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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Попова Анастасія Андріївна*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки інформаційно-телекомунікаційної системи ТОВ Fox Design Studio*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	проф. Корнієнко В.І.			
розділів:				
спеціальний	ст.вик. Тимофєєв Д.С.			
економічний	доц. Пілова Д.П.			

Рецензент				

Нормоконтролер				

Дніпро
2021

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

«_____»_____2021 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту ***Поповій А.А.*** **академічної групи** ***125-17-2***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Політика безпеки інформаційно-телекомунікаційної системи TOB Fox Design Studio***

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

Розділ	**Зміст**	**Термін виконання**
1. Стан питання. Постановка задачі	Проаналізувати проблеми захисту інформації в ІТС на малих підприємствах в ІТ сфері. Виконати аналіз нормативно-правових документів. Здійснити постановку задачі.	05.05.2021
2. Спеціальна частина	Виконати обстеження ОІД, категоріювання об'єкту. Створити моделі загроз та порушника. Обрати профіль захисту. Розробити основні елементи політики безпеки.	20.05.2021
3. Економічний розділ	Розрахувати економічну доцільність створення політики безпеки.	08.06.2021

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: ***10.01.2021***

Дата подання до екзаменаційної комісії: ***11.06.2021***

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 70 с., 9 рис., 21 табл., 7 додатків, 24 джерел.

Об'єкт дослідження: інформаційно-телекомунікаційна система “Fox Design Studio”

Предмет дослідження: політика безпеки інформації ІТС підприємства

Мета роботи: досягнення достатнього рівня захищеності інформації в ІТС підприємства.

Методи розробки: спостереження, порівняння, аналіз, опис.

В першому розділі кваліфікаційної роботи надано загальний аналіз проблем інформаційної безпеки світу та України, розглянуто стан інформаційної безпеки на малих підприємствах ІТ галузі.

В другому розділі кваліфікаційної роботи розглянуто необхідність розробки політики безпеки, стан інформаційної безпеки на теперішній час. Наведено загальні відомості про об’єкт інформаційної діяльності. Складено акт обстеження об’єкту інформаційної діяльності, обрано профіль захищеності. Розроблено моделі загроз та порушника, розроблено політику безпеки інформації.

В третьому розділі кваліфікаційної роботи розраховано доцільність використання розробки політки безпеки для ІТС “Fox Design Studio”.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, АКТ ОБСТЕЖЕННЯ, ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ, ПОКАЗНИК ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ.

РЕФЕРАТ

Объект исследования: информационно-телекоммуникационная система "Fox Design Studio"

Предмет исследования: политика безопасности информации ИТС предприятия

Цель работы: достижение достаточного уровня защищенности информации в ИТС предприятия.

Методы разработки: наблюдение, сравнение, анализ, описание.

В первом разделе квалификационной работы предоставлено общий анализ проблем информационной безопасности мира и Украины, рассмотрено состояние информационной безопасности на малых предприятиях ИТ отрасли.

Во втором разделе квалификационной работы рассмотрена необходимость разработки политики безопасности, состояние информационной безопасности в настоящее время. Приведены общие сведения об объекте информационной деятельности. Составлен акт обследования объекта информационной деятельности, избран профиль защищенности. Разработаны модели угроз и нарушителя, разработаны политику безопасности информации.

В третьем разделе квалификационной работы рассчитаны целесообразность использования разработки политики безопасности для ИТС "Fox Design Studio".

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИИ, ОБЪЕКТ информационной деятельности, модели угроз, МОДЕЛЬ НАРУШИТЕЛЯ, акт обследования, экономическая целесообразность, ПОКАЗАТЕЛЬ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ.

ABSTRACT

Object of research: information and telecommunication system "Fox Design Studio"

Subject of research: ITS information security policy of the enterprise

Purpose: achieving a sufficient level of information security in the ITS of the enterprise.

Development methods: observation, comparison, analysis, description.

The first section of the qualification work provides a general analysis of the problems of information security in the world and Ukraine, the state of information security in small enterprises of the IT industry.

The second section of the qualification work considers the need to develop a security policy, the state of information security at present. General information about the object of information activity is given. The act of inspection of the object of information activity is made, the profile of protection is chosen. Models of threats and violators have been developed, information security policy has been developed.

The third section of the qualification work calculates the feasibility of using the development of a security policy for ITS "Fox Design Studio".

COMPREHENSIVE INFORMATION PROTECTION SYSTEM, INFORMATION SECURITY POLICY, OBJECT OF INFORMATION ACTIVITY, THREAT MODEL, INTRUDER MODEL.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС - автоматизована система;

ДСТУ - державний стандарт України;

ІзОД — інформація з обмеженим доступом;

ІТС – інформаційно-телекомунікаційна система;

КЗЗ — комплекс засобів захисту;

КС — комп'ютерна система;

КСЗІ — комплексна система захисту інформації;

НД — нормативний документ;

НД ТЗІ - нормативний документ системи технічного захисту інформації;

НСД — несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ОС — обчислювальна система;

ПЗ — програмне забезпечення.

ЗМІСТ

ВСТУП

Об'єкт дослідження: інформаційно-телекомунікаційна система “Fox Design Studio”

Предмет дослідження: політика безпеки інформації ІТС підприємсвта

Мета роботи: досягнення достатнього рівня захищеності інформації в ІТС підприємства.

Інформація є одним з найцінніших активів сучасності у будь-якому підприємстві, саме тому вона потребує захисту. Технології невпинно розвиваються кожен день, що породжує потребу у нових способах захисту інформації до цього невідомих. Однак з тим злочинний світ теж не стоїть на місці. Разом з появою нових методів захисту інформації приходять і нові загрози та способи знайти слабкі місця у системах організацій, як великих, так і малих. Тому стан питання створення політики безпеки та комплексу захисту інформації є як ніколи актуальним.

Наразі підприємства разом зі їх інфраструктурою невпинно розвиваються, навіть швидше за їх засоби захисту, що дає змогу використовувати це як у дослідницьких цілях, так і задля отримання вигоди незаконним шляхом.

Ця проблема стосується як великих, так і малих компаній. Проте, коли великі компанії бачать загрозу для бізнесу та прибутків у недосконалому захисті інформації, що циркулює, малі швидше за все не приділяють цьому увагу. Проблема ж у тому, що як великі, так і малі компанії однаково схильні до одних і тих же загроз. Тут можна сказати, що захист великих компаній, які більше приділяють увагу захисту своїх активів важче обійти, проте і ймовірність заволодіти цінною інформацією, яка буде коштувати більше грошей також більша, на відміну від маленьких компаній, в яких слабка система захисту або ж повністю відсутня, але скоріше за все крадіжка такої інформації не принесе великого прибутку.

Захист інформації неможливий без якісного обстеження і аналізу на предмет тієї чи іншої загрози. Без використання нових технологій захисту інформації, інформація буде більше схильна до викрадення або спотворення.

Аналітичною компанією Canalys [1] було проведене дослідження на предмет стану захищеності інформації, та зробила висновки, що за 2020 рік було більше інцидентів, ніж за останні 15 років. А інвестиції в захист даних за 2020 рік збільшилися на 10% з попереднього року і становлять близько 53 мільярдів доларів.

Оскільки 2020 рік був переломним для всього світу, багато компаній перейшли на віддалену роботу. У зв'язку з цим збільшилися витрати на хмарні сховища (на 33%), покупку роутерів (на 40%), покупку веб-камер (продажи марки Logitech піднялися на 138%), також дохід компанії Zoom виріс у 3 рази.

Проблема використання вразливостей малих організацій є актуальною, тому що зазвичай ІТС в таких компаніях не защихена як слід або не захищена зовсім, що є легкою наживою для злодіїв. Більше того, за останній рік більшість IT компаній перейшла на віддалену роботу, що означає появу нових загроз та вразливостей.

Актуальність роботи полягає у необхідності вдосконалення організаційних методів захисту інформації на малих підприємствах шляхом впровадження адекватної політики безпеки інформації.

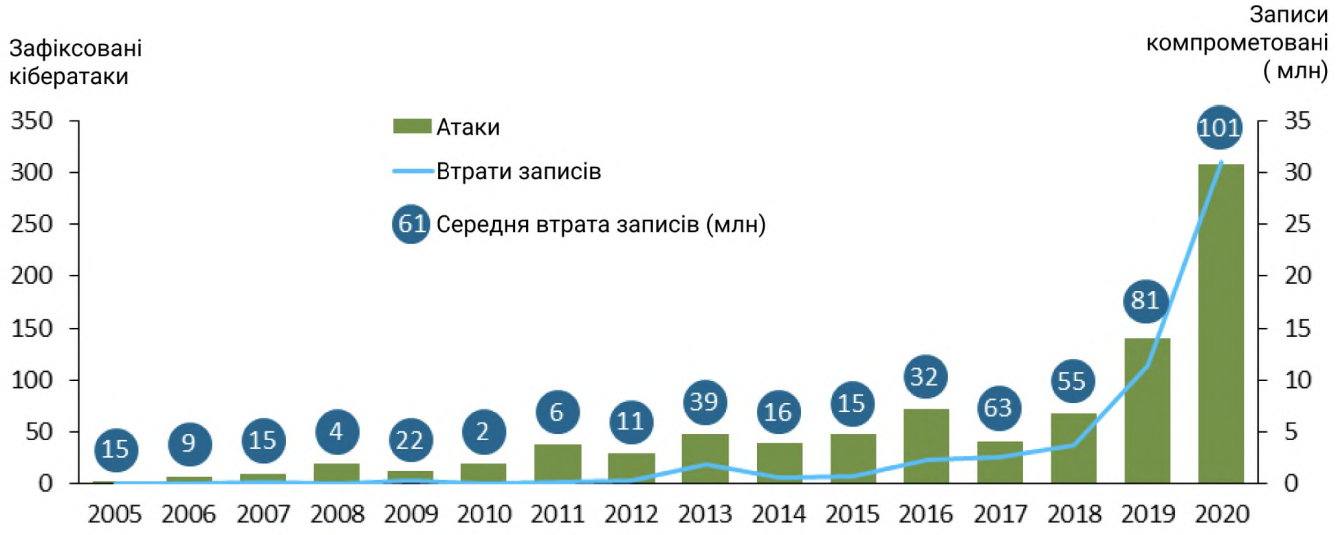

Рисунок 1.1 Зафіксовані кібератаки та втрати записів

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

За даними Національного альянсу з кібербезпеки США [2], 60% малих підприємств, які зазнали кібератаки, припиняють свою діяльність протягом півроку. Якщо кіберзлочинець успішно порушить дані малого бізнесу, то високі шанси на те, що цей бізнес закривається лише за півроку. Тому що малі підприємства найчастіше зовсім не готові до цього. Кібератаки коштують великих грошей, щоб вистояти. І, на жаль, більшість малих підприємств не можуть знайти кошти для цього.

Як не дивно, але 43% кібератак здійснюються проти малого бізнесу. І ця кількість серйозно зросла - лише кілька років тому це було лише 18%. Оскільки великі компанії приділяють більше ресурсів та стають все більш підкованими щодо кібербезпеки, кіберзлочинці, здається, в результаті звертаються до дрібного бізнесу.

І оскільки вони найчастіше переслідують гроші бізнесу, вони, як правило, націлені на працівника, який займається фінансами бізнесу або на внутрішніх працівників, які володіють результатами роботи компанії, комерційною таємницею.

Цього цілком достатньо, наприклад, для шантажу. Оскільки для малих організацій важливий кожей клієнт для створення хорошої репутації, вони готові погоджуватися з умовами злодіїв, аби не зганьбити своє ім'я. Звісно, це стосується лише тих 40%, які в змозі протистояти або вистояти після такої події. На жаль, інші 60% зникають менше ніж за рік.

Швидкість зростання кібератак на малий бізнес минулого року становить приголомшливих 424%. Це означає, що в минулому році кіберпорушення малого бізнесу зросли більш ніж у 5 разів порівняно з попереднім роком.

Це скоріш за все пов'язано з переходом більшості компаній на віддалену роботу у зв'язку з пандемією. Вся інформація у такому випадку обробляється на

сторонніх серверах, таких як Google, Dropbox та інші. Це доволі захищені сервіси, проте людський фактор, неуважність та соціальна інженерія мають місце бути.

Згідно з дослідженням, проведеним Hiscox, 66% малого бізнесу стурбовані ризиком кібербезпеки. Кібербезпека малого бізнесу - це те, на що слід звернути увагу, і цифри це підтверджують.

А саме це стосується Fox Studio — організації, яка вже затвердила себе на ринку та намагається надбати хорошу репутацію та створити для себе правильні процеси ведення бізнесу, у тому числі з точки зору кібербезпеки.

Сфера інформаційних технологій наразі є дуже важливою для України. Завдяки коштам, які поступають робітникам компаній з розробки дизайну та програмного забезпечення із-за кордону, виникає змога витрачати більше грошей усередині країни, що позитивно впливає на економіку.

А оскільки більшість організацій та компаній у сфері інформаційних технологій саме невеликі, за даними Dou.ua [3], то слід вважати, що саме на них тримається ця галузь.

Це є ще одним доказом того, наскільки важливим є створення та впровадження правильного функціонування політики інформаційної безпеки для кожного підприємства.

При створенні політики інформаційної безпеки необхідно брати до уваги деякі фактори, такі як:

- розміри компанії;
- фінансовий стан компанії;
- стан інформаційної безпеки на момент створення політики.

При створенні політики інформаційної безпеки слід дотримуватися основних вимог:

- системність;
- комплексність;
- адекватність;
- відкритість алгоритму;
- простота реалізації її на підприємстві.

Процеси та опис політики безпеки повинні бути простими і інтуїтивно зрозумілими, не вимагати особливих знань та навичок від співробітників організації, додаткових витрат при виконанні роботи або базуватися лише на принципах розподілення доступу, і до того треба, не змушувати користувача виконання рутинних малозрозумілих йому дій.

Політика інформаційної безпеки включає в себе:

- Базову політика інформаційної безпеки;
- Спеціальні політики інформаційної безпеки;
- Процедури забезпечення інформаційної безпеки.

1.2 Аналіз нормативно-правового забезпечення захисту інформації

У цьому розділі розглядаються правові норми, що визначають порядок створення, правовий статус і функціонування захищених інформаційно-комунікаційних систем і мереж, регламентують порядок одержання, перетворення та використання інформації і інформаційних ресурсів.

Створення КСЗІ базується на відповідності до вимог чинного законодавства України та на основі нормативно правових документів, серед яких можна виділити наступні.

1.2.1 Закон України "Про інформацію»

Цей Закон закріплює право громадян України на інформацію, закладає правові основи інформаційної діяльності. Дія цього Закону поширюється на інформаційні відносини, які виникають у всіх сферах життя і діяльності суспільства і держави при одержанні, використанні, поширенні та зберіганні інформації.

Закон встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації.

1.2.2 НД ТЗІ 1.1-002-99: Загальні положення з захисту інформації в комп'ютерних системах від НСД (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. No 22).

У цьому документі наведена інформація щодо заходів та засобів захисту інформації та їх впровадження. Також наведена інформація щодо керування доступом та концепції забезпечення захисту інформації.

1.2.3 НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. No 22).

У цьому документі містить перелік термінів та понять у сфері захисту інформації в ІТС від несанкційного доступу;

1.2.6 НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. No 22).

Цей документ встановлює критерії, за якими оцінюються стан захищеності інформації, яка обробляється в АС від несанкціонованого доступу;

1.2.7 ДСТУ ISO/IEC 27001:2015 - Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)- На заміну ДСТУ ISO/IEC 27001:2010.

У цьому документі наведені методи захисту інформації та системи управління інформаційною безпекою.

1.2.8 ДСТУ ISO/IEC 27005:2015 - (ISO/IEC 27005:2011, IDT).

У цьому документі наведена інформація щодо управління ризиками інформаційної безпеки.

1.2.9 Стандарти ДСТУ ISO/IEC, що засновані на міжнародних стандартах і відповідно до вимог, що висуваються до захисту інформації на підприємстві;

1.2.10 НД ТЗІ 1.6-005-2013

У цьому документі наведені положення про захист інформації на ОІД та інформацію про категоріювання об'єктів, де циркулює ІзОД, що не становить державної таємниці;

1.3 Постановка задачі

Задача базується на аналізі проблем у пункті 1.1, де було засвідчено проблему малого бізнесу в ІТ сфері. А саме проблема використання вразливостей малих організацій, які не приділяють увагу захищення інформації, що обробляється в їх ІТС. Відповідно до виконаного аналізу та вимог нормативних документів у спеціальній частині необхідно виконати наступні задачі:

- Ознайомитись з особливостями підприємства;
- Проаналізувати фізичні характеристики об'єкту;
- Проаналізувати логічну характеристику об'єкту;
- Проаналізувати види інформації та особливості взаємодії інформації на об'єкті;
- Обрати профіль захищеності;
- Розробити основні елементи політики безпеки.

Висновки до першого розділу

У першому розділі кваліфікаційної роботи було описано стан інформаційної захищеності в галузі інформаційних технологій, був проаналізований список нормативно-правових документів в сфері захисту інформації. Розкрито проблему та потребу у створенні політики безпеки на малих підприємствах. Серед етапів, які використані у кваліфікаційній роботі створення політики безпеки, виділені наступні згідно з нормативної документації:

- обґрунтування необхідності створення;
- обстеження на ОІД;
- аналіз та оцінка інформаційних загроз та розробка політики безпеки, що враховує загрози найвищого рівня.

Робота виконується з урахуванням нормативних документів та законів, наведені у пункті 1.2.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про типове підприємство

У якості типового об’єкта дослідження є інформаційно-телекомунікаційна система (ІТС) компанії “Fox Design Studio”, яка розробляє дизайн інтерфейсів мобільних додатків. Всі дані про підприємство були частково змінені в цілях забезпечення анонімності підприємства.

Повна юридична назва: ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ FOX DESIGN STUDIO

Форма власності: товариство з обмеженою відповідальністю.

Напрям діяльності: діяльність в області дизайну інтерфейсів мобільних додатків та веб сайтів, дослідження продуктів та консультативні послуги у сфері дизайну інтерфейсів.

Організаційна структура: організаційна структура підприємства зазначеного вище складається з:

- директора;
- арт-директора;
- 3 дизайнерів;
- бухгалтера;
- бізнес-аналітика;

На розглядаємому підприємстві ТОВ «Fox Design Studio» циркулює інформація з обмеженим доступом, а саме конфіденційна, що містить:

- персональні дані як клієнтів так і співробітників;
- штатний розклад компанії;
- заробітну платню працівників;
- вартість виконання робіт;
- інформація щодо організації процесів у компанії;
- інформація щодо розміщення та функціонування охоронної системи;

і комерційна таємниця, що містить вхідні дані для ведення проектів та результати роботи організації, а саме:

- технічні завдання;
- дизайн-файли у розробці;
- вихідні файли дизайнів.

2.2 Обґрунтування необхідності створення КСЗІ

Проведено категоріювання об'єкта, на основі якого було створено акт категоріювання об'єкта (ДОДАТОК А). Об'єкт відноситься до 4 категорії, що означає, відсутність потреби в обов'язковому створенні КСЗІ, але власник компанії створив наказ “Про визначення відповідального за забезпечення технічного захисту інформації та створення КСЗІ на ТОВ Fox Design Studio” (ДОДАТОК Б), за яким потрібно створити КСЗІ.

2.3 Організаційна структура підприємства

Кількість співробітників компанії - 7 чоловік:

- директор;
- арт-директор;
- 3 дизайнери;
- бухгалтер;
- бізнес-аналітик.

Обов’язки директора, який є власником компанії, — організаційні питання та умови договору з замовниками, вирішення проблем клієнтів, підбір персоналу; арт-директора – заступник директора, керування дизайнерами та бізнес-аналітиком; дизайнерів — виконання основної роботи — створення дизайну інтерфейсів мобільних додатків та веб сайтів; бізнес аналітика — дослідження продуктів та консультативні послуги у сфері дизайну інтерфейсів; бухгалтера — підготовка звітів по людино-годинах за місяць, розрахунок та виплата заробітної плати співробітникам.

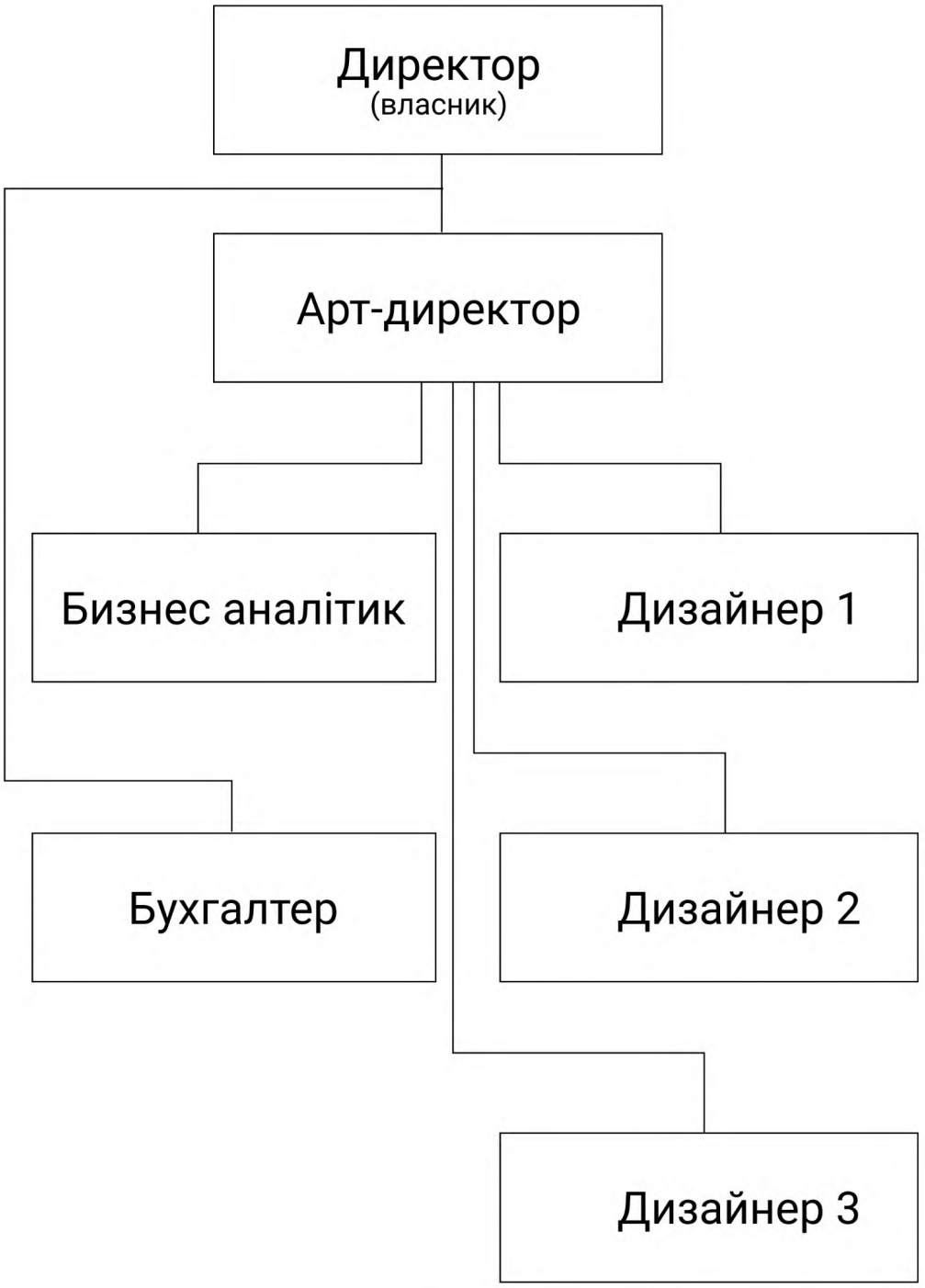

Рисунок 2.1 – Схема організаційної структури ТОВ Fox Design Studio

Також крім співробітників компанії “Fox Design Studio” задіяний обслуговуючий персонал компанії власника будівлі, а саме:

- 2 прибиральниці, які працюють позмінно;
- електрик;
- сантехник;
- 2 вахтери на КПП, які працюють позмінно.

За необхідністю їм може бути наданий доступ до ОІД.

2.4 Аналіз підприємства

В організації співробітниками обробляється інформація з обмеженим доступом: технічна документація, структури додатків, макети готового дизайну, трудові договори.

Вся документація існує лише в електронному вигляді, яка створюється працівниками у хмарному сховищі Google Drive за допомогою Google Docs. Після втрати чинності, документи знищуються. Дизайн проекти розробляються за допомогою сервісу Figma. Компанія не використовує зовнішніх носіїв інформації. Облік місця на підприємстві не відстежується. Детальний перелік інформації, правовий режим, вид зберігання та вимогу до захисту наведено у Таблиці 2.4.1

К – вимоги до конфіденційності, 3 - підвищена, 2 - середня, 1 - низька.

Ц – вимога до цілісності, 3 - підвищена, 2 - середня, 1 - низька.

Д – вимога до доступності, 3 - підвищена, 2 - середня, 1 - низька.

Таблиця 2.1 Інформація, що обробляється в ОІД

№	**Інформація**	**Режим доступу**	**Правовий режим**	**Вимоги до власт. інф.**		
				К	**Ц**	**Д**
1	Персональні дані робітників, клієнтів	Обмежений доступ	Конфіденційна	3	1	1
2	Штатний розклад компанії	Обмежений доступ	Конфіденційна	1	1	1
3	Інформація про заробітну платню працівників	Обмежений доступ	Конфіденційна	2	1	1
4	вартість виконання робіт	Обмежений доступ	Конфіденційна	3	1	1
5	інформація щодо організації процесів у компанії	Обмежений доступ	Конфіденційна	2	3	2
6	інформація про систему охорони	Обмежений доступ	Конфіденційна	3	1	1

Продовження таблиці 2.1

№	Інформація	Режим доступу	Правовий режим	Вимоги до власт. інф.		
				К	Ц	Д
7	Технічні завдання	Обмежений доступ	Комерційна таємниця	3	2	1
8	дизайн файли у розробці	Обмежений доступ	Комерційна таємниця	3	2	1
9	Вихідні файли дизайнів	Обмежений доступ	Комерційна таємниця	3	2	1
10	Дані заявки клієнта	Обмежений доступ	Комерційна таємниця	2	2	1

2.5 Обстеження об’єкту інформаційної діяльності

2.5.1 Ситуаційний план ОІД

Приміщення компанії, є об’єктом інформаційної діяльності (ОІД), що досліджується в кваліфікаційній роботі. Об'єкт інформаційної діяльності розташований на 1 поверсі 6-поверхового офісного будинку за адресою вул. Князя Ярослава Мудрого 3б

Контрольована зона (далі КЗ) обмежена зовнішніми стінами будівлі з півночі, заходу та сходу, а з південної сторони обмежена внутрішньою стіною (коридором) офісного будинку; знизу - підлогою, під якою розташована їдальня, а зверху - стелею.

Стіни будинку цегляні з залізобетонним перекриттям.

Територія навколо будинку огороджена невисоким парканом зі шлагбаумом, упорядкована, асфальтована, є місця для паркові місця для авто, які вказані на Рисунку 2.2

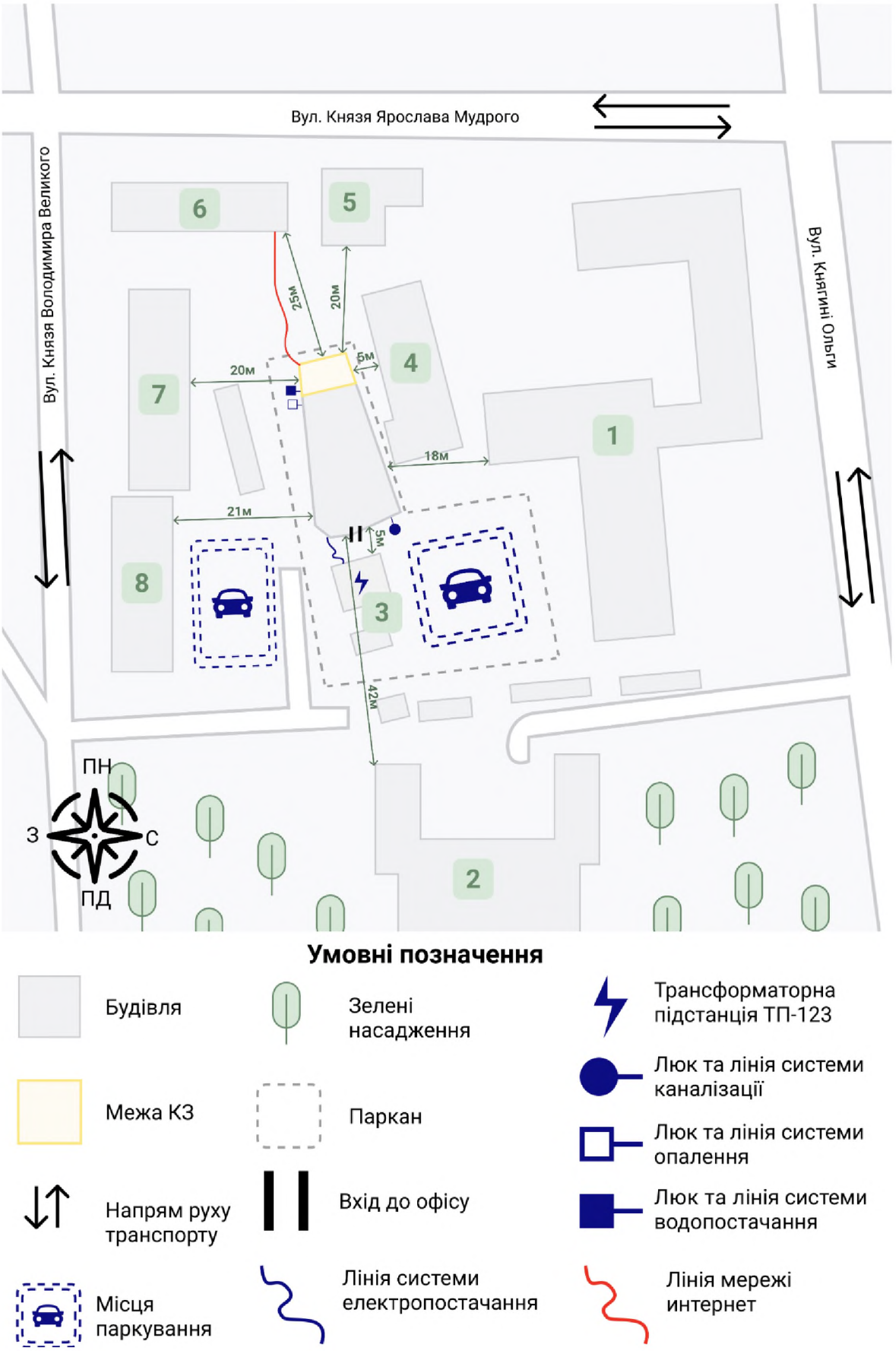

Рисунок 2.2 Схема ситуаційного плану ОІД

До даного будинку підключені наступні комунікації:

- електропостачання - від трансформаторної підстанції через підземні комунікації до розподільного щитка, який розташований на стіні всередині будинку біля входу до приміщення;
- каналізація та водооснащення - підключені до міських магістралей та заходять до підвального приміщення даного будинку;
- система опалення - централізована, труби стояку йдуть з 0 поверху до КЗ, а потім до офісів вище.

Схема заземлення зображена на Ситуаційному плані Рисунку 2. Заземлення іде від трансформаторної підстанції до розподільного щита. Безпосередньо у квартирі заземлення немає.

КЗ розташована в офісному будинку, комунікації, а саме труби системи опалення, лінія електропостачання та лінія комп'ютерної мережі виходять за межі КЗ. Інформація про навколишні будинки та споруди приведена у Таблиці 2.2.

Таблиця 2.2 Характеристика будівель та споруд.

№	Найменування	К-ть поверхів	Адреса	Відстань до ОІД, м
1	Лікарня	5	вул. Княгині Ольги,1	18
2	Театр	4	вул. Князя Святослава,1	42
3	Трансформаторна підстанція ТП-104	1	біля входу до КЗ	5
4	Житловий будинок	9	вул. Володимира Великого,10а	5
5	Житловий будинок	9	вул. Ярослава мудрого, 6	20
6	Житловий будинок	9	вул. Ярослава мудрого, 8	25
7	Житловий будинок	9	вул. Володимира Великого, 8	20
8	Житловий будинок	9	вул. Володимира Великого, 6	21

Прилеглі вулиці відносно ОІД вказані у Таблиці 2.3.

Таблиця 2.3 Прилеглі вулиці відносно ОІД

Назва	Опис
вул. Ярослава Мудрого	Відносно ОІД вулиця розташована на півночі. Автомобільний трафік становить 150 - 230 машин на годину.
вул. Княгині Ольги	Відносно ОІД вулиця розташована на сході. Автомобільний трафік становить 100 - 180 машин на годину.
вул. Володимира Великого	Відносно ОІД вулиця розташована на заході. Автомобільний трафік становить 100 - 180 машин на годину.

2.5.2 Опис генерального плану:

- площа ОІД: 27м²;
- висота стелі – 2,45м. Поверх – 1-ий;
- стеля (матеріал – бетон, товщина – 0,5м.), підлога (матеріал – бетон+кахель, товщина – 1м.), стіни (матеріал – цегла+гіпсокартон, товщина 0,5м);
- вікно (к-кість – 6шт, матеріал – пластик (полівінілхлорид або ПВХ)), розміри: 2м х 1,3м. Вікна виходять на двір. Сектор прямої видимості – це парковка та ближні жилі будинки;
- лінія електропостачання іде до поверхового щитка ЩО-1, а звідти — до основного електрощитка ;
- сигналізація підключена до ПКП біля КПП;
- лінія комп'ютерної мережі — оптичний кабель: Wi-Fi роутер підключений до мережевого обладнання провайдеру;
- система опалення – горизонтальна.

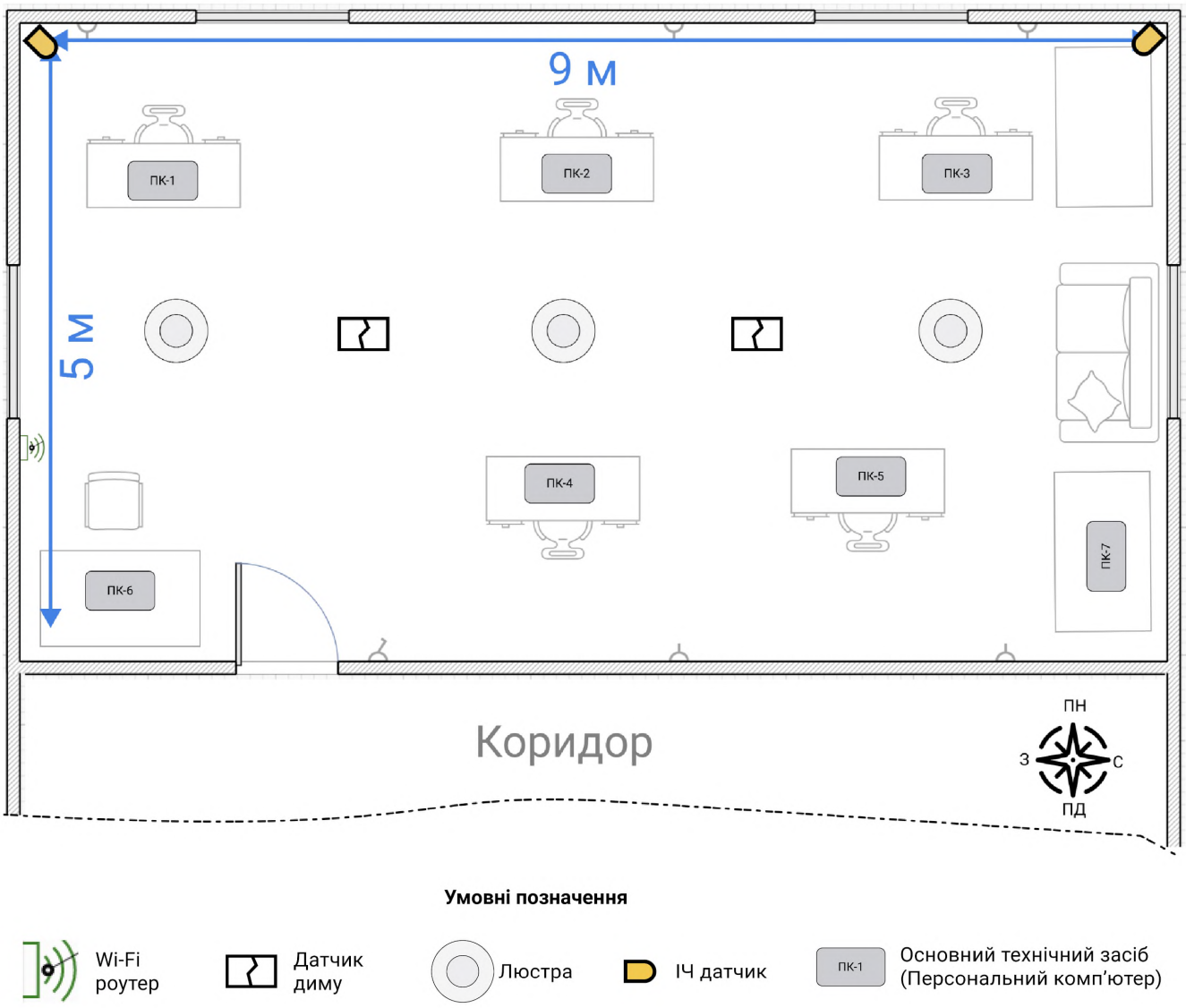

Рисунок 2.3 Генеральный план

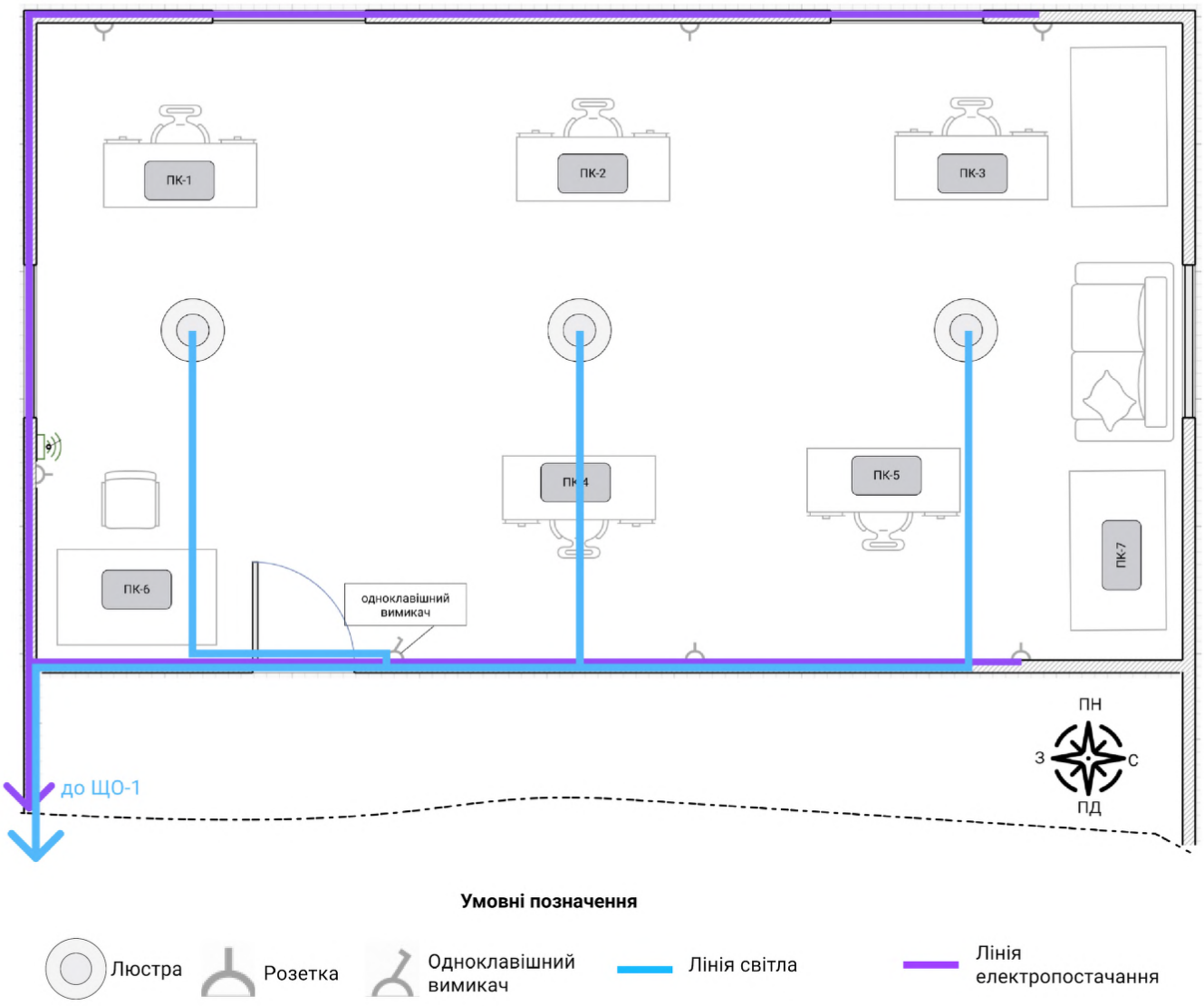

Рисунок 2.4. Генеральный план. Схема систем електропостачання та освітлення

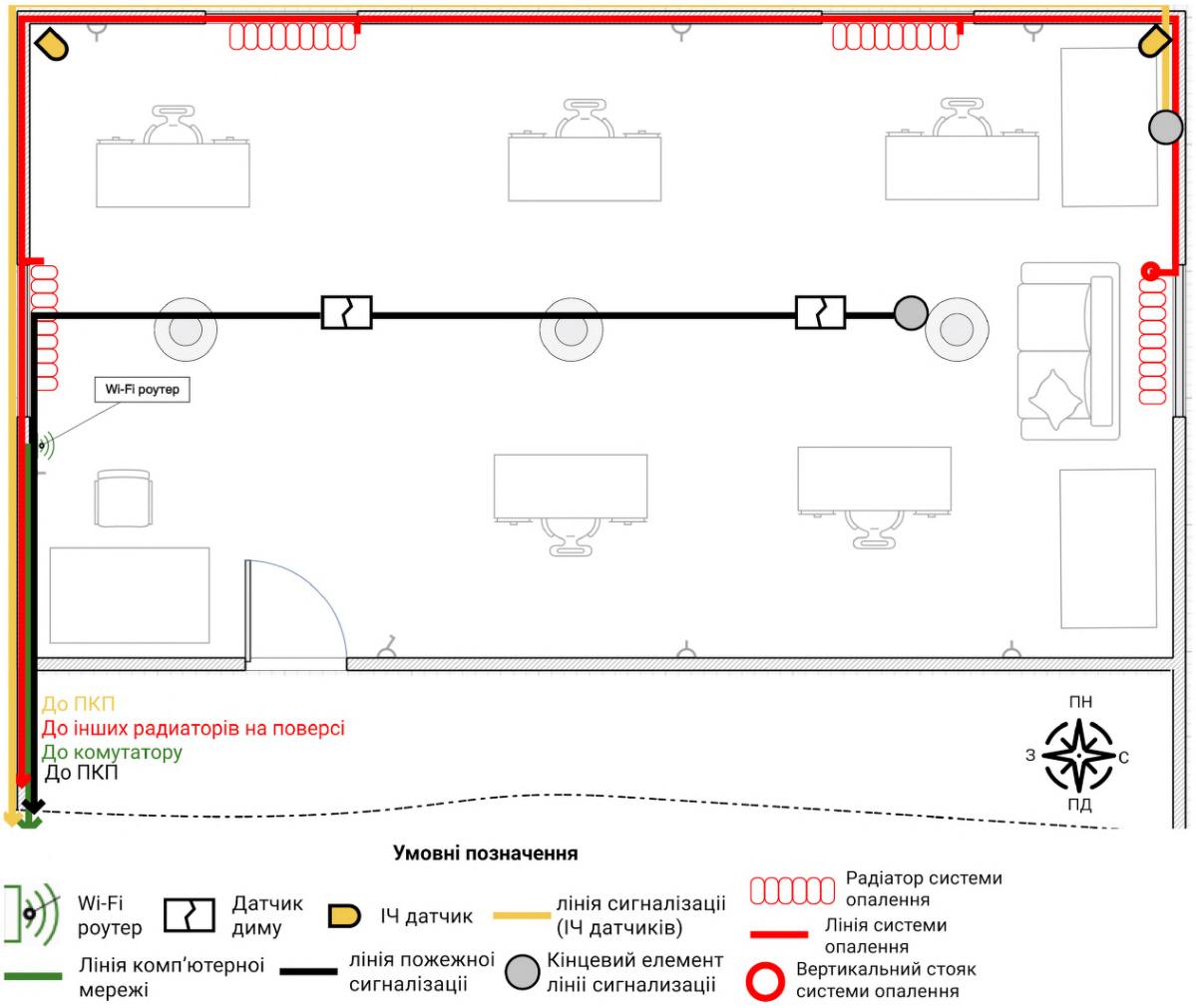

Рисунок 2.5. Генеральный план. Схеми ліній комп'ютерної мережі, системи сигналізації та системи опалення

Режим КЗ забезпечується таким чином:

- у робочий час забезпечується співробітниками охоронної організації та системою контролю управління доступом. Чергові знаходяться біля контрольно пропускного пункту, біля входу;
- у неробочий час забезпечується силами охорони з використанням засобів відеоспостереження, гратів на вікнах, вхідними металопластиковими дверями, які закриваються на ключ. Також застосовується автономна сигналізація приміщень всього будинку, яка підключена до приймально-контрольного пристрою, який знаходяться біля чергових, ПКП. Чергові мають тривожну кнопку, яка

застосовується для виклику наряду поліції. Сигналізація КЗ входить до составу системи сигналізації всієї будівлі.

Комунікаційні системи КЗ вказані у Таблиці 2.4. Вони також відображені на генеральному плані (Рисунки 2.3-2.5).

Таблиця 2.4 Комунікаційні системи

Вид комунікації	Характеристика
Система електропостачання	від трансформаторної підстанції через підземні комунікації до розподільного щитка, який розташований на стіні всередині будинку біля входу до приміщення.
Система опалення	Централізована, труби стояку йдуть з 0 поверху до КЗ, а потім до офісів вище.
Система каналізації	Підключені до міських магістралей та заходять до підвального приміщення даного будинку.
Система водопостачання	
Телефонна лінія та Інтернет	Підключені до інтернет-провайдера “Воля”. Кабель локальної мережі являє собою неекранована вита пара (1000BASE-T) категорії 5e
Система сигналізації	Складається з датчиків руху (пасивні інфрачервоні), датчиків диму, система відеоспостереження, пропускні електронні пункти. Адмініструється службою безпеки власника будівлі.

Опис технічних засобів підприємства наведений у Таблиці 2.5.

Таблиця 2.5 Технічні засоби

№	Назва	Марка	Модель	Розміщення	Серійний номер	Відстань до границі КЗ, м
1	Портативний комп'ютер	Apple	Pro 2019	На столі	BU3456BK	1
2	Портативний комп'ютер	Apple	Pro 2019	На столі	GI4567NH	1
3	Портативний комп'ютер	Apple	Pro 2019	На столі	GF5678GP	1
4	Портативний комп'ютер	Apple	Pro 2019	На столі	FO5329WF	1
5	Портативний комп'ютер	Apple	Pro 2019	На столі	FI3569SM	1
6	Портативний комп'ютер	Apple	Pro 2019	На столі	PO4346FI	1
7	Портативний комп'ютер	Apple	Pro 2019	На столі	FJ1394FP	1
8	Wi-Fi роутер	Mikrotik	hAP RB951Ui-2ND	На стіні	MA3831HD	0

Засоби ДТЗС вказані в таблиці 2.6

Таблиця 2.6 Опис допоміжних технічних засобів

№	Назва	Модель	Розміщення	Відстань до границі КЗ, м
1	Светильник светодиодный настенно-потолочный накладной с пультом (3)	W-625/72W RM WW+NW+CW	на стелі	0
2	Датчик диму (2)	СТРАЖ М-501	на стелі	0
3	ІЧ датчик (2)	Страж М-302	на стіні	0

2.6 Опис обчислювальної системи

Опис обчислювальних систем, що використовуються на ОІД, наведено в Таблиці 2.7.

Таблиця 2.7 Опис обчислювальної системи

№	Специфікація	Назва в системі
1	CPU: 2,6 GHz 6-Core Intel Core i7 | 16 GB 2400 MHz DDR4 | 1TB SSD | Видеокарта: Radeon Pro 560X 4 GB Serial number: BU3456BK	ПК-1
2	CPU: 2,6 GHz 6-Core Intel Core i7 | 16 GB 2400 MHz DDR4 | 1TB SSD | Видеокарта: Radeon Pro 560X 4 GB Serial number: GI4567NH	ПК-2
3	CPU: 2,6 GHz 6-Core Intel Core i7 | 16 GB 2400 MHz DDR4 | 1TB SSD | Видеокарта: Radeon Pro 560X 4 GB Serial number: GF5678GP	ПК-3
4	CPU: 2,6 GHz 6-Core Intel Core i7 | 16 GB 2400 MHz DDR4 | 1TB SSD | Видеокарта: Radeon Pro 560X 4 GB Serial number: FO5329WF	ПК-4
5	CPU: 2,6 GHz 6-Core Intel Core i7 | 16 GB 2400 MHz DDR4 | 1TB SSD | Видеокарта: Radeon Pro 560X 4 GB Serial number: FI3569SM	ПК-5
6	CPU: 2,6 GHz 6-Core Intel Core i7 | 16 GB 2400 MHz DDR4 | 1TB SSD | Видеокарта: Radeon Pro 560X 4 GB Serial number: AO2349JF	ПК-6
7	CPU: 2,6 GHz 6-Core Intel Core i7 | 16 GB 2400 MHz DDR4 | 1TB SSD | Видеокарта: Radeon Pro 560X 4 GB Serial number: FK4579LF	ПК-7

Програмне забезпечення обчислювальних систем наведено у таблиці 2.8

Таблиця 2.8 Встановлене програмне забезпечення

№	ПО	Версія	Де встановлено	Ліцензія
1	MacOs	11.2.3 (Big Sur)	ПК-1-7	Придбана
2	Figma	98.13	ПК-2-5	Придбана
3	Вбудований антивірус	1.3.32	ПК-1-7	Придбана
4	Google Chrome	90.0.4430.212	ПК-1-7	Безкоштовний

На рисунку 2.6 зображена схема інформаційної системи ОІД ТОВ “Fox Design”.

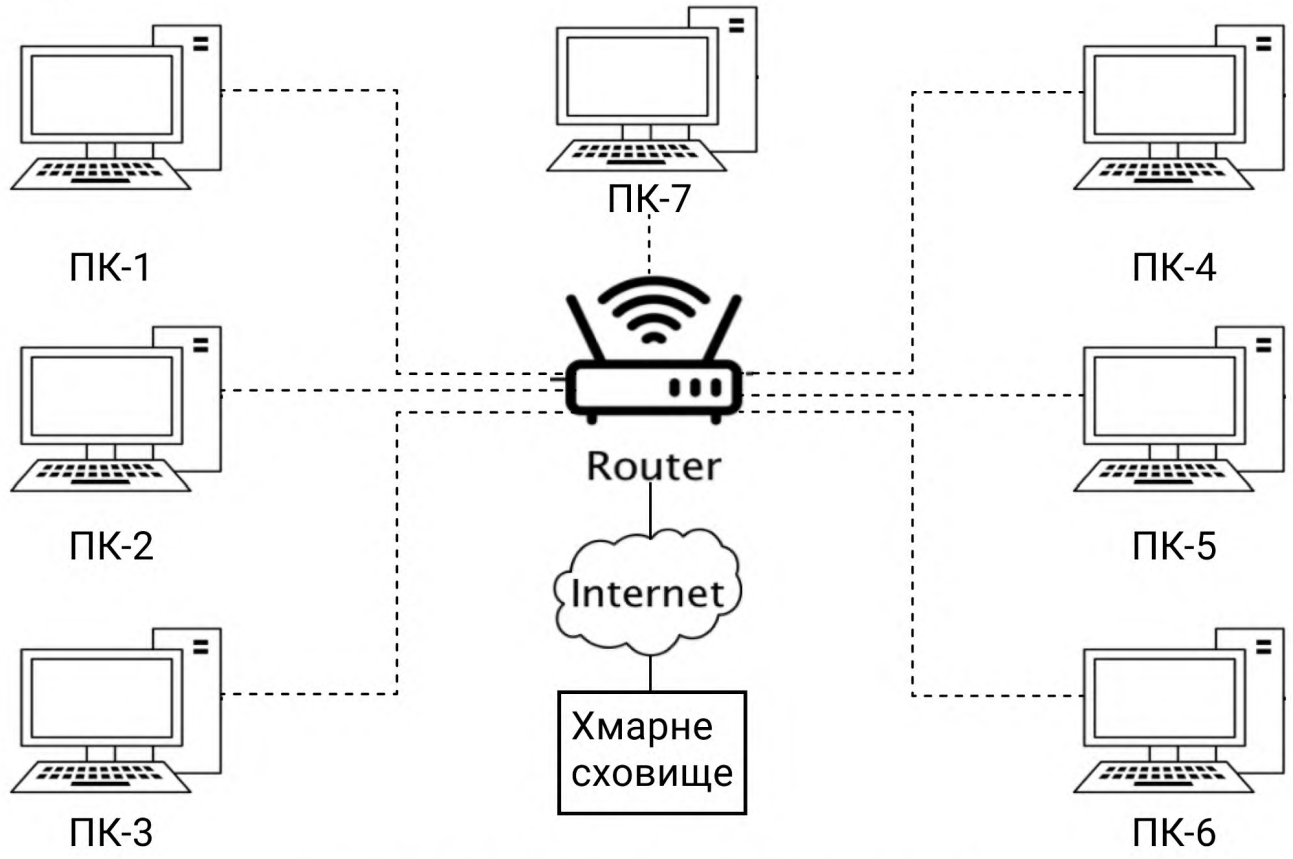

Рисунок 2.6 Схема інформаційних системи

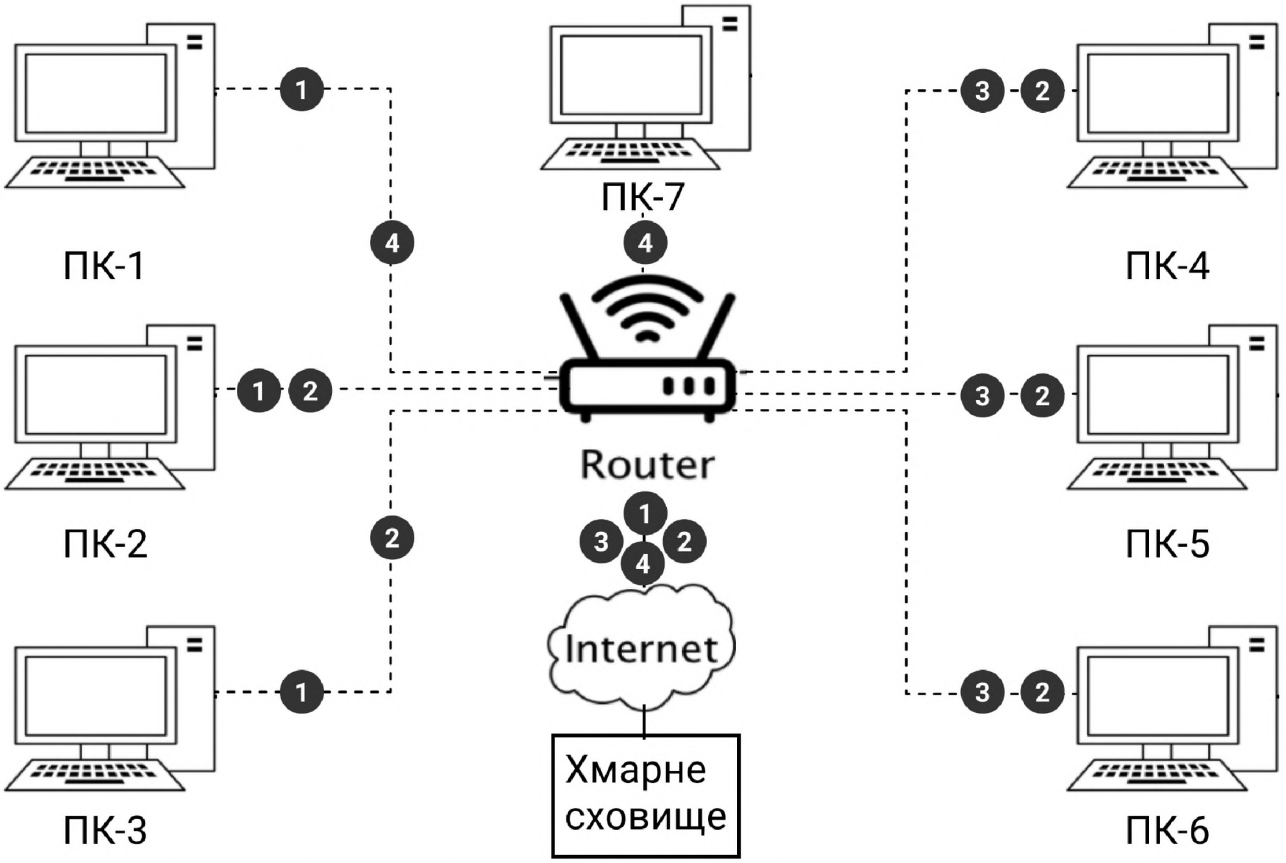

Рисунок 2.7 Схема інформаційних потоків

1 — робота з клієнтом; 2 —постановка задач; 3 — розробка дизайн проектів; 4 — обробка бухгалтерських звітів

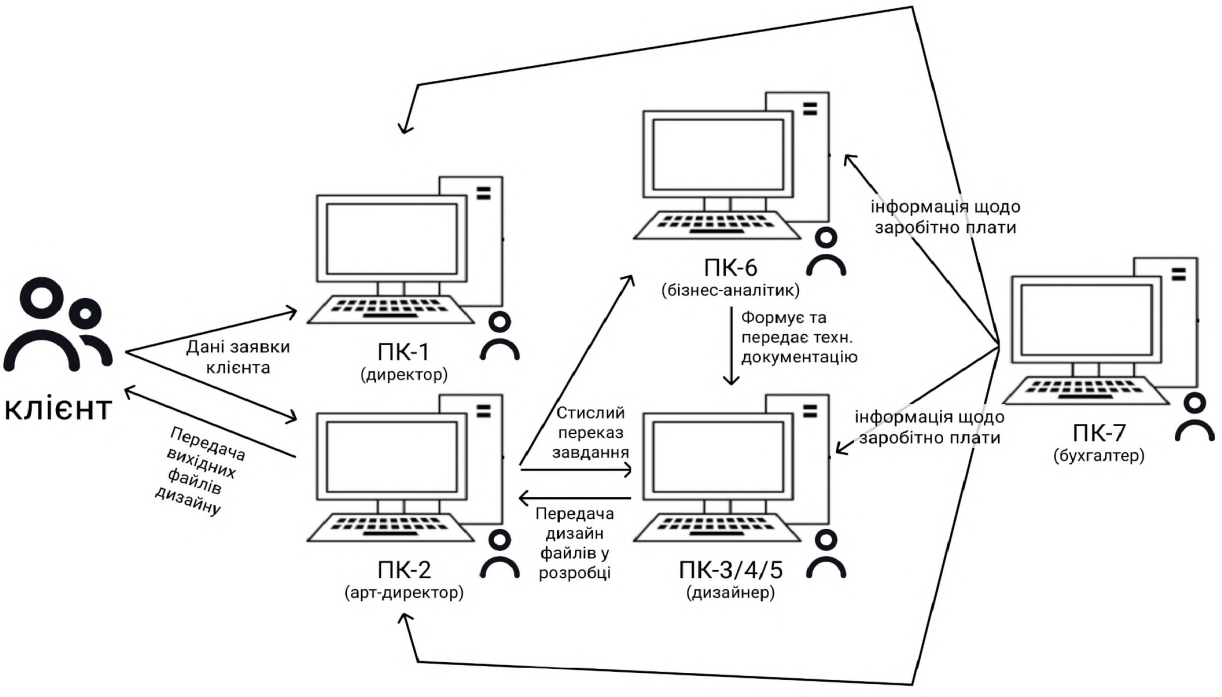

Рисунок 2.8 Схема бізнес процесів

2.7. Аналіз загроз та вразливостей

На цьому етапі здійснюється аналіз ризиків, а саме опрацювання моделі загроз і моделі порушника, припущення можливих наслідків від реалізації потенційних загроз. Також визначається перелік критичних загроз, що є метою етапу формування завдання на створення КСЗІ.

Цей етап аналізу суттєвості загроз інформаційної безпеки виконаний на основі нормативного документу ДСТУ ISO/IEC 27005:2015 - Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT) з урахуванням особливостей діяльності підприємства.

Аналіз загроз та вразливостей включає в себе:

- модель порушника;
- модель загроз;
- ідентифікація наслідків реалізації загроз; - оцінка ризиків та ймовірності їх появи.

2.8. Модель порушника

Особа, що намагається отримати несанкціонований доступ до об'єктів захисту з ціллю їх ознайомлення, зміни, знищення тощо є порушником.
Порушників можна умовно поділити на дві групи:

- Зовнішні;
- Внутрішні;

До зовнішніх порушників відносяться особи, які знаходяться за межами ІТС. Це можуть бути конкуренти та крадії або персонал з обслуговування приміщення, особи, яким не передбачено доступ до ІзОД, але які мають доступ до приміщень, де розміщено компоненти ІТС і можуть отримати доступ до ІзОД, наприклад, клінінг, електрики тощо.

До внутрішніх порушників відносяться особи, що мають можливість фізичного підключення до каналів зв’язку або інших складових мережі передачі даних, користувачі АС, персонал, який безпосередньо пов’язан із забезпеченням функціонування ІТС.

В таблиці 10 наведені категорії порушників, що використовуються при створенні моделі. Модель порушника наведена зі специфікаціями за різними показниками:

- за мотивами здійснення порушень;
- за рівнем кваліфікації та обізнаності щодо ІТС;
- за показником можливостей використання засобів ІТС для реалізації загроз;
- за часом та місцем дії.

Профіль порушника визначає сукупність цих характеристик.

Таблиця 2.9 Рейтингова оцінка рівня загроз:

Рейтингова оцінка	Опис
0	не становить загрози
1	незначний
2	низький
3	середній
4	високий
5	критичний

Спираючись на отримані результати аналізу характеристик обробляємої інформації, категорій порушників, що мають потенційну можливість порушення конфіденційності та цілісності інформації, вважаються найбільш небезпечними, доступності - менш небезпечними, а спостережності - найменш небезпечними.

Таблиця 2.10 Категорії порушників. Внутрішні по відношенню до ІТС.

Позначення	Визначення категорії	Рівень загроз
ПВ0	Директор	0
ПВ1	Бухгалтер	2
ПВ2	Дизайнери, бізнес-аналітик	3
ПВ3	Арт-директор	4

Таблиця 2.11 Категорії порушників. Зовнішнішні по відношенню до ІТС

Позначення	Визначення категорії	Рівень загроз
П30	Відвідувачі	1
П31	Комунальні служби, служби з питань благоустрою	1
П32	Вахтери, сантехнік, електрик, прибиральниці	1

Таблиця 2.12 Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність, помилка	1
М2	Самоствердження	1
М3	Корисний інтерес	1

Таблиця 2.13 Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Рівень кваліфікації	Рівень загроз
К1	Низький рівень знань, вміння працювати з компонентами ІТС	1
К2	Середній рівень знань, має практичний досвід з роботи з компонентами ІТС та їх обслуговування	2

Таблиця 2.14 Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту (обізнаність щодо використання технічних засобів розвідки)

Позначення	Характеристика можливостей порушника	Рівень загроз
30	Не має навичок	0
31	Підглядання за робочим процесом	1
32	Взлом, підбір паролю до облікових записів	2

Таблиця 2.15 Специфікація моделі порушника за часом дії

Позначення	Час дії	Рівень загроз
Ч1	Під час призупинення використання компонентами ІТС (залишити ноутбук в офісі та піти)	2
Ч2	Під час ремонту компонентів ІТС	1
Ч3	Під час роботи компонентів ІТС	1
Ч4	У будь-який час, маючи доступ до інформації у хмарному сховищі (до обл. зап.)	2

Таблиця 2.16 Специфікація моделі порушника за місцем дії

Позначення	Час дії	Рівень загроз
МД1	Робочі місця робітників	2
МД2	У приміщенні, де розташовані ІТС	2
МД3	У будь-якому місці, маючи доступ до інформації у хмарному сховищі	2

Профілі порушників всіх категорій наведено у Таблиці 2.17, у колонці «Сума загроз» наведено рейтингову оцінку загроз порушника з відповідними характеристиками.

Таблиця 2.17 Профілі можливостей порушників

Посада	Кат. пор.	Мотив поруш.	Можливості	Рів.обіз. ІТС	Час	Місце	Сума загроз
Директор	**ПВ0**	**М1**	**З0**	**К2**	**Ч3**	**МД1**	6
	0	1	0	2	1	2	
Бухгалтер	**ПВ1**	**М1**	**З1**	**К2**	**Ч3**	**МД1**	8
	1	1	1	2	1	2	
Дизайнер, Бізнес аналітик	**ПВ2**	**М1**	**З2**	**К2**	**Ч3**	**МД1**	11
	3	1	2	2	1	2	
Арт-директор	**ПВ3**	**М1**	**З2**	**К2**	**Ч3**	**МД1**	12
	4	1	2	2	1	2	
Відвідувачі	**П30**	**М3**	**З1**	**К1**	**Ч1**	**МД2**	8
	2	1	1	1	1	2	
Комунальні служби	**П31**	**М3**	**З1**	**К1**	**Ч3**	**МД2**	7
	1	1	1	1	1	2	
прибиральниці, сантехник, електрик, вахтери	**П32**	**М3**	**З1**	**К1**	**Ч3**	**МД2**	7
	1	1	1	1	1	2	

Найбільшу загрозу представляють внутрішні робітники організації, а саме Арт-директор, дизайнери та бізнес-аналітик, оскільки вони мають безпосередній доступ до системи ІТС та працюють з її компонентами.

2.9. Модель загроз

За результатами впливу на інформацію та систему її обробки, загрози поділяються на чотири класи:

1) Порушення конфіденційності інформації (К) - отримання інформації користувачами або процесами всупереч встановленим правилам розмежування доступу до інформації.

2) Порушення цілісності інформації (Ц) - повне або часткове знищення, викривлення, модифікація інформації, нав'язування хибної інформації тощо.

3) Порушення доступності інформації (Д) - часткова або повна втрата працездатності системи, блокування доступу до інформації в результаті некоректних дій адміністраторів, технічного обслуговуючого персоналу.

4) Втрата спостережності (керованості системою) (С) - порушення процедур ідентифікації та автентифікації адміністраторів або процесів і надання їм повноважень, втрата контролю за їх діяльністю, можливість відмови від отримання або пересилання повідомлень.

Потенційно загрози можуть завдати шкоди обробляємої інформації, працівникам, клієнтам, технічним засобам і процесам. Загрози також можна поділити на:

- навмисні (Н);
- випадкові (В);
- природні (П).

Потрібно ідентифікувати як випадкові, так і навмисні джерела загроз. Загрози можуть бути ідентифіковані в загальному вигляді або за типами.

Таблиця 2.18 Шкала оцінки ймовірності реалізації загрози

Оцінка ймовірності	Характеристика
1	Виникнення інциденту практично неможливо
2	Виникнення інциденту малоймовірне (не частіше ніж 1 раз на 1 рік)
3	Виникнення інциденту ймовірне до 1 разу на 3 місяці
4	Виникнення інциденту ймовірне до 1 разу на тиждень
5	Виникнення інциденту ймовірне до 1 разу на добу

Зроблено якісну оцінку ймовірності реалізації загрози та визначено сукупний рівень загрози. Результати аналізу викладені в таблиці 2.19.

Таблиця 2.19.1 Результати аналізу загроз та вразливостей інформації в ІТС. Навмисні загрози (антропогенні та техногенні)

№	Джерело	Вразливість	Загроза	Ймовірність	Порушення	Рівень загрози	Загальн о
1	Внутрішнє	Вразлива система охорони; Порушення правил використання КС; Відсутність системи розмежування доступом.	Несанкціонований доступ до ІзОД	3	КЦДС	4	3,5
2	Внутрішнє	Зловживання повноважень адміністраторів системи; Помилки при розмежуванні доступу.	Порушення правил розмежування доступу	3	КЦДС	4	3,5
3	Внутрішнє	Відсутність політики безпеки, яка регулює правила копіювання інформації; Порушення правил встановлених політикою безпеки.	Копіювання ІзОД без дозволу	3	КЦДС	5	4

Продовження таблиці 2.19.1

4	Внутрішнє	Відсутність політики безпеки, яка регулює використання дозволених програмних засобів; Порушення правил встановлених політикою безпеки.	Крадіжка ІзОД шляхом використання електронної пошти, месенджерів, файлообмінників	2	КЦДС	3	2.5
5	Внутрішнє	Відсутність Антивірусних програмних засобів; Наявність неконтрольовани х каналів витоку інформації.	Впровадження і використання комп'ютерних вірусів, закладних програм для порушення безпеки даних	2	КЦДС	3	2.5
6	Внутрішнє	Погано підібраний персонал; Низька заробітна плата та мотивації співробітників	Соціальна інженерія	2	КЦДС	2	2
7	Внутрішнє	Відсутність Політики використання КС; Порушення, встановлених політикою безпеки, правил.	Використання КС не в цілях ведення бізнесу	4	КЦДС	1	2.5
8	Внутрішнє	Відсутність політики інформаційної безпеки	Неправомірне використання КС	4	КЦДС	2	3

Продовження таблиці 2.19.1

9	Внутрішнє	Вразлива система охорони; Поганий контроль за системами відеоспостереження; Відсутність планової та позапланової інвентаризації КС; Відсутність контролю цілісності компонентів КС.	Навмисне порушення цілісності та працездатності КС	1	КЦДС	4	2.5
10	Внутрішнє	Відсутність або вразливість системи розмежування прав користувачів; Піратське ПЗ; Недосконалість системи розмежування доступом.	Втручання та/або зміна ПЗ(видалення, блокування, встановлення, редагування, архівування)	3	КЦДС	3	3
11	Внутрішнє	Відсутність політики, яка регулює використання дозволених програмних засобів; Наявність неконтрольованих каналів передачі даних.	Використання ПЗ, які заборонені політикою безпеки	5	КЦДС	3	4

Таблиця 2.19.2 Результати аналізу загроз та вразливостей інформації в ІТС. Випадкові загрози

№	Джерело	Вразливість	Загроза	Ймовірність	Порушення	Рівень загрози	Загально
1	Внутрішнє	Низький рівень кваліфікації користувачів; Доступ до елементів, які не використовуються у бізнес процесах; Відсутність спеціалістів, які забезпечують працездатність мережі, її елементів, обладнання.	Не навмисні дії користувачів, що призводять до відмови функціонування мережі чи окремих її елементів, пошкодження обладнання	2	КЦДС	3	2.5
2	Внутрішнє	Порушення цілісності інформації, що зберігається, внаслідок не навмисних дій користувачів	Некомпетентність персоналу з питання користування КС; Застарілі ПЗ; Відсутність резервного копіювання.	2	КЦДС	2	2
3	Внутрішнє	Відсутність резервного копіювання	Ненавмисне пошкодження носіїв інформації чи інформації, яка зберігається на цих носіях	2	КЦДС	5	3.5
4	Внутрішнє	Відсутність або застарілість антивірусного ПЗ.	Випадкове зараження програмних засобів комп'ютерними вірусами	1	КЦДС	3	2

Продовження таблиці 2.19.3

5	Внутрішнє	Відсутність політики безпеки або розділу у політиці безпеки про регулювання дозволених ПЗ; Відсутність системи адміністрування дозволених ПЗ.	Використання ПЗ, які заборонені політикою безпеки	3	КЦДС	3	3
6	Внутрішнє	Відсутність резервного копіювання; Використання піратських ПЗ	Порушенні цілісності інформації, що зберігається внаслідок апаратного або програмного збою	3	ЦД	4	3.5

Таблиця 2.19.3 Результати аналізу загроз та вразливостей інформації в ІТС. Стихійні фактори

№	Джерело	Вразливість	Загроза	Ймовірність	Порушення	Рівень загрози	Загально
1	Зовнішнє	Пошкодження фундаменту; Застарілі лінії забезпечення.	Землетрус	1	ЦД	3	2
2	Зовнішнє	Старе приміщення; Пошкодження фундаменту.	Повінь	1	ЦД	2	2
3	Зовнішнє	Наявність легкозаймистих речовин; Відсутність протипожежної системи.	Пожежа	2	ЦД	3	2.5
4	Зовнішнє	Відсутність заземлення, стабілізаторів напруги, громовідводів.	Грозові розряди	1	ЦД	3	2

Серед найбільш критичних загроз можна виділити наступні:

- Несанкціонований доступ до ІзОД;
- Копіювання ІзОД без дозволу;
- Відсутність резервного копіювання;
- Використання піратських ПЗ;
- Використання ПЗ, які заборонені політикою безпеки;

2.10 Профіль захищеності

Проаналізувавши основні характеристики ІТС об'єкту кваліфікаційної роботи, та вимог до властивостей інформації, відповідно до НД ТЗІ 2.5-004-99 зі змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 No 806 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

АС підприємства – АС «3» класу. Тобто, це розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу. Для даної АС «3» класу обрано наступний профіль захищеності:

3.КЦ.1 = { КД-1, КА-3, КО-1, КК-1, КВ-2,
ЦД-1, ЦА-3, ЦО-1, ЦВ-2,
ДР-1, ДС-1, ДЗ-1, ДВ-2,
НР-2, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2, НА-1, НП-1 }

Таблиця 2.20 Профіль захищеності

№	Послуга	Назва	Опис
1	КД-2	Базова довірча конфіденційність	Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта.
2	КА-3	Повна адміністративна конфіденційність	Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості управління. Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права отримувати інформацію від об'єкта .

Продовження таблиці 2.20

3	КО-1	Повторне використання об'єктів	Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.
4	КК-1	Виявлення прихованих каналів	Аналіз прихованих каналів виконується з метою виявлення і усунення потоків інформації, які існують, але не контролюються іншими послугами. Рівні даної послуги ранжируються на підставі того, чи виконується тільки виявлення, контроль або перекриття прихованих каналів. Всі приховані канали, які існують в апаратному і програмному забезпеченні, а також в програмах ПЗП, повинні бути документовані. Має бути документована максимальна пропускна здатність кожного знайденого прихованого каналу, одержана на підставі теоретичної оцінки або вимірів. Для прихованих каналів, які можуть використовуватися спільно, повинна бути документована сукупна пропускна здатність.
5	КВ-2	Базова конфіденційність при обміні	Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Політика конфіденційності при обміні, що реалізується КЗЗ, повинна відноситись до всіх об'єктів і існуючих інтерфейсних процесів. Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається. Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження.

Продовження таблиці 2.20

			Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу. Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу.
6	ЦД-1	Мінімальна довірча цілісність	Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації.
7	ЦА-3	Повна адміністративна цілісність	Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Політика адміністративної цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта. Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження. КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта.

Продовження таблиці 2.20

8	ЦО-1	Обмежений відкат	Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат. Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.
9	ЦВ-2	Базова цілісність при обміні	Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається, а також фактів його видалення або дублювання. Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу.

Продовження таблиці 2.20

10	ДР-1	Квоти	Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС. Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.
11	ДС-1	Стійкість при обмежених відмовах	Стійкість до відмов гарантує доступність КС (можливість використання інформації, окремих функцій або КС в цілому) після відмови її компонента. Рівні даної послуги ранжируються на підставі спроможності КЗЗ забезпечити можливість функціонування КС в залежності від кількості відмов і послуг, доступних після відмови. Розробник повинен провести аналіз відмов компонентів КС Політика стійкості до відмов, що реалізується КЗЗ, повинна визначати множину компонентів КС, до яких вона відноситься, і типи їх відмов, після яких КС в змозі продовжувати функціонування. Повинні бути чітко вказані рівні відмов, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги. Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг, а має в гіршому випадку проявлятися в зниженні характеристик обслуговування. КЗЗ повинен бути спроможний повідомити адміністратора про відмову будь-якого захищеного компонента.

Продовження таблиці 2.20

12	ДЗ-1	Модернізація	Ця послуга дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів. Рівні даної послуги ранжируються на підставі повноти реалізації. Політика гарячої заміни, що реалізується КЗЗ, повинна визначати політику проведення модернізації КС Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість провести модернізацію (upgrade) КС. Модернізація КС не повинна призводити до необхідності ще раз проводити інсталяцію КС або до переривання виконання КЗЗ функцій захисту.
13	ДВ-2	Автоматизоване відновлення	Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення. Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС. Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування.

Продовження таблиці 2.20

14	НР-2		Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень. Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються. КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє або непряме відношення до безпеки. Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події. КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.
15	НИ-2	Одиночна ідентифікація і автентифікація	Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації. Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму. КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

Продовження таблиці 2.20

16	НК-1	Одно направлений достовірний канал	Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін. Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.
17	НО-2	Розподіл обов'язків адміністраторів	Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів. Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконує певні дії, що підтверджують прийняття їм цієї ролі.
18	НЦ-3		Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами. Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів. КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування. КЗЗ повинен гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ

Продовження таблиці 2.20

19	НТ-2	Самотестування при старті	Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжируються на підставі можливості виконання тестів у процесі запуску або штатної роботи. Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ і в процесі штатного функціонування.
20	НВ-2	Аутентифікація джерела даних	Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації. Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації. КЗЗ повинен використовувати захисні механізми для встановлення джерела кожного об'єкта, що експортується та імпортується.

Продовження таблиці 2.20

21	НА-1	Базова автентифікація відправника	Ця послуга дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною. Політика автентифікації відправника, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-відправника і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем. Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації.
22	НП-1	Базова аутентифікація отримувача	Ця послуга дозволяє забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною. Політика автентифікації одержувача, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-одержувача і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був одержаний певним користувачем. Встановлення одержувача має виконуватися на підставі затвердженого протоколу автентифікації.

2.11 Розробка політики безпеки інформації

Спираючись на отримані результати аналізу моделі загроз та порушників і дивлячись на на показники профілю захищеності, розроблено базові елементи політики безпеки інформації для типового підприємства.

У таблиці 2.21 представлено перелік основних загроз, та відповідних політик, що спрямовані на забезпечення захисту від них.

Таблиця 2.21 Перелік основних загроз, відповідних політик інформації

№	Загроза	Назва політики	Опис
1	Несанкціонований доступ до ІзОД	5 Політика чистого робочого столу	5.3.1 Співробітники повинні забезпечити, щоб уся конфіденційна інформація була захищена в робочій зоні наприкінці дня та коли, як очікується, їх немає на тривалий період. 5.3.2 Комп'ютерні робочі станції повинні бути заблоковані, коли робоча область не зайнята.
3	Копіювання ІзОД без дозволу	7 Політика користування інтернетом	Використання, передача, тиражування або добровільне отримання матеріалів, що порушують авторські права, торгові марки, комерційну таємницю або патентні права будь-якої особи або організації. Припустимо, що всі матеріали в Інтернеті захищені авторським правом та / або запатентовані, якщо в конкретних повідомленнях не зазначено інше.
4	Відсутність резервного копіювання;	3 Антивірусна політика	3.1.7 Регулярно створювати резервні копії критичних даних та конфігурацій системи та зберегти їх у безпечному місці.

Продовження Таблиці 2.21

5	Використання піратських ПЗ	2 Політика встановлення програмного забезпечення	2.3.1 Співробітники не можуть встановлювати програмне забезпечення на обчислювальні пристрої Компанії, що працюють у мережі Компанії. 2.3.2 Запити на програмне забезпечення повинні спочатку схвалити менеджер запитувача, а потім надіслати їх до відділу інформаційних технологій або довідкової служби в письмовій формі або електронною поштою.
6	Використання ПЗ, які заборонені політикою безпеки		

Наведені пункти політики безпеки підвищують ефективність забезпечення захисту інформації в ІТС.

Висновки до другого розділу

У другій частині кваліфікаційної роботи наведені загальні відомості про підприємство ТОВ “Fox Design Studio”. Спираючись на проведений аналіз обробляємої інформації, був створений акт обстеження об'єкта. Результатом обстеження ОІД став аналіз загроз та вразливостей підприємства. Таким чином, показана необхідність розробки політики безпеки інформації. На актуальних загроз ОІД були розроблені елементи політики безпеки інформації, що циркулює на ОІД.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Економічне обґрунтування доцільності впровадження політики безпеки інформації

Для економічного обґрунтування доцільності розробки політики безпеки інформації ТОВ “Fox Design Studio” потрібно провести розрахунки, щоб визначити економічну ефективність використання основних результатів, які будуть отримані після розрахунків.

Економічна доцільність визначається:

- розрахунками капітальних витрат, що потребує розроблена політика безпеки;
- розрахунками експлуатаційних витрат;
- розрахунками річного економічного ефекту від розробки інформаційної політики

безпеки.

3.1.1 Розрахунок суми витрат на розробку політики безпеки інформації.

Спочатку розраховується трудомісткість розробки політики безпеки інформації, для цього потрібно скласти час, який знадобиться для кожної робочої операції:

$$t = tmз + tв + ta + tвз + tозб + tовр + tд, \text{ годин, де}$$

- t*mз* - тривалість складання ТЗ на розробку ПБІ = 72 години;
- *tв* - тривалість розробки концепції безпеки інформації у організації = 36 годин;
- *ta* - тривалість процесу аналізу ризиків = 48 годин;
- t*вз* - тривалість визначення вимог заходів, методів та засобів захисту = 24 години;
- t*озб* - тривалість виробу основних рішень з забезпечення БІ = 96 годин;
- t*овр* - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організацій = 164 години;
- *tд* - тривалість документального оформлення політики безпеки = 38 годин.

$$t = 72 + 36 + 48 + 24 + 96 + 164 + 38 = 478 \text{ годин.}$$

3.1.2 Розрахунок суми витрат на реалізацію політики безпеки інформації.

Сума витрат на розробку політики безпеки (***Крп***) складається з витрат на:

- Заробітну плату спеціаліста з кібербезпеки — ***Ззп,*** грн;
- Вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації — Змч.

$$Крп = Ззп + Змч = 26423{,}5 \text{ грн}$$

Заробітна плата спеціаліста складається з основної та додаткової заробітної плати, соціальних виплат та визначається за формулою:

$$Ззп = t \cdot Зіб = 23762{,}575 \text{ грн}$$

де t – загальна тривалість розробки політики безпеки інформації = 478 годин;

Зіб – середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями = 7954 / 160 = 49,7125 грн/годину [25].

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$Змч = t \cdot Смч = 2661 \text{ грн}$$

де t – трудомісткість підготовки документації на ПК =4 години;

Смч – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot tнал \cdot Се + Фзал \cdot На / Fр + Клпз \cdot Напз / Fр = 5{,}6 \text{ грн.}$$

де P – встановлена потужність ПК = 0,058 кВт;

Се – тариф на електричну енергію = 1,68 грн/кВт · година [24];

Фзал – залишкова вартість ПК на поточний рік = 14200 грн;

На – річна норма амортизації на ПК = 50% частки одиниці;

Напз – річна норма амортизації на ліцензійне програмне забезпечення = 0,1 частки одиниці;

Клпз – вартість ліцензійного програмного забезпечення = 28400 грн;

Fр – річний фонд робочого часу (за 40-годинного робочого тижня Fр = 1920)

Сума амортизації:

$$A = \frac{Ф_п - Ф_{лікв}}{T}$$

де Фп - первісна вартість = 28400 грн

Флікв - ліквідаційна = 0 грн

Т - термін корисної дії = 2 роки

А = (28400-0)/2=14200

Норма амортизації:

$$H_a = \frac{Ф_п - Ф_{лікв}}{Ф_п \cdot T} \cdot 100\%$$

На = (28400)/2*28400*100%=50%

Фзал = Фп - А = 28400-14200 = 14200 грн

Програмний засіб	**Вартість, грн**
Clean my Mac	4200
Figma Professional для 5 працівників	24200
Загально	28400

Відповідно до розроблених рекомендацій, планується використання ліцензійних програмних засобів, як вже встановлених, так і нових.

Розрахована вартість розробки політики безпеки інформації ***Крп*** є складовою одноразових капітальних витрат разом з витратами на придбання програмних засобів, які рекомендовані для використання.

Отже фіксована сума капітальних витрат на розробку політики безпеки інформації складає:

$$К = Крп + Кзпз + Кпз + Каз + Кнавч + Кн = 60423{,}5 \text{ грн.}$$

де *Кпр* – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх спеціалістів, тис. грн;

Кзпз – вартість закупівель ліцензійного основного і додаткового програмного забезпечення (ПЗ), тис. грн;

Крп – вартість розробки політики безпеки інформації, тис. грн;

Каз – вартість закупівли апаратного забезпечення та допоміжних матеріалів, тис. грн;

Кнавч – вартість витрати на навчання технічних фахівців і обслуговуючого персоналу = 5600 грн;

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

3.2.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$C = C_в + C_к + C_{ак} = 52614 \text{ грн.}$$

де $C_в$ - вартість відновлення й модернізації системи $C_в = 0$;

$C_к$ - витрати на керування системою в цілому;

$C_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки = $C_{ак} = 0$ грн.

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

$$C_к = C_н + C_а + C_з + C_{ел} + C_о + C_{тос} = 52614 \text{ грн}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються = Сн = 5600 грн.

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

$$C_з = З_{осн} + З_{дод} \text{ , грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 7 954 грн. Додаткова заробітна плата – 10% від основної заробітної плати.

З 01.01.2019 р. Ставка ЄСВ для всіх категорій платників складає 22%. Виконання роботи потребує залучення спеціаліста на 0,25 ставки

Отже,

$$С_з = (7954*12+7954*12*0,1)*0,25*1,22=32022,8 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року (*Сел*), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е = 0,058 \cdot 1920 \cdot 1,68 = 90 \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,058 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,68 грн./кВт за годину).

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1%

$$С_{тос} = К \cdot 1\% = 604,2 \text{ грн}$$

Річний фонд амортизаційних відрахувань: $С_а = А$ = 14200 грн

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 52614 грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 3 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 4 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі 4 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 5500 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 11000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особа;

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

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 2 млн грн. у рік;

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

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 14.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U=П_п+П_в+V=13764,4,$$

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

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

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

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:

$$П_П = \frac{\sum Зс}{F} \cdot t_П \quad ,$$

$$Пп = ((11000 * 7)/176) * 3 = 1312{,}5 \text{ грн},$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

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

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де Пви – витрати на повторне уведення інформації, грн.;

Ппв – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

Пзч – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації Пви розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу tви:

$$Пви = \Sigma Зс / F * tви$$

$$П_{ви} = ((11000 * 7)/176) * 4 = 1750 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі Ппв визначаються часом відновлення після атаки tв і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$Пвп = \Sigma Зо / F * t_в$$

$$П_{вп} = ((5500 * 1)/176) * 4 = 125 \text{ грн.}$$

Витрати на заміни устаткування або запасних частин можуть скласти 3200 грн.

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$П_в = 1312,5 + 1750 + 125 = 1875$ грн.

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

$$V = \frac{O}{F_Г} \cdot (t_П + t_В + t_{ВИ})$$

$$V = (2000000/2080)* (3+4+4) = 10577 \text{ грн.}$$

де $F_Г$ – річний фонд часу роботи компанії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

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

$$B = \sum_i \sum_n U$$

$$B = 1 * 14 * 13764,4 = 19270 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B * R – C$$

де – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці = 57%;

C – щорічні витрати на експлуатацію системи інформаційної безпеки. Загальний ефект від впровадження системи інформаційної безпеки

визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 19270* 0,57 – 52614 = 57226$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = E / K, \text{ частки одиниці}$$

де – E загальний ефект від впровадження системи інформаційної безпеки грн.;
K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$57226 / 60423{,}5 = 0{,}95$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$ROSI > (N_{деп} – N_{інф})/100$,
де $N_{деп}$ – річна депозитна ставка, (23%);
$N_{інф}$ – річний рівень інфляції, (14%).
Розрахункове значення коефіцієнта повернення інвестицій:
$0{,}95 > (23 – 14)/100 = 0{,}95 > 0{,}09$

Термін окупності капітальних інвестицій To показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років}$$

T = 1/0,95 = 1.05 років.

Висновок

Розробка політики інформаційної безпеки для ТОВ «Fox Design Studio» є економічно доцільною, оскільки коефіцієнт повернення інвестицій ROSI складає

0,95, що означає отримання 0,95 грн. економічного ефекту на кожну гривню капітальних вкладень на розробку політики інформаційної безпеки підприємства. Отримане значення коефіцієнту повернення інвестицій значно вище дохідності альтернативного вкладення коштів. Термін окупності при цьому складатиме 1,05 років (біля 12 місяців). Капітальні витрати складають 60423,5 грн.

ВИСНОВКИ

У першому розділі кваліфікаційної роботи було описано стан інформаційної захищеності в галузі інформаційних технологій, був проаналізований список нормативно-правових документів в сфері захисту інформації. Розкрито проблему та потребу у створенні політики безпеки на малих підприємствах. Серед етапів, які використані у кваліфікаційній роботі створення політики безпеки, виділені наступні згідно з нормативної документації:

- обґрунтування необхідності створення;
- обстеження на ОІД;
- аналіз та оцінка інформаційних загроз та розробка політики безпеки, що враховує загрози найвищого рівня.

У другій частині кваліфікаційної роботи наведені загальні відомості про підприємство ТОВ “Fox Design Studio”. Спираючись на проведений аналіз обробляємої інформації, був створений акт обстеження об'єкта. Результатом обстеження ОІД став аналіз загроз та вразливостей підприємства. Таким чином, показана необхідність розробки політики безпеки інформації. На актуальних загроз ОІД були розроблені елементи політики безпеки інформації, що циркулює на ОІД.

У третьому розділі кваліфікаційної роботи був проведений розрахунок економічної доцільності розробки політики безпеки інформації. Розробка політики інформаційної безпеки для ТОВ «Fox Design Studio» є економічно доцільною, оскільки коефіцієнт повернення інвестицій ROSI складає 0,95, що означає отримання 0,95 грн. економічного ефекту на кожну гривню капітальних вкладень на розробку політики інформаційної безпеки підприємства. Отримане значення коефіцієнту повернення інвестицій значно вище дохідності альтернативного вкладення коштів. Термін окупності при цьому складатиме 1,05 років (біля 12 місяців). Капітальні витрати складають 60423.5грн.

ПЕРЕЛІК ПОСИЛАНЬ

1. Статистика кібератак на підприємства [Електронний ресурс]. - Режим доступу https://techexpert.ua/cyber-attacks-number-statistics/
2. Статистика кібератак на малі підприємства за 2021 рік [Електронний ресурс]. - Режим доступу https://www.fundera.com/resources/small-business-cyber-security-statistics#
3. Інформація щодо IT компаній, які ведуть бізнес на території України [Електронний ресурс]. - Режим доступу https://jobs.dou.ua/ratings/
4. Закон України «Про інформацію» від 02.10.1992 No 2657-XII // Відомості Верховної Ради України. - 1992. - No 48. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2657-12 Класифікація “інформації в законодавстві України”.
5. Закон України “Про захист персональних даних” від 01.06.2010 No 2297-VI // Відомості Верховної Ради України. - 2010. - No 5. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2297-17.
6. Закон України “Про доступ до публічної інформації” від 13.01.2011 No 2939-VI // Відомості Верховної Ради України. - 2011. - No 32. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2939-17.
7. Закон України “Про захист інформації в інформаційно- телекомунікаційних системах” від 05.07.1994 No80-VI // Відомості Верховної Ради України. -
8. 1994. - No 80. [Електронний ресурс]. - Режим доступу http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
9. ДСТУ ISO/IEC 27002:2015 [Електронний ресурс] // ДСТУ. - 2015. - Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911.
10. ДСТУ ISO/IEC 27005:2017 [Електронний ресурс] // ДСТУ. - 2017. - Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66912.
11. НД ТЗІ 3.7-003 - Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно - телекомунікаційній системі. -

[Чинний від 08.11.2005] - К. : ДССЗЗІ, 2005. - No125 - (Нормативний документ системи технічного захисту інформації).

12. НД ТЗІ 1.4-001 - Типове положення про службу захисту інформації в автоматизованій системі. - [Чинний від 04.12.2000] - К. : ДСТСЗІ СБУ, 2000. - No53 - (Нормативний документ системи технічного захисту інформації).
13. НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. - [Чинний від 28.04.1999] - К. : ДСТСЗІ СБУ, 1999. - No22 - (Нормативний документ системи технічного захисту інформації).
14. НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. - [Чинний від 28.04.2000] - К. : ДСТСЗІ СБУ, 2000. - No22- (Нормативний документ системи технічного захисту інформації).
15. НД ТЗІ 1.6-005 - Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. - [Чинний від 15.04.2013] - К. : ДССЗЗІ, 2013. - No125 - (Нормативний документ системи технічного захисту інформації).
16. Етапи створення КСЗІ [Електронний ресурс] - Режим доступу до ресурсу:http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive-zavdannya-sogodennya/.
17. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека/Упоряд. Д. П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019.
18. Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека / О.В. Герасіна, Д.С.Тимофєєв, О.В. Кручинін, Ю.А.Мілінчук – Дніпро: НТУ "ДП", 2020. – 47 с.

19. НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. - [Чинний від 28.04.1999] - К. : ДСТСЗІ СБУ, 1999. - No22 - (Нормативний документ системи технічного захисту інформації).
20. НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. - [Чинний від 28.04.2000] - К. : ДСТСЗІ СБУ, 2000. - No22- (Нормативний документ системи технічного захисту інформації).
21. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2–004–99. – Київ: ДСТСЗІ СБ України, 1999. – 55 с.
22. Інформація щодо середньої заробітної плати спеціаліста з кібербезпеки. [Електронний ресурс]. - Режим доступу https://ua.trud.com/ua/salary/2/67683.html
23. Актуальні ціни на електроенергію [Електронний ресурс]. - Режим доступу https://yasno.com.ua/b2c-tariffs
24. Середня заробітна плата спеціаліста з кібербезпеки [Електронний ресурс]. - Режим доступу https://ua.trud.com/ua/salary/2/67682.html

ДОДАТОК А. Акт категоріювання

Гриф обмеження доступу
Прим. No ___
ЗАТВЕРДЖУЮ
Керівник установи-власника (розпорядника, користувача) об’єкта
директор Слобода М. О.
(посада, підпис, ініціали, прізвище)

АКТ
категоріювання ***ТОВ “Fox Design Studio”***
(найменування об’єкта категоріювання)

1. Підстава для категоріювання _____
(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання,
_____
зміна ознаки, за якою була встановлена категорія об’єкта, тощо;
_____
посилання/реквізити на розпорядчий документ про призначення комісії з категоріювання)

2. Вид категоріювання _____***первинне***_____
(первинне, чергове, позачергове)
_____
(у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання; посилання/реквізити на документ, яким було встановлено цю категорію)

3. На ОІД здійснюється ***обробка інформації технічними засобами***_____

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об’єкті _____ конфіденційна***інформація***_____
(передбачена законом таємниця (крім державної); службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України “Про доступ до публічної інформації”; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом)

5. Встановлена категорія___***4 категорія, до четвертою категорії відносяться об'єкти, в яких циркулює службова та конфіденційна інформація, вимога щодо захисту якої встановлена законом***_____

Голова комісії _____ Члени комісії: _____ __.__.20__
(ініціали, прізвище,підпис) (ініціали, прізвище,підпис)

ДОДАТОК Б. Наказ

НАКАЗ

м. Дніпро

05.03.2021 №1

Про створення комплексної системи захисту інформації в автоматизованій системі класу «3» ІТС ТОВ “Fox Design Studio”

На виконання вимог статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (зі змінами) та п.16 «Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджених Постановою Кабінету Міністрів України від 26.03.2006 року No 373 (зі змінами).

НАКАЗУЮ:

1.Створити комплексну систему захисту інформації в автоматизованій системі класу «3» для обробки інформації з обмеженим доступом.

2. Відповідальному за службу захисту інформації в автоматизованих системах Михайлову І.С., забезпечити супроводження робіт зі створення комплексної системи захисту інформації.

3. Контроль за виконанням наказу покласти на заступника та арт-директора компанії Міщенко Н. В.

Директор Слобода М.О.

ДОДАТОК В. Перелік документів на оптичному носії

1 Пояснювальна_записка_Попова.doc

2 Пояснювальна_записка_Попова.pdf

3 Презентація_Попова.pptx

4. Презентація_Попова.pdf

ДОДАТОК Г. Відгук керівника економічного розділу

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Д. Розроблена політика безпеки

ЗАТВЕРДЖУЮ

Керівник установи-власника

(розпорядника, користувача) об’єкта

Директор _____
(ініціали, прізвище,підпис)

__.__.20__

Політика безпеки інформації в ІТС ТОВ “Fox Design Studio”

2021 р.

м. Дніпро

ЗМІСТ

1 Вступ

Цей Політичний документ охоплює всі аспекти безпеки навколо конфіденційної інформації про товариство з обмеженою відповідальністю “Fox Design Studio” (далі – Компанія) і повинен бути розповсюджений серед усіх працівників компанії. Усі працівники компанії повинні повністю прочитати цей документ і підписати форму, яка підтверджує, що вони прочитали та повністю розуміють цю політику. Цей документ буде розглядатися та оновлюватися керівництвом щорічно або, коли це доречно, для включення нещодавно розроблених стандартів безпеки до політики та повторного розповсюдження серед усіх працівників та підрядників, де це можливо

1.1 Огляд політики інформаційної безпеки

Компанія надає послуги з розробки дизайну интерфейсів мобільних додатків. Керівництво Компанії прагне зберегти конфіденційність, цілісність та доступність усіх фізичних та електронних інформаційних активів у всій своїй організації, щоб забезпечити дотримання законних, нормативних та договірних норм та захистити цілісність бізнесу та комерційну репутацію.

Компанія демонструє свою прихильність до забезпечення інформаційної безпеки шляхом:

- Призначення спеціального персоналу та розподіл бюджету на управління безпекою.
- Впровадження відповідних технологій безпеки та високої доступності, відновлюваних систем та засобів.
- Постійне оцінювання та вдосконалення процедур, пов’язаних із безпекою.
- Прийняття та забезпечення необхідних політик та забезпечення того, щоб працівники були в курсі та відповідальні за це через програми зв’язку та навчання.

Компанія використовує політику та стандарти безпеки для підтримки бізнес-цілей у своїх інформаційних системах та процесах. Ці політики та

стандарти впроваджуються, передаються та переглядаються на регулярній основі та відображають прихильність виконавчих управлінських команд до інформаційної безпеки. Політика та стандарти існують, щоб регулювати захист інформаційних активів Компанії та будь-яких інформаційних активів клієнтів , які були довірені Компанії.

1.2 Працівники

Усі працівники несуть відповідальність за обізнаність щодо питань інформаційної безпеки під час своєї щоденної роботи. Для підвищення обізнаності працівників Компанії проводять навчання з таких тем, як політика безпеки компаній, їх обов'язки щодо захисту конфіденційності довіреної їм інформації, належне використання ресурсів, додатковий догляд, необхідний для захисту мобільних пристроїв, та інші суміжні теми.

1.3 Положення про конфіденційність

Компанія укладає угоди про нерозголошення інформації зі своїми , працівниками, щоб захистити на підставі договору особисту та іншу конфіденційну інформацію, що належить Компанії або знаходиться під опікою Компанії.

1.4 Сфера застосування

Ця політика застосовується до всіх співробітників Компанії, підрядників, постачальників та агентів, що мають мобільні пристрої, що належать Компанії. Ця політика поширюється на всі комп’ютери, сервери, смартфони, планшети та інші обчислювальні пристрої, що працюють у межах Компанії.

2 Політика встановлення програмного забезпечення

2.1 Огляд

Дозвіл працівникам встановлювати програмне забезпечення на обчислювальні пристрої компанії відкриває організацію для непотрібного впливу. Суперечливі версії файлів або бібліотеки DLL, які можуть запобігти програмам

від запуску, впровадження шкідливого програмного забезпечення із зараженого програмного забезпечення для встановлення, неліцензійного програмного забезпечення, яке можна було виявити під час аудиту, та програм, які можуть бути використані для злому мережі організації, - приклади проблем, які можуть виникнути, коли працівники встановлюють програмне забезпечення на обладнання компанії.

2.2 Призначення

Метою цієї політики є викласти вимоги щодо встановлення програмного забезпечення на обчислювальних пристроях Компанії. Щоб мінімізувати ризик втрати функціональності програми, викриття конфіденційної інформації, що міститься в обчислювальній мережі Компанії, ризик впровадження зловмисного програмного забезпечення та юридичний вплив запуску неліцензійного програмного забезпечення.

2.3 Політика

2.3.1 Співробітники не можуть встановлювати програмне забезпечення на обчислювальні пристрої Компанії, що працюють у мережі Компанії.
2.3.2 Запити на програмне забезпечення повинен спочатку схвалити директор, в письмовій формі або електронною поштою.
2.3.4 Програмне забезпечення має обиратися із затвердженого списку програмного забезпечення, який веде відділ інформаційних технологій, якщо жоден вибір у списку не відповідає потребам запитувача.

2.4.5 Працівники не мають право використовувати корпоративні облікові записи для реєстрації на ресурсах, які не схвалишви їх попередньо з директором.

3 Антивірусна політика

3.1 Рекомендовані процеси для запобігання проблемам вірусів.

3.1.1 Завжди запускати підтримуване Компанією антивірусне програмне забезпечення, доступне у хмарному сховищі Компанії. Завантажувати та запускати

поточну версію; завантажувати та встановлювати оновлення антивірусного програмного забезпечення у міру їх появи.

3.1.2 НІКОЛИ не відкривати будь-які файли чи макроси, прикріплені до електронного листа з невідомого, підозрілого або ненадійного джерела. Негайно видаляти ці вкладення, у тому числі з “Корзини”.

3.1.3 Видаляти спам та інші небажані електронні листи без пересилання відповідно до Політики прийнятного використання Компанії.

3.1.4 Ніколи не завантажувати файли з невідомих або підозрілих джерел.

3.1.5 Уникати прямого спільного використання диска з доступом для читання / запису, якщо для цього немає абсолютно ділових вимог.

3.1.6 Завжди сканувати файли, що завантажуються з невідомого джерела на наявність вірусів перед їх використанням.

3.1.7 Регулярно створювати резервні копії критичних даних та конфігурацій системи та зберегти їх у безпечному місці.

3.1.8 Якщо лабораторне тестування конфліктує з антивірусним програмним забезпеченням, запустити антивірусну утиліту, щоб забезпечити чисту машину, вимкнути програмне забезпечення, а потім запустити лабораторний тест. Після лабораторного тесту увімкнути антивірусне програмне забезпечення. Якщо антивірусне програмне забезпечення вимкнено, не запускати програми, які можуть передавати вірус, наприклад, електронну пошту або спільний доступ до файлів.

3.1.9 Нові віруси виявляються майже щодня. Періодично перевіряти лабораторну антивірусну політику та цей список Рекомендованих процесів на наявність оновлень.

4 Політика автоматичного пересилання електронної пошти

4.1 Призначення

Щоб запобігти несанкціонованому або ненавмисному розголошенню конфіденційної інформації компанії.

4.2 Політика

Співробітники повинні проявляти крайню обережність, надсилаючи будь-який електронний лист із внутрішньої частини Компанії у зовнішню мережу. Якщо не схвалено менеджером, електронна пошта Компанії не буде автоматично переадресована на зовнішнє місце призначення. Конфіденційна інформація, не передаватиметься будь-якими способами, за винятком випадків, коли цей електронний лист є критичним для бізнесу.

5 Політика чистого робочого столу

5.1 Огляд

Політика чистого робочого столу може бути інструментом імпорту, щоб гарантувати, що всі важливі / конфіденційні матеріали видаляються з робочої області кінцевого користувача та замикаються, коли предмети не використовуються або працівник залишає свою робочу станцію. Це одна з найкращих стратегій, яку слід використовувати, намагаючись зменшити ризик порушення безпеки на робочому місці. Така політика може також підвищити обізнаність працівників щодо захисту конфіденційної інформації.

5.2. Призначення

Метою цієї політики є встановлення мінімальних вимог щодо підтримання "чистого робочого столу" - де конфіденційна / критична інформація про співробітників, інтелектуальну власність, клієнтів та постачальників Компанії знаходиться в безпеці. Політика є частиною стандартних основних засобів контролю конфіденційності.

5.3 Політика

5.3.1 Співробітники повинні забезпечити, щоб уся конфіденційна інформація була захищена в робочій зоні наприкінці дня та коли, як очікується, їх немає на тривалий період.

5.3.2 Комп'ютерні робочі станції повинні бути заблоковані, коли робоча область не зайнята.

5.3.3 Комп'ютерні робочі станції повинні бути повністю вимкнені в кінці робочого дня.

5.3.4 Ключі, що використовуються для доступу до обмеженої або конфіденційної інформації, не можна залишати за столом без нагляду.

5.3.5 Ноутбуки повинні бути заблоковані за допомогою замкового троса або зафіксовані в шухляді.

5.3.6 Паролі не можна залишати на липких нотатках, розміщених на комп'ютері чи під ним, а також залишати записаними у доступному місці.

6 Політика електронної пошти

6.1 Огляд

Електронна пошта широко використовується майже у всіх галузях і часто є основним методом спілкування та обізнаності в організації. У той же час зловживання електронною поштою може спричинити чимало правових ризиків, конфіденційності та безпеки, тому для користувачів важливо розуміти правильне використання електронних комунікацій.

6.2 Мета

Метою цієї політики щодо електронної пошти є забезпечення належного використання системи електронної пошти Компанії та інформування користувачів про те, що Компанія вважає прийнятним та неприйнятним використання її системи електронної пошти. Ця політика визначає мінімальні вимоги щодо використання електронної пошти в мережі Компанії.

6.3 Політика

6.3.1 Будь-яке використання електронної пошти повинно відповідати політиці та процедурам етичної поведінки, безпеки, дотриманню чинного законодавства та належної ділової практики.

6.3.2 Обліковий запис електронної пошти Компанії створюється Компанією для кожного співробітника Компанії, її слід використовувати переважно для бізнес-цілей, що стосуються Компанії; особисте спілкування та комерційне використання, не пов'язане з Компанією, заборонено.

6.3.3 Всі дані Компанії, що містяться в повідомленні електронної пошти або додатку, повинні бути захищені відповідно до стандарту захисту даних.

6.3.4 Електронну пошту слід зберігати лише в тому випадку, якщо вона відповідає діловому запису Компанії. Електронна адреса є діловою історією Компанії, якщо існує законна та діюча ділова причина для збереження інформації, що міститься в електронному листі.

6.3.5 Електронна пошта, яка ідентифікується як бізнес-запис Компанії, зберігається відповідно до Графіку зберігання записів Компанії.

6.3.6 Система електронної пошти Компанії не повинна використовуватися для створення або розповсюдження будь-яких руйнівних або образливих повідомлень, включаючи образливі коментарі щодо раси, статі, кольору волосся, інвалідності, віку, сексуальної орієнтації, порнографії, релігійних переконань та практики, політичних вірування, або національне походження. Співробітники, які отримують електронні листи з таким вмістом від будь-якого працівника Компанії, повинні негайно повідомити про це свого керівника.

6.3.7 Користувачам забороняється автоматично пересилати електронні листи Компанії сторонній системі електронної пошти (зазначено в 6.4.8 нижче). Індивідуальні повідомлення, які пересилає користувач, не повинні містити конфіденційну інформацію або назву компанії.

6.3.8 Користувачам забороняється використовувати сторонні системи електронної пошти та сервери зберігання, окрім тих, що передбаченні політикою компанії, для ведення бізнесу Компанії.

7 Політика користування інтернетом

7.1. Огляд

Підключення до Інтернету створює перед компанією нові ризики, які необхідно вирішити, щоб захистити важливі інформаційні активи закладу. Ці ризики включають:

- Доступ до Інтернету персоналу, який не відповідає потребам бізнесу, призводить до неправильного використання ресурсів. Ці заходи можуть негативно вплинути на продуктивність через час, витрачений на користування Інтернетом або його "серфінг". Крім того, компанія може зіткнутися з втратою репутації та можливими судовими позовами через інші види зловживання.
- Всю інформацію, знайдену в Інтернеті, слід вважати підозрілою, поки її не підтвердить інше надійне джерело. В Інтернеті не існує процесу контролю якості, а значна частина його інформації застаріла або неточна.
- Доступ до Інтернету надаватиметься користувачам для підтримки підприємницької діяльності і лише за необхідності для виконання своїх робочих обов'язків та професійних ролей.

7.2. Призначення

Метою цієї політики є визначення відповідного використання Інтернету працівниками Компанії.

7.3. Сфера застосування

Політика використання Інтернету поширюється на всіх користувачів Інтернету (фізичних осіб, що працюють у компанії, включаючи постійних штатних і неповних працівників, контрактників, працівників тимчасових агентств, ділових партнерів та постачальників), які отримують доступ до Інтернету через обчислювальні або мережеві ресурси . Очікується, що користувачі Інтернету Компанії будуть ознайомлені з цією політикою та дотримуватимуться її під час користування послугами Інтернету.

7.3.1 Дозволені Інтернет-послуги

- Електронна пошта - надсилання / отримання електронних повідомлень в / з Інтернету (з вкладеннями документів або без них).
- Навігація - послуги WWW, необхідні для комерційних цілей, за допомогою інструмента браузера протоколу передачі гіпертексту (HTTP). Повний доступ до Інтернету.

Керівництво залишає за собою право додавати або видаляти послуги в міру зміни бізнес-потреб або умов.

Усі інші послуги вважатимуться несанкціонованим доступом до Інтернету / з Інтернету та не дозволяти муться.

7.3.2 Процедури запиту та затвердження

Доступ до Інтернету надаватиметься користувачам для підтримки підприємницької діяльності і лише за необхідності для виконання їх роботи.

3.2.1 Запит на доступ до Інтернету

Як частина процесу запиту на доступ до Інтернету, працівник повинен прочитати як цю Політику користування Інтернетом, так і відповідну Політику безпеки Інтернету / Інтранета. Користувачі, які не дотримуються цих правил, можуть бути піддані дисциплінарному стягненню аж до припинення співробітництва.

7.3.2.2 Скасування привілеїв

Доступ до Інтернету буде припинено при припиненні найму працівника, завершенні контракту або притягненні до дисциплінарної відповідальності через порушення цієї та / або будь-якої політики. У разі зміни функції роботи та / або передачі оригінального коду доступу буде припинено, і повторно видано, якщо це необхідно, і буде затверджено новий запит на доступ.

Усі ідентифікатори користувачів, які були неактивними протягом тридцяти (30) днів, будуть скасовані. Привілеї, що надаються користувачам, повинні щороку переоцінюватися керівництвом.

7.4. Політика

7.4.1 Дозволене використання

Доступ до використання Інтернету надається з єдиною метою - підтримка ділової діяльності, необхідної для виконання робочих функцій. Усі користувачі повинні дотримуватись корпоративних принципів щодо використання ресурсів. Допустиме використання Інтернету для виконання робочих функцій може включати:

- Спілкування між працівниками та не працівниками в комерційних цілях;
- IT-технічна підтримка завантаження оновлень програмного забезпечення та виправлень;
- Самоосвіта;
- Створення і розробка дизайн проектів;
- Отримання доступу до хмарного сховища компанії;
- Довідкова нормативна або технічна інформація;
- Дослідження.

7.4.2 Особисте використання

Дозволяється використання комп'ютерних ресурсів для доступу до Інтернету в особистих цілях.

Усі користувачі Інтернету повинні знати, що мережа компанії створює журнал аудиту, що відображає запит на надання послуги, як вхідні, так і вихідні адреси, і періодично перевіряється.

Користувачі, які вирішили зберігати або передавати особисту інформацію, таку як приватні ключі, номери кредитних карток або сертифікати, або користуватися Інтернет-гаманцями, роблять це на власний ризик. Компанія не несе відповідальності за будь-яку втрату інформації, наприклад, інформацію, що зберігається в гаманці, або будь-яку наслідкову втрату особистого майна

7.4.3 Заборонене використання

Інформація, що зберігається у гаманці, або будь-яка наслідкова втрата особистого майна. Збір, зберігання та розповсюдження даних, які є незаконними,

порнографічними або негативно відображають расу, стать або віросповідання, заборонено.

Компанія також забороняє ведення підприємницької діяльності, політичну діяльність, участь у будь-якій формі збору розвідувальних даних з наших установ, участь у шахрайських діях або завідомо розповсюдження неправдивих або непристойних матеріалів.

Інші види діяльності, які суворо заборонені, включають, але не обмежуючись цим:

• Доступ до інформації про компанію, яка не входить до сфери роботи. Це включає несанкціоноване зчитування інформації про обліковий запис клієнта, несанкціонований доступ до інформації про файли персоналу та доступ до інформації, яка не потрібна для належного виконання робочих функцій.

• Зловживання, розголошення без належного дозволу або зміна інформації про клієнта чи персонал. Сюди входить внесення несанкціонованих змін до картотеки персоналу або обмін електронними даними про клієнтів або персонал з несанкціонованим персоналом.

• Навмисне гіперпосилання веб-сайта Компанії на інші веб-сайти Інтернету / WWW, зміст яких може суперечити цілям або політиці компанії або порушувати їх.

• Використання, передача, тиражування або добровільне отримання матеріалів, що порушують авторські права, торгові марки, комерційну таємницю або патентні права будь-якої особи або організації. Припустимо, що всі матеріали в Інтернеті захищені авторським правом та / або запатентовані, якщо в конкретних повідомленнях не зазначено інше.

• Передача будь-якої власної, конфіденційної або іншої конфіденційної інформації без належного контролю.

• Створення, розміщення, передача або добровільне отримання будь-якого незаконного, образливого, наклепницького, загрожуючого, переслідуючого матеріалу, включаючи, але не обмежуючись цим, коментарі на основі раси,

національного походження, статі, сексуальної орієнтації, віку, інвалідності, релігії чи політичних переконань .

• Будь-яка форма азартних ігор.

Якщо спеціально не дозволено положеннями розділу 7.4.3, наступні види діяльності також суворо заборонені:

Несанкціоноване завантаження будь-яких програм або файлів умовно-безкоштовних програм для використання без попереднього дозволу директора.

- Будь-яке замовлення (покупка) предметів або послуг в Інтернеті.
- Гра в будь-які ігри.
- Пересилання ланцюгових листів.
- Участь у будь-якому он-лайн конкурсі чи акції.
- Прийом рекламних подарунків.

Пропускна здатність як у межах компанії, так і при підключенні до Інтернету - це спільний, обмежений ресурс.

Користувачі повинні докласти зусиль для використання цього ресурсу способами, які не впливають негативно на інших працівників. Конкретні відділи можуть встановлювати вказівки щодо використання смуги пропускання та розподілу ресурсів, а також можуть забороняти завантаження певних типів файлів.

7.4.4 Ліцензія на програмне забезпечення

Компанія настійно підтримує суворе дотримання ліцензійних угод постачальників програмного забезпечення. При роботі, або використанні обчислювальних або мережевих ресурсів компанії, копіювання програмного забезпечення у спосіб, що не відповідає ліцензії постачальника, категорично заборонено. Питання, що стосуються законного та незаконного копіювання, слід направляти до керівництва для розгляду до того, як буде здійснено копіювання.

Подібним чином відтворення матеріалів, доступних через Інтернет, повинно здійснюватися лише з письмового дозволу автора або власника документа. Якщо спочатку не отримано дозволу власника авторських прав, копіювання матеріалів із журналів, журналів, бюлетенів, інших публікацій та Інтернет-документів

заборонено, якщо це не є обґрунтованим та звичним. Це поняття "добросовісного використання" відповідає міжнародним законам про авторське право.

7.4.5 Очікування конфіденційності

7.4.5.1 Моніторинг

Користувачі повинні вважати свою діяльність в Інтернеті періодичним контролем та обмежувати свою діяльність

відповідно.

Керівництво залишає за собою право перевіряти електронну пошту, каталоги особистих файлів, доступ до Інтернету та іншу інформацію, що зберігається на комп'ютерах компанії, у будь-який час і без попередження. Ця експертиза забезпечує дотримання внутрішньої політики та допомагає в управлінні інформаційними системами компанії.

7.4.5.2 Конфіденційність електронної пошти

Користувачі повинні пам’ятати, що електронний лист із чітким текстом не є конфіденційним засобом спілкування. Компанія не може гарантувати, що електронні комунікації будуть приватними. Співробітники повинні знати, що електронні комунікації можуть, в залежності від технології, пересилатися, перехоплюватися, друкуватися та зберігатися іншими. Користувачі також повинні знати, що після передачі електронного повідомлення воно може бути змінено. Видалення повідомлення електронної пошти з окремої робочої станції не обмежує його з різних систем, через які воно було передане.

7.4.8 Підтримка корпоративного іміджу

7.4.8.1 Представлення

Користуючись ресурсами компанії для доступу та використання Інтернету, користувачі повинні усвідомлювати, що представляють Компанію.

4.8.2 Матеріали компанії

Користувачі не повинні розміщувати матеріали Компанії (приклади: внутрішні пам’ятки, прес-релізи, інформація про товар чи використання, документація тощо) у будь-якому списку розсилки, публічній групі новин або такій службі.

Будь-яке розміщення матеріалів повинно бути схвалене керівником працівника та відділом зв'язків з громадськістю та розміщуватися уповноваженою особою.

7.4.9 Періодичні огляди

7.4.9.1 Огляди відповідності використання

Для забезпечення відповідності цій політиці будуть проводитися періодичні перевірки. Ці огляди включатимуть перевірку ступеня відповідності політиці використання.

7.4.9.2 Огляди технічного обслуговування політики

Проводитимуться періодичні огляди для забезпечення доцільності та ефективності політики використання. Ці огляди можуть призвести до модифікації, додавання або видалення політики використання, щоб краще відповідати потребам компанії в інформації.

8 Політика створення паролів

8.1 Огляд

Паролі є найважливішою складовою інформаційної безпеки. Паролі служать для захисту облікових записів користувачів; однак, погано побудований пароль може призвести до компрометації окремих систем, даних або мережі. Ця політика містить найкращі практики щодо створення захищених паролів.

8.2 Призначення

Метою політики є надання найкращих практик для створення надійних паролів.

8.3 Політика

Надійні паролі довгі, чим більше символів у вас, тим сильніший пароль. Ми рекомендуємо щонайменше 14 символів у паролі. Крім того, настійно рекомендується використовувати парольні фрази, паролі, що складаються з декількох слів. Приклади включають "It's time for vacation" або "block-curious-sunny-leaves". Парольні фрази легко запам'ятовувати і друкувати,

але при цьому відповідають вимогам до міцності. Слабкі паролі мають такі характеристики:

- Містить вісім символів або менше.
- Містити особисту інформацію, таку як дати народження, адреси, номери телефонів або імена членів родини, домашніх тварин, друзів та персонажів фантазії.
- Містять шаблони чисел, такі як aaabbb, qwerty, zyxwvuts або 123321.
- Є деякі версії “Welcome123” “Password123” “Changeme123”

Крім того, кожен робочий обліковий запис повинен мати інший, унікальний пароль. По можливості також дозволяйте використовувати багатофакторну автентифікацію.

9 Політика роботи з хмарним сховищем і онлайн сервісами

9.1 Огляд

Використання хмарних сховищ, особливо сторонніх хмарних сховищ є важливою частиною роботи Компанії. У цій політиці описані правила роботи з хмарним сховищем та онлайн сервисами.

9.2 Призначення

Призначенням цієї політики є встановлення правил з користування хмарним сховищем та онлайн сервісами.

9.3 Політика

Компанія використовує певні сторонні онлайн сервіси для ведення діяльності, які допомагають створювати та / або зберігати інформацію:

- Google Drive;
- Google Docs;
- Google Sheets;
- Figma.

Після закінчення роботи працівники компанії зобов'язані перевірити інформацію на предмет завантаження її до хмарного сховища, щоб вона завжди була актуальною.

10 Відповідність політиці

10.1 Вимірювання відповідності

Копманія перевірить відповідність цій політиці різними методами, включаючи, але не обмежуючись цим, звіти про бізнес-інструменти, внутрішні та зовнішні перевірки та відгуки власнику політики.

10.2 Винятки

Будь-які винятки з політик повинні бути затверджені Компанією заздалегідь.

10.3 Невиконання

Працівник, який виявив порушення політики, може бути підданий дисциплінарному стягненню аж до припинення трудових відносин включно.

Крім того, компанія може на власний розсуд шукати юридичні засоби захисту від збитків, заподіяних внаслідок будь-якого порушення. Законодавство може також вимагати від компанії повідомляти відповідні органи правопорядку про певну незаконну діяльність.

Лист ознайомлення

№	ПІБ	Посада	Дата	Підпис
1				
2				
3				
4				
5				
6				
7				
8				
9				

ДОДАТОК Е. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	1 Розділ	5	
5	А4	2 Розділ	40	
6	А4	3 Розділ	10	
7	А4	Висновки	1	
8	А4	Перелік посилань	3	
9	А4	Додаток А	1	
10	А4	Додаток Б	1	
11	А4	Додаток В	1	
12	А4	Додаток Г	1	
13	А4	Додаток Д	19	
14	А4	Додаток Е	1	
15	А4	Додаток Ж	1	

ДОДАТОК Ж. Відгук керівника кваліфікаційної роботи

Відгук

на кваліфікаційну роботу студентки групи 125-17-2

Попової А.А.

на тему: «Політика безпеки інформаційно-телекомунікаційної системи ТОВ Fox Design Studio»

Пояснювальна записка складається зі вступу, трьох розділів і висновків.

Метою кваліфікаційної роботи є досягнення достатнього рівня захищеності інформації в ІТС підприємства.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз нормативно-правової бази у сфері забезпечення кібербезпеки; ознайомлення з особливостями підприємства, проаналізувати види інформації та особливості взаємодії інформації на об’єкті, вибір профіль захищеності, розробка основних елементів політики безпеки..

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні ефективності забезпечення безпеки інформації, за рахунок розробки основних елементів політики безпеки інформації.

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

За час дипломування Попова А.А. 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 « ».

Керівник кваліфікаційної роботи
Проф. Корнієнко В.І.

Керівник спеціальної частини
ст. викл. Тимофєєв Д.С.