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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Кабанова Артема Олександровича*

академічної групи *УБіт-15-1*

напряму підготовки *6.170103 Управління інформаційною безпекою*

спеціалізації[1]

за освітньо-професійною програмою

на тему *«Розробка політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Вебпіар»»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ас. Ковальова Ю.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2019

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Кабанову Артему Олександровичу*** **академічної групи** ***УБіт-15-1***
(прізвище ім'я по-батькові) (шифр)

напряму підготовки *6.170103 Управління інформаційною безпекою*
(код і назва спеціальності)

на тему ***«Розробка політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Вебпіар»»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	**Зміст**	**Термін виконання**
Розділ 1	*Аналіз стану забезпечення безпеки інформації та постановка задачі для її реалізації на ТОВ «Вебпіар»*	20.03.2019
Розділ 2	*Аналіз інформаційно-телекомунікаційної системи ТОВ «Вебпіар», виконання обстеження підприємства та розробка політики безпеки інформації*	30.05.2019
Розділ 3	*Техніко-економічне обґрунтування створення політики безпеки інформації*	15.06.2019

Завдання видано _____ Корнієнко В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2019р.

Дата подання до екзаменаційної комісії: 17.06.2019р.

Прийнято до виконання _____ Кабанов А.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 81 с., 2 рис., 30 табл., 6 додатків, 30 джерел.

Об’єкт розробки: інформаційно-телекомунікаційна система товариства з обмеженою відповідальністю «Вебпіар».

Предмет розробки: політика безпеки інформації в інформаційно-телекомунікаційній системі товариства з обмеженою відповідальністю «Вебпіар».

Мета дипломної роботи: підвищення рівня захищеності інформаційно-телекомунікаційної системи товариства з обмеженою відповідальністю «Вебпіар».

В першому розділі сформовано питання і поставлена задача в галузі інформаційної безпеки, визначено необхідність та актуальність розробки політики безпеки інформації на підприємстві. Виконано аналіз нормативно-правової бази в сфері захисту інформації. Визначено нормативні документи, основні закони та державні стандарти, які мають бути задіяні в процесі розробки політики безпеки інформації на підприємстві.

В спеціальній частині наведено загальну характеристику обстежуваного об’єкту інформаційної діяльності, розроблено модель загроз, виконано аналіз та оцінка ризиків інформаційної безпеки, сформовано загальні положення політики безпеки інформації.

В економічній частині проведено розрахунок витрат на впровадження та експлуатацію політики безпеки інформації.

Практичне значення роботи полягає в розробці, впровадженні та експлуатації політики безпеки інформації інформаційно-телекомунікаційної системи.

ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАГРОЗИ, ВРАЗЛИВОСТІ, ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, ПРОФІЛЬ ЗАХИЩЕНОСТІ, МОДЕЛЬ ЗАГРОЗ, ОЦІНКА РИЗИКУ.

РЕФЕРАТ

Пояснительная записка: 81 с., 2 рис., 30 табл., 6 прилож., 30 источн.

Объект разработки: информационно-телекоммуникационная система общества с ограниченной ответственностью «Вебпиар».

Предмет разработки: политика безопасности информации в информационно-телекоммуникационной системе общества с ограниченной ответственностью «Вебпиар».

Цель дипломной работы: повышение уровня защищенности информационно-телекоммуникационной системы общества с ограниченной ответственностью «Вебпиар».

В первом разделе сформирован вопрос и поставлена задача в области информационной безопасности, определена необходимость и актуальность разработки политики безопасности информации на предприятии. Выполнено анализ нормативно-правовой базы в сфере защиты информации. Определены нормативные документы, основные законы и государственные стандарты, которые должны быть задействованы в процессе разработки политики безопасности информации на предприятии.

В специальной части приведена общая характеристика исследуемого объекта информационной деятельности, разработана модель угроз, выполнено анализ и оценка рисков информационной безопасности, сформированы общие положения политики безопасности информации.

В экономической части проведен расчет расходов на внедрение и эксплуатацию политики безопасности информации.

Практическое значение работы состоит в разработке, внедрении и эксплуатации политики безопасности информации информационно-телекоммуникационной системы.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УГРОЗЫ, УЯЗВИМОСТИ, ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА, ПРОФИЛЬ ЗАЩИЩЕННОСТИ, МОДЕЛЬ УГРОЗ, ОЦЕНКА РИСКА.

ABSTRACT

Explanatory note: 81 p., 2 images, 30 tables, 6 supplements, 30 sources.

Object of research: information and telecommunication system of the limited liability company «WebPR».

Subject of research: information security policy in the information and telecommunication system of the limited liability company «WebPR».

The idea of work: increasing the level of protection of information and telecommunication system of the limited liability company «WebPR».

In the first section the question is formed and the task in the field of information security is set, the necessity and relevance of the development of information security policy at the enterprise is determined. The analysis of the regulatory framework in the field of information security. The normative documents, the basic laws and the state standards which should be involved in the process of development of information security policy at the enterprise are defined.

The special part provides a general description of the object of information activity, the threat model is developed, analysis and assessment of information security risks, formed the general provisions of information security policy.

In the economic part of the calculation of costs for the implementation and operation of information security policy.

The practical significance of the work is the development, implementation and operation of information security policy of information and telecommunication system.

INFORMATION SECURITY, THREATS, VULNERABILITIES, INFORMATION AND TELECOMMUNICATION SYSTEM, THE PROFILE OF SECURITY, THE THREAT MODEL, RISK ASSESSMENT.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АРМ – автоматизоване робоче місце;

АС – автоматизована система;

ДТЗС – допоміжні технічні засоби та системи;

ІзОД – інформація з обмеженим доступом;

ІКС – інформаційно-комунікаційні системи;

ІТС – інформаційно-телекомунікаційна система;

КЗ – контрольована зона;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

НСД – несанкціонований доступ (дії)

ОІД – об’єкт інформаційної діяльності;

ОС – операційна система;

ОТЗ – основні технічні засоби;

ПБІ – політика безпеки інформації;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ТЗ – технічне завдання.

ЗМІСТ с.

ВСТУП

Впровадження обчислювальної техніки на підприємство несе не тільки автоматизацію виробництва або підвищення обсягів продажу, а також і великий перелік загроз. Однією з найбільш важливих проблем інформаційного суспільства є захист інформації, оскільки будь-які дані, що обробляються і накопичуються в обчислювальній техніці, почали визначати напрямок діяльності людини та організації в цілому, що зацікавлює третіх осіб.

За допомогою незаконного володіння інформацією можна здійснювати найрізноманітніші протиправні діяння, наприклад, виробляти незаконний оборот фінансових коштів, отримувати доступ до секретної комерційної інформації та ін.

Крім цього варто зазначити, що конфіденційна інформація представляє величезний інтерес для конкуруючих організацій. Саме вона стає причиною посягань з боку зловмисників. З інформаційною безпекою тісно пов'язане і таке поняття, як комерційна таємниця.

Багато проблем інформаційної безпеки пов'язані з недооціненням важливості такої загрози, як конфіденційність інформації. В результаті для підприємства це може обернутися банкрутством. Навіть одиночний випадок халатності персоналу підприємства може принести йому багатомільйонні збитки, втрату репутації фірми і довіри клієнтів.

Збереження цілісності, забезпечення безвідмовної доступності, дотримання заздалегідь зазначеного рівня конфіденційності інформаційних ресурсів і зменшення ймовірності несанкціонованого доступу та протиправних дій до цих ресурсів – це і є головною задачею для інформаційно-телекомунікаційної системи товариства з обмеженою відповідальністю «Вебпіар».

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

В епоху розквіту та розвитку хакерських та кібератак, забезпечення захищеності інформаційних активів підприємства – є найголовнішим завданням для всіх державних та комерційних установ. Спеціалісти з інформаційної безпеки будують захисні механізми, що можуть протистояти натиску різних загроз і захистити інформацію, що оброблюється, передається та зберігається в інформаційно-телекомунікаційній системі підприємства.

Під інформаційною безпекою слід розуміти стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [1].

Одним із методів забезпечення інформаційної безпеки підприємства є створення комплексної системи захисту інформації (КСЗІ). Під КСЗІ слід вважати сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС [2]. Виконуючи вимоги законодавства України [3,4] і створюючи КСЗІ, замовник (він же керівник підприємства) отримує пакет документів, який складається з: акту обстеження об’єкту інформаційної діяльності, моделі загроз, моделі порушника, політики безпеки, плану захисту інформації, календарного плану робіт з захисту інформації, технічного завдання на створення КСЗІ, проектної та експлуатаційної документації, актів про завершення проведення етапів і дозвіл про перехід до наступного етапу створення КСЗІ, актів випробувань і акту відповідності.

Головною метою створення КСЗІ є досягнення максимальної ефективності захисту за рахунок одночасного використання всіх необхідних ресурсів, методів і засобів, що виключають несанкціонований доступ до інформації, та створення умов обробки інформації відповідно до чинних нормативно-правових актів України у сфері захисту інформації [5].

КСЗІ складається із засобів та заходів, які реалізують способи, методи, механізми захисту інформації від:

– витоку технічними каналами, до яких відносяться канали ПЕВН, акустичні, та інші канали;

– несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів тощо;

– спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту [6].

Кожна інформаційно-телекомунікаційна система має власний склад, структуру, клас АС, профілі захищеності інформації в комп'ютерних системах, методи обробки та зберігання інформації. Саме тому неможливо створити уніфіковану структуру, яка буде регламентувати методи і способи забезпечення захисту інформації в ІТС.

Схема реалізації інформаційної безпеки підприємства складається з п'яти складових: технічної, організаційної, дозвільної, попереджувальної та правової.

Оскільки в будь-якій системі всі елементи та підсистема є взаємопов'язаними, більшість завдань інформаційної безпеки виконується разом із основними та допоміжними підсистемами системи економічної безпеки підприємства.

Технічна складова покликана забезпечити захист інформації та об’єктів підприємства, а також виявлення фактів витікання інформації та неправомірних дій персоналу та сторонніх осіб щодо даного підприємства за допомогою технічних засобів.

Організаційна складова повинна забезпечити належне поводження персоналу підприємства із секретною інформацією та іншими об’єктами захисту господарюючого суб’єкта.

Дозвільна складова системи інформаційної безпеки має здійснювати розподіл інформації підприємства за рівнями секретності та визначити ступінь доступу до неї.

Попереджувальна складова необхідна для уникнення ефекту дезінформації та прийняття в наслідок цього хибних управлінських рішень, а також максимального зниження ймовірності витікання секретної інформації.

Правова складова покликана забезпечити правовий захист інтересів підприємства щодо захисту інформації, а також закріплення прав підприємства щодо комерційної таємниці в установчих документах, договорах та інших нормативних актах.

В умовах забезпечення захищеності інформаційних активів, підприємство, яке працює з особистими даними своїх клієнтів повинне виконувати вимоги із захисту персональних даних, адже саме ці відомості є «ласим шматком» для хакерів та порушників. За порушення збереженості персональних даних наданих підприємству для обробки передбачається відповідальність згідно чинного законодавства України.

В часи збільшення загроз, підприємство повинне вміти розробляти та впроваджувати політику інформаційної безпеки. В свою чергу політика інформаційної безпеки повинна [18]:

- бути оформлена як документована інформація;
- бути доведена до відома співробітників в організації;
- бути доступною в установленому порядку для зацікавлених сторін.
- відповідати цілям організації;

– містити цілі інформаційної безпеки або зазначати основні положення для визначення таких цілей (завдань);

– містити зобов'язання відповідати чинним вимогам, пов'язаним з інформаційною безпекою;

– містити зобов'язання щодо постійного вдосконалення системи управління інформаційною безпекою.

Актуальність теми дипломної роботи зумовлена стрімким розвитком загроз інформаційній безпеці малих та середніх комерційних установ. Саме тому дотримання норм, установ, вимог та правил, які трактуються політикою безпеки, є найбільш вагомим і дієвим важелем в питанні підвищення рівня захищеності інформаційно-телекомунікаційної системи.

1.2 Аналіз нормативно-правової бази в сфері захисту інформації

Нормативно-правова база в сфері захисту інформації має велику кількість документів, які регламентують методи та способи збереження властивостей інформації, встановлюють основні вимоги до розробки політики безпеки інформації, етапи побудови комплексної системи захисту інформації, вимоги до оформлення технічного завдання, порядок проведення обстеження середовища функціонування ІТС, склад плану захисту та ін.

Законом України «Про інформацію» [7] визначено поняття «захист інформації», а також статтею 9 затверджено, що захист інформації є одним із видів інформаційної діяльності.

Закон України «Про захист персональних даних» [8] регулює вимоги, пов’язані із захистом і обробкою персональних даних, а також спрямований на захист прав і свобод людини і громадянина.

В Законі України «Про основні засади забезпечення кібербезпеки України» [9] було вперше визначено поняття «кібербезпека», «кіберзагроза», «кіберзлочин», «критична інформаційна інфраструктура», тощо. Цей закон визначає правові та організаційні основи забезпечення захисту життєво

важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі.

Вперше про криптографічний захист інформації було згадано в Указі Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» [10], який дає визначення поняттю «криптографічний захист інформації». Саме положення визначає порядок здійснення криптографічного захисту ІзОД, розголошення якої може завдати шкоди державі, суспільству або особі.

Указ Президента України «Про Положення про технічний захист інформації в Україні» [11] визначає правові та організаційні засади технічного захисту інформації. В Положенні також надано визначення поняттю «комплекс технічного захисту інформації».

В Постанові Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [12] визначено, яка інформація підлягає захисту в системі, які саме операції над інформацією необхідно захистити від НСД, як забезпечується захист в системі таємної та службової інформації, як передається ця інформація, тощо.

Перед тим, як розпочати побудову КСЗІ, необхідно виконати категоріювання об’єктів інформаційної діяльності. Для цього створюється комісія з категоріювання, яка, згідно з НД ТЗІ 1.6-005-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці [16] проводить категоріювання ОІД.

Для створення КСЗІ необхідно ураховувати вимоги нормативних документів у сфері технічного захисту інформації, серед яких НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [3] регламентує етапи побудови КСЗІ, НД ТЗІ 2.5.004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу [13] визначає критерії

конфіденційності, цілісності, доступності, спостережності та критерії гарантії комп'ютерних систем задля забезпечення необхідних функціональних послуг, НД ТЗІ 2.5.005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [14] формулює класифікацію автоматизованих систем та пропонує стандартні функціональні профілі захищеності, які складаються з функціональних послуг.

Важливим етапом створення КСЗІ є розробка технічного завдання, яка трактується НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі [15].

1.3 Постановка задачі

Враховуючи вищезазначене можна визначити, що інформаційно-телекомунікаційна система ТОВ «Вебпіар» потребує вирішення наступних задач в дипломній роботі:

1 Проведення обстеження автоматизованої системи ТОВ «Вебпіар», розглядаючи її як організаційно-технічну систему, що об'єднує фізичне середовище, обчислювальну систему, середовище користувачів, оброблювальну інформацію і технологію її обробки.

2 Розробка моделі загроз та моделі порушника обстежуваного підприємства.

3 Оцінка інформаційних ризиків за обраною методологією.

4 Створення політики безпеки інформації.

5 Перевірка ефективності впровадження політики безпеки шляхом повторної оцінки інформаційних ризиків.

6 Визначення та аналіз економічної ефективності розробки політики безпеки інформації

1.4 Висновок

Визначено загальний стан розвитку загроз інформаційній безпеці підприємства, сформовано основні цілі дипломної роботи, а також проаналізовано нормативно-правову базу, яка забезпечує побудову етапів комплексних систем захисту інформації, а саме: розробку акту обстеження об’єкту інформаційної діяльності, побудову моделі загроз та моделі порушника, проведення оцінки інформаційних ризиків, створення політики безпеки інформації, а також проведення повторної оцінки інформаційних ризиків з урахуванням впровадження політики безпеки.

Розробка комплексної системи захисту інформації є важливим кроком в сфері забезпечення захищеності автоматизованих систем інформаційно-телекомунікаційної системи підприємства, який потребує контролю виконання вимог, встановлених законодавством України в сфері технічного захисту інформації.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про підприємство ТОВ «Вебпіар»

Дослідження дипломної роботи ґрунтується на базі ТОВ «Вебпіар», що знаходиться за адресою: м. Дніпро, вул. Європейська, 4, оф. 424, Україна.

ТОВ «Вебпіар» засновано в 2008 році. Основний напрям роботи – розробка та супровід корпоративних сайтів, інтернет-магазинів, проведені SMM, SEO, e-mail та YouTube-просунення, автоматизація маркетингу та продажів, управління та розробка стартапів.

Форма власності: товариство з обмеженою відповідальністю.

Підприємство складається з наступних підрозділів:

- відділ проектного менеджменту;
- фінансовий відділ;
- відділ програмного забезпечення;
- відділ текстового оздоблення;
- відділ з налаштування контекстної реклами та SEO-оптимізації сайту.

Організаційна структура підприємства представлена на рисунку 2.1.

Штат ТОВ «Вебпіар» налічує 8 осіб, серед них:

- генеральний директор – 1 особа;
- фінансовий директор – 1 особа;
- проектний менеджер – 2 особи;
- менеджер з SEO-оптимізації – 1 особа;
- менеджер з налаштування контекстної реклами – 1 особа;
- програміст – 1 особа;
- копірайтер – 1 особа;

Генеральний директор координує роботу всіх відділів, приймає управлінські рішення, проводить співбесіди з потенційними робітниками, відвідує конференції, світські заходи, торгівельні майданчики, де підшукує клієнтів. Формує план робіт на місяць для кожного підрозділу підприємства.

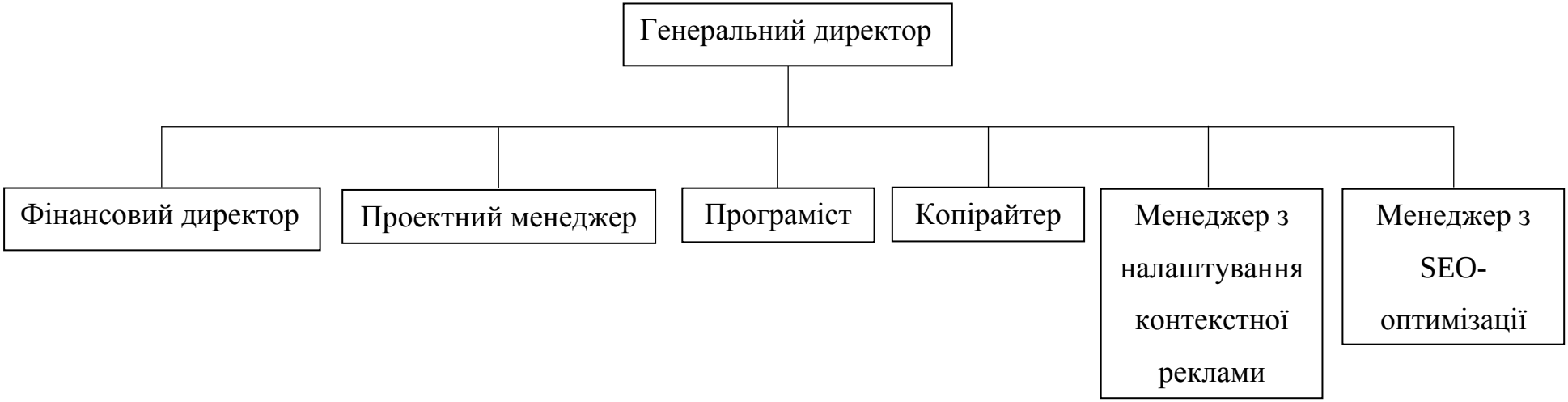


Рисунок 2.1 – Організаційна структура ТОВ «Вебпіар»

Менеджер з SEO-оптимізації отримує технічне завдання від проектного менеджера, проводить SEO-аналіз сайту, пише ТЗ проектному менеджеру (для ознайомлення з обсягами робіт) та програмісту, отримує виправлення від ПМ, виконує роботи, звітує перед ПМ про виконані роботи, вносить виправлення (якщо вони є) в виконану роботу.

Менеджер з налаштування контекстної реклами отримує технічне завдання від проектного менеджера, оцінює завдання, доповідає про це проектному менеджеру, виконує поставлені роботи, вносить виправлення (якщо вони є) в виконану роботу.

Копірайтер отримує технічне завдання від проектного менеджера, оцінює завдання, доповідає про це проектному менеджеру, виконує роботи, звітує перед проектним менеджером, вносить виправлення (якщо вони є) в виконану роботу.

Роботу системного адміністратора виконує проектний менеджер.

Основний бізнес-процес ТОВ «Вебпіар» складається з наступних дій: проектний менеджер разом із замовником складає картку клієнта на проведення робіт, в якій вказують контактні дані замовника, тип робіт, особливості та побажання до виконуваних робіт. Після цього, отримані дані передаються фінансовому директору, який вносить їх у базу даних клієнтів.

Проектний менеджер формує календарний план проведення робіт, аналізує витрати на майбутній перелік робіт, розділює обов’язки між командою і передає фінансовому директору інформацію про витрати.

Фінансовий директор, в свою чергу, формує акт на закупівлю програмного та апаратного забезпечення і подає його генеральному директору. Вищезазначений акт в підсумку вплине на формування щомісячного та щорічного фінансового звіту.

В ході виконання визначених робіт, проектний менеджер працює з конфіденційними даними замовника, які відповідають за адміністрування (логін та пароль від хостингу, доступи до FTP, логін та пароль від сайту та ін.). Крім

цього, проектний менеджер формує технічне завдання програмісту, SEO-менеджеру, копірайтеру та менеджеру з налаштування контекстної реклами.

Після отримання технічного завдання від проектного менеджера, програміст, копірайтер, менеджер з налаштування контекстної реклами та SEO-менеджер виконують оцінку обсягу робіт (в часовому вигляді) і надсилають її проектному менеджеру. Час на виконання переліку робіт проектний менеджер відображає в звіті виконаних робіт проекту.

Після того, як проектний менеджер отримає виконані роботи, що поставлені в технічному завданні, він передає фінансовому директору інформацію про виконані роботи своїх підлеглих (скільки часу було витрачено, який обсяг робіт було виконано). Ця інформація відобразиться в звіті з нарахування заробітної плати.

Далі фінансовий директор надсилає замовнику банківські дані підприємства (реквізити, банківський рахунок та ін.). Замовник, оцінюючи поточний обсяг виконаних робіт, надсилає певну частину суми за роботу і очікує на виконаний проект.

Проектний менеджер проводить заключний етап робіт: перевіряє виконані роботи, виправляє помилки, готує проект до експлуатації. Складає звіт виконаних робіт проекту, з яким ознайомлює генерального директора, фінансового директора і замовника. Отримавши останній фінансовий транш від замовника, проект здається в експлуатацію, проектний менеджер пише інструкцію для персоналу замовника і надсилає його їм.

ТОВ «Вебпіар» працює з понеділка по п’ятницю. Вихідний – субота, неділя. Графік роботи з 9.30 до 18.30.

Прибирання приміщення проводиться прибиральницею кожний вівторок. Графік проведення прибирання з 9.00 до 9.30.

Охорона працює цілодобово в 3 зміни. Зміна відбувається о 8 годині ранку, 16 годині дня та о 12 годині ночі. Ключі від офісу знаходяться у генерального директора та у охоронця. Контроль доступу на територію підприємства відбувається за допомогою шлагбауму та контрольно-

пропускного пункту на сході відносно будівлі з ОІД. Доступ сторонніх осіб в приміщення відбувається тільки в робочий час і здійснюється через пункт охорони, який розташований на вході і оснащений турнікетом.

2.2 Обґрунтування необхідності створення комплексної системи захисту інформації

Необхідність створення комплексної системи захисту інформації зумовлена тим фактором, що в майбутньому організація планує виходити на європейський ринок, де важливим критерієм захищеності даних є забезпечення конфіденційності, цілісності та доступності оброблювальної інформації.

Маючи 10-річний досвід в створенні корпоративних сайтів, автоматизації продажів та маркетингу, розробці стартапів і отримавши певне визнання в межах країн СНД, керівництвом ТОВ «Вебпіар» було прийняте рішення – вихід на європейський ринок в сфері розробці стартапів.

Організація, в якій більша частина циркулюючої інформації зберігається в електронному вигляді, має дані, що становлять інформацію з обмеженим доступом (ІзОД).

У зв’язку зі співпрацею з іноземним замовником в розробці стартапу, на ОІД значно збільшилися обсяги інформаційних потоків даних, що оброблюються автоматизованим способом.

Для того, щоб визначити рівень захищеності оброблювальної інформації на об’єкті було проведене категоріювання об’єкта інформаційної діяльності (ОІД). Згідно з НД ТЗІ 1.6-005-2013 [16] організації була надана IV категорія.

IV категорія встановлюється об’єктам де оброблюється технічними засобами та/або озвучується інформація з обмеженим доступом.

2.3 Обстеження на об’єкті інформаційної діяльності

За 10 років свого існування на ІТ-ринку про ТОВ «Вебпіар» дізналися за межами України і СНД, завдяки прийняття участі в міжнародних конференціях

з Інтернет-маркетингу, електронної комерції та стартапів. Від європейських клієнтів надходить багато замовлень на супровід стартапів, які будуть впроваджені в країнах першого світу, керівництвом установи було прийнято рішення провести обстеження ОІД ТОВ «Вебпіар».

Головною підставою на проведення обстеження були умови двостороннього договору між європейським клієнтом та обстежуваною установою, а також наказ головного директора. В наказі також визначено, що обстеження ОІД ТОВ «Вебпіар» буде відбуватися з дотриманням норм та визначень НД ТЗІ 3.7-003-05 [3].

Для проведення обстеження ОІД необхідно:

– проаналізувати умови функціонування ОІД, виконати опис розташування його на місцевості, з зазначенням меж контрольованої зони КЗ, архітектурно-будівельних особливостей приміщень та ін.;

– визначити розташування комунікаційних систем життєзабезпечення і металоконструкцій, які знаходяться як в межах КЗ, так і поза ними;

– сформувати ситуаційний та генеральний план (згідно отриманих вхідних даних), який стане в нагоді при виявлені джерел загроз та ймовірних вразливостей;

– визначити та проаналізувати основні та допоміжні технічні засоби, які оброблюють і не оброблюють ІзОД, зафіксувати місця їх розташування на ОІД;

– провести аналіз щодо необхідності впровадження інженерних та технічних заходів захисту від витоку ІзОД технічними каналами.

До акту обстеження ОІД закріплюються додатки, серед яких:

– генеральний план ОІД, з вказанням площі, розмірів стін, вікон, дверей, систем комунікацій, відстаней від ОТЗС, ДТЗС до межі КЗ, систем пожежної та охоронної сигналізації та ін.

– ситуаційний план ОІД, з вказанням будівлі з ОІД, комунікацій, які підключені до будівлі обстежуваного об’єктом, вказанням прилеглих вулиць і будівель відносно ОІД та ін.

– план систем життєзабезпечення ОІД в якому визначається лінія та напрям підключення комунікаційних, пожежних та охоронних систем.

2.3.1 Обстеження фізичного середовища функціонування ІТС

При обстеженні фізичного середовища функціонування ІТС аналізу підлягали наступні характеристики:

– територіальне розташування компонентів ІТС (ситуаційний план, генеральний план);

– наявність охорони території та перепускний режим;

– наявність категорійованих приміщень, в яких мають розміщуватися компоненти ІТС;

– режим доступу до компонентів фізичного середовища ІТС;

– наявність елементів комунікацій, систем життєзабезпечення і зв’язку, що мають вихід за межі контрольованої зони;

Офіс ТОВ «Вебпіар» знаходиться в центрі міста за адресою: м. Дніпро, вул. Європейська, буд. 4, оф. 424. Розташований на 4 поверсі 7-поверхової офісної будівлі.

Фірма працює з понеділка по п’ятницю. Вихідні дні – субота та неділя. Графік роботи з 9.30 до 18.30. Прибирання відбувається 1 раз у 2 тижні (у вівторок). Охорона цілодобова. Охоронні послуги надаються ТОВ «ЩИТ-сервіс». Робота охорони відбувається в 2 зміни (з 18:00 до 9:00 та з 9:00 до 18:00). Територія офісної будівлі оздоблена зовнішнім контрольно-пропускним пунктом зі шлагбаумом на півночі, черговим пунктом з турнікетом на центральному вході, а також зовнішніми кодовими дверима на півдні (ситуаційний план наведено у Додатку Б). На кожному поверсі будівлі розміщені камери відеоспостереження (на сходовому майданчику та в коридорі). Відеоспостереження ведеться з чергового пункту, який розташований на 1 поверсі.

За сусідством розташовані й інші організації, такі як: на півдні– головний офіс ТОВ «Севен Севенті Петроліум», на півночі – аварійні сходи і ліфт, на

заході - адвокатське бюро Олега Бовкуна та редакція газети «Aviso» (генеральний план наведено у Додатку В).

Таблиця 2.1 – Прилеглі будівлі відносно ОІД ТОВ «Вебпіар»

№	Тип споруди	Адреса	Розташування відносно ОІД	Мінімальна відстань від ОІД до споруди
1	Житловий будинок	вул. Глінки, 15	північ	60 метрів
2	Ресторан	вул. Глінки, 16	північ-схід	65 метрів
3	Житловий будинок	вул. Європейська, 8Б	Північ-схід-схід	45 метрів
4	Офісна будівля	вул. Глінки, 12	схід	50 метрів
5	Учбовий заклад	вул. Глінки, 11	південь-схід	25 метрів
6	Офісна будівля	вул. Глінки, 11А	південь	35 метрів
7	Офісна будівля	вул. Європейська, 4А	Південь-захід	50 метрів
8	Житловий будинок	вул. Європейська, 2	захід	50 метрів
9	ТРЦ	Європейська площа, 1Д	Північ-захід	100 метрів

Таблиця 2.2 – Прилеглі вулиці відносно ОІД ТОВ «Вебпіар»

№	Назва вулиці	Опис
1	вул. Європейська	Знаходиться на північному сході відносно ОІД, в 10 метрах від ОІД, інтенсивність руху – 300 автомобілів в годину, ширина проїжджої частини – 5 метрів (односмугова в північному напрямі), ширина пішохідної частини – 2 метри (2 метри ліворуч та 2 метри праворуч відносно вулиці), уздовж вулиці є можливість паркування.
2	Європейська площа	Знаходиться на півночі відносно ОІД, в 2 метрах від ОІД, проїжджої частини немає, ширина пішохідної частини – 30 метрів, паркування відбувається на північному сході (кінцева зупинка громадського транспорту).
3	вул. Глінки	Знаходиться на сході відносно ОІД, в 2 метрах від ОІД, ширина проїжджої частини – 6 метрів (односмугова в західному напрямі), ширина пішохідної частини – 8 метрів, уздовж вулиці є можливість паркування.
4	вул. Центральна	Знаходиться на заході відносно ОІД, в 80 метрах від ОІД, проїжджої частини немає, ширина пішохідної частини – 6 метрів, паркування автомобілів відбувається на початку та кінці вулиці (в спеціально відведених місцях).
5	вул. Харківська	Знаходиться на півдні відносно ОІД, в 60 метрах від ОІД, ширина проїжджої частини – 8 метрів (двосмугова в північному та південному напрямі), ширина пішохідної частини – 4 метри (2 метри ліворуч та 2 метри праворуч відносно вулиці), уздовж вулиці є можливість паркування.

Зовнішні стіни будівлі виконані з бетону, фундамент будівлі – подушка з щебню. Дах виконаний з рубероїдної покрівлі. Територія навколо будівлі з обстежуваним ОІД заасфальтована на задньому дворі (південний схід), а на заході має бруківельне покриття (пішохідна зона Європейської площі). Вхідні двері центрального входу металопластикові, складаються з 3 блоків. Вхідні двері запасного входу металеві.

Системи електропостачання ОІД підключені до трансформаторної підстанції (ТП) №172 (що обслуговується «ДТЕК Дніпровські електромережі») і з'єднуються з міською системою електропостачання надземним способом.

Лінії електроживлення проведені від ТП до головного розподільного щитка, що розташований на 1 поверсі приміщення. Від головного розподільного щитка лінії електропостачання проведені вгору до розподільного щитка (ЩО-1), який розташований на кожному поверсі. Від цих щитків лінії електропостачання під'єднані до ОІД.

Каналізаційні системи будівлі ОІД підключені до каналізаційних систем міста підземним способом. Ці системи обслуговуються ЖЕК №18

Системи водопостачання будівлі ОІД підключені до систем водопостачання міста підземним способом та обслуговуються КП «Дніпроводоканал». З'єднання регулюється в підвальному приміщенні.

Матеріал труб – пластиковий.

Системи теплопостачання будівлі ОІД підключені до міської системи теплопостачання за допомогою теплотраси і обслуговуються КП «Теплоенерго». Напрям руху теплоносія по стояку – знизу-вгору. Рух теплоносія по стояку починається від підвального приміщення до останнього поверху будівлі.

Тип підключення: двотрубна горизонтальна система опалення з розводкою по периметру.

Матеріал труб – металевий.

Стрижні заземлення вкопані у внутрішньому дворі. Заземлені на загальний контур заземлення, який є замкнутим і виходить за межі КЗ.

Телефонна лінія підключена до АТС-322 «Укртелеком» кабелем діаметром 24 мм маркування ТПП 100 * 2 * 0.4. На офіс відведено 2 номери.

Підключення до мережі Інтернет відбувається від комутатора, що розташований на поверсі до маршрутизатора за допомогою кабелю UTP cat. 5e. Послуги надаються Інтернет-провайдером «Укртелеком».

Контрольована зона (КЗ) визначена наказом керівника підприємства №3 від 28.08.2015 р. і обмежена площею офісу. ОІД обладнано системою пожежної сигналізації та контролю доступу. Офіс підключено до пульту приватного охоронного підприємства «ЩИТ-сервіс».

Товщина зовнішніх стін - 500 мм.

Висота перекриття - 2900 мм.

Склад внутрішніх стін - оштукатурений гіпсокартон.

Стеля - залізобетонна монолітна заливна товщиною 150 мм.

Підлога - монолітна бетонна стяжка товщиною 100 мм.

Покриття підлоги - ламінована підлога 10 мм.

Вікна (1 шт. розміром 1400Х1400 мм; 2 шт. розміром 1800Х1400 мм) - металопластикові з двокамерним склопакетом. товщина скла 3 мм. На всіх вікнах знаходяться горизонтальні жалюзі.

Внутрішні двері (1 шт.) Типові дерев'яні одностулкові, розміром 950х2100 мм. товщиною 40 мм.

Зовнішні (1 шт. - двостулкові розміром 950х2100 мм.) – дерев’яні, завтовшки 100 мм. Замок врізний, основний. Тип металу – хром.

Загальна площа ОІД – 27 м^2.

2.3.2 Обстеження ІТС ТОВ «Вебпіар»

Локальна мережа фізично має архітектуру «зірка». Вихід в інтернет здійснюється через кабель Ethernet підключеного до Wi-Fi роутера, з'єднання здійснюються за допомогою екранованого кабелю «вита пара».

Обладнання, за допомогою якого оброблюється інформація на ОІД:

1 Ноутбук проектного менеджера 1;

2 Ноутбук проектного менеджера 2;

3 Ноутбук генерального директора;

4 Ноутбук фінансового директора;

5 Принтер, що з’єднаний з ноутбуком фінансового директора;

6 Комп’ютер менеджера з SEO-оптимізації;

7 Комп’ютер менеджера з налаштування контекстної реклами;

8 Комп’ютер програміста;

9 Комп’ютер копірайтера;

10 Wi-Fi маршрутизатор

11 Мережа Internet

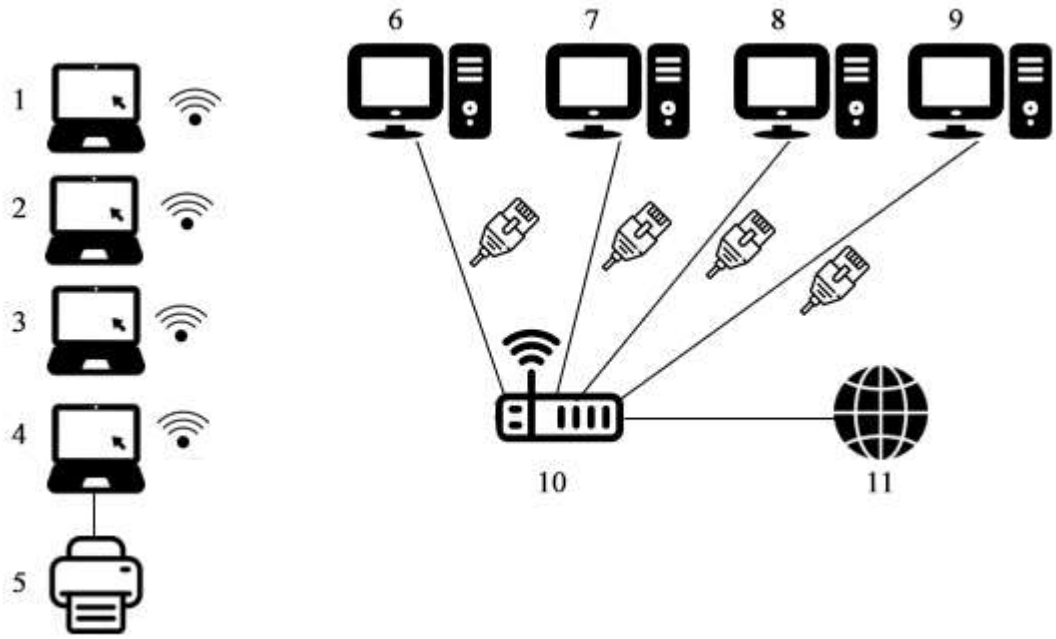


Рисунок 2.2 – Функціональна схема мережі ОІД ТОВ «Вебпіар»

Ноутбуки проектних менеджерів, генерального директора і фінансового директора (1, 2, 3, 4) мають бездротове підключення до Wi-Fi маршрутизатора.

Комп’ютери SEO-менеджерів, програміста і менеджера з налаштування контекстної реклами і копірайтера, (6, 7, 8, 9) підключені до Wi-Fi маршрутизатора (10) за допомогою кабелю UTP cat. 5e.

Всі комп’ютери і ноутбуки належать до однієї робочої групи – WGWEBPR.

На підприємстві використовується АС класу 3 – розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності. Де є необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

У зв'язку з тим, що є 2 види АРМ, розглянемо склад системи і склад ПЗ ноутбуків і комп'ютерів ОІД.

Таблиця 2.3 – Апаратний склад комп'ютера ТОВ «Вебпіар»

Тип	Повна назва	Серійний номер	Обсяг (Потужність)
Процесор	Core i3 2x2800 МГц	763Q6279-i3	–
Материнська плата	ASRock Socket 1155 Z77M	391MP53888/2	–
Графічний відеоадаптер	nVidia GTX 550 ti	392082SER/550ti	1024 Мб
ОЗП	Goodram DDR3 1300	RAM291073YT	4096 Мб
ПЗП (SSD)	Samsung Evo 860 SATA III	20374518195372-860	256 Гб
Монітор	LG 19EN33	LG920361192-EN33	–
Блок живлення	V-Power 750QQ	2910Q92-750	750 Вт
Дротова клавіатура	Logitech K200	2073K949w71690	–
Дротова мишка	Logitech M100	302918M6371922T	–

Таблиця 2.4 – Апаратний склад ноутбука ТОВ «Вебпіар»

Тип	Повна назва	Серійний номер	Обсяг (Потужність)
Процесор	Core i3 2x2800 МГц	357Z65412-i3	–
Материнська плата	Globex MPlate P3310	U6382I03729	–
Графічний відеоадаптер	nVidia GeForce 920M	209641SER/920M	2048 Мб
Інтегрований відеоадаптер	Intel HD 5500	8930201T94302-5500	2048 Мб
ОЗП	HyperX 3D 2133	203846820O	4096 Мб
ПЗП (SSD)	Grotex Speed+ L2 SATA 2.5	8392916JJ829ON	512 Гб
Дротова мишка	Logitech M310	1825LZ002379	–

Таблиця 2.5 – Склад ПЗ комп'ютера ТОВ «Вебпіар»

№	Повна назва	Тип ПЗ	Наявність	Кількість

			ліцензії	ПЗ
А	nVidia GeForce Experience	Системне	Є	4
Б	DriverPack Solution	Системне	Є	4

Продовження таблиці 2.5

№	Повна назва	Тип ПЗ	Наявність ліцензії	Кількість ПЗ
В	Win7_8_10x64_LG19EN33_driver	Драйвери	Є	4
Г	Google Chrome	Прикладне	Є	4
Ґ	Opera	Прикладне	Є	4
Д	FileZilla	Прикладне	Є	2
Е	Skype	Прикладне	Є	4
Є	Viber	Прикладне	Є	4
Ж	Telegram Desktop	Прикладне	Є	4
З	Microsoft Office 2013 SP1	Прикладне	Немає	4
И	ESET NOD 32	Спеціалізоване	Немає	4
І	Notepad++	Прикладне	Є	3
Й	TesauRUS	Прикладне	Немає	1
К	Windows 10 Home Single	Системне	Є	4

Таблиця 2.6 – Склад ПЗ ноутбука ТОВ «Вебпіар»

№	Повна назва	Тип ПЗ	Наявність ліцензії	Кількість ПЗ
	nVidia GeForce Experience	Системне	Є	4
	DriverPack Solution	Системне	Є	4
Л	HP_LJ1018_driver_win10x64_win7x64	Драйвери	Є	1
	Google Chrome	Прикладне	Є	4
	Opera	Прикладне	Є	4
М	TeamViewer	Прикладне	Є	1
	Skype	Прикладне	Є	4
	Viber	Прикладне	Є	4
	Telegram Desktop	Прикладне	Є	4
	Microsoft Office 2013 SP1	Прикладне	Немає	4
	ESET NOD 32	Спеціалізоване	Немає	4
	Notepad++	Прикладне	Є	2
	TesauRUS	Прикладне	Немає	2
	Windows 10 Home Single	Системне	Є	4

Таблиця 2.7 – Корпусний опис основних технічних засобів ТОВ «Вебпіар»

Тип	Ім’я	Інвентарний	Місце	Мінімальна

		номер	розташування	відстань до кордонів ОІД
Принтер	HP LaserJet 1018	20043929001	На столі	2100 мм
Маршрутизатор	TP-Link TL-WR841N	20043929010	На столі	200 мм
Монітор	LG 19EN33	200439290021	На столі	2000 мм

Продовження таблиці 2.7

Тип	Ім’я	Інвентарний номер	Місце розташування	Мінімальна відстань до кордонів ОІД
Монітор	LG 19EN33	200439290031	На столі	2000 мм
Монітор	LG 19EN33	200439290041	На столі	1300 мм
Монітор	LG 19EN33	200439290051	На столі	1300 мм
Системний блок	Lenovo IdeaCentre 300	20043929002	На підлозі	1300 мм
Системний блок	Lenovo IdeaCentre 300	20043929003	На підлозі	1300 мм
Системний блок	Lenovo IdeaCentre 300	20043929004	На підлозі	2100 мм
Системний блок	Lenovo IdeaCentre 300	20043929005	На підлозі	2100 мм
Ноутбук	HP 15-g023er	20043929008	На столі	600 мм
Ноутбук	HP 15-g023er	20043929009	На столі	600 мм
Ноутбук	HP 15-g023er	20043929011	На столі	800 мм
Ноутбук	HP 15-g023er	20043929012	На столі	800 мм

Крім основних технічних засобів на ОІД також фігурують допоміжні технічні засоби і системи.

Таблиця 2.8 – Опис елементів ДТЗС ТОВ «Вебпіар»

Тип	Ім’я	Інвентарний номер	Місце розташування	Мінімальна відстань до кордонів ОІД
Мікрохвильова піч	Perfezza FZ-0719	20043929100	На столі	300 мм
Електрочайник	Vitek VT-7008	20043929101	На столі	300 мм
Електрочайник	Vitek VT-7008	20043929102	На столі	500 мм
Дротовий телефон	Panasonic KX-TS2356	20043929104	На столі	100 мм
Дротовий телефон	Panasonic KX-TS2356	20043929105	На столі	300 мм

Датчик диму	Артон СПД-3	20043929106	На стелі	950 мм
Датчик диму	Артон СПД-3	20043929107	На стелі	1550 мм
ПКП	Тирас 4П	20043929108	На стіні	100 мм

Облік місця та режиму зберігання носіїв інформації а також їх переміщення на обстежуваному ОІД не ведеться.

2.3.3 Обстеження інформаційного середовища функціонування ІТС

В ТОВ «Вебпіар» оброблюється та зберігається багато інформації з обмеженим доступом – картка клієнта на проведення робіт, БД клієнтів, фінансові звіти та ін. Неправомірний доступ або втрата інформації може привести до втрати клієнтів, погіршення фінансового положення та втрати іміджу. Саме тому необхідно забезпечити захист інформаційних ресурсів від несанкціонованих дій.

Вся інформація створюється і зберігається за допомогою хмарових сервісів Google Cloud.

Таблиця 2.9 – Аналіз оброблювальної інформації ТОВ «Вебпіар»

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
I	Картка клієнта на проведення робіт	Електронний, паперовий	ІзОД	Службова	КЦД
II	Щомісячний фінансовий звіт	Електронний	ІзОД	Комерційна таємниця	КЦД
III	Щорічний фінансовий звіт	Електронний	ІзОД	Комерційна таємниця	КЦД
IV	БД клієнтів	Електронний	ІзОД	Комерційна таємниця	КЦД
V	Адміністративні дані сайту	Електронний	ІзОД	Службова	КЦД
VI	Звіт про нарахування зарплати	Електронний, паперовий	ІзОД	Службова	КЦД
VII	Відомості про працівників	Електронний	ІзОД	Службова	КЦД
VIII	Технічне завдання програмісту	Електронний	ІзОД	Службова	ЦД
IX	Технічне завдання SEO-	Електронний	ІзОД	Службова	ЦД

	менеджеру				
X	Технічне завдання менеджеру з налаштування контекстної реклами	Електронний	ІзОД	Службова	ЦД
XI	Контент майбутнього сайту	Електронний	Відкрита	-	ЦД

Продовження таблиці 2.9

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
XII	Технічне завдання копірайтеру	Електронний	ІзОД	Службова	ЦД
XIII	Акт на закупівлю додаткового апаратного та/або програмного забезпечення	Електронний	ІзОД	Службова	КЦД
XIV	Звіт виконаних робіт проекту	Електронний	ІзОД	Службова	КЦД
XV	Банківські дані підприємства (о/р, ЄДРПОУ та ін.)	Електронний, паперовий	Відкрита	-	ЦД

К – вимоги до конфіденційності;

Ц – вимога до цілісності;

Д – вимога до доступності;

Вся оброблювальна інформація створюється і зберігається в Google Cloud.

Після проведення перемовин між генеральним директором і клієнтом і підписання контракту, голова компанії закріпляє за проектним менеджером цього клієнта.

Проектний менеджер в очній або дистанційній формі (з використанням телефону або Skype) разом з клієнтом заповнює Картку клієнта на проведення робіт, в якій вказуються особисті дані (ПІБ клієнта, телефон). Ці дані проектний менеджер вносить (з використанням клавіатури) в БД клієнтів, яка знаходиться в хмарній базі даних Google BigQuery. Окрім особистих даних клієнта, вказується тип виконуваних робіт та примітки.

Після формування Картки клієнта на проведення робіт, фінансовий директор надсилає клієнту Банківські дані підприємства (о/р, ЄДРПОУ та ін.). Ці дані надсилаються з використанням месенджеру Telegram або Viber.

Після цього, проектний менеджер в Google Документ формує Акт на закупівлю додаткового апаратного та/або програмного забезпечення на закупівлю необхідного ПЗ для виконання проектних завдань і надає доступ до редагування для облікового запису фінансового директора. Отриману URL-адресу проектний менеджер надсилає фінансовому директору за допомогою месенджеру Telegram.

Отримавши Картку клієнта на проведення робіт, проектний менеджер створює облікові записи, які необхідні для адміністрування сайту (особистий кабінет в хостингу, Google AdWords, додаткових віджетів та ін.). Всі логіни і паролі до облікових записів зберігаються в спеціальному документі в сервісі Google Документи – Адміністративні дані сайту. Після завершення проектних робіт, проектний менеджер надає доступ до документа обліковому запису системного адміністратора клієнта.

Проектний менеджер створює Технічне завдання програмісту в сервісі Google Документ. Після цього, проектний менеджер надає доступ до читання та коментування для облікового запису програміста. Отриману URL-адресу проектний менеджер надсилає програмісту за допомогою месенджеру Telegram.

Проектний менеджер створює Технічне завдання SEO-менеджеру в сервісі Google Документ. Після цього, проектний менеджер надає доступ до читання та коментування для облікового запису SEO-менеджеру. Отриману URL-адресу проектний менеджер надсилає SEO-менеджеру за допомогою месенджеру Telegram.

Проектний менеджер створює Технічне завдання менеджеру з налаштування контекстної реклами в сервісі Google Документ. Після цього, проектний менеджер надає доступ до читання та коментування для облікового запису менеджеру з налаштування контекстної реклами. Отриману URL-адресу

проектний менеджер надсилає менеджеру з налаштування контекстної реклами за допомогою месенджеру Telegram.

Проектний менеджер створює Технічне завдання копірайтеру в сервісі Google Документ. Після цього, проектний менеджер надає доступ до читання та коментування для облікового запису копірайтера. Отриману URL-адресу проектний менеджер надсилає копірайтеру за допомогою месенджеру Telegram.

Надіславши технічне завдання своїм підлеглим, проектний менеджер розроблює Контент майбутнього сайту: в Google Документ він створює файл, в якому будує структуру сайту – сторінки, розташування графічних і текстових блоків та ін. Цей документ підлягає редагуванню, адже на етапі розробки сайту, клієнт (він же замовник сайту) вносить свої коригування.

Виконавши всі поставленні завдання в Картці клієнта на проведення робіт, проектний менеджер формує в Google Документ Звіт виконаних робіт проекту, в якому освітлює графік виконання робіт, графічно ілюструє виконану роботу. Доступ до цього звіту надається клієнту для ознайомлення, а URL-адреса закріпляється в хмаровій базі даних Google BigQuery (в документі БД клієнтів).

Щомісячно в Google Документ оновлюється Звіт про нарахування зарплати, в якому фінансовий директор звітує перед головним директором щодо заробітної плати персоналу. Фінансовий директор надає доступ до читання цього документу обліковому запису головного директора.

В хмарній базі даних Google BigQuery зберігаються Відомості про працівників – особисті дані, ІПН, серія та номер паспорту, особовий банківський рахунок для нарахування заробітної плати. Відповідальність за конфіденційність персональних даних покладена на фінансового директора.

Наприкінці поточного місяця фінансовий директор формує Щомісячний фінансовий звіт в сервісі Google Таблиця. До цього документу фінансовий директор надає доступ до читання головному директору і надсилає отриману URL-адресу в месенджері Telegram.

Отримані фінансові дані 12 місячних звітів висвітлюються в Щорічному фінансовому звіті, який створюється наприкінці поточного року в сервісі Google Таблиця. Фінансовий директор надає доступ до читання обліковому запису головного директора і надсилає отриману URL-адресу в месенджері Telegram.

2.3.4 Обстеження середовища користувачів ІТС

1. Головний директор – 1 людина. Координує роботу всіх відділів.

2. Фінансовий директор – 1 людина. Веде бухгалтерський та фінансовий облік, а також проводять інші економічні розрахунки.

3. Проектний менеджер – 2 людини. Заповнюють проектну картку клієнта, визначають обсяги виконуваних робіт, пишуть ТЗ (технічні завдання) програмісту, менеджеру з SEO оптимізації, менеджеру з налаштування контекстної реклами, копірайтеру (за необхідністю), перевіряють виконані роботи, налаштовують додаткове ПЗ (за необхідністю), проводять аналіз виконаних робіт, пишуть звіт виконаних робіт, здають проект, отримують винагороду, відстежують роботу сайту за допомогою сервісу Google Analytics.

4. Програміст – 1 людина. Отримує ТЗ від проектного менеджера, проводить оцінку майбутніх робіт (в грошовому та часовому сенсі), надає оцінену інформацію проектному менеджеру, виконує поставлені завдання згідно ТЗ, звітує перед проектним менеджером про виконаний обсяг робіт, вносить виправлення (якщо вони є) в виконану роботу.

5. Менеджер з SEO оптимізації – 1 людина. Отримує ТЗ (технічне завдання) від проектного менеджера, проводить SEO-аналіз сайту, пише ТЗ проектному менеджеру (для ознайомлення з обсягами робіт) та програмісту, отримує виправлення від ПМ, виконує роботи, звітує перед ПМ про виконані роботи, вносить виправлення (якщо вони є) в виконану роботу.

6. Менеджер з налаштування контекстної реклами – 1 людина. Отримує ТЗ від проектного менеджера, оцінює завдання, доповідає про це проектному

менеджеру, виконує поставлені роботи, вносить виправлення (якщо вони є) в виконану роботу.

7. Копірайтер – 1 людина. Отримує ТЗ від проектного менеджера, оцінює завдання, доповідає про це проектному менеджеру, виконує роботи, звітує перед проектним менеджером, вносить виправлення (якщо вони є) в виконану роботу.

Роботу системного адміністратора виконує проектний менеджер.

Всього – 8 осіб.

Перелік інформації наведений в таблиці 2.9.

Таблиця 2.10 – Матриця доступу до інформації ТОВ «Вебпіар»

Інформація	Посада						
	1	2	3	4	5	6	7
I	-	RW	RWD	-	-	-	-
II	R	RWD	-	-	-	-	-
III	R	RWD	-	-	-	-	-
IV	R	R	RW	-	-	-	-
V	-	-	RWD	RW	RW	RW	RW
VI	R	RWD	-	-	-	-	-
VII	R	RWD	-	-	-	-	-
VIII	-	-	RWD	R	-	-	-
IX	-	-	RWD	-	R	-	-
X	-	-	RWD	-	-	R	-
XI	-	-	RWD	-	RW	RW	RWD
XII	-	-	RWD	-	-	-	R
XIII	R	RWD	-	-	-	-	-
XIV	R	R	RWD	-	-	-	-
XV	RWD	RWD	-	-	-	-	-

R – перегляд інформації; W – модифікація інформації; D – знищення інформації

Перелік ПЗ наведено в таблиці 2.5 та таблиці 2.6.

Таблиця 2.11 – Матриця доступу до ПЗ ТОВ «Вебпіар»

ПЗ	Посада						
	1	2	3	4	5	6	7
A	-	-	IWU	-	-	-	-

Б	-	-	IWU	-	-	-	-
В	-	-	-	IWU	IWU	IWU	IWU
Г	W	W	IWU	W	W	W	W
Ґ	W	W	IWU	W	W	W	W
Д	-	-	IWU	W	W	-	-
Е	W	W	IWU	W	W	W	W
Є	W	W	W	W	W	W	W
Ж	W	W	W	IW	IW	IW	IW
З	W	W	IWU	W	W	W	W
И	W	W	IWU	W	W	W	W
І	-	-	IWU	W	W	W	-
Й	-	-	IWU	-	-	-	W
К	W	W	IWU	W	W	W	W
Л	-	IWU	-	-	-	-	-
М	IWU	-	-	-	-	-	-

I – інсталяція ПЗ; W – використання ПЗ; U – деінсталяція ПЗ

2.4 Аналіз та оцінка інформаційних ризиків

Для аналізу та оцінки інформаційних ризиків проведемо класифікацію, інформації, оброблювальної в АС.

Модель класифікації інформаційних ресурсів характеризують ознаки: конфіденційність, цілісність та доступність. Таким чином, можливо визначити найцінніший інформаційний ресурс ІТС. Класифікацію інформації наведено в таблицях 2.12-2.14.

Таблиця 2.12 – Класифікація інформації за конфіденційністю

Рівень	Ступінь важливості	Оцінка	Характеристика
К1	Малозначима інформація	1	Розголошення цієї інформації не призведе до збитків підприємства.
К2	Значима інформація	2	Розголошення цієї інформації призведе до певних збитків в певних ситуаціях.
К3	Важлива інформація	3	Розголошення цієї інформації призведе до певних збитків підприємства, якщо не буде протидій.
К4	Дуже важлива	4	Розголошення цієї інформації призведе до збитків підприємства, якщо не буде протидій.
К5	Критично важлива інформація	5	Розголошення цієї інформації призведе до суттєвих збитків підприємства та подальшого

			банкрутства.

Таблиця 2.13 – Класифікація інформації за цілісністю

Рівень	Ступінь важливості	Оцінка	Характеристика
Ц1	Мало значима інформація	1	Модифікація інформації не призведе до збитків підприємства.
Ц2	Значима інформація	2	Модифікація інформації призведе до певних збитків в певних ситуаціях.
Ц3	Важлива інформація	3	Модифікація інформації призведе до певних збитків підприємства, якщо не буде протидій.
Ц4	Дуже важлива	4	Модифікація інформації призведе до збитків підприємства, якщо не буде протидій.

Продовження таблиці 2.13

Рівень	Ступінь важливості	Оцінка	Характеристика
Ц5	Критично важлива інформація	5	Модифікація інформації призведе до суттєвих збитків підприємства та подальшого банкрутства.

Таблиця 2.14 – Класифікація інформації за доступністю

Рівень	Ступінь важливості	Оцінка	Характеристика
Д1	Мало значима інформація	1	Інформація, яка не впливає на роботу ресурсів і не завдає збитків.
Д2	Значима інформація	2	Інформація, яку можна замінити задля роботи ресурсів, але її використання економить ресурси.
Д3	Важлива інформація	3	Інформація, яку можна замінити на певний час задля роботи ресурсів, але вона все-одно знадобиться.
Д4	Дуже важлива	4	Інформація, яку можна замінити на короткий проміжок часу задля роботи ресурсів, але вона все-одно знадобиться.
Д5	Критично важлива інформація	5	Інформація, без якої підприємство не зможе функціонувати.

Оцінка інформації, яка циркулює на ОІД (у відповідності до класифікованої раніше моделі інформаційних ресурсів), наведена в таблиці 2.15.

Таблиця 2.15 – Оцінка інформації, яка циркулює на ОІД

Інформація	Ступінь важливості			Всього
	К	Ц	Д	
Картка клієнта на проведення робіт	4	5	3	12
Щомісячний фінансовий звіт	5	5	4	14
Щорічний фінансовий звіт	5	5	5	15
БД клієнтів	5	4	5	14
Адміністративні дані сайту (логін і пароль від хостингу, доступи до FTP та ін.)	4	3	3	10
Звіт про нарахування зарплати	4	3	3	10
Відомості про працівників	4	4	3	11
Технічне завдання програмісту	2	1	2	5
Технічне завдання SEO-менеджеру	2	1	2	5
Технічне завдання менеджеру з налаштування контекстної реклами	2	1	2	5

Продовження таблиці 2.15

Інформація	Ступінь важливості			Всього
	К	Ц	Д	
Контент майбутнього сайту	1	1	2	4
Технічне завдання копірайтеру	2	1	2	5
Акт на закупівлю додаткового апаратного та/або програмного забезпечення	2	2	3	7
Звіт виконаних робіт проекту	3	2	4	9
Банківські дані підприємства (о/р, ЄДРПОУ та ін.)	1	5	5	11

К – конфіденційність; Ц – цілісність; Д – доступність.

Аналізуючи отримані дані та спираючись на НД ТЗІ 2.5.005-99 [14] був визначений функціональний профіль захищеності в КС, що входять до складу АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації.

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

Згідно з НД ТЗІ 2.5.004-99 [11]:

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.

КА-2 – Базова 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.

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.

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.

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.

ЦА-2 – Базова 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.

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.

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.

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.

ДВ-1 – Ручне 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.

НР-2 – Захищений журнал. 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.

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.

НК-1 – Однонаправлений 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.

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.

НЦ-2 – КЗЗ з гарантованою цілісністю. Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

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.

НВ-1 – Автентифікація вузла. 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.

Спираючись на отримані дані в таблиці 2.15 можна зробити підсумок, що належному захисту підлягають наступний перелік інформації (сума балів яких вище 7): картка клієнта на проведення робіт, щомісячний фінансовий звіт, щорічний фінансовий звіт, БД клієнтів, адміністративні дані сайту (логін і пароль від хостингу, доступи до FTP та ін.), звіт про нарахування зарплати, відомості про працівників, звіт виконаних робіт проекту та банківські дані підприємства (о/р, ЄДРПОУ та ін.).

Розглянемо модель загроз.

Використаємо методику побудови моделі загроз від НСД, яка складається з класифікації джерел загроз, класифікації вразливостей та аналізу взаємозв'язку загроз та вразливостей з подальшим вирахуванням коефіцієнту небезпеки.

Джерела загроз можна розділити на антропогенні, техногенні та стихійні, за допомогою яких в подальшому вираховується коефіцієнт рівня небезпеки.

Коефіцієнт небезпеки вираховується за допомогою наступної формули:

$$К_{неб} = \frac{К_1 \times К_2 \times К_3}{125} \quad (2.1)$$

де $К_1$, $К_2$, $К_1$ – показники критеріїв джерел загроз (оцінюється в межах від 1 до 5);

125 – максимальне число добутків показників К.

Для антропогенних джерел загроз коефіцієнти визначають:

$К_1$ – ступінь доступності до об'єкту;

$К_2$ – ступінь кваліфікації і мотивації;

$К_3$ – рівень наслідків (фатальність).

Таблиця 2.16 – Антропогенні джерела загроз

Джерело загроз	$К_1$	$К_2$	$К_3$	$К_1*К_2*К_3$	$К_{неб}$
Проектний менеджер	5	4	5	100	0,800
Програміст	3	3	3	27	0,216
Менеджер з SEO-оптимізації	4	2	2	16	0,128
Менеджер з налаштування контекстної реклами	4	2	2	16	0,128
Фінансовий директор	5	1	3	15	0,120
Копірайтер	3	1	1	3	0,024
Хакери	2	4	5	40	0,320
Конкуренти	2	5	4	40	0,320
Технічний персонал (майстри з налаштування Інтернету, кур'єр)	4	2	2	16	0,128

Для техногенних джерел загроз коефіцієнти визначають:

$К_1$ – ступінь віддаленості від об'єкту захисту (можливість виникнення);

$К_2$ – наявність необхідних умов;

$К_3$ – рівень наслідків (фатальність).

Таблиця 2.17 – Техногенні джерела загроз

Джерело загроз	$К_1$	$К_2$	$К_3$	$К_1*К_2*К_3$	$К_{неб}$
Неякісне апаратне забезпечення	4	2	4	32	0,256
Неліцензоване програмне забезпечення	3	3	5	45	0,36
Неякісні ДТЗС	2	2	3	12	0,096
Система доступу до мережі Інтернет	4	3	4	48	0,384
Телефонні лінії зв'язку	3	2	3	18	0,144
Мережі інженерних комунікацій	3	3	4	36	0,288

Для стихійних джерел загроз коефіцієнти визначають:

$К_1$ – особливості місцевості;

$К_2$ – наявність необхідних умов;

$К_3$ – рівень наслідків (фатальність).

Таблиця 2.18 – Стихійні джерела загроз

Джерело загроз	$К_1$	$К_2$	$К_3$	$К_1*К_2*К_3$	$К_{неб}$
Пожежа	3	4	4	48	0,384
Землетрус	2	1	2	4	0,032
Повінь	2	1	2	4	0,032

Ураган	1	1	2	2	0,016
Інші нез'ясовані явища	1	1	2	2	0,016

Джерела загроз з коефіцієнтом нижче 0,1 вважаються неактуальними.

Найбільш небезпечні вразливості можна розділити на об'єктивні, суб'єктивні і випадкові.

Для класифікації вразливостей визначаються наступні критерії:

$К_1$ – ступінь впливу вразливості на неусунення наслідків (фатальність);

$К_2$ – можливість (зручність) використання вразливості джерелом загроз

$К_3$ – кількість елементів об'єкту.

Коефіцієнт небезпеки вразливостей визначається так само, як і коефіцієнт небезпеки джерела загроз (згідно з формулою (2.1)).

Виконаємо ранжування вразливостей.

Таблиця 2.19 – Об'єктивні вразливості

Вразливість	$К_1$	$К_2$	$К_3$	$К_1*К_2*К_3$	$К_{неб}$
1. Вразливості, що активізуються					
1.1 Апаратні закладки	3	3	2	18	0,144
1.2 Неліцензоване ПЗ	3	3	3	27	0,216
2. Вразливості, які обумовлені особливостями об'єкта захисту					
2.1 Використання Wi-Fi каналу при передачі ІзОД	3	3	2	18	0,144
2.2 Місцезнаходження об'єкту	2	2	2	8	0,064

Таблиця 2.20 – Суб'єктивні вразливості

Вразливість	$К_1$	$К_2$	$К_3$	$К_1*К_2*К_3$	$К_{неб}$
3. Помилки					
3.1 Помилки користувачів системи	3	3	3	27	0,216
3.2 Помилки системного адміністратора	5	4	3	60	0,480
3.3 Помилки при використані засобів обміну інформацією (з використанням месенджерів)	4	3	3	36	0,288
4. Порушення					
4.1 Порушення режиму конфіденційності	5	4	5	100	0,800
4.2 Порушення режиму доступу на об'єкт	5	2	4	8	0,320

Таблиця 2.21 – Випадкові вразливості

Вразливість	$К_1$	$К_2$	$К_3$	$К_1*К_2*К_3$	$К_{неб}$

5. Збої та відмови					
5.1 Старіння і розмагнічування носіїв інформації	3	3	4	36	0,288
5.2 Збої програмного забезпечення	3	2	2	12	0,096
5.3 Збої систем електроживлення	2	3	3	18	0,144
5.4 Відмови в роботі технічних засобів	3	3	3	27	0,216
6. Пошкодження					
6.1 Пошкодження систем життєзабезпечення	3	2	3	18	0,144
6.2 Пошкодження огороджувальних конструкцій	2	1	3	6	0,048

Проаналізуємо взаємозв'язок джерел загроз і вразливостей. Для визначення актуальних загроз аналізуються можливі поєднання джерел загроз і вразливості і розраховується коефіцієнт небезпеки за формулою:

$$К_{неб} = К_{неб\ (дж.з.)} \times К_{неб\ (вр.)} \quad (2.2)$$

Таблиця 2.22 – Взаємозв'язок джерел загроз і об'єктивних вразливостей

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливість	$К_{неб\ (вр.)}$	$К_{неб}$
Антропогенні джерела загроз				
Проектний менеджер	0,800	1.2 Неліцензоване ПЗ	0,216	0,173
		2.1 Використання Wi-Fi каналу при передачі ІзОД	0,144	0,115
		2.2 Місцезнаходження об'єкту	0,064	0,051
Хакери	0,320	1.1 Апаратні закладки	0,144	0,046
		2.1 Використання Wi-Fi каналу при передачі ІзОД	0,144	0,046
		2.2 Місцезнаходження об'єкту	0,064	0,020
Конкуренти	0,320	2.2 Місцезнаходження об'єкту	0,064	0,020
Технічний персонал	0,128	2.2 Місцезнаходження об'єкту	0,064	0,008
Програміст	0,216	1.2 Неліцензоване ПЗ	0,216	0,047
		2.1 Використання Wi-Fi каналу при передачі ІзОД	0,144	0,031
		2.2 Місцезнаходження об'єкту	0,064	0,014
Менеджер з SEO-оптимізації	0,128	1.2 Неліцензоване ПЗ	0,216	0,028
		2.1 Використання Wi-Fi каналу при передачі ІзОД	0,144	0,018
		2.2 Місцезнаходження	0,064	0,008

		об’єкту		
Менеджер з налаштування контекстної реклами	0,128	1.2 Неліцензоване ПЗ	0,216	0,028
		2.1 Використання Wi-Fi каналу при передачі ІзОД	0,144	0,018
		2.2 Місцезнаходження об’єкту	0,064	0,008
Фінансовий директор	0,120	1.2 Неліцензоване ПЗ	0,216	0,026
		2.1 Використання Wi-Fi каналу при передачі ІзОД	0,144	0,017
		2.2 Місцезнаходження об’єкту	0,064	0,008
Техногенні джерела загроз				
Неякісне апаратне забезпечення	0,256	1.1 Апаратні закладки	0,144	0,037
		1.2 Неліцензоване ПЗ	0,216	0,078
		2.1 Використання Wi-Fi каналу при передачі ІзОД	0,144	0,052
Система доступу до мережі Інтернет	0,384	2.1 Використання Wi-Fi каналу при передачі ІзОД	0,144	0,055

Продовження таблиці 2.22

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливість	$К_{неб\ (вр.)}$	$К_{неб}$
Техногенні джерела загроз				
Телефонні лінії зв’язку	0,144	2.2 Місцезнаходження об’єкту	0,064	0,009
Мережі інженерних комунікацій	0,288	2.2 Місцезнаходження об’єкту	0,064	0,018
Стихійні джерела загроз				
Пожежа	0,384	2.2 Місцезнаходження об’єкту	0,064	0,025

Таблиця 2.23 – Взаємозв’язок джерел загроз і суб’єктивних вразливостей

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливість	$К_{неб\ (вр.)}$	$К_{неб}$
Антропогенні джерела загроз				
Проектний менеджер	0,800	3.1 Помилки користувачів системи	0,216	0,173
		3.2 Помилки системного адміністратора	0,480	0,384
		3.3 Помилки при використані засобів обміну інформацією (з використанням месенджерів)	0,288	0,230
		4.1 Порушення режиму конфіденційності	0,800	0,640
Хакери	0,320	4.2 Порушення режиму	0,320	0,102

		доступу на об’єкт		
Конкуренти	0,320	4.2 Порушення режиму доступу на об’єкт	0,320	0,102
Технічний персонал	0,128	4.2 Порушення режиму доступу на об’єкт	0,320	0,041
Програміст	0,216	3.1 Помилки користувачів системи	0,216	0,047
		3.3 Помилки при використані засобів обміну інформацією (з використанням месенджерів)	0,288	0,062
		4.1 Порушення режиму конфіденційності	0,800	0,173
Менеджер з SEO-оптимізації	0,128	3.1 Помилки користувачів системи	0,216	0,028
		3.3 Помилки при використані засобів обміну інформацією	0,288	0,037

Продовження таблиці 2.23

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливість	$К_{неб\ (вр.)}$	$К_{неб}$
Антропогенні джерела загроз				
Менеджер з SEO-оптимізації	0,128	4.1 Порушення режиму конфіденційності	0,800	0,102
Менеджер з налаштування контекстної реклами	0,128	3.1 Помилки користувачів системи	0,216	0,028
		3.3 Помилки при використані засобів обміну інформацією (з використанням месенджерів)	0,288	0,037
		4.1 Порушення режиму конфіденційності	0,800	0,102
Фінансовий директор	0,120	3.1 Помилки користувачів системи	0,216	0,026
		3.3 Помилки при використані засобів обміну інформацією (з використанням месенджерів)	0,288	0,035
		4.1 Порушення режиму конфіденційності	0,800	0,097

Таблиця 2.24 – Взаємозв’язок джерел загроз і випадкових вразливостей

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливість	$К_{неб\ (вр.)}$	$К_{неб}$
Техногенні джерела загроз				

Неякісне апаратне забезпечення	0,256	5.1 Старіння і розмагнічування носіїв інформації	0,288	0,074
Неліцензоване програмне забезпечення	0,36	5.2 Збої програмного забезпечення	0,096	0,035
Система доступу до мережі Інтернет	0,384	5.4 Відмови в роботі технічних засобів	0,216	0,083
Телефонні лінії зв’язку	0,144	5.4 Відмови в роботі технічних засобів	0,216	0,031
Мережі інженерних комунікацій	0,288	5.3 Збої систем електроживлення	0,144	0,041
		6.1 Пошкодження систем життєзабезпечення	0,144	0,041
Стихійні джерела загроз				
Пожежа	0,384	6.2 Пошкодження огороджувальних конструкцій	0,048	0,018

Отримані результати, показники яких більше 0,1, становлять загрозу для ТОВ «Вебпіар».

Розглянемо модель порушника.

Порушника можна класифікувати за 3 рівнями загрози:

1 – низький рівень. Реалізація даної загрози малоймовірна через недостатню кваліфікованість особи та через відсутність доступу до інформаційних активів організації.

2 – середній рівень. Реалізація даної загрози можлива при наявності доступу до інформаційних активів та недостатню кваліфікованість особи.

3 – високий рівень. Реалізація даної загрози найбільш ймовірна при наявності доступу до інформаційних активів та при кваліфікованості особи.

Порушниками обстежуваного ОІД можуть бути:

I. Основний персонал установи (Менеджери, програмісти, копірайтери);

II. Керівництво компанії;

III. Допоміжний персонал установи (прибиральники, кур’єри з постачання води);

IV. Клієнти;

V. Представники служби охорони будівлі;

VI. Конкуренти;

VII. Зацікавлені особи, що знаходяться за межами КЗ (хакери та ін.).

Розглянемо «портрет» порушника, класифікуючи за певними ознаками і визначаючи рівень загрози, яку за собою несе та чи інша несанкціонована дія.

Отриманий «портрет» стане у нагоді при остаточному формуванні моделі порушника.

Таблиця 2.25 – «Портрет» порушника

№	Ознаки порушника	Класифікація порушника	Рівень загрози
1.1	За межами КЗ	За місцем дії	1
1.2	В межах КЗ, без доступу до КС		2

Продовження таблиці 2.25

№	Ознаки порушника	Класифікація порушника	Рівень загрози
1.3	В межах КЗ, з доступом до КС	За місцем дії	3
2.1	В неробочий час	За часом дії	1
2.2	В робочий час		2
2.3	В будь-який час		3
3.1	Має поверхні знання в питаннях захисту інформаційних активів	За рівнем кваліфікації	1
3.2	Знає певні особливості в захисті інформаційних активів		2
3.3	Знає механізми, функції, структуру систем захисту інформаційних активів а також має певні практичні навички в цих питаннях		3
4.1	«Ігрові» дії в мережі	За мотивами	1
4.2	Реакція на догану, невиплату за роботу, злий намір		2
4.3	Промислове шпигунство, продаж інформації		3
5.1	Домашній ПК в мережі	За технічним озброєнням	1
5.2	Робочий ПК в мережі + мови програмування		2
5.3	ПК останнього покоління в мережі та		3

	наявність пакету сучасного ПЗ		

Таблиця 2.26 – Модель порушника

Ознаки порушника	Ймовірні порушники						
	I	II	III	IV	V	VI	VII
За місцем	3	3	2	1	2	2	1
За часом	2	3	2	1	3	3	3
За рівнем кваліфікації	2	2	1	1	1	1	3
За мотивами	2	3	2	3	2	3	3
За технічним озброєнням	2	2	1	1	1	2	3
Підсумок	11	13	8	7	9	11	13

Аналізуючи отримані дані в таблиці 2.26 можна зробити висновок, що загрозу для ТОВ «Вебпіар» становлять порушники, показники яких більше 10, а саме: основний персонал, керівництво компанії, конкуренти та зацікавлені особи, що знаходяться за межами контрольованої зони (хакери, друзі ображеного співробітника та ін.).

Для оцінки ризику було обрано метод Information Security Assessment & Monitoring Method (ISAMM) [17]. Грошові дані, які використовуються при обчисленні збитків є приблизними і можуть змінюватися при різних факторах впливу. Він ґрунтується на трьох базових компонентах: аналіз об'єкта, оцінка ризику, звітність. Цей кількісний метод оцінювання ризиків ІБ відображає їх через щорічні очікувані збитки в грошових одиницях (Annual Loss Expectancy (ALE)). На перших етапах роботи з методом визначаються загрози ІБ.

При оцінці ризику для кожної загрози (Т) оцінюється ймовірність її появи (коефіцієнт небезпеки) – p_T і очікувані наслідки – I_T. Щорічні очікувані збитки ALE_T для конкретної загрози t визначаються добутком імовірності виникнення і впливу загрози:

$$ALE_T = p_T \times I_T \quad (2.3)$$

Також обчислюється сума збитків за об’єктом оцінювання:

$$ALE = \sum_T ALE_T \quad (2.4)$$

Оцінимо проаналізовані в моделі загроз ризики (згідно з таблицями 2.19-2.21).

Таблиця 2.27 – Оцінка ризиків методом ISAMM

Джерело загроз	Вразливість	Ймовірність	Вплив, грн	Очікуваний збиток, грн
Проектний менеджер	1.2	0,173	90 000	15 570
	2.1	0,115	40 000	4 600
	3.1	0,173	50 000	8 650
	3.2	0,384	75 000	28 800
	3.3	0,230	35 000	8 050
	4.1	0,640	100 000	64 000
Хакери	4.2	0,102	75 000	7 650
Конкуренти	4.2	0,102	60 000	6 120
Програміст	4.1	0,173	50 000	8 650

Продовження таблиці 2.27

Джерело загроз	Вразливість	Ймовірність	Вплив, грн	Очікуваний збиток, грн
Менеджер з SEO-оптимізації	4.1	0,102	30 000	3 060
Менеджер з налаштування контекстної реклами	4.1	0,102	30 000	3 060
Всього		0,209	635 000	158 210

Аналізуючи отримані дані можна зробити висновок, що найбільший збиток може завдати порушення конфіденційності проектним менеджером і помилки системного адміністратора (функції якого також виконує проектний менеджер).

2.5 Розробка політики безпеки інформації

Політика безпеки інформації ТОВ «Вебпіар» створена з урахуванням всіх вимог чинного законодавства України, а також з виконанням рекомендацій, наведених у міжнародному стандарті ISO 27001 [18].

Метою розробки політики безпеки є впровадження та ефективне управління інформаційною безпекою організації, яка спрямована на зниженні

ризиків інформаційної безпеки, забезпеченні неперервної роботи установи, дотриманні правил збереження інформаційних активів задля позитивних інформаційних відносин з партнерами і клієнтами, а найголовніше – захист інформаційних активів від зовнішніх та внутрішніх загроз.

У дипломній роботі розробка політики безпеки інформації в інформаційно-телекомунікаційній системі ТОВ «Вебпіар» виконується з урахуванням існуючої політики безпеки, яка містить в собі: політику управління інформаційною безпекою, політику управління інцидентами інформаційної безпеки, політику безпеки інформації з обмеженим доступом.

1) Політика захисту персональних даних:

Прийнято та надано чинності: червень 2019 р.

Відповідальний – системний адміністратор.

Власник документа – генеральний директор організації.

1 Опис. Політика захисту персональних даних складена відповідно до вимог Закону України «Про захист персональних даних» і визначає порядок оброблювання та заходи забезпечення безпеки персональних даних ТОВ «Вебпіар» (далі – Організація).

2 Призначення. Ця політика використовується у випадках, коли Організація оброблює персональні дані своїх Клієнтів, їх співробітників, тощо. В такому разі організація несе відповідальність за збереження захисту оброблювальних персональних даних.

3 Область застосування. Вимоги політики захисту персональних даних стосуються всіх працівників Організації, що працюють з персональними даними Клієнтів.

4 Політика.

4.1 Організація гарантує збереження конфіденційності, цілісності отриманих відомостей, що несуть персональні дані, а також унеможливлює несанкціонований доступ до них неуповноваженими особами.

4.2 Працівники Організації починають роботу з відомостям, що несуть персональні дані тільки у разі згоди Клієнта, які зазначені у відповідних документах.

4.3 Працівники Організації вносять до Бази даних тільки прізвище, ім’я, по-батькові, контактний телефон Клієнта і перелік виконаних робіт попередньо шифруючи ці дані власним 6-значним паролем в базі даних. Пароль повинен містити латинські літери і цифри.

4.4 При передачі відомостей, що містять персональні дані (з використанням Wi-Fi каналу) працівник Організації повинен використовувати електронно-цифровий підпис (ЕЦП). Отримувач цих відомостей повинен використати спеціальний ключ ЕЦП, який надає доступ до них.

4.5 Отримуючи паперовий носій, що містить персональні дані, працівник Організації повинен залишити примітку в «Журналі обліку носіїв», в якому вказати своє ПІП, назву паперового носія, номер, дату отримання і поставити підпис.

4.6 Повертаючи паперовий носій, що містить персональні дані, працівник Організації повинен залишити примітку в «Журналі обліку носіїв», в якому вказати дату повернення і поставити підпис.

4.7 Відповідальність за цілісність і нерозголошення персональних даних паперового носія несе працівник Організації, який отримав цей носій. У разі порушення вимог ЗУ «Про захист персональних даних» на працівника Організації накладається відповідальність, встановлена законом (ст. 28 Закону України «Про захист персональних даних»).

4.8 Працівник Організації може видалити персональні дані Клієнта з інформаційних ресурсів у разі відкликання згоди останнього на обробку його даних.

5 Політика відповідальності.

Керівництво Організації повинне ознайомити своїх працівників з цією Політикою і оголосити відповідальність у разі невиконання вимог.

2) Політика безпеки обліку та зберігання носіїв інформації:

Прийнято та надано чинності: червень 2019 р.

Відповідальний – системний адміністратор.

Власник документа – генеральний директор організації.

1 Опис. Політика безпеки обліку та зберігання носіїв інформації складена відповідно до вимог Постанови №736 Кабінету Міністрів України від 19.10.2016 «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» і визначає порядок ведення обліку і зберігання носіїв інформації ТОВ «Вебпіар» (далі – Організація).

2 Призначення. Ця політика безпеки призначена для ведення контролю за носіями інформації: встановленні причасних у знищенні, модифікуванні та/або передачі службової інформації, визначенні місця збереження носіїв інформації.

3 Область застосування. Вимоги політики безпеки обліку та зберігання носіїв інформації стосуються всіх працівників Організації, що працюють з персональними даними Клієнтів.

4 Політика.

4.1 Працівник Організації, на початку своєї роботи з паперовим або електронним носієм інформації, повинен залишити примітку в «Журналі обліку носіїв», в якому вказати своє ПІП, назву паперового носія (або інвентарний номер електронного носія), номер, дату отримання і поставити підпис. Зробивши ці дії, відповідальна особа – фінансовий директор, видає працівнику вказаний носій інформації.

4.2 Працівник Організації, наприкінці своєї роботи з паперовим та/або електронним носієм інформації, повинен залишити примітку в «Журналі обліку носіїв», в якому вказати дату повернення і поставити підпис. Зробивши ці дії, відповідальна особа – фінансовий директор, приймає у працівника вказаний носій інформації і перевіряє його. У разі виявлення недостачі паперів та/або пошкодження носіїв, відповідальна особа повідомляє про це керівництво організації.

4.3 Працівник Організації, отримавши носій інформації, несе відповідальність за збереження цілісності і доступності носія. У разі, якщо працівник залишає своє робоче місце, він повинен повернути носій інформації відповідальній особі і залишити відмітку в «Журналі обліку носіїв».

4.4 Працівник Організації повинен отримати та повернути носій інформації відповідальній особі з 10 години дня до 18 години вечора.

4.5 Відповідальна особа в проміжку з 18 години до 18 години 30 хвилини повинна провести облік носіїв інформації. У разі виникнення проблем повідомити про них керівництво організації.

4.6 Відповідальна особа за зберігання носіїв інформації повинна зберігати носії інформації в спеціальному сейфі, який обладнаний кодовим та механічним замком. Другий ключ від замка зберігається у керівництва Організації.

4.7 Друкування і розмноження документів, що становлять службову інформацію відбуваються згідно п.42 Постанови №736 Кабінету Міністрів України.

4.8 Працівники Організації повинні обробляти, зберігати, модифікувати та передавати інформацію з обмеженим доступом тільки з використанням ліцензованого ПЗ.

4.9 Працівники Організації повинні блокувати можливість ознайомлення з носіями, на яких міститься ІзОД, сторонніми особами.

4.10 Працівники Організації, винні у порушенні порядку ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, їх втраті або розголошенні службової інформації, що в них міститься, притягуються до дисциплінарної або іншої відповідальності, передбаченої законом.

5 Політика відповідальності.

Відповідальна особа за зберігання носіїв інформації ознайомлює працівників Організації з вимогами цієї Політики під розпис.

3) Політика забезпечення антивірусного захисту інформації:

Прийнято та надано чинності: червень 2019 р.

Відповідальний – системний адміністратор.

Власник документа – генеральний директор організації.

1 Опис. Політика забезпечення антивірусного захисту інформації ТОВ «Вебпіар» (далі – Організація) визначає вимоги захисту інформаційних ресурсів антивірусним ПЗ від втручання шкідливих програм, що можуть призвести до призупинення роботи АС.

2 Призначення. Метою цієї політики є запобігання діяльності шкідливих програм і забезпечення антивірусного захисту інформаційних ресурсів

3 Область застосування. Вимоги політики забезпечення антивірусного захисту інформації стосуються всіх працівників, які працюють з інформаційними ресурсами Організації.

4 Політика.

4.1 Системний адміністратор повинен встановити і налаштувати антивірусне ПЗ на АРМ працівника Організації, а також встановити ПЗ для дистанційного контролю за КС цього працівника.

4.2 Системний адміністратор, налаштовуючи антивірусне ПЗ, повинен вказати наступні параметри:

- цілодобовий захист від вірусів та загроз: увімкнений;
- цілодобовий захист в Інтернеті: увімкнений
- часткове сканування файлів: щосереди та щоп’ятниці о 18 годині;
- повне сканування файлів: 1 понеділок на 2 тижні о 9.30;
- заборонити відімкнення та зміну параметрів антивірусного ПЗ.

4.3 Системний адміністратор повинен своєчасно встановлювати оновлення антивірусного ПЗ на АРМ працівників організації. Встановлення оновлень повинно відбуватись кожного дня з 9.30 до 10 години ранку.

4.4 Працівник Організації, отримавши і завантаживши файл з корпоративної пошти, повинен перевірити цей файл на наявність вірусів, використовуючи антивірусне ПЗ.

4.5 Працівники Організації, оброблюючи інформацію з електронного носія, повинні проводити перевірку файлів на наявність вірусів.

4.6 Системний адміністратор, отримавши повідомлення в своїй КС про наявність вірусів на комп’ютері працівників Організації, повинен негайно ліквідувати загрозу, провести аналіз її виникнення і встановити відповідальних за скоєння цієї загрози\.

4.7 Системний адміністратор повинен встановлювати тільки ліцензоване програмне забезпечення на АРМ всіх працівників Організації.

5 Політика відповідальності.

Системний адміністратор повинен ознайомити працівників Організації з вимогами цієї політики і доповісти про відповідальність за недотримання цих вимог.

2.6 Аналіз інформаційних ризиків після впровадження політики безпеки

Проведемо повторний аналіз інформаційних ризиків, але вже після впровадження в дію політики безпеки за допомогою методу ISAMM.

Таблиця 2.28 – Оцінка ризиків методом ISAMM після впровадження політики безпеки

Джерело загроз	Вразливість	Ймовірність	Вплив, грн	Очікуваний збиток, грн
Проектний менеджер	1.2	0,173	30 000	5 190
	2.1	0,115	10 000	1 150
	3.1	0,173	12 000	2 076
	3.2	0,384	25 000	9 600
	3.3	0,230	8 000	1 840
	4.1	0,640	40 000	25 600
Хакери	4.2	0,102	25 000	2 550
Конкуренти	4.2	0,102	18 000	1 836
Програміст	4.1	0,173	15 000	2 595
Менеджер з SEO-оптимізації	4.1	0,102	5 000	510
Менеджер з налаштування контекстної реклами	4.1	0,102	5 000	510
Всього		0,209	193 000	53 457

Після проведення повторної оцінки ризиків можна зробити висновок, що отримані грошові дані свідчать про те, що після впровадження політики безпеки інформації на підприємстві очікуваний щорічний збиток зменшився майже в 3 рази.

Порівняння очікуваних щорічних збитків наведено в таблиці 2.29.

Таблиця 2.29 – Порівняльна таблиця оцінки ризиків до та після впровадження політики безпеки

Джерело загроз	Вразливість	Очікуваний збиток до впровадження ПБІ, грн	Очікуваний збиток після впровадження ПБІ, грн
Проектний менеджер	1.2	15 570	5 190
	2.1	4 600	1 150

Продовження таблиці 2.29

Джерело загроз	Вразливість	Очікуваний збиток до впровадження ПБІ, грн	Очікуваний збиток після впровадження ПБІ, грн
Проектний менеджер	3.1	8 650	2 076
	3.2	28 800	9 600
	3.3	8 050	1 840
	4.1	64 000	25 600
Хакери	4.2	7 650	2 550
Конкуренти	4.2	6 120	1 836
Програміст	4.1	8 650	2 595
Менеджер з SEO-оптимізації	4.1	3 060	510
Менеджер з налаштування контекстної реклами	4.1	3 060	510
Всього		635 000	158 210

2.7 Висновок

Спеціальна частина містить в собі обстеження фізичного, обчислювального, інформаційного середовища і середовища користувачів, аналіз інформаційних ризиків, за результатами яких було сформовано перелік інформаційних ресурсів, що становлять цінність організації.

За цими результатами було обрано функціональний профіль захищеності АС, на базі якого було побудовано модель загроз та визначено модель порушника.

Після цього, було проведено оцінку інформаційних ризиків підприємства з використанням методу ISAMM. Отримані дані відобразили суму очікуваних збитків при реалізації загроз, що допомогло обрати напрям написання політики безпеки.

Останньою дією в цьому розділі стало проведення повторної оцінки інформаційних ризиків з урахуванням написаної політики безпеки.

3 ЕКОНОМІЧНА ЧАСТИНА

3.1 Обґрунтування витрат на розробку політики безпеки інформації

Метою обґрунтування витрат на розробку політики безпеки інформації є розрахунок капітальних та експлуатаційних витрат, оцінка величини можливого збитку від атаки, визначення та аналіз показників економічної ефективності

3.2 Розрахунки витрат на розробку політики безпеки інформації

При розробці та експлуатації політики безпеки інформації необхідно розрахувати витрати ТОВ «Вебпіар» (більш детально з діяльністю організації можна ознайомитись в розділі 2.1).

3.2.1 Розрахунок капітальних (фіксованих) витрат

Капітальні (фіксовані) витрати на розробку та впровадження політики безпеки інформації складають [19]:

$$К = К_{пр} + К_{аз} + К_{зпз} + К_{н} \quad (3.1)$$

де $К_{пр}$ – вартість розробки політики безпеки інформації та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

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

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

Вихідні дані ТОВ «Вебпіар» становлять:

$К_{пр}$ = 8000 грн (вартість розроблення політики безпеки інформації та залучення до цього зовнішніх консультантів);

$К_{аз}$ = 10870 грн (вартість екранованого сейфу);

$$К_{зпз} = 40185 \text{ грн} \begin{cases} 972 \text{ грн за ЕЦП} \\ 11832 \text{ грн за ліцензоване ПЗ } Office\ 365 \\ 8949 \text{ грн за ліцензоване ПЗ } TesauRUS \\ 18432 \text{ грн за ліцензоване антивірусне ПЗ } Eset\ NOD32 \end{cases}$$

$К_{н}$ = 250 грн (витрати на встановлення обладнання та налагодження системи інформаційної безпеки).

Визначимо капітальні витрати:

$$К = 8000 + 40185 + 10870 + 250 = 59305 \text{ грн}$$

3.2.2 Розрахунок річних поточних (експлуатаційних) витрат

Річні поточні витрати складаються з:

$$С = С_{а} + С_{ел} + С_{о} + С_{тос} \quad (3.2)$$

де $С_{а}$ – річний фонд амортизаційних відрахувань;

$С_{ел}$ – вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = Р \times F_р \times Ц_е \quad (3.3)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки;

$Ц_е$ – тариф на електроенергію, грн/кВт·годин;

$С_о$ – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу;

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки.

Річний фонд амортизаційних відрахувань ($С_а$) складає 25% від капітальних витрат:

$$С_а = 59305 \times 0{,}25 = 14826{,}25 \text{ грн}$$

Потужність (Р) комп’ютерів та ноутбуків становить 1,12 кВт.

За 40-годинного робочого тижня річний фонд робочого часу системи інформаційної безпеки ($F_р$) становить 1920.

Тариф на електроенергію ($Ц_е$) складає 1,68 грн/кВт·годин.

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

$$С_{ел} = 1{,}12 \times 1920 \times 1{,}68 = 3612{,}67 \text{ грн}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_о$) складають 7500 грн.

$$С_о = 7500 \text{ грн}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) визначаються ТОВ «Вебпіар» і складають 2% від вартості капітальних витрат.

$$С_{тос} = 59305 \times 0,02 = 1186,10 \text{ грн}$$

Визначимо річні поточні витрати:

$$С = 14826,25 + 3612,67 + 7500 + 1186,10 = 27125,02 \text{ грн}$$

3.3 Оцінка величини можливого збитку від атаки

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

$$U = П_{п} + П_{в} + V \quad (3.4)$$

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:

$$П_п = \frac{\sum З_с \times Ч_с}{F} \times t_п \quad (3.5)$$

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

$З_с$ – місячна заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі з нарахуванням єдиного соціального внеску, грн на місяць;

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

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

Розрахунок витрат на заробітну плату співробітників за місяць з нарахуванням ЄСВ наведено в таблиці 3.1

Таблиця 3.1 – Витрати на заробітну плату співробітників за місяць з нарахуванням ЄСВ

Посада	Кількість співробітників, осіб	Місячна заробітна плата, грн	Витрати на заробітну плату, грн	Єдиний соціальний внесок, грн	Витрати на заробітну плату з урахуванням ЄСВ, грн
Фінансовий директор	1	13000	13000	2860	15860
Проектний менеджер	2	10000	20000	4400	24400
Програміст	1	9000	9000	1980	10980
Менеджер з SEO-оптимізації	1	7000	7000	1540	8540
Менеджер з налаштування контекстної реклами	1	7000	7000	1540	8540
Копірайтер	1	5000	5000	1100	6100
Всього					74420

Визначимо оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі:

$$П_п = (74420 / 176) \times 3 = 1268{,}53 \text{ грн}$$

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

$$П_в = П_{ви} + П_{пв} + П_{зч} \quad (3.6)$$

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

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

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

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

$$П_{ви} = \frac{\sum З_с \times Ч_с}{F} \times t_{ви} \quad (3.7)$$

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

$$П_{ви} = (74420 / 176) \times 4 = 1691{,}37 \text{ грн}$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати системного адміністратора:

$$П_{пв} = \frac{\sum З_о \times Ч_о}{F} \times t_в \quad (3.8)$$

де $З_о$ – місячна заробітна плата системного адміністратора з нарахуванням єдиного соціального внеску, грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу, осіб;

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

$$З_о = 10000 + 10000 \times 0{,}22 = 12\ 200 \text{ грн}$$

$$П_{пв} = (12200 / 176) \times 2 = 138{,}64 \text{ грн}$$

Визначимо вартість відновлення працездатності вузла або сегмента корпоративної мережі:

$$П_в = 1691{,}37 + 138{,}64 + 0 = 1830{,}01 \text{ грн}$$

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

$$V = \frac{O}{F_г} \times (t_п + t_в + t_{ви}) \quad (3.9)$$

де О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік;

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

$$V = 2500000 / 2080 \times (3 + 4 + 2) = 10817{,}31 \text{ грн}$$

Визначимо упущену вигоду від простою атакованого вузла або сегмента корпоративної мережі:

$$U = 1268{,}53 + 1830{,}01 + 10817{,}31 = 13915{,}84 \text{ грн}$$

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

$$B = \sum\sum U \times N \times I \quad (3.10)$$

де N – середнє число можливих атак на рік;

I – число атакованих вузлів або сегментів корпоративної мережі.

$$B = 13975{,}84 \times 1 \times 8 = 111326{,}72 \text{ грн}$$

3.4 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = (B \times R + B_{ISAMM} \times R_{ISAMM}) - C \quad (3.11)$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі організації;

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

B_{ISAMM} – загальний збиток, який прораховано методом ISAMM (згідно з таблицею 2.27);

R_{ISAMM} – очікувана ймовірність, яка прорахована методом ISAMM (згідно з таблицею 2.27);

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

$$E = (111326{,}72 \times 0{,}5 + 158210 \times 0{,}209) - 27125{,}02 = 61604{,}23 \text{ грн}$$

3.5 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломної роботи, здійснюється на основі визначення та аналізу наступних показників:

а) коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

б) термін окупності капітальних інвестицій T_o.

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

$$ROSI = \frac{E}{K} \tag{3.12}$$

де ROSI – коефіцієнт повернення інвестицій;

Е – загальний ефект від впровадження системи інформаційної безпеки, тис. грн;

К – капітальні інвестиції, що забезпечили цей ефект, тис. грн.

$$ROSI = 61604{,}23 / 59305 = 1{,}04$$

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

$$T_o = \frac{K}{E} = \frac{1}{ROSI} \quad (3.13)$$

де T_o – термін окупності капітальних інвестицій.

T_o = 59305 / 61604,23 = 0,96, що становить 11 місяців 16 днів.

3.6 Висновок

В економічному розділі була визначена економічна ефективність розробки та впровадження політики безпеки інформації в ТОВ «Вебпіар».

Було розраховано капітальні та експлуатаційні витрати, які склали 59305 грн та 27125,02 грн відповідно.

Оцінено величину можливого збитку від реалізованої атаки через упущену вигоду – 111326,72 грн.

Визначено термін окупності капітальних інвестицій. Він склав 11 місяців 16 днів.

Таким чином можна вважати, що впровадження політики безпеки інформації на підприємство є економічно доцільним рішенням, яке ефективно захистить інформаційні активи від негативних зовнішніх та внутрішніх впливів.

ВИСНОВКИ

В перші частині дипломної роботи було визначено поняття інформаційної безпеки, сформовано складові схеми реалізації інформаційної безпеки підприємства, а також було охарактеризовано конкретні цілі, вимоги та задачі, що висуваються до політики безпеки. Проаналізовано нормативно-правову базу в сфері захисту інформації, а також визначено задачі, які необхідно вирішити в цій роботі.

В спеціальній частині було обґрунтовано необхідність розробки та впровадження політики безпеки інформації в ТОВ «Вебпіар». Крім цього, було виконано обстеження середовищ функціонування ІТС, за результатами якого було визначено функціональний профіль захищеності КС, спираючись на який побудовано модель загроз та сформовано модель порушника. Отримані загрози та ймовірності реалізації були оцінені за допомогою методу ISAMM (Information Security Assessment & Monitoring Method).

Для мінімізації ймовірності реалізації проаналізованих та оцінених ризиків була розроблена політика безпеки інформації ТОВ «Вебпіар», яка складається з документів «Політика захисту персональних даних», «Політика забезпечення антивірусного захисту інформації» та «Політика безпеки обліку та зберігання носіїв інформації».

Була повторно проведена оцінка інформаційних ризиків, яка показала ефективність після впровадження політики безпеки інформації, а також наведено порівняльний графік доцільності розробки ПБІ.

В економічній частині було обґрунтовано доцільність витрат на розробку ПБІ, а також проведені розрахунки капітальних та експлуатаційних витрат, оцінено величину можливого збитку від атаки, визначено ефект від впровадження політики безпеки інформації, а також проаналізована та визначена економічна ефективність системи захисту інформації.

СПИСОК ЛІТЕРАТУРИ

1. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 № 537-V // Відомості Верховної Ради України. – 2007. – № 12. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/537-16

2. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу – [Чинний від 1999.04.28]. – К. : ДСТСЗІ СБУ, 1999. – № 22. – (Нормативний документ системи технічного захисту інформації).

3. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі – [Чинний від 2005.08.11]. – К. : ДСТСЗІ СБУ, 2005. – № 125. – (Нормативний документ системи технічного захисту інформації).

4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

5. Вінницький апеляційний адміністративний суд. Захист інформаційних систем [Електронний ресурс]. - Режим доступу http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive-zavdannya-sogodennya/

6. ДССЗЗІ України. Порядок створення комплексних систем захисту інформації, проведення експертизи та видачі Експертних висновків і Атестатів відповідності [Електронний ресурс]. - Режим доступу http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=39479&cat_id=38689&ctime=1127824089206

7. Закон України «Про інформацію» від 02.10.1992 №2657-XII // Відомості Верховної Ради України. – 1992. – № 48. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/2657-12

8. Закон України «Про захист персональних даних» від 01.06.2010 №2297-VI // Відомості Верховної Ради України. – 2010. – № 34. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/2297-17

9. Закон України «Про основні засади забезпечення кібербезпеки України» від 21.06.2018 № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 45. [Електронний ресурс]. – Режим доступу http://zakon5.rada.gov.ua/laws/show/2163-19

10. Указ Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» від 22.05.1998 №505/98 // Відомості Верховної Ради України. – 1998. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/505/98

11. Указ Президента України «Про Положення про технічний захист інформації в Україні» від 27.09.1999 №1229/99 // Відомості Верховної Ради

України. – 1999. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/1229/99

12. Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373 // Офіційний вісник України. – 2006. – № 13.

13. НД ТЗІ 2.5.004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – [Чинний від 1999.04.28]. – К. : ДСТСЗІ СБУ, 1999. – № 22. – (Нормативний документ системи технічного захисту інформації).

14. НД ТЗІ 2.5.005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – [Чинний від 1999.04.28]. – К. : ДСТСЗІ СБУ, 1999. – № 22. – (Нормативний документ системи технічного захисту інформації).

15. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. – [Чинний від 1999.04.28]. – К. : ДСТСЗІ СБУ, 1999. № 22. – (Нормативний документ системи технічного захисту інформації).

16. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.– [Чинний від 2013.04.15]. – К. : ДССЗЗІ, 2013. № 215. – (Нормативний документ системи технічного захисту інформації).

17. Приставка Ф., Павленко П., Казмирчук С., Коломієць М. «Дослід засобів оцінювання ризиків безпеки ресурсів інформаційних систем», [Електронний ресурс]. – Режим доступу http://er.nau.edu.ua/bitstream/NAU/37138/1/2017_%D0%98%D0%A1%D0%A1%D0%9B%D0%95%D0%94%D0%9E%D0%92%D0%90%D0%9D%D0%98%D0%95%20%D0%A1%D0%A0%D0%95%D0%94%D0%A1%D0%A2%D0%92%20%D0

%9E%D0%A6%D0%95%D0%9D%D0%98%D0%92%D0%90%D0%9D%D0%98%D0%AF.pdf

18. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою // ISO/IEC 27001, який прийнято як ДСТУ ISO/IEC 27001:2015

19. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: І.В. Шереметьєва, Д.П. Пілова, Н.М. Романюк. – Дніпро: Національний технічний університет "Дніпровська політехніка", 2017. – 17 с.

20. Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека, 172 Телекомунікаціїї та радіотехніка / О.Ю.Гусєв, О.В. Герасіна, О.М. Алексєєв,О.В. Кручінін – Дніпро: НГУ, 2018. – 52 с.

21. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки // ISO/IEC 27002, який прийнято як ДСТУ ISO/IEC 27002:2015

22. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки // ISO/IEC 27005, який прийнято як ДСТУ ISO/IEC 27005:2015

23. Захист інформації. Технічний захист інформації. Основні положення // ДСТУ 3396.0-96

24. Захист інформації. Технічний захист інформації. Порядок проведення робіт // ДСТУ 3396.1-96

25. Захист інформації. Технічний захист інформації. Терміни та визначення // ДСТУ 3396.2-97

26. Закон України «Про електронні документи та електронний документообіг» від 07.11.2018 №851-IV // Відомості Верховної Ради України. – 2003. – № 36. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/851-15

27. Закон України «Про електронну комерцію» від 26.04.2017 №675-VIII // Відомості Верховної Ради України. – 2015. – № 45. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/675-19

28. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. — К.: Кондор, 2004. — №2 — 384 с.

29. С. В. Кавун, В. В. Носов, О. В. Манжай. Інформаційна безпека. Навчальний посібник — Харків: Вид. ХНЕУ, 200’. — 352 с.

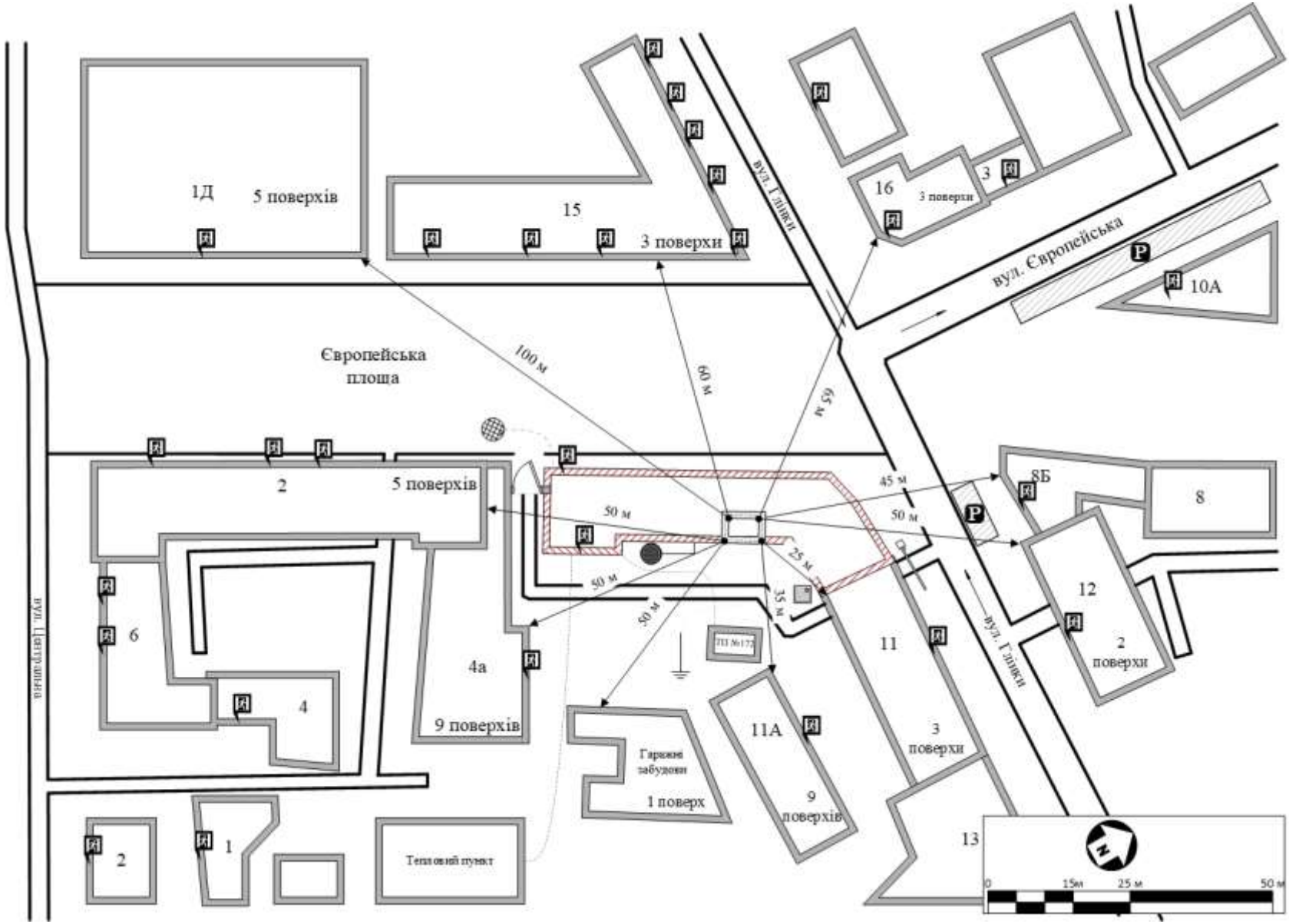
30. В. Л. Ортинський, І. С. Керницький, З. Б. Живко. Економічна безпека підприємств: підручник / Алерта - 2011. – 704 с.

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ ДИПЛОМНОЇ РОБОТИ

№	**Формат**	**Найменування**	**Кількість листів**	**Примітки**
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	7	
6	А4	Спеціальна частина	42	
7	А4	Економічна частина	10	

8	А4	Висновки	1	
9	А4	Список літератури	4	
10	А4	Додаток А	1	
11	А4	Додаток Б	2	
12	А4	Додаток В	2	
13	А4	Додаток Г	1	
14	А4	ДОДАТОК Ґ	1	
15	А4	ДОДАТОК Д	1	

ДОДАТОК Б. СИТУАЦІЙНИЙ ПЛАН ТОВ «ВЕБПІАР»

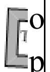
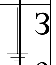


опис	значення	опис	значення
Підземні канали зв'язку		Будівлі споруди	

			і труби, що під'єднані до буді

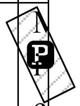
			влі з ОІД
	Контур ОІД з КЗ		Теплотраса КП «Теплое

			нерго»
	К Г		Теплоовий пункт
	Шлагбаум		Лінія забезе

			млення
	Трансформаторна підстанц		Земля

	ія №172		
	Надземні лінії системе	Вхід в будівлю	

	лектроживлення		
	Люк Дніпроводока		Відстань між об’

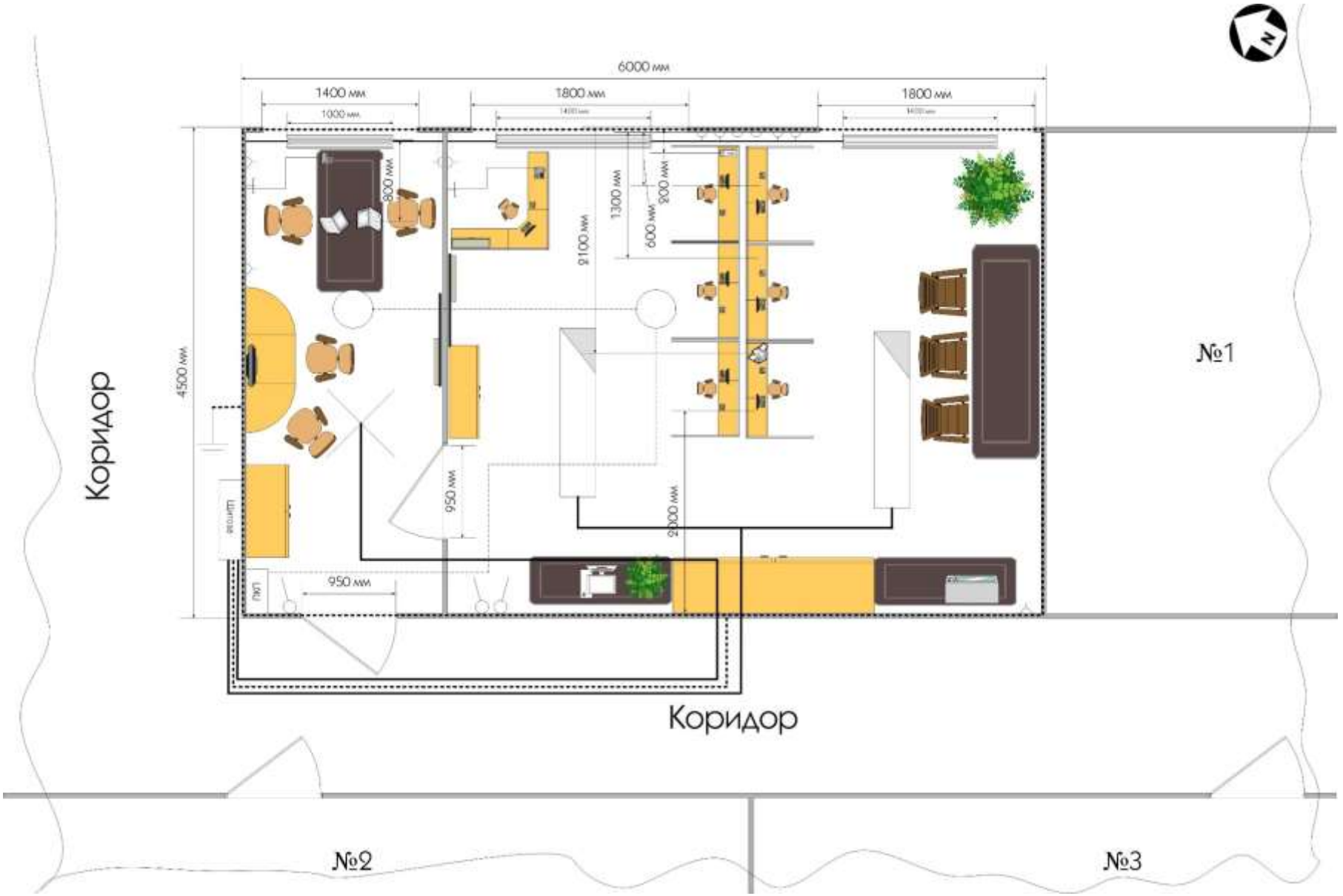
	налу			єктами
	Підземні труби водопоста			Місце паркування автомоб

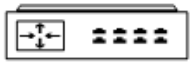
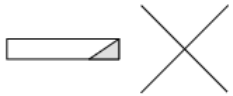
	чання, що підєднані до будівл		ілів

	і з С І Д		
	К а н а л і з а ц і й н и й л к		Н а п р я м р у х у а в т о м о б і л і в

Примітка. Умовні позначення ситуаційного плану

ДОДАТОК В. ГЕНЕРАЛЬНИЙ ПЛАН ТОВ «ВЕБПІАР»



Позначення	Опис	Позначення	Опис
№1	ТОВ «Севен Севенті Петроліум» (суміжне приміщення)		Лінії АТС
№2	Адвокатське бюро Олега Бовкуна (суміжне приміщення)		Щитова систем електроживлення
№3	Редакція газети Aviso (суміжне приміщення)		Wi-Fi маршрутизатор
	Приймально-контрольний прилад		Освітлення
	Датчик пожежної сигналізації		Розетка
	Лінії систем електроживлення		Вимикач світла
	Лінії систем теплопостачання		Радіаторна батарея
	Принтер		КЗ, зона циркулювання інформації
	Телефонна розетка		ПК, ноутбук
	Лінія заземлення		Мікрохвильова піч
	Телевізор		Шафа

Примітка. Умовні позначення генерального плану

ДОДАТОК Г. ПЕРЕЛІК МАТЕРІАЛІВ НА ОПТИЧНОМУ НОСІЇ

Кабанов А.О. УБіт-15-1.docx

Кабанов А.О. УБіт-15-1.pptx

ДОДАТОК Ґ. ВІДГУКИ КЕРІВНИКІВ РОЗДІЛІВ

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Д. ВІДГУК КЕРІВНИКА ДИПЛОМНОЇ РОБОТИ

ВІДГУК

на дипломну роботу студента групи УБіт-15-1 Кабанова А.О.

на тему: «Розробка політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Вебпіар»»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 81 сторінках.

Мета дипломної роботи є актуальною, оскільки вона направлена на збереження цілісності інформації в аспекті розробки політики безпеки інформаційно-телекомунікаційної системи ТОВ «Вебпіар».

При виконанні дипломної роботи автор продемонстрував достатній кваліфікаційний рівень теоретичних та практичних знань в сфері кібернетичної безпеки. На основі аналізу статистичних даних кіберзлочинності та потреб щодо інформаційної безпеки ТОВ «Вебпіар» була сформована задача на створення політики безпеки інформації, вирішення якої відображено в спеціальному розділі роботи. В дипломній роботі проведено аналіз сучасної нормативно-правової бази в сфері інформаційної безпеки, складені моделі загроз та порушника в межах зазначеного підприємства. За результатами досліджень розроблено політику безпеки інформації підприємства та оцінено її вартість та ефективність при впровадженні.

Практична цінність роботи полягає в реалізації розробленої політики безпеки інформації в інформаційно-телекомунікаційну систему ТОВ «Вебпіар».

В якості недоліків слід відзначити наступне: нечіткість окремих висновків, окремі невідповідності вимогам при оформленні.

В цілому дипломна робота задовольняє усім вимогам, що висуваються до дипломних робіт бакалаврів, заслуговує оцінки «_____», а її автор Кабанов А.О. – присвоєння кваліфікації «фахівець з організації інформаційної безпеки» за спеціальністю 6.170103 - управління інформаційною безпекою.

Керівник дипломної роботи,
доктор технічних наук, професор **В.І. Корнієнко**

Керівник спеціального розділу,
асистент **Ю.В. Ковальова**