2 – Самоствердження.
- М3 – Корисливий мотив.

Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС:

- К0 – Не знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами системи.

- 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 особам, 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 до неї;
- 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.
- Специфікація моделі порушника за часом дії:
- Ч1 – До впровадження АС або її окремих компонентів.
- Ч2 – Під час бездіяльності компонентів системи (в неробочий час, під час планових перерв у роботі, перерв для обслуговування і ремонту і т.д.).
- Ч3 – Під час функціонування АС (або компонентів системи).
- Ч4 – Як у процесі функціонування АС, так і під час зупинки компонентів системи.

Висновок:

З таблиці видно, що найбільшу загрозу, яка має відношення до проблеми захисту інформації, становлять TeamLead, Business Analyst, Product Manager та хакери. Організація, яка працює з великою кількістю персональних даних, стає мішенню як для внутрішніх порушників (TeamLead, Business Analyst, Product Manager), так і для зовнішніх (хакери). ІТС повинна бути більш контрольованою, а доступ до найважливіших даних у системі – розділені.

1.4.5 Модель загроз

Таблиця 1.10 - Перелік загроз з визначенням порушень властивостей інформації та ІТС

№	Загрози	Властивості		
		К	Ц	Д
1. Загрози об’єктивної природи				
1.1	Стихійні явища (аварії, пожежі, урагани)	-	+	+
1.2	Втрата електроживлення	-	-	+
1.3	Втрата / пошкодження комунікаційних каналів	-	-	+
1.4	Перенавантаження системи	-	-	+
1.5	Збої та відмови обчислювальної техніки, програмного забезпечення	-	+	+
1.6	Збої, відмови та пошкодження носіїв інформації	-	+	+
2. Загрози суб’єктивної природи				
2.1Зовнішні загрози				
2.1.1	Несанкціоноване підключення до каналів зв’язку	+	-	-
2.1.2	Перехоплення інформації за рахунок ПЕМВ від технічних засобів	+	-	-
2.1.3	Несанкціоноване підключення до технічних засобів	+	-	-
2.1.4	Хакерські атаки через глобальну мережу Інтернет	+	+	-

Продовження таблиці 1.10

№	Загрози	Властивості		
		К	Ц	Д
2.1.5	Читання даних, що виводяться на екран, роздруковуються, читання залишених без догляду документів, підслуховування	+	-	-
2.2 Порушення нормальних режимів роботи				
2.2.1	Зараження системи комп'ютерними вірусами	+	+	+
2.2.2	Втрата (розголошення) засобів розмежування доступу, носіїв інформації, резервних копій	+	+	+
2.2.3	Несанкціоноване внесення змін у технічні засоби, програмне забезпечення	-	+	+
2.2.4	Використання стороннього програмного забезпечення	-	+	+
2.2.5	Вхід у систему недопущених осіб	+	+	+
2.2.6	Пошкодження носіїв інформації	-	+	+
2.3 Помилки				
2.3.1	Помилки при інсталяції ОС, ПЗ	-	+	+
2.3.2	Помилки при експлуатації ПЗ	+	+	+
2.3.3	Помилки при експлуатації технічних засобів	-	+	+
2.3.4	Помилки при введенні даних	-	+	+

Продовження таблиці 1.10

№	Загрози	Властивості		
		К	Ц	Д
2.3.5	Недбале зберігання та облік документів, носіїв інформації	+	+	+
2.3.6	Розголошення інформації персоналом ІТС	+	-	-

Таблиця 1.11 Модель загроз з визначенням рівня ризиків та збитків

№	Джерело	Механізм реалізації	Рівень		Сума загроз
			Ризиків	Збитків	
1. Загрози конфіденційності інформації					
1.1	Персонал з доступом до ІТС	Навмисне розголошення конфіденційної інформації стороннім особам	2	3	5
1.2	Персонал з доступом до ІТС	Ненавмисне розголошення інформації стороннім особам	2	3	5
1.3	Персонал з доступом до ІТС	Копіювання конфіденційної інформації на зовнішні носії з метою ознайомлення сторонніх осіб	2	3	5

Продовження таблиці 1.11

№	Джерело	Механізм реалізації	Рівень		Сума загроз
			Ризиків	Збитків	
1.4	Персонал з доступом до ІТС	Друк конфіденційної інформації з метою ознайомлення сторонніх осіб	2	3	5
1.5	Персонал, зовнішні порушники	Викрадення носіїв конфіденційної інформації	1	3	4
1.6	Персонал, зовнішні порушники	Перегляд інформації на екранах моніторів, робочих місцях	2	2	4
1.7	Персонал з доступом до ІТС	Несанкціонований доступ до інформації	3	3	6
1.8	Зовнішні порушники	Перехоплення трафіку	2	3	5
2. Загрози цілісності інформації					
2.1	Персонал з доступом до ІТС	Несанкціонована модифікація інформації	1	2	3
2.2	Персонал з доступом до ІТС	Помилки при експлуатації ПЗ, (ненавмисна модифікація даних)	1	2	4
2.3	Персонал з доступом до ІТС	Несанкціонована модифікація або встановлення ПЗ	2	2	4

Продовження таблиці 1.11

№	Джерело	Механізм реалізації	Рівень		Сума загроз
			Ризиків	Збитків	
2.4	Персонал з доступом до ІТС (системний адміністратор)	Модифікація журналу подій	1	2	3
2.5	Персонал, що не має доступу до ІТС; зовнішні порушники	Доступ до ІТС сторонніми особами	1	3	4
2.6	Техногенне джерело	Помилки програмного забезпечення	1	2	3
3. Загрози доступності					
3.1	Персонал з доступом до ІТС	Несанкціоноване знищення інформації	2	2	4
3.2	Персонал з доступом до ІТС	Помилки при експлуатації ПЗ, технічних засобів (ненавмисне знищення даних)	2	2	4
3.3	Персонал з доступом до ІТС	Несанкціоноване видалення ПЗ	1	1	2
3.4	Персонал, що не має доступу до ІТС; зовнішні порушники	Доступ до ІТС сторонніми особами	1	3	4

Продовження таблиці 1.11

№	Джерело	Механізм реалізації	Рівень		Сума загроз
			Ризиків	Збитків	
3.5	Персонал з доступом до ІТС (системний адміністратор)	Вимкнення засобів захисту	1	2	3
3.6	Техногенне джерело	Помилки програмного забезпечення	2	2	4
3.7	Техногенне джерело	Збій каналу зв'язку	2	3	5
3.8	Техногенне джерело	Збій системи електроживлення	2	3	5

Рівні ризиків та загроз:

- Високий – якщо реалізація загрози надає великих збитків (3 бали);
- Середній – якщо реалізація загрози надає помірних збитків (2 бали);
- Низький – якщо реалізація загрози надає незначних збитків (1 бал).

Актуальні загрози:

- Конфіденційності:

1. Несанкціонований доступ до інформації персоналом – відсутність коректного розмежування доступу в PhpStom, MySQL Workbench, CRM
2. Друк інформації з метою ознайомлення третіх осіб – відсутність протоколювання операцій друку у журналі подій
3. Копіювання інформації на зовнішні носії з метою ознайомлення третіх осіб – можливість підключати сторонні носії.

4. Можливий перехват та підміна трафіку через наявність незахищеного зовнішнього каналу.
5. Ненавмисне розголошення конфіденційної інформації – низький рівень підготовки з питань безпеки інформації та/або некомпетентність персоналу, доступ до інформації про користувачів та співробітників.

– Цілісності:

1. Несанкціонована модифікація або встановлення ПЗ – інформаційна безграмотність працівників.

– Доступності:

1. Помилки при експлуатації ПЗ, технічних засобів (ненавмисне знищення даних) – доступ до коду та БД усім працівникам.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Формування вимог щодо захисту інформації в ІТС підприємства

2.1.1 Профіль захищеності

Автоматизована система являє собою організаційно-технічну систему, що об’єднує ОС, фізичне середовище, персонал і оброблювану інформацію.

Згідно з результатами обстеження, АС підприємства відноситься до класу «3». Тобто, це розподілений багатомашинний, розрахований на багато користувачів комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Прибуток компанії безпосередньо залежить від доступності АС та цілісності вихідного коду. Також модель загроз показує, що найбільшу небезпеку становлять загрози конфіденційності. Тому АС компанії має підвищенні вимоги до конфіденційності, цілісності та доступності.

Загрози витоку інформації технічними каналами не є актуальними з урахуванням відношення вартості і технічної складності реалізації до потенційного прибутку.

Об’єкти на підприємстві, шо підлягають захисту, умовно були розділені на дві множини:

1. інформація на дисковому просторі віддалених серверів CRM та бази даних, репозиторію
2. ПЗ (прикладне, спеціальне і системне) та інформація, яка міститься в файлах, що зберігаються на просторі жорстких дисків на робочих станціях співробітників.

Відповідно до документа [8] для даної АС класу «3» обрано наступний профіль захищеності:

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

Опис послуг безпеки наведено у таблиці:

Таблиця 2.1 - Профіль захищеності

Критерії	Послуги безпеки	Вимоги до рівнів послуг безпеки
	1	2
Конфіденційності	Довірча конфіденційність	КД-1 (мінімальна довірча конфіденційність)
	Адміністративна конфіденційність	КА-2 (базова адміністративна конфіденційність)

Продовження таблиці 2.1

Критерії	Послуги безпеки	Вимоги до рівнів послуг безпеки
	1	2
	Повторне використання об'єктів	КО-1 (повторне використання об'єктів)
	Конфіденційність при обміні	КВ-2 (базова конфіденційність при обміні)
Цілісності	Довірча цілісність	ЦД-1 (мінімальна довірча цілісність)
	Адміністративна цілісність	ЦА-2 (базова адміністративна цілісність)
	Відкат	ЦО-1 (обмежений відкат)
	Цілісність при обміні	ЦВ-2 (базова цілісність при обміні)
Доступності	Використання ресурсів	ДР-1 (квоти)
	Відновлення після збоїв	ДВ-1 (ручне відновлення)
Спостережності	Реєстрація	НР-2 (захищений журнал)
	Ідентифікація і автентифікація	НИ-2 (одиночна ідентифікація і автентифікація)
	Достовірний канал	НК-1 (однонаправлений достовірний канал)
	Розподіл обов’язків	НО-2 (розподіл обов’язків адміністраторів)
	Цілісність комплексу засобів захисту	НЦ-2 (КЗЗ з гарантованою цілісністю)

Критерії	Послуги безпеки	Вимоги до рівнів послуг безпеки
	1	2
	Самотестування	НТ-2 (самотестування при старті)
	Ідентифікація і автентифікація при обміні	НВ-1 (автентифікація вузла)

Послуги безпеки: [7]

Мінімальна довірча конфіденційність (КД-1)

Реалізація послуги забезпечує користувачеві можливість управляти потоками інформації від об'єктів великої кількості 1, які належать його домену, до користувачів. Політика послуги поширюється на:

- усіх користувачів
- інформаційні об’єкти

Управління доступом до об'єктів здійснюється на основі списків контролю доступу.

Послугу реалізовано.

Базова адміністративна конфіденційність (КА-2)

Реалізація послуги забезпечує адміністратору можливість керувати потоками інформації від об’єктів множини 2 до користувачів. Політика послуги поширюється на:

- усіх користувачів
- процеси;
- інформаційні об’єкти;
- програмні засобі;
- зовнішні та внутрішні носії інформації.

Керування доступом до об’єктів виконується на підставі атрибутів об’єкту та користувача. Атрибути призначаються при створенні об’єктів/користувачів.

Послугу не реалізовано.

Повторне використання об’єктів (КО-1)

Реалізація послуги унеможливлює отримання залишкової інформації з розділюваних об’єктів. Відноситься до множини 2. Політика послуги поширюється на:

- сторінки оперативної пам’яті;
- зовнішні та внутрішні носії інформації.

Послугу частково реалізовано.

Базова конфіденційність при обміні (КВ-2)

Реалізація послуги забезпечує захист інформації, яка зберігається на внутрішніх чи зовнішніх носіях, від несанкціонованого ознайомлення у разі вилучення носіїв з-під контролю засобів захисту. Відноситься до множини 2. Політика послуги поширюється на:

- користувачів усіх категорій;
- логічні диски на внутрішніх та зовнішніх носіях.

Послугу не реалізовано.

Мінімальна довірча цілісність (ЦД-1)

Реалізація послуги забезпечує користувачеві можливість управляти потоками інформації від процесів, ініційованих іншими користувачами, до інформації, яка належать його домену. Відноситься до множини 1. Політика послуги поширюється на:

- усіх користувачів
- інформаційні об’єкти

Контроль дозволених процесів виконується ядром системи.

Послугу реалізовано.

Базова адміністративна цілісність (ЦА-2)

Реалізація послуги забезпечує адміністратору можливість керувати потоками від інформації процесів, ініційованих користувачами, до захищених об'єктів. Відноситься до множини 2. Політика послуги поширюється на:

- користувачів усіх категорій;
- процеси;
- інформаційні об'єкти;
- програмні засоби;
- зовнішні та внутрішні накопичувачі інформації.

В повній аналогії з адміністративною конфіденційністю, керування доступом до об'єктів виконується на підставі атрибутів користувача та об'єкту. Атрибути призначаються при створенні об'єктів/користувачів.

Послугу не реалізовано.

Обмежений відкат (ЦО-1)

Реалізація послуги забезпечує можливість відміни послідовності операцій над захищеним об'єктом. Політика послуги поширюється на послідовність операцій, які виконуються при встановленні захисту на файл або каталог. Відноситься до множини 2.

Послугу не реалізовано.

Базова цілісність при обміні (ЦВ-2)

Реалізація послуги забезпечує виявлення фактів несанкціонованої модифікації інформації, яка зберігається на внутрішніх чи зовнішніх носіях, у разі вилучення носіїв з-під контролю засобів захисту. Відноситься до множини 2. Політика послуги поширюється на:

- користувачів усіх категорій;
- логічні диски на внутрішніх та зовнішніх носіях.

Послугу не реалізовано.

Використання ресурсів (ДР-1)

Реалізація послуги унеможливлює захоплення користувачами надмірного об’єму ресурсів. Відноситься до множини 1. Політика послуги поширюється на:

- користувачів усіх категорій;
- дисковий простір внутрішніх носіїв, що зберігають створені користувачами захищені інформаційні об’єкти.

Адміністратор має можливість встановити максимально допустимий розмір дискового простору для кожного користувача окремо і/або групи користувачів.

Послугу не реалізовано.

Ручне відновлення після збоїв (ДВ-1)

Реалізація послуги забезпечує повернення системи у захищений стан у разі відказу або переривання обслуговування. Відноситься до множини 2. Політика послуги поширюється на програмне забезпечення.

У разі відмови ПЗ системи система повинна переходити у стан, в якому неможлива обробка ІзОД. Повернути систему до нормального функціонування може тільки системний адміністратор, відновивши працездатність ПЗ з копії.

Послугу не реалізовано.

Захищений журнал (НР-2)

Реалізація послуги забезпечує контроль подій в системі. Відноситься до множин 1 і 2. Політика послуги поширюється на:

- користувачів усіх категорій;
- інформаційні ресурси;
- системне та прикладне ПЗ.

Послугу не реалізовано.

Одиночна ідентифікація та автентифікація (НИ-2)

Реалізація послуги дозволяє визначити і перевірити особистість користувача. Відноситься до множин 1 і 2. Політика послуги поширюється на усіх користувачів системи, які намагаються:

- одержати доступ до КС;
- виконати дію з правами адміністратора.

Послугу реалізовано.

Однонапрямлений достовірний канал (НК-1)

Реалізація послуги гарантує користувачеві взаємодію з системою в процесі ідентифікації та автентифікації. Відноситься до множини 2. Політика послуги поширюється на користувачів усіх категорій.

Послугу реалізовано.

Розподіл обов'язків адміністраторів (НО-2)

Реалізація послуги дозволяє розділити повноваження користувачів. Відноситься до множини 1. Політика послуги поширюється на користувачів усіх категорій.

Послугу не реалізовано.

КЗЗ з гарантованою цілісністю (НЦ-2)

Реалізація послуги забезпечує захист системи від зовнішніх впливів і гарантує її здатність управляти захищеними об'єктами. Відноситься до множини 2. Політика послуги поширюється на:

- програмні засоби;
- ядро системи.

Послугу не реалізовано.

Самотестування при старті (НТ-2)

Реалізація послуги надає можливість перевірити та на основі цього гарантувати правильність функціонування та цілісність функцій системи. Відноситься до множини 2. Політика послуги поширюється на:

- програмні засоби;
- конфігураційні файли програмних засобів.

Послугу не реалізовано.

Автентифікація вузла (НВ-1)

Реалізація послуги надає можливість ідентифікувати і аутентифікувати віддалений ресурс. Відноситься до множини 1.

Послугу не реалізовано.

Рівень гарантій до обраного профілю захищеності - Г-3.

2.1.2 Проектні рішення

НР-2 — для множини 1 необхідно встановити на серверах службу аудиту Auditd. Ця служба забезпечує реєстрацію таких подій :

- вхід/вихід в систему
- реєстрація/видалення облікових записів
- порушення правил розмежування доступу
- установка/видалення правил розмежування доступу
- системні події

```
[root@trusted ~]# tail -n 3 /var/log/secure
May 15 12:46:52 trusted login: pam_unix(login:session): session opened for user
john by LOGIN(uid=0)
May 15 12:46:52 trusted login: LOGIN ON tty2 BY john
May 15 12:48:44 trusted login: pam_unix(login:session): session closed for user
john
```

Рисунок 2.1 Вхід і вихід користувача John у систему

Для множини 2 необхідно провести закупівлю і інсталяцію КЗЗ.

Наразі існують операційні системи з засобами захисту та окремі комплекси засобів захисту:

- Комплекс засобів захисту операційної системи Microsoft Windows 10 Professional – ТОВ «Майкрософт Україна».
- Комплекс засобів захисту програмного забезпечення «Операційна система Січ» – ТОВ «Трайбекс».

- Комплекс засобів захисту програмного забезпечення «Операційна система Ubuntu*Pack 18.04» – ТОВ «УАЛІНУКС».
- Засіб технічного захисту інформації від несанкціонованого доступу «Гриф мережа».

У додатку Д наведена порівняльна таблиця зазначених КЗЗ. Через специфічне програмне забезпечення на підприємстві, варто розглядати КЗЗ на ОС Windows, отже вибір є між комплексом засобів захисту операційної системи Microsoft Windows 10 Professional, і засобом технічного захисту інформації від несанкціонованого доступу «Гриф мережа». Розглядаючи наступну колонку, було визначено, що за функціональним профілем захищеності, для даної ІТС підходить засіб технічного захисту інформації від несанкціонованого доступу «Гриф мережа».

Засоби КЗЗ забезпечують реєстрацію таких подій, які мають пряме або непряме відношення до безпеки:

- вхід користувача в ОС та завершення роботи користувача (вихід);
- запуск АРМ адміністратора КЗЗ;
- запуск АРМ адміністратора безпеки;
- зміна стану БД та ПЗ КЗЗ: реєстрація, видалення користувачів;
- реєстрація, видалення захищених ресурсів (встановлення/ зняття захисту на каталог);
- факти призначення/зміни прав доступу користувачів до захищених ресурсів;
- факти доступу користувачів до захищених каталогів та файлів;
- факти виведення файлів з ІзОД на друк;
- факти імпорту/експорту файлів з ІзОД з використанням знімних носіїв;
- факти порушення прав доступу користувачів до захищених ресурсів;
- факти перезавантаження, вимкнення РС та ФС та виникнення інших системних подій;
- подій, пов’язаних з спостереженням за процесами (запуск, завершення);

– подій, пов’язаних з функціонуванням активного мережевого обладнання.

В кожному запису протоколу аудита фіксується дата та час події, тип та атрибути операції (наприклад, відкриття файлу для читання/ запису), атрибути процесу та користувача, які ініціювали подію, ознака успішності завершення операції і, у випадку відмови – причина, а також інша інформація. Збір інформації аудита та її аналіз в реальному часі.

Перегляд та аналіз протоколів реєстрації виконується адміністратором безпеки.

ДР-1 — файлова система XFS підтримує установку максимально допустимого розміру дискового простору для кожного користувача або групи користувачів. Системному адміністраторові усього лише необхідно виконати команду, вказавши в її параметрах користувача і ліміт. Наприклад:

#: xfs_quota limit bsoft=1g bhard=2g john,

Встановить ліміт в 2 гігабайти для користувача john.

```
xfs_quota> report -h -u
User quota on /storage (/dev/sda5)
                        Blocks
User ID      Used   Soft   Hard Warn/Grace
---------- --------------------------------
root            0      0      0  00 [------]
john            0     1G     2G  00 [------]
```

Рисунок 2.3 Ліміти, встановлені для користувачів

НО-2 - необхідно встановити на серверах CRM і репозиторія систему примусового управління доступом SELinux, щоб обмежити функції адміністратора до строго певного набору. Треба виділити як мінімум дві ролі: системний адміністратор і адміністратор безпеки. У функції системного адміністратора входитиме:

– інсталяція та оновлення ПЗ;
– конфігурація системи та ПЗ;
– моніторинг протоколів реєстрації системних подій.

У функції адміністратора безпеки буде входити:

– керування засобами захисту;

- керування користувачами та захищеними ресурсами;
- аналіз даних аудиту безпеки.

НВ-1 — необхідно провести закупівлю і інсталяцію VPN клієнтів на робочі станції користувачів і сервера CRM і репозиторіїв, щоб забезпечити шифрування каналу комунікацій, об'єднати усі вузли у віртуальну мережу і забезпечити ідентифікацію і аутентифікацію усіх вузлів в мережі.

Було проведено порівняння найпопулярніших сервісів VPN, порівняльна таблиця наведена у додатку Е.

Для даної ІТС та підприємства в цілому важливі такі критерії вибору: шифрування (AES-256), протокол (повинен бути IPSec або L2TP), а також VPN повинен бути на великій кількості пристроїв. Усі зі списку сервісів використовують шифрування AES-256, протоколи IPSec або L2TP використовують також усі сервіси, але безліміт на пристрої на одній ліцензії є лише у ZenMate.Крім того, він має найнижчу ціну за місяць користування.

2.2 Політика безпеки

На даний час, на підприємстві вже розроблено та діють політики безпеки, що стосуються прав доступу до інформації, правила розмежування доступу до певних приміщень підприємства; політика використання зовнішніх електронних носіїв інформації та правила зберігання та знищення інформації.

Дані політики безпеки були розроблені системним адміністратором та директором підприємства. Затверджені були директором компанії.

Усі працівники були ознайомлені із розробленими політиками безпеки за п’ять робочих днів до дати набуття чинності політик безпеки. Відповідальність за виконання вище зазначених ПБ несе системний адміністратор.

2.2.1 Організаційні заходи щодо забезпечення політики безпеки

Були визначені наступні організаційні заходи щодо забезпечення політики безпеки:

1. Розробити та запровадити посадові інструкції користувачів та персоналу ІТС.
2. Визначити правила обліку, зберігання, розмноження, знищення носіїв конфіденційної інформації, яка обробляється на ОІД.
3. Створити на програмному рівні системи розпізнавання й розмежування доступу до інформації засобами ідентифікації й автентифікації користувачів даної ІТС.
4. Блокувати облікові записи користувачів після певного числа невдалих спроб входу в систему, що зменшить вірогідність підбору паролю неавторизованим користувачем.
5. Створити набір прав, що дозволяє надавати користувачеві доступ на виконання окремих операцій та використання окремих програм за допомогою програмного продукту – комплекс «Гриф мережа».
6. Організувати захист атрибутами файлів. При цьому передбачена можливість встановлювати, чи може індивідуальний файл бути змінений або розділений визначеним користувачем. Захист атрибутами файлів використовується для запобігання випадкових змін або видалення окремих файлів. При захисті даних використовуються файлові атрибути: «модифікація, читання, копіювання, друкування, знищення» програмними засобами.
7. Контролювати доступ користувачів до CD-і DVD-дисководів, жорстких дисків, зовнішніх USB-носіїв, USB-портів за допомогою програмного продукту – комплекс «Гриф мережа», чим забезпечиться мінімізація занесення вірусу з боку зовнішніх носіїв та зменшиться вірогідність копіювання інформації;
8. Знищувати інформацію (або створити резервну копію), що зберігається в ПЗП, при списанні або відправці ПЕВМ в ремонт;
9. Ідентифікувати зовнішні носії на які здійснюється архівування даних, ідентифікувати периферійні засоби вводу\виводу інформації (клавіатури, миші, принтери), надаючи користувачеві доступ до пристрою з відповідним ідентифікатором (драйвером або серійним номером) програмним методом;

10. Протоколювати всі дії користувачів з пристроями і файлами.
11. Обмежувати доступ до соціальних мереж та засобів миттєвого обміну повідомленнями, а також до сайтів, які не зв'язані з робочим процесом програмними засобами.
12. Заборонити користувачам скачування та встановлення будь-яких програм програмними засобами.
13. Встановити на об'єкті, де обробляється конфіденційна інформація, відео спостереження (встановлення камер відео спостереження).
14. Впровадити підписання договорів про заборону розголошення конфіденційної інформації, що обробляється в ІТС для всіх категорій працівників, що мають доступ до ІТС.
15. Створення гостьової мережі для виходу в Інтернет задля унеможливлення несанкціонованого доступу до АС підприємства.
16. Впровадити квартальні семінари та навчання персоналу (користувачів АС), що спрямоване на покращення навичок роботи з ІТС. [10]

2.2.2 Положення для забезпечення захисту інформації

Положення про забезпечення доступу до віддалених ресурсів компанії

Мета:

Встановити правила та порядок доступу до віддалених ресурсів підприємства. Дотримання даних вимог підвищує захищеність інформації, що зберігається та обробляється на сервері.

Область дії:

Дане положення розповсюджується на всіх користувачів системи.

Відповідальні особи:

Відповідальною особою за виконання доступу до серверу є TeamLead.

Відповідальність:

TeamLead несе відповідальність за виконання політики доступу до серверу та серверного приміщення.

Положення:

Задля запровадження та дотримання положення про забезпечення доступу до віддалених ресурсів необхідно:

- перейти на зашифрований протокол https для безпечного доступу до CPM;
- купити поштовий сервіс, на якому буде реалізоване шифрування задля передачі конфіденційної інформації без ризику її перехоплення;
- постійне використання VPN для підключення працівників до корпоративної мережі, що дозволяє запобігти атакам методом Man-in-the-Middle (MitM) за допомогою віддалених робочих місць - введення політики й контроль її дотримання;
- використання багатофакторної аутентифікації (MFA), яка надає доступ до хмарних ресурсів та інших систем лише для авторизованих користувачів.

Порядок та періодичність перегляду:

Положення переглядається раз на рік TeamLead'ом. У разі виникнення форс-мажорних ситуацій положення може бути переглянуто раніше вказаного терміну.

У зв'язку з необхідністю використовувати VPN як складову забезпечення доступу до віддалених ресурсів компанії – виникає потреба в запровадженні положення щодо використання VPN.

Положення про використання VPN

Мета:

Призначення цього положення - визначення правил для VPN- підключень з використанням IPSec або L2TP до корпоративної мережі компанії «Oxgaming».

Область дії:

Це положення призначено для усіх співробітників компанії. При використанні VPN через концентратор IPSec, це стосується і ситуації, якщо компанія в майбутньому буде мати співробітників, що працюють за контрактом, консультантами, тимчасовими і іншими працівниками, включаючи персонал третіх організацій, що використовують VPN для доступу до локальної мережі підприємства.

Відповідальність:

Будь-який співробітник, що порушив це положення, може бути схильний до стягнення аж до звільнення.

Положення:

Певні співробітники підприємства і авторизовані партнери можуть використовувати VPN, що є службою, контрольованою користувачем. Це означає, що користувач відповідальний за вибір провайдера послуг інтернет, координацію установки устаткування і ПЗ і оплату відповідних тарифів.

Додатково:

- користувачі VPN не повинні допускати неавторизованого доступу інших користувачів до внутрішніх мережевих ресурсів компанії;
- доступ по VPN повинен здійснюватися по одноразовому паролю за допомогою токена або за допомогою інфраструктури відкритих ключів із стійкою парольною фразою;
- коли VPN-підключення активне, увесь вхідний і вихідний трафік комп'ютера, йде через VPN- тунель; інший трафік скидається;
- подвійне тунелювання не допускається; дозволено тільки одно мережеве підключення;
- VPN-шлюзи налаштовуються і обслуговуються групою мережевої підтримки;
- користувачі VPN повинні автоматично відключатися від локальної мережі Oxgaming після 30 хвилин простою. Користувач повинен авторизуватися ще раз, щоб підключитися до мережі. Пінги або інша штучна мережева активність не повинна використовуватися для підтримки з'єднання;
- VPN- концентратор має обмеження на безперервну сесію у 24 години;
- Тільки схвалене Info Sec клієнтське ПЗ VPN підлягає використанню;
- Використовуючи технологію VPN на особистому устаткуванні користувачі повинні розуміти, що їх устаткування є частиною мережі підприємтва і вони тим самим підкоряються тим же вимогам і правилам, що відносяться до устаткування

компанії, тож їх комп'ютери мають бути конфігуровані у відповідність з політиками безпеки адміністратора/групи безпеки;

Положення про використання мережі Інтернет на підприємстві

Мета:

Підвищити рівень інформаційної безпеки компанії шляхом введення правил і інструкцій для співробітників, які при виконанні своїх прямих обов'язків використовують Інтернет.

Область дії:

Положення поширюється на співробітників закладу, які при виконанні своїх прямих обов'язків використовують мережу Інтернет. Дане положення не відміняє інші політики.

Відповідальні особи:

Відповідальною особою за виконання є системний адміністратор підприємства.

Положення:

Доступ до мережі Інтернет виконувати лише через устаткування і системи підприємства.

Використання мережі Інтернет можливо лише для:

- отримання та обробки замовлень;
- підтримки і розвитку бізнесу і комунікації співробітників фірми;
- досліджень і розробок;
- збору інформації для більшої обізнаності у фінансових, законодавчих питаннях, якщо ці питання безпосередньо впливають на виконання своїх посадових обов'язків.

Забороняється:

- грати на комп'ютері в робочий час і під час обіду;
- вести діяльність не від імені фірми;
- передавати конфіденційну інформацію третім особам;

- здійснювати дії що суперечать статуту ділової етики підприємства, законодавству, політикам і процедурам підприємства;
- доступ до неавторизованої інформації і її копіювання;
- доступ до системи під іншим паролем.

Використання електронної пошти, дошок оголошень, чат-кімнат в робочий час, на устаткуванні фірми і застосовуючи імена користувачів і паролі фірми в особистих цілях, для переговорів з друзями і членами сім'ї розглядається як експлуатація ресурсів компанії в особистих цілях і категорично забороняється. Жодних виключень не робиться з даного питання для обідніх перерв і неробочого часу.

Відповідальність:

У разі явного порушення даного положення працівником підприємства, будуть застосовані дисциплінарні міри.

Порядок і періодичність перегляду

Положення переглядається раз на рік системним адміністратором та директором. У разі виникнення форс-мажорних ситуацій положення може бути переглянуто раніше вказаного терміну.

Положення про резервне копіювання

Мета:

Мета резервного копіювання - запобігання втраті інформації, а також її відновлення при відмовах устаткування, програмного забезпечення, в критичних і кризових ситуаціях, тощо. Інформаційні ресурси підприємства є найважливішою складовою компанії, тож їхня втрата може призвести до критичних збитків.

Підприємство має ризик втрати інформації через ймовірність апаратних збоїв, неумисне знищення інформації, помилки користувачів, підхоплення вірусів, або навіть умисне знищення інформації зацікавленими особами. Резервне копіювання зменшує залежність цілісності інформації від конкретного робочого місця, не будучи прив'язаною до одного комп'ютера, або іншого місця її зберігання. При виникненні критичних ситуацій, які можуть привести до втрати

працездатності устаткування або програмного забезпечення, можна в короткі терміни перенести дані і ПЗ в інше місце, на інший комп'ютер або в інше приміщення.

Область дії:

Положення про резервне копіювання повинне поширюватися на такі види інформації на підприємстві, як:

- фінансова звітність
- інформація про користувачів
- інформація про партнерів
- вихідний код
- аналітична інформація
- технічна документація

Відповідальні особи:

Відповідальною особою за виконання є системний адміністратор (TeamLead).

Положення:

Рекомендовані такі заходи по забезпеченню політики резервного копіювання на підприємстві:

- запровадження повного резервного копіювання;
- розглядання питання про найм адміністратора резервного копіювання, адже процеси, що мають вестися потребують багато часу, що буде відволікати Team Lead`а від його основних обов'язків;
- встановлення життєвих циклів та календарю операцій;
- регулярний перегляд логів після проведення операцій резервного копіювання;
- створення і підтримка регулярних звітів по резервному копіюванню;

- розвиток системи резервного копіювання, а саме: налагодження процесів, вдосконалення календарю операцій, перевірка актуальності інформації, що підлягає резервному копіюванню, і тд.;
- вимагати від користувачів системи чіткого дотримання встановленої технології і виконання інструкцій по забезпеченню резервного копіювання і відновлення інформації.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Для ТОВ «Oxgaming», як і для будь-якого іншого підприємства, основна мета захисту інформації від внутрішніх загроз – це мінімізація збитків при порушенні інформаційної безпеки компанії.

Щоб вжиті заходи по поліпшенню інформаційної безпеки на підприємстві буди економічно доцільними, витрати на забезпечення інформаційної безпеки не повинні перевищувати збитки від реалізації загрози її порушення. У даному розділі перевіряється ця умова і дається техніко-економічне обґрунтування доцільності запровадження запропонованих в проекті рішень.

3.1 Визначення витрат на розробку КСЗІ

В першу чергу слід підрахувати трудомісткість процесу створення.

Трудомісткість розробки КСЗІ визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

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

де $t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_в$ – 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.

Таким чином трудомісткість розробки дорівнює:

t=18+8+12+8+6+12

t = 64 год.

Тепер необхідно розрахувати витрати на запровадження КСЗІ. Розрахунок проводиться за формулою 3.2:

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

де $K_{рп}$ – витрати на формування проектних рішень;

$З_{зп}$ – заробітна плата спеціаліста з інформаційної безпеки;

$З_{мч}$ – вартість витрат машинного часу, що необхідні для формування проектних рішень.

Витрати на заробітну плату спеціаліста ІБ розраховуються за формулою 3.3:

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

де t – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Средньогодинна заробітна плата спеціаліста з інформаційної безпеки, що може дозволити підприємство, становить – 85 грн/год.

Відповідно до формули 3.3, витрати на заробітну плату спеціаліста ІБ становлять:

$З_{зп}$ = 64 год · 85 грн/год,

$З_{зп}$ = 5440 грн.

У свою чергу, витрати машинного часу підраховуються за формулою 3.4:

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

де t – трудомісткість розробки на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою 3.5:

$$С_{мч} = P \cdot t_{нал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р} \text{ грн,} \qquad (3.5)$$

де

P – 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;

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

$K_{лпз}$ – 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.

$C_{мч}$ = 0,14 · 1 · 1.68 + 90 + 0,7 грн,

$C_{мч}$ = 90,93 грн.

$З_{мч}$ = 64 · 90,93 = 5819.52 грн.

Отже, витрати на створення КСЗІ за формулою 3.2 становлять:

$K_{рп}$ = 5440+5819.52= 11259.52 грн.

В результаті розрахунків, вартість розробки КСЗІ становить – 11259.52 гривень.

Повна вартість капітальних витрат розраховується за формулою 3.6:

$$K = K_{рп} + K_{аз} \text{ грн.} \qquad (3.6)$$

де $К_{рп}$ – вартість розробки КСЗІ, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн.

Для впровадження необхідно придбати наступне апаратне забезпечення:

- Комп’ютер (контроллер домена) (1 шт., 12999 грн);
- Комплекс «Гриф мережа» (14 шт., 6950 грн. шт., 6950*14=97300 грн)

Відповідно до цього вартість закупівлі апаратного забезпечення становить 110299 грн.

Таким чином, згідно з формулою 3.6:

K = 121558.52 грн.

3.2 Розрахунок експлуатаційних (поточних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

Поточні витрати розраховуються за формулою 3.7:

$$C = C_a + C_з + C_е + C_{лпз} \text{ грн}, \quad (3.7)$$

де C_a – річний фонд амортизаційних відрахувань;

$C_з$ – річний фонд заробітної плати інженерно-технічного персоналу;

$C_е$ – вартість електроенергії, що споживається апаратурою;

$C_{лпз}$ – річні витрати на поновлення ліцензії ПЗ.

Річний фонд амортизаційних відрахувань розраховується за формулою 3.8:

$$C_a = Ф_п / T \text{ грн} \quad (3.8)$$

де $Ф_п$ – первісна вартість придбаного обладнання;

T – мінімальний строк корисного використання (5 років для апаратного забезпечення).

C_a = (12999+97300)/5=22059.8 грн.

У свою чергу, витрати на заробітну плату інженерно-технічного персоналу розраховуються за формулою 3.9:

$$C_{знад} = З_{дод1} + З_{дод2} + З_{дод3}\ грн, \quad (3.9)$$

де $З_{дод1}$ – додаткова заробітна плата інженерно-технічного персоналу за проведення квартальних семінарів та навчання персоналу, що спрямоване на покращення навичок роботи з ІТС;

$З_{дод2}$ – додаткова заробітна плата інженерно-технічного персоналу за додаткові обов'язки – відповідальність за виконання впроваджених розділів положень щодо безпеки інформації;

$З_{дод3}$ – додаткова заробітна плата інженерно-технічного персоналу за модернізацію існуючих положень щодо захисту інфориації на підприємстві.

За формулою 3.9, можна розрахувати:

$C_з = (1200 + 1000 + 1500) \cdot 12$ місяців,

$C_з = 44400$ грн.

Річні витрати на поновлення ліцензії складаються з:

- Корпоративний VPN ZenMate (12$/місяць=330 грн/місяць);
- Корпоративна пошта Private email (необхідна усій компанії, але в перерахуванні на Дніпровський офіс 3$/місяць 1 поштова скринька, 13шт = 1072.5 грн/ місяць);

Загалом, річні витрати на поновлення ліцензії ПЗ становлять:

$С_{лпз} = 16830$ грн.

Вартість електроенергії, що споживається апаратурою становить:

$C_е = 36288$ грн.

Отже повна вартість річних експлуатаційних витрат становить:

$C = 22059.8 + 44400 + 36288 + 16830$ грн,

і, таким чином,

$C = 119577.8 \approx 119578$ грн.

3.3 Оцінка величини збитку у разі реалізації загроз

Метою цієї оцінки є визначення обсягів матеріальних збитків, виходячи з імовірності реалізації конкретної загрози й можливих матеріальних втрат від неї.

Для розрахунку збитків від реалізації даних загроз потрібно використати формулу 3.7:

$$U = П_п + П_в + V \text{ грн}, \tag{3.10}$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла, грн;

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

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

У свою чергу, для розрахунку $П_п, П_в$ і V, використовують формули 3.8, 3.9, 3.10 відповідно.

$$П_п = \frac{\sum Зс \cdot Чс}{F} \cdot t_п \text{ грн}, \tag{3.11}$$

де F – місячний фонд робочого часу;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць;

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

$Ч_с$ – чисельність співробітників атакованого вузла.

$$П_в = П_{ви} + П_{пв} + П_{зч}\ грн, \tag{3.12}$$

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.

$$V = \frac{O}{F} \cdot (t_п + t_в + t_{ви})\ грн, \tag{3.13}$$

де F – місячний фонд робочого часу;

O – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у місяць;

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

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

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин.

У свою чергу, $П_{ви}$ і $П_{пв}$ розраховуються за формулами 3.11 і 3.12 відповідно.

$$П_{ви} = \frac{\sum Зс \cdot Чс}{F} \cdot t_{ви} \ грн, \qquad (3.14)$$

де F – місячний фонд робочого часу;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць;

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

$Ч_с$ – чисельність співробітників атакованого вузла.

$$П_{пв} = \frac{\sum Зо \cdot Чо}{F} \cdot t_{в} \ грн, \qquad (3.15)$$

де F – місячний фонд робочого часу;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць;

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

$Чо$ – чисельність обслуговуючого персоналу.

Вихідні дані для розрахунків наведені у таблиці 3.1.

Таблиця 3.1 – Вихідні дані для розрахунку збитків від реалізації загроз

Умовні позначення	Величина
$t_п$	16 год
$t_в$	5 год
$t_{ви}$	6 год
$З_о$	15000 грн
$З_с$	20000 грн
$Ч_о$	1 особа
$Ч_с$	4 особи у кожному
$О$	300000 грн
$П_{зч}$	4000 грн
$І$	3 шт
N	5 шт
F	176 год
$F_г$	8760 год

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки становлять:

$П_п$ = 3*(20000*4)/176*16=21818.18 грн.

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

$П_в$ = 8181.81+426.13+4000=12607.94 грн,

де $П_{ви}$ = 8181.81 грн, а $П_{пв}$ = 426.13 грн, а $П_{зч}$ наведено у таблиці 3.1.

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

V = 300000/176*(16+5+6)=46022.73 грн.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

U = 21818.18+12607.94+46022.73=80448.85 грн.

Загальний збиток від атаки на вузол або сегмент корпоративної мережі організації розраховується за формулою 3.16.

$$B = \sum_i \sum_n U. \qquad (3.16)$$

B = 3*5*80448.85=1206732.75 грн.

3.4 Визначення та аналіз показників економічної ефективності запропонованих в кваліфікаційній роботі проектних рішень

Загальний ефект від впровадження системи інформаційної безпеки розраховується за формулою 3.17:

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

де B – загальний збиток від атаки на вузол корпоративної мережі, грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці (0.4);

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

Тож, економічний ефект становить:

E = 1206732.75*0.4-119578=363114.8 грн.

Оцінка економічної ефективності системи захисту інформації здійснюється на основі визначення та аналізу наступних показників:

– сукупна вартість володіння (TCO);

– коефіцієнт повернення інвестицій ROSI (Return on Investment for Security);

– термін окупності капітальних інвестицій T_o.

У даному випадку TCO не використовується, оскільки було визначено величину відверненого збитку.

ROSI, у свою чергу, показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки, розраховується за формулою 3.18:

$$ROSI = E / K, \qquad (3.18)$$

де E – загальний ефект від впровадження системи інформаційної безпеки, грн;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Таким чином,

$ROSI$ = 363114.8 грн / 121558.52 грн,

$ROSI$ = 2.98.

Для остаточної оцінки варіантів і вибору найбільш ефективного з них необхідно порівняти значення ROSI з бажаним значенням показника ефективності $E_н$.

ТОВ “Oxgaming” здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів, тому в якості $E_н$ приймається бажана норма прибутковості альтернативних варіантів вкладення коштів К (на депозитний рахунок у банку).

Проект вважається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта, розраховується за формулою 3.19:

$$ROSI > (N_{деп} - N_{інф}) / 100 \quad (3.19)$$

де $N_{деп} = 17$ – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, %;

$N_{інф} = 5$ – річний рівень інфляції, %.

Оскільки 2.98 > 0,12, проект є економічно доцільним.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупаються за рахунок загального ефекту від впровадження системи інформаційної безпеки, розраховується за формулою 3.20:

$$T_o = K/E = 1 / ROSI = 0{,}34 \text{ року}. \quad (3.20)$$

3.5 Висновок економічного розділу

В цьому розділі були проведені розрахунки:

– капітальних витрат на створення КСЗІ (121558.52 грн.);

– річних експлуатаційних витрат на підтримку заходів захисту, регламентованих обраних проектних рішень (119578 грн).

В ході розрахунків з’ясовано, що введення в експлуатацію засобів та заходів захисту вигідне для підприємства. Це підтверджується наступними показниками:

– економічний ефект (363114.8 грн);

– коефіцієнт ефективності, що перевищує річний рівень прибутковості альтернативного варіанта (2.98 > 0,12);

– термін окупності капітальних інвестицій (0,34 року).

Отже, впровадження та використання обраних проектних рішень повністю доцільне.

ВИСНОВКИ

У першому розділі кваліфікаційної роботи було описано стан питання, а також проаналізована нормативно-інформаційна база, що дало змогу визначити підстави для створення КСЗІ на підприємстві “Oxgaming”.

Визначивши необхідність у створенні КСЗІ, було проведено обстеження фізичного, інформаційного середовища, та середовища користувачів на підприємстві. Також у першому розділі була розроблена модель порушника, та модель загроз і вразливостей.

У спеціальній частині був обраний профіль захищеності, а також виконано аналіз рівня реалізації послуг безпеки. Для реалізації послуг було запропоновано проектні рішення і організаційні заходи задля забезпечення необхідного рівня захисту інформації.

Також були розроблені такі документи, як:

- «Положення для забезпечення захисту інформації»
- «Положення про використання VPN»
- «Положення про використання мережі Інтернет на підприємстві».

Положення рекомендовано додати до існуючої політики безпеки.

Розроблені рекомендації повинні сприяти забезпеченню належного стану захищеності ІТС підприємства.

В третьому розділі було проведено розрахунки капітальних витрат на введення в експлуатацію політики безпеки інформації, річних експлуатаційних витрат на підтримку заходів захисту, регламентованих політикою безпеки.

В ході розрахунків з’ясовано, що введення в експлуатацію засобів та заходів захисту економічне доцільне для підприємства.

Для реалізації КСЗІ необхідно виконати впровадження запропонованих проектних рішень, провести попередні випробування, отримати дозвіл на експлуатацію та пройти державну експертизу.

ПЕРЕЛІК ПОСИЛАНЬ

1 Закон України "Про інформацію" [Електронний ресурс] // 2657-XII. – 01.01.2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12.

2 НД ТЗІ 1.6-005-2013 "Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці" [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://tzi.com.ua/nd-tz-1.6-005-2013.html.

3 Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [Електронний ресурс] // 80/94-ВР. – 19.04.2014. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-вр.

4 ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення." [Електронний ресурс]. – 1998. – Режим доступу до ресурсу: https://tzi.com.ua/478.html.

5 НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.1-003-99.pdf.

6 НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" [Електронний ресурс]. – 2005. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=46074&cat_id=38835.

7 НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.ua/ru/nd_tz_2.5-004-99.html.

8 НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від

несанкціонованого доступу" [Електронний ресурс]. – 28.04.1999. – Режим доступу до ресурсу: https://tzi.ua/ua/nd_tz_2.5-005-99.html.

9 НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу " [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106340.

10 НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі" [Електронний ресурс]. – 2000. – Режим Доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106341.

11. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека/Упорядн. Д. П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019.

12. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін , Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. –47 с

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість аркушів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Розділ 1. Стан питання. Постановка задачі.	43	
6	А4	Розділ 2. Спеціальна частина	21	
7	А4	Розділ 3. Економічна частина	13	
8	А4	Висновок	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А. Відомість матеріалів дипломної роботи	1	
11	А4	Додаток Б. Перелік документів на оптичному носії	1	
12	А4	Додаток В. Відгук керівника економічного розділу	1	
13	А4	Додаток Г. Відгук керівника дипломної роботи	1	
14	А4	Додаток Д. Порівняння КЗЗ	1	
15	А4	Додаток Е. Порівняння сервісів VPN	1	

ДОДАТОК Б. Перелік документів на оптичному носії

– Білова.Ю.О диплом.pptx
– Білова.Ю.О диплом.docx

ДОДАТОК В. Відгук керівника економічного розділу

Керівник економічного розділу к.е.н., доц. Пілова Д.П.

Дата: _____ Підпис: _____

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студентки групи 125-17-2
Білової Юлії Олексіївни
на тему: «Комплексна система захисту інформації інформаційно телекомунікаційної системи Дніпровського офісу ТОВ «Oxgaming»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 86 сторінках.

Метою кваліфікаційної роботи є забезпечення заданого рівня безпеки інформації, яка обробляється в ІТС Дніпровського офісу товариства з обмеженою відповідальністю «Oxgaming».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: обстеження середовищ функціонування ІТС, аналіз джерел загроз та вразливостей, виявлення актуальних загроз, формування вимог до рівня захищеності інформації від НСД, розробка проектних рішень та елементів політики безпеки. Обґрунтовано вибір КЗЗ та VPN системи. Практичне значення результатів кваліфікаційної роботи полягає у запропонованих налагодженнях операційної системи.

До недоліків роботи можна віднести недостатньо обґрунтований вибір КЗЗ.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Білова Ю.О. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» . Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки «відмінно».

Керівник кваліфікаційної роботи, професор **Кагадій Т.С.**

Керівник спец. розділу, ст. викладач **Кручінін О.В.**

ДОДАТОК Д. Порівняння КЗЗ

Назва КЗЗ	ОС	Функціолнальний профіль
Комплекс засобів захисту операційної системи Microsoft Windows 10 Professional – ТОВ «Майкрософт Україна».	Windows	КД-2, КВ-1, КО-1, ЦД-1, ЦА-1, ЦВ-1, ЦО-1, ДР-1, ДЗ-2, ДВ-2, НР-1, НР-2, НИ-1, НК-1, НО-3, НЦ-2, НТ-2, НВ-1
Комплекс засобів захисту програмного забезпечення «Операційна система Січ» – ТОВ «Трайбекс».	Linux	КД-2, КА-1, КА-2, КО-1, КВ-1, ЦД-1, ЦА-1, ЦА-2, ЦВ-1, ДР-3, ДС-1, ДЗ-2, ДВ-1, НР-2, НИ-2, НИ-3, НК-1, НО-3, НЦ-2, НВ-1
Комплекс засобів захисту програмного забезпечення «Операційна система Ubuntu*Pack 18.04»	Linux	КД-2, КА-1, КА-2, КО-1, КВ-2, ЦД-1, ЦА-1, ЦА-2, ЦВ-2, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-3, НИ-3, НК-1, НО-3, НЦ-2, НТ-3, НВ-1
Засіб технічного захисту інформації від несанкціонованого доступу «Комплекс «Гриф» версії 4»	Windows	КА-2, КО-1, КВ-2, ЦА-1, ЦО-1, ЦВ-2, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-3, НИ-3, НК-1, НО-2, НЦ-2, НТ-2

ДОДАТОК Е. Порівняння сервісів VPN

	ZenMate	Express VPN	NordVPN	Ivacy
Кількість стран	74	94	59	100
Кількість серверів	3800+	3000+	5800+	1000+
Додаток для ПК	+	+	+	+
Додаток iOs/Android	+	+	+	+
Розширення браузера	+	+	+	+
Кількість пристроїв на ліцензію	безліміт	5	6	5
Шифрування	AES-256	AES-256	AES-256	AES-256
Протоколи	OpenVPN, IPSec, IKEv2, L2TP	OpenVPN, L2TP/IPsec, PPTP	IKEv2/IPsec, OpenVPN, NordLynx	OpenVPN, L2TP, IKEv.
Ціна за місяць	$2.41	$6.67	$6.99	$3.50