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 *Димарьової Марії Костянтинівни*

академічної групи *125-20-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-комунікаційної системи підприємства «Vodafone Україна Першотравенськ»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	проф. Кагадій Т.С.			
розділів:				
спеціальний	ас. Мілінчук Ю.А.			
економічний	к.е.н., доц. Пілова Д.П.	90	відмінно	

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.
«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту ***Димарьовій Марії Костянтинівні*** **академічної групи** ***125-20-3***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації[1]

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

на тему ***Комплексна система захисту інформації інформаційно-комунікаційної системи підприємства «Vodafone Україна Першотравенськ»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024_ №_469-с_

Розділ	Зміст	Термін виконання
Розділ 1	Структура ІКС підприємства, зокрема ІКС «Vodafone Першотравенськ»	15.03.2024
Розділ 2	Аналіз існуючих загроз та методи боротьби з ними. Напрямки покращання системи безпеки ІКС «Vodafone Першотравенськ»	10.05.2024
Розділ 3	Аналіз собівартості впровадження удосконалень системи захисту ІКС «Vodafone Першотравенськ»	11.06.2024

Завдання видано _____ ___Юлія МІЛІНЧУК_____
(підпис керівника) (ім'я, прізвище)

Дата видачі завдання: __15.01.2024р._____

Дата подання до екзаменаційної комісії: __04.07.2024р._____

Прийнято до виконання _____ _Марія ДИМАРЬОВА_____
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 75 с., 18 табл., 3 додатки, 2 рисунки, 45 джерел.

Об`єкт дослідження: інормаційно-комунікаційна система підприємства «Vodafone Україна Першотравенськ».

Предмет дослідження: система безпеки інформації на підприємстві «Vodafone Україна Першотравенськ».

Мета роботи: підвищити рівень захисту інформації в інформаційно-комунікаційній системі підприємства «Vodafone Україна Першотравенськ».

Методи, які застосовуються під час дослідження: спостереження, порівняння, аналіз, опис, вивчення фахової літератури.

У першому розділі кваліфікаційної роботи подано загальний опис підприємства «Vodafone Україна Першотравенськ», розглянуто його організаційну структуру, проаналізовано нормативно-правову базу, а також проведено дослідження зовнішнього середовища підприємства «Vodafone Україна Першотравенськ».

У другій частині кваліфікаційної роботи розроблено модель загроз і порушника, проаналізовано актуальні загрози та вразливості, а також обрано профіль захищеності та рішення для захисту інформації в «Vodafone Україна Першотравенськ».

В економічному розділі кваліфікаційної роботи розраховано капітальні та поточні витрати, проведено оцінку можливого збитку від атаки та виконано аналіз економічної доцільності запропонованих рішень.

Практична цінність роботи полягає в підвищенні рівня захисту інформації в інформаційно-комунікаційній системі «Vodafone Україна Першотравенськ» завдяки розробленню рекомендацій щодо впровадження проектних рішень.

ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, ЗАХИСТ ІНФОРМАЦІЇ, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ВРАЗЛИВОСТІ, АКТ ОБСТЕЖЕННЯ, ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ

ABSTRACT

Explanatory note: 75 pp., 18 tables, 3 appendices, 2 pictures, 45 sources.

The object of the study: information and communication system of the enterprise "Vodafone Ukraine Pershotravensk".

The subject of the research: the information security system at the "Vodafone Ukraine Pershotravensk" enterprise.

The purpose of the work: to increase the level of information protection in the information and communication system of the enterprise "Vodafone Ukraine Pershotravensk".

Methods used during research: observation, comparison, analysis, description, study of specialized literature.

In the first section of the qualification work, a general description of the company "Vodafone Ukraine Pershotravensk" is presented, its organizational structure is considered, the legal framework is analyzed, and the external environment of the company "Vodafone Ukraine Pershotravensk" is also studied.

In the second part of the qualification work, a threat and offender model was developed, current threats and vulnerabilities were analyzed, and a security profile and information protection solutions were selected at Vodafone Ukraine Pershotravensk.

In the economic section of the qualification work, capital and current costs were calculated, an assessment of possible damage from the attack was carried out, and an analysis of the economic feasibility of the proposed solutions was performed.

The practical value of the work consists in increasing the level of information protection in the "Vodafone Ukraine Pershotravensk" information and communication system thanks to the development of recommendations for the implementation of project solutions.

OBJECT OF INFORMATION ACTIVITY, INFORMATION PROTECTION, COMPLEX INFORMATION PROTECTION SYSTEM, THREAT MODEL, VIOLATOR MODEL, VULNERABILITIES, SURVEY ACT, ECONOMIC FEASIBILITY

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система

БФП – багатофункціональний пристрій

ДТЗС – допоміжні технічні засоби

ЗП – заробітна плата

ОС – обчислювальна система

ІКС – інформаційно-комунікаційна система

КЗЗ – комплекс засобів захисту від несанкціонованого доступу

КС – комп'ютерна система

КСЗІ – комплексна система захисту інформації

КМ – Кабінет Міністрів

НД – нормативний документ

НД ТЗІ – нормативний документ системи технічного захисту інформації

НСД – несанкціонований доступ

ОТЗ – основні технічні засоби

ОП – оперативна пам'ять

ТЗІ – технічний захист інформації

ЗМІСТ

с.

ВСТУП

Проблеми захисту стають особливо актуальними в сучасних умовах, як ми бачимо на прикладі масованої атаки на інформативно-комунікаційну систему підприємства Київстар. Подібні випадки становлять велику загрозу не тільки для даних підприємства та користувачів, а й роблять неможливим подальше функціювання самого підприємства. Тому важливість цього питання важко переоцінити.

Сучасний світ постійно змінюється, і разом з ним трансформується і діяльність підприємств та організацій. Ці зміни спровоковані сучасним інформаційним середовищем, оскільки ми все більше часу проводимо в інтернеті. Важливо розуміти вплив нових технологій на стратегію розвитку компанії та на реакцію споживачів.

По мірі впровадження технологічних рішень з кожним роком збільшуються очікування клієнтів. Деякі інструменти, які тільки з'являються на ринку, вже активно використовуються компаніями для задоволення потреб користувачів. І все менше часу приділяється виявленню слабких місць і вразливостей даних методів, які впливають на подальше життя компанії.

Зі зростанням впливу технологій постає також питання захисту інформації [1, с. 15]. З підвищенням впливу компаній на ринку з'являються конкуренти, впроваджується нове програмне забезпечення, обладнання та технологічні рішення. Це призводить до того, що зростає ймовірність перехоплення конфіденційної інформації, її знищення або модифікація.

Щоб уникнути цього компанії використовують комплексні системи захисту інформації, які являють собою сукупність організаційних і інженерних заходів, програмно-апаратних засобів. Завдяки цьому забезпечується захист інформації в інформаційно-комунікаційних системах (ІКС). Адже гарантований захист інформації, вдосконалення впроваджених технологій, постійний аналіз існуючих системи безпеки і сучасних технологічних змін забезпечує розвиток компаній та закріплення їх позицій на ринку.

У даній роботі вивчається інформаційно-комунікаційна система підприємства «Vodafone Україна Першотравенськ». За допомогою цієї системи відбувається обмін даними між компанією та користувачами. Структура цієї системи буде детально розглянута у першому розділі.

Предмет розробки - комплексна система захисту інформації, яка циркулює в інформаційно-комунікаційній системі «Vodafone Україна Першотравенськ». Слово «комплексний» у даному випадку відноситься до сукупності засобів, які поєднують різні методи захисту даних. Ці методи будуть детально розглянуті у другому розділі.

Мета роботи полягає у розробці методів та засобів комплексного захисту інформації в інформаційно-комунікаційній системі, які дозволять убезпечити дані як від злочинних посягань, так і від випадкових факторів.

В роботі розглядаються наступні питання:

1. Структура інформаційно-комунікаційної системи.

2. Захист даних, які циркулюють в інформаційно-комунікаційній системі.

3. Напрямки вдосконалення структури інформаційно-комунікаційної системи.

4. Комплекс методів та засобів, спрямованих на захист інформації в інформаційно-комунікаційній системі.

5. Аналіз економічної собівартості вдосконалень, які запроваджуються в цілях системі захисту інформації, що циркулює в інформаційно-комунікаційній системі.

Практичне значення роботи полягає у розробці комплексної системи захисту чутливої інформації, яка циркулює в інформаційно-комунікаційній системі компанії взагалі, і в ІКС «Vodafone Україна Першотравенськ».

Ці методи дозволять суттєво зекономити на поточних витратах та запобігти втраті важливих даних.

Власники бізнесу розуміють важливість надання своїм клієнтам найкращих продуктів та послуг. Дані чи інформація - це основа сучасного бізнесу.

Лише уявіть, що станеться у випадку втрати бази даних клієнтиів! Це буде просто катастрофа. У цьому випадку сума збитків буде просто астронгомічною.

Завоювати позиції на сучаному ринку непросто, але відновити втрачене ще тяжче. Якщо інформацію про клієнта було втрачено або скомпрометовано, то він назавжди покине вас і впаде в обійми ваших конкурентів. І коли про це прикрий інцидент стане відомо вашим ворогам, про нових клієнтів можна забути.

Одним із найбільш серйозних наслідків втрати даних є можливість витоку конфіденційної інформації. Якщо дані клієнтів або акаунти співробітників будуть скомпрометовані, ви можете мати справу не лише з втратою нових клієнтів, але й з мільонними судовими позовами з невеселими перспективами для вас.

Майже у кожному сучасному підприємстві розгорнута автоматизована інформаційнпї система. І зачасту її потрібно реструктуризувати. В процесі реструктуризації ця система поділяється на підсистеми, що мають меншу складність і нижчий рівень ієрархічної структури [2, с. 7].

Підсистема автоматизованої інформаційної системи (АІС) – це частина загальної системи, яка виділена за функціональною або структурною ознакою, що відповідає конкретним цілям та завданням.

В процесі відбору принципів виділення окремих елементів АІС необхідно враховувати аспекти окремого підприємства, найважливішими з яких є особливості виробничого процесу, апарат управління, інформаційна взаємодія підрозділів і фахівців і т.п. Крім того, слід також враховувати специфіку вирішення управлінських завдань, які виконуються різними структурними підрозділами, що ускладнює структуризацію АІС. Причина цього полягає в тому, що організаційна структура підприємства часто не збігається з функціональною структурою. Наприклад, ряд структурних підрозділів виконують окремі функції управління в масштабах підприємства (плановий відділ, бухгалтерія, відділ кадрів тощо), а інші підрозділи організаційно виділяються за іншим принципом, наприклад, за типами ресурсів та послуг, що

забезпечують основне виробництво (маркетинг серед клієнтів), за напрямами вдосконалення виробництва та управління (інноваційний відділ, центр інформаційних технологій тощо). У таких підрозділах деякі функції управління в масштабі підприємства не проглядаються, а окремі функції виконуються частково у взаємодії з іншими управлінськими підрозділами.

Невідповідність функціональної та організаційної структур ускладнює завдання виділення функціональних елементів АІС, проте не перешкоджає тому, щоб через визначення управлінських функцій та засобів їх забезпечення виділити дві групи підсистем: функціональні та допоміжні. Функціональні підсистеми покликані вирішувати конкретні завдання управління, які забезпечують забезпечувати їх надійне рішення.

У цій структурі особливе місце посідає відділу ІТ, який реалізує операції обробки економічної інформації, автоматизує вирішення функціональних завдань. При цьому допоміжні підсистеми орієнтовані як на підтримку функціонування інформаційних технологій в менеджменті, так і на підтримку автоматизованої інформаційної системи підприємства в цілому.

Функціональні підсистеми формуються з урахуванням поділу управлінського процесу між конкретними службами, які реалізують функції бізнесу [3, с. 8].

Процес формування функціональних підсистем та встановлення зв'язків між ними передбачає виділення в комплексній задачі управління підприємством кілька самостійних завдань з управління функціями бізнесу, які і утворюють основні функціональні підсистеми АІС.

До функцій підсистем АІС можна віднести наступні:

- поширення підприємницьких ідей, ініціативи та досвіду управління;
- діяльність з розробки та реалізації нових технологічних процесів або нової продукції для покращення підприємництва, підвищення ефективності, розширення пропозиції нової продукції;
- здійснення та управління відносинами між підприємством та громадськими структурами.

В АІС підприємства виділяються п'ять основних функціональних підсистем:

- керування виробництвом;
- управління постачанням;
- управління маркетингом (збутом);
- керування фінансами;
- управління персоналом.

Функціональні підсистеми виробляють основний взаємопов'язаний комплекс показників, які передбачають раціональний розвиток виробництва. Ці підсистеми здійснюють контроль за реальним ходом виробництва та намічають шляхи ліквідації відхилень від запланованого режиму. Отже, функціональні підсистеми грають вирішальну роль ІТ, визначаючи логіку її функціонування.

Усі функціональні підсистеми у свою чергу поділяються на низку завдань – бізнес-процесів. На різних підприємствах перелік бізнес-процесів кожної функціональної підсистеми різний і залежить від таких факторів [4, с. 12]:

- розміру підприємства;
- галузевої власності;
- ступеня спеціалізації та кооперування;
- наявності соціальної інфраструктури тощо.

Наприклад, для виробничих підприємств функціональна підсистема «Управління виробництвом» включає бізнес-процеси управління технічною підготовкою виробництва, оперативне управління основним виробництвом тощо, для кредитної установи функціональна підсистема «Управління виробництвом» орієнтована на управління кредитами, управління депозитами та ін. а для торговельного підприємства у сфері товарного обігу - на управління закупівлями та реалізацію товарів тощо.

Місце кожної функціональної підсистеми визначає модель бізнесу будь-якого підприємства. Центральне місце в моделі займає виробнича функція або функціональна підсистема управління виробництвом, яка опосередковано через

інші функціональні підсистеми взаємодіє із зовнішнім середовищем підприємства. У свою чергу, зовнішнє середовище також впливає на функціонування підприємства.

Слід зазначити, що основні функції управління інтегровані в різні функціональні підсистеми та взаємопов'язані в управлінський процес, що охоплює різні сторони функціонування підприємства

Підсистеми, що забезпечують, є основним засобом реалізації функцій управління на підприємствах шляхом ефективного вирішення завдань функціональних підсистем на базі ІТ в менеджменті.

Склад і рівень прогресивності елементів кожної підсистеми, що забезпечує, визначаються функціональними і структурними особливостями підприємства, прийнятою моделлю управління і т.д. Підсистеми, що забезпечують, у свою чергу за допомогою ІТ в менеджменті впливають на структуру моделі управління, її формальне уявлення.

Отже, можна дійти невтішного висновку, що й автоматизована інформаційна система — це насамперед сукупність всієї інформації підприємства, програмних і апаратних засобів, фахівців тощо., то ІТ у менеджменті є процесом, на основі якого реалізуються найважливіші управлінські функції. Тому доцільніше говорити про що забезпечує АІС стосовно динаміці управлінського процесу з урахуванням інформаційних технологій, підтримка функціонування яких здійснюється з допомогою що забезпечують підсистем.

РОЗДІЛ 1. СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про підприємство «Vodafone Першотравенськ».

Підприємство «Vodafone Першотравенськ» - комунікаційна компанія, яка займається наданням послуг зв'язку. Ця організація працює на ринку вже більше 20 років. Компанія розташована за адресою вулиця Василя Стуса, 1, Першотравенськ, Дніпропетровська область, 52801.

Штат працівників компанії навдений на рисунку 1.1.

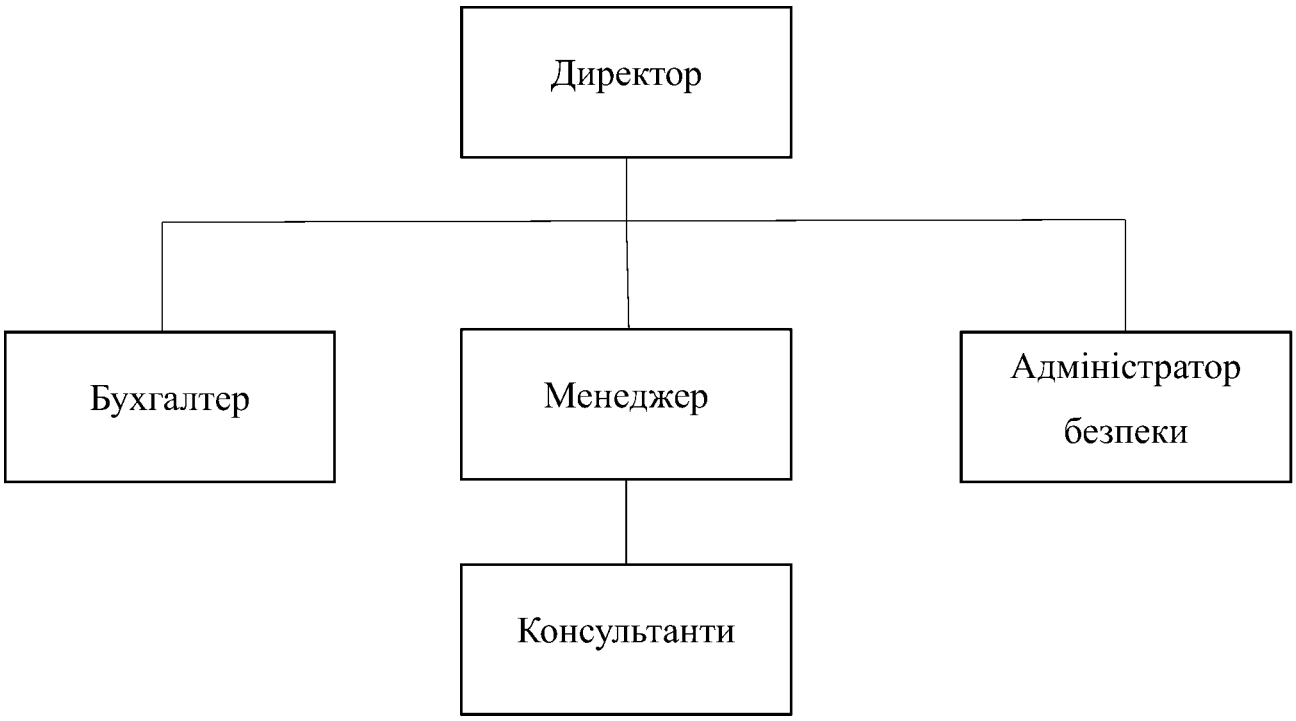

Рисунок 1.1. - Організаційна струкрура підприємства

Обов'язки працівників

Директор розробляє та впроваджує стратегічні плани розвитку, виконує нагляд за виконанням стратегічних планів розвитку. Забезпечує безпеку інформаційних систем, виконує управління IT-інфраструктурою, налаштування мереж та серверів. Також до обов'язків директора входить вирішення технічних проблем та усунення несправностей, підтримка та оновлення програмного забезпечення, а також взаємодія з партнерами та постачальниками IT-рішень.

Бухгалтери ведуть бухгалтерський облік відділу; підготовка фінансових звітів та документів; облік доходів і витрат, контроль за фінансовими операціями; робота з податковою документацією та звітністю; обробка платежів і банківських операцій; забезпечення відповідності фінансової документації нормативним вимогам.

Адміністратор безпеки веде постійний контроль систем безпеки для виявлення можливих загроз і вразливостей. Займається організацією та контролем фізичної безпеки об'єктів компанії, включаючи відеоспостереження.

Менеджер займаються координацією роботи команди та забезпечення виконання поставлених завдань. Також до обов'язків менеджерів входить аналіз ринку та конкурентів, розроблюють стратегій продажу. Контроль за виконанням планів продажу та бюджетів.

До обов'язків консультантів сходить безпосередньо надання консультацій клієнтам щодо послуг та продуктів компанії, вирішення проблем та запитів клієнтів. Підтримка клієнтів у користуванні послугами компанії, а також оформлення та обробка замовлень. Ведення клієнтської бази даних. Підтримка постійного контакту з клієнтами для забезпечення їх задоволеності. Участь у проведенні маркетингових кампаній та акцій.

1.2 Аналіз нормативно-правової бази

Згідно з Законом України «Про інформацію» [5, с. 12], який описує види інформації та відповідальність за порушення законодавства про інформацію, встановлено, що інформація про фізичну особу та інформація з обмеженим доступом повинна отримувати особливий та обов'язковий захист. Для цього передбачено спеціальний порядок захисту такої інформації.

Відповідно до Закону України «Про персональні дані» [6, с. 14], визначаються суб'єкти відносин, пов'язаних з персональними даними, об'єкти захисту, загальні та особливі вимоги до обробки персональних даних, а також контроль за дотриманням законодавства про захист персональних даних.

Згідно з Законом України «Про захист інформації в інформаційно-комунікаційних системах» [7, с. 12], розглядаються заходи щодо забезпечення

захисту інформації в системі. Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Організація технічного захисту інформації на підприємстві покладається на керівництво підприємства. Також встановлюється відповідальність за порушення вимог щодо захисту технічної інформації згідно з Положенням про технічний захист інформації в Україні.

Для створення комплексної системи захисту інформації (КСЗІ) використовуються засоби захисту інформації, які мають сертифікати відповідності або затверджений експертний висновок (Положення про державну експертизу в сфері технічного захисту інформації).

Згідно з НД ТЗІ 3.7-003-2005 [8, с. 14], встановлено порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі.

Концепція технічного захисту інформації в Україні затверджена Постановою КМ України від 08.10.1997 №1126.

1.3 Структура компанії «Vodafone Першотравенськ»

1.3.1 Опис приміщення

Підприємство «Vodafone Першотравенськ» орендує офіс на 1 поверсі житлового будинку. Об'єктом інформаційної діяльності (ОІД) є приміщення та коридори офісу.

Територія навколо підприємства «Vodafone Першотравенськ» - відкрита. Вхід у приміщення здійснюється через вхідні двері. Відеоспостереження – зовнішнє та внутрішнє цілодобове.

Територія навколо будівлі асфальтована, з південно-західної та західної сторони є місця паркування. З південно-східної сторони за парканом знаходиться невелика зелена зона. З північно-східної сторони будівлі прилягає дорога з двостороннім рухом. Підвал та криша зачинені, до них має доступ лише охоронець, що має ключ.

Інформація про навколишні будинки та споруди надана в таблиці 1.1.

Таблиця 1.1 – Характеристика будівель та споруд

Призначення будівлі	Адреса	Кількість поверхів	Відстань від офіса
Будинок, в якому знаходиться офіс	Вулиця Василя Стуса, 1	2	-
Призначення будівлі	Адреса	Кількість поверхів	Відстань від офіса
Житлова будівля, в якій знаходиться ломбард	Вулиця Василя Стуса, 3	5	30 м
Житлова будівля	Вулиця Василя Стуса, 2	4	50 м

Система електроживлення – централізована. Трансформаторна підстанція розташована на відставні 0,5 км від офіса.

Система водопостачання – централізована. Підключена до водоканалу та підземними комунікаціями під'єднана через підвальне приміщення.

Система каналізації теж централізована. Під'єднана через підвальне приміщення.

Система опалення – централізована. Під'єднана через підвальне приміщення.

Підключення до Інтернету забезпечує провайдер «Vodafone». Проведений до офісу оптоволоконним кабелем. Вита пара підключена до комутатора, який утворює локальну мережу (VLAN).

Система телефонної лінії – локальна. Доступ робітників через міні АТС «Panasonic», до якої підключено 2 телефона менеджерів.

Система вентиляції – приточно-витяжна, виходить за межі офіса. Шахти вентиляції проходять через всі поверхи будівлі.

Система сигналізації – централізована, з виходом на пульт сигналізації, виходить за межі офіса. При спрацьовуванні охоронних датчиків, сигнал з панелі сигналізації направляється на пульт охорони.

1.3.2 Обчислювальна та інформаційна система

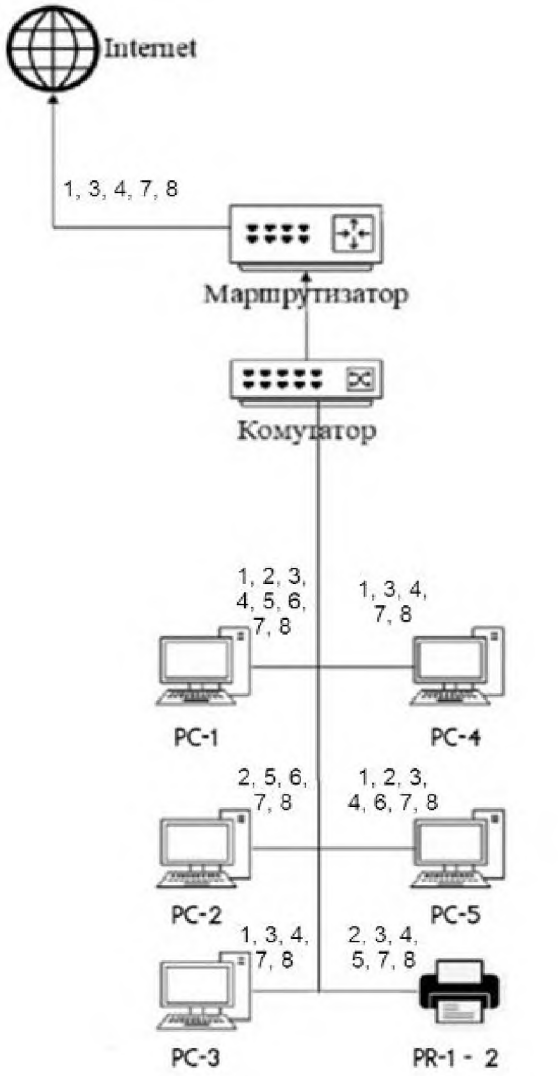

Рисунок. 1.2. – Схема інформаційних потоків

Інформаційні потоки:

1. Обробка інформації про клієнтів;
2. Обробка інформації про працівників;
3. Обробка інформації про продукти підприємства;
4. Обробка інформації про надання послуг, контакна інформація;
5. Обробка організаційно-розпорядчої інформації;
6. Обробка бухгалтерської звітності, договорів;
7. Обробка фінансової звітності;
8. Обробка рекламних даних;

Кабель інтернету проведено до офісу за допомогою оптоволоконного кабелю. Вита пара підключена до маршрутизатора, який обслуговує локальну мережу (VLAN) і підключений напряму до комутатора. Комп'ютери PC 1…PC 5 з'єднані з комутатором прямими підключеннями за допомогою витої пари. Принтери PR_1 і PR_2 також підключені до комутатора прямими підключеннями.

Також наглядно у таблиці 1.2 перераховано програмне забезпечення, встановлене на всіх ПК, які використовують співробітники «Vodafone Першотравенськ».

Таблиця 1.2 – Характеристики апаратного забезпечення ОС

№	Позначення та назва	Характеристика
1	PC-1 (робоча станція в офісі)	Intel Pentium Gold G6400 (4.0 ГГц) RAM 4 ГБ SSD 120 ГБ Intel UHD Graphics 610
2	PC-2 (робоча станція в офісі)	
3	PC-3 (робоча станція в офісі)	
4	PC-4 (робоча станція в офісі)	
5	PC-5 (робоча станція в офісі)	Intel Core i5-9400F (2.9 – 4.1 ГГц) RAM 16 ГБ HHD 1 ТБ + SSD 240 ГБ n Vidia GeForce GTX 1650, 4 ГБ
6	PR-1 - 2	Epson EcoTank L3251 with Wi-Fi (C11CJ67413)

Таблиця 1.3 – Програмне забезпечення ІКС

Програма	Тип	Ліцензія	Встановлено
Windows 11	Системне	Комерційна	На всіх комп'ютерах
Драйвери	Системне	Freeware	На всіх комп'ютерах
MS Office 2019	Прикладне	Комерційна	На всіх комп'ютерах
«My Vodafone»	Прикладне	Комерційна	На всіх комп'ютерах
1С:Підприємство	Спеціалізоване	Комерційна	На комп'ютері бухгалтера
360 Total Security	Антивірусна програма	Безкоштовна	На всіх комп'ютерах

Інформація, що циркулює в інформаційно-комунікаційній системі (ІКС), включає персональні дані клієнтів і працівників підприємства, фінансову та бухгалтерську звітність, інформацію про діяльність компанії, а також відкриту інформацію (рекламу). Класифікація цієї інформації представлена в таблиці 1.4.

З метою автоматизації управління торговим процесом на підприємстві створюється інформаційна система, яка може включати:

- внутрішню систему обліку і звітності;
- систему маркетингової інформації. Дану інформаційну систему можна визначити і як розвідувальну, тому що вона забезпечує збір, обробку та аналіз даних про діяльність конкурентів.

Дані в інформаційну систему надходять від персоналу компані. Надалі вони використовуються для оперативного управління підприємством, контролю та аналізу діяльності компанії в цілому. Споживачами даної інформаційної мережі є менеджери і керівники компанії. На рисунку 1.2 наведені основні інформаційні потоки, що циркулюють в системі управління підприємством, показані їх основні джерела і споживачі.

Таблиця 1.4 – Класифікація інформації, що обробляється в ІКС

Вид інформації	Режим доступу	Правовий режим	Вид представлення в ІКС	Вимоги до захисту		
				К	Ц	Д
Інформація про клієнтів	ІзОД	Конфіден-ційна інформація	Електронний	3	4	3
Інформація щодо працівників	ІзОД	Конфіденційна інформація	Текстовий	3	4	3
Продукти підприємства	ІзОД	Конфіденційна інформація	Електронний, текстовий	3	4	4
Інформація про надання послуг, контакна інформація	Відкрита інформація	Відкрита інформація	Електронний, текстовий	1	1	2
Бухгалтерська звітність, договори	ІзОД	Конфіденційна інформація	Електронний, текстовий	4	5	4
Фінансова звітність	ІзОД	Службова інформація	Електронний	3	4	4
Організаційно-розпорядча	ІзОД	Конфіденційна інформація	Електронний, текстовий	2	3	2
Реклама	Відкрита інформація	Відкрита інформація	Електронний, текстовий	1	2	2

Застосовуються наступні рівні конфіденційності:

К1 – рівень конфіденційності інформації, при якому збитки у разі розкриття інформації особам без доступу до неї можна знехтувати, або інформація не є конфіденційною;

К2 – рівень конфіденційності інформації, при якому компанія зазнає незначних збитків у разі розкриття інформації особам без доступу до неї;

К3 – рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам без доступу до неї;

К4 – рівень конфіденційності інформації, що може призвести до значних матеріальних втрат у разі розкриття інформації особам без доступу до неї;

К5 – критичний рівень конфіденційності інформації, розкриття якої може призвести до краху компанії.

Застосовуються наступні рівні цілісності:

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

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

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

Ц4 – рівень цілісності інформації, втрата якої може призвести до значних матеріальних втрат;

Ц5 – критичний рівень цілісності інформації, втрата якої може призвести до краху компанії.

Рівні доступності:

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

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

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

Д4 – рівень доступності інформації, втрата якої може призвести до значних матеріальних втрат;

Д5 – критичний рівень доступності інформації, втрата якої може призвести до краху компанії.

Всі ресурси обробляються працівниками підприємства – 2 менеджера, 1 бухгалтер та 3 консультанти.

Вся текстова документація зберігається в зачиненій на ключ архівній кімнаті з обмеженим доступом. Електронна інформація, копії важливих даних яких, записуються на зовнішні жорсткі диски з великим обсягом пам’яті (1 Тб), які зберігаються у зачинених сейфах. Додатково електронна інформація зберігається у зашифрованих хмарних сховищах, що забезпечують високий

рівень безпеки і доступності даних. Щоденно виконується резервне копіювання всієї інформації на ці диски, а також у хмарне сховище.

Інформація про клієнтів (персональна) – зберігається у спеціалізованій базі даних CRM на захищеному сервері підприємства з обмеженим доступом лише для авторизованих працівників.

Інформація про працівників (персональна) – обробляється менеджерами та бухгалтером, може бути надрукована. Особисті справи працівників у паперовому вигляді зберігаються в зачиненій на ключ архівній кімнаті з обмеженим доступом.

Продукти роботи підприємства включають вхідні та вихідні документи, правки, розрахунки, аналітичні матеріали, а також інформацію про клієнтоорієнтованість.

Бухгалтерська та фінансова звітність підприємства обробляється бухгалтерами та перевіряється керівниками різних напрямків. Інформація про зарплати працівників зберігається у електронному та паперовому форматах.

Підприємство активно просуває свої послуги через активну рекламу.

Клієнти можуть звертатися до підприємсвтва самостійно або менеджери активно знаходять потенційних клієнтів через спеціальні платформи та проведення аналізу нових компаній та підприємств. Клієнт звертається до підприємства із своїм питанням/проблемою до консультанта компанії з яким це питання/проблему повинні вирішити. Дані про клієнта вносять в програми (CRM, ERP). Всю допоміжну інформацію та свої персональні данні клієнти можуть надати через застосунок «My Vodafone». Після ознайомленням з питанням/проблемою, консультант повинен надати відповідь/допомогу з приводу звернення клієнта. Після отримання консультації клієнт обирає оптимальне для себе вирішення проблеми. Після відвідування магазину з клієном підтримується зворотній зв'язок у вигляді телефонного дзвінка, де клієнт може відповісти на 5 запитань, стосовно обслуговування та вирішення питання/проблеми з якою звертилися нещодавно. Також з клієном підтримується постійний зв'язок у вигляді реклами та sms нагадувань.

Наприклад про оновлення тарифів, спеціальні пропозиції, акції на техніку та смартфони. Також Vodafone може надсилати своїм клієнтам сповіщення про рахунок, як нагадування про потрібність сплати рахунку, також технічні повідомлення, про стан мережі або інші технічні аспекти.

Матриця розмежування доступу наведена в таблиці 1.5

Таблиця 1.5 – Матриця розмежування доступу

Користувач		Директор	Бухгал-тер	Адміні-стратор безпеки	Менеджер 2	Консуль-тант
Інформація	Інформація про клієнтів	R, W, M, C, T, D	-	T	R	R, W, M, C, T, D
	Інформація про працівників	R	R, W, M, D, C, T	R	-	-
	Продукти підприємства	R, W, M, D, C, T	-	R	R	R
	Про надання послуг, контакна інформація	R, W, M, D, C, T	-	R, W, M, D, C, T	R	R
	Бухгалтер-ська звітність, договори	R, W, M, D, C, T	R, W, M, C, T	-	-	-
	Фінансова звітність	R, W, M, D, C, T	R, W, C, T	D, T	-	-
	Організаційно-розпорядча	R, W, M, C,	R, W, M, C,	R, T	R	R
	Реклама	R, W, D	R	R, M, D	R	R
Повноваження інсталювання ПЗ		+	+	+	+	+
Ресурси		PC 1	PC 2	PC 5	PC 3	PC 4

R – читання; D – видалення;

W – запис; C – створення нових файлів;

T – перенесення; M – модифікація;

1.4 Постановка задачі

На підприємстві «Vodafone Першотравенськ», де обробляється обмежено доступна інформація, власник – директор відділення прийняв рішення про впровадження комплексної системи захисту інформації (КСЗІ). Це включає в себе ряд важливих завдань:

- аналіз моделі загроз: ідентифікація потенційних загроз і вразливостей;
- аналіз моделі порушника: визначення характеристик потенційних нападників і їх методів;
- вибір профілю захищеності: визначення найбільш ефективних методів захисту інформації;
- пропозиції щодо програмно-організаційних заходів: розробка стратегій і заходів для підвищення рівня безпеки;
- аналіз рівня загроз і збитків: оцінка впливу запропонованих заходів на загрози та можливі збитки.

1.5 Висновки до першої частини

Розглянуто важливість маркетингових технологій та захисту інформації в умовах швидкого розвитку технологій.

Було проведено аналіз нормативно-правової бази, в якому визначено основні положення, законодавчі акти України, а також накази, що стосуються захисту інформації, зокрема персональних даних, інформації з обмеженим доступом та технічного захисту інформації.

Були розглянуті загальні відомості про підприємство «Vodafone Першотравенськ», проведено обстеження ситуаційного та генерального плану, оцінено обчислювальну та інформаційну системи, а також вивчено організаційну структуру підприємства. Визначена необхідність створення комплексної системи захисту інформації (КСЗІ) на підприємстві «Vodafone Першотравенськ», а також сформульовано постановку задачі щодо її реалізації.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

Для покращення системи безпеки ІКС слід виконати низку операцій, спрямованих на досягнення наступних принципів.

Перший принцип – конфіденційність. Доступ до даних надається за правилом «мінімальної необхідної обізнаності». Іншими словами, користувач повинен мати право доступу лише до частини інформації, яка йому необхідна для виконання своїх службових обов'язків.

Один із методів виконання даного принципу – ранжування (категоризація) даних. Наприклад, всередині організації інформація поділяється на 3 типи: публічна, внутрішня та суворо конфіденційна.

Другий принцип – цілісність. Інформація має бути захищена від змін чи спотворень. Вона повинна зберігатися, оброблятися та передаватися надійними каналами зв'язку.

Для забезпечення цілісності на рівні користувачів використовують правило «розмежування повноважень», тобто будь-яка зміна вноситься одним користувачем, а підтвердження чи відмова іншим. В обов'язковому порядку ведеться протоколювання будь-яких операцій на інформаційній системі.

Третій принцип – доступність. Це означає, що інформація повинна бути доступна користувачеві за необхідності. Ідеальний варіант 24*7*365.

Цей пункт містить як людський чинник, а й природний (наприклад, цунамі чи ураган). Інформаційна система має забезпечувати доступність за будь-яких умов.

Для досягнення зазначених принципів застосовують наступні засоби.

- правові. На об'єкті інформатизації розробляють спеціальні документи, якими керуються задля забезпечення ІБ. Основним є політика ІБ, з урахуванням якого будується захист.
- організаційні. До них відносяться робочі місця співробітників (комп'ютери, ДБЖ і т. д.), ЦОДи (комутація, системи зберігання даних, обчислювальні потужності тощо), резервування (створення дублюючих каналів зв'язку, бекапірування даних).

- програмні. ПЗ, що допомагає контролювати дії співробітників, зберігати інформацію, забезпечувати надійний доступ до даних.
- технічні. Спеціалізоване обладнання, яке захищає інформацію від витоку чи злому. Наприклад, шифрування, двоетапна процедура аутентифікації, віртуальні робочі середовища тощо.

Забезпечення інформаційної безпеки у компанії полягає у комплексному підході до побудови надійної та відмовостійкої системи. Вищезазначені пункти рекомендовані для реалізації на будь-якому об'єкті інформатизації.

2.1 Модель порушника

Стрімке проникнення інформаційно-комунікаційних технологій в усі сфери життедіяльності людини і суспільства спричинило як позитивні, так і негативні наслідки. Комп'ютеризація різних організацій дозволила прискорити взаємодію між службовцями, а також оптимізувати їх роботу. Однак поряд зі збільшенням швидкості роботи з'явилися нові можливості і для недобросовісних співробітників. Тепер вони можуть швидко і просто, не покидаючи свого робочого місця, передати конфіденційну інформацію третій особі.

Забезпечення безпеки підприємств вимагає комплексу заходів, спрямованих на попередження, припинення та усунення загроз і небезпечних ситуацій. Цей комплекс повинен будуватися за принципом системного підходу і включати сукупність організаційних заходів, технічних засобів безпеки та фізичної охорони.

Порушником є особа, яка здійснює спробу несанкціонованого доступу до об'єктів захисту (ознайомлення, модифікаця, знищення, зміна режимів використання чи функіонування тощо). Потенційними порушниками є:

- особи, які знаходяться за межами ІКС, мають можливість фізичного підключення до каналів зв'язку або інших складових мережі передачі даних;
- користувачі АС;

- персонал, який безпосередньо пов'язан із забезпеченням функціонування ІКС;
- особи, яким не передбачено доступ до ІЗОД, але які мають доступ до примішень, де розміщено компоненти ІТС і можуть отримати доступ до ІЗОД

Модель порушника - абстрантний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце ді тощо.

Зовнішній порушник (ЗП) - це порушник, що діє із зовнішнього, відносно ІКС, боку. У цій моделі розглядається як особа, що має доступ до приміщень, у яких розташовані засоби обчислювальної техніки, але не є авторизованим користувачем.

Категорії осіб, які можуть бути зовнішніми порушниками:

- конкуренти;
- персонал сусідніх компаній;
- клієнти.

Внутрішній порушник (ВП) - це порушник, що діє зсередини ІКС. У цій моделі розглядається як особа, що має доступ до примішень, у яких розташовані засоби обчислювальної техніки та с авторизованим користувачем ІКС.

Внутрішнім порушником може бути особа з персоналу:

- директор;
- бухгалтер;
- адміністратор безпеки;
- менеджер;
- консультант.

У таблиці 2.1. наведені категорії порушників, що будуть використовуватися при створенні моделі.

Таблиця 2.1. – Категорії порушників, що визначені в моделі

Позначення	Визначення категорії	Потенційний рівень загрози
П1	Адміністратор безпеки	5
П2	Співробітники підприємства	4
П3	Конкуренти	5
П4	Персонал сусідніх компаній	3
П5	Клієнти	2

Для розробки моделі порушника можна використовувати табличний метод (Таблиці 2.2 – 2.7). Для створення моделі використовуються категорії, ознаки та характеристики порушників, що дозволяє точніше їх аналізувати. Ступінь небезпеки кожної категорії вказується в дужках і оцінюється за 4-бальною шкалою.

Таблиця 2.2 – Опис моделі порушника за мотивами здійснення неправомірних дій

Позначення	Мотив неправомірних дій	Ступінь небезпеки
М1	Недбалість	1
М2	Самоствердження	2
М3	Власна вигода	3
М4	Професійне зобов'язання	4

Таблиця 2.3 – Опис моделі порушника відповідно до кваліфікації та інформованості щодо ІКС

Позначення	Основні кваліфікаційні ознаки порушника	Ступінь небезпеки
К1	Ця особа має обмежені знання, але добре орієнтується у використанні технічних засобів ІКС	1
К2	Ця особа має достатні знання і вміння в роботі з технічними засобами ІКТ та їх обслуговуванням	2

Продовження таблиці 2.3 – Опис моделі порушника відповідно до кваліфікації та інформованості щодо ІКС

Позначення	Основні кваліфікаційні ознаки порушника	Ступінь небезпеки
К3	Ця особа має високу експертизу у програмуванні, обчислювальній техніці, проектуванні та експлуатації інформаційно-комунікаційних систем	3
К4	Ознайомлений з усіма аспектами захисту інформації в інформаційно-комунікаційних системах, включаючи їх структуру, функції, механізми дії, а також можливі недоліки та переваги	4

Таблиця 2.4 – Опис моделі порушника за ефективністю використання засобів та методів подолання системи захисту інформації

Позначення	Можливості порушника	Ступінь небезпеки
З1	Здатний лише до здійснення підслуховування розмов у приміщеннях та підгляду за документами на робочих місцях	1
З2	Застосовує пасивні технічні засоби для перехоплення інформації в ІКС без втручання у її зміст або компоненти	2
З3	Використовує дозволені засоби та використовує недоліки системи захисту для її обхіду, а також скористається компактними машинними носіями інформації, які можуть бути приховані і пронесені через охорону	3
З4	Застосовує активні технічні засоби для зміни інформації та компонентів ІТС, а також для дезорганізації систем обробки інформації.	4

Таблиця 2.5 – Опис моделі порушника за часом дії

Позначення	Можливості порушника	Ступінь небезпеки
Ч1	Під час повної недоступності ІКС для відновлення та ремонту	1
Ч2	Під час призупинки компонентів ІКС для проведення технічного обслуговування та модернізації	2
Ч3	Під час функціонування ІКС (або компонентів системи)	3
Ч4	Як під час роботи ІКС, так і під час призупинення її компонентів	4

Таблиця 2.6 – Опис моделі порушника за місцем дії

Позначення	Опис місця діїі порушника	Ступінь небезпеки
Д1	Всередині приміщень, але без можливості використовувати технічні засоби інформаційно-комунікаційних систем	1
Д2	З робочих місць користувачів ІКС	2
Д3	З доступом до зони, де зберігаються бази даних, архіви та інші матеріали	3
Д4	З доступом до зони управління засобами забезпечення безпеки інформаційно-комунікаційних систем	4

На основі систем таблиць будується модель внутрішнього порушника , та модель зовнішнього порушника.

Таблиця 2.7 – Модель внутрішнього та зовнішнього порушника

Порушник	Категорія	Характер дій порушника					Сума загроз
		Мотив	Кваліфікація	Можливо-сті	Час дії	Місце дії	
Внутрішні порушники (ВП)							
Адміністратор безпеки	П1	М4	К4	З3	Ч4	Д4	24
Директор	П2	М4	К3	З3	Ч4	Д4	22
Бухгалтер	П2	М3	К2	З2	Ч3	Д2	16
Менеджер	П2	М1	К2	З2	Ч2	Д3	14
Консультант	П2	М4	К1	З1	Ч3	Д2	15

Продовження таблиці 2.7 – Модель внутрішнього та зовнішнього порушника

Порушник	Категорія	Характер дій порушника					Сума загроз
Зовнішні порушники (ЗП)							
Персонал сусідніх компаній	П3	М3	К3	З2	Ч2	Д1	14
Конкуренти	П4	М3	К3	З3	Ч3	Д2	19
Клієнти	П5	М3	К1	З1	Ч3	Д1	11

Основними потенційними порушниками можуть бути:

- директор;
- адміністратор безпеки;
- бухгалтер;
- консультант;
- конкуренти.

Тому організація роботи цих осіб має бути найбільш контрольованою.

2.2 Модель загроз

Всі джерела загроз безпеці інформації можна розділити на три основні групи:

А - обумовлені діями суб'єкта (антропогенні джерела загроз):

Т - обумовлені технічними засобами (техногенні джерела загроз);

С - обумовлені стихійними джерелами.

Антропогенними джерелами загроз безпеці інформації виступають суб'єкти, дії яких можуть бути кваліфіковані як умисні або випадкові злочини.

Як антропогенного джерела загроз можна розглядати суб'єкта, що має доступ (санкціонований або несанкціонований) до роботи зі штатними засобами об'єкта, що захищається. Суб'єкти (джерела), дії яких можуть призвести до порушення безпеки інформації можуть бути як зовнішні (А.З), так і внутрішні (А.В).

Зовнішні джерела можуть бути випадковими або навмисними і мати різний рівень кваліфікації. До них відносяться:

А.3.1 - конкуренти;

А.3.2 - персонал сусідніх компаній;

А.3.3 - клієнти.

До внутрішніх відносяться:

А.В.1 – адміністратор безпеки;

А.В.2 - пересонал (співробітники).

Для ранжування антропогенних джерел загроз використовуються наступні коефіцієнти:

К1 - визначає ступінь доступності до об'єкта, що захищається;

К2 – визначає рівень кваліфикаці;

КЗ - визначає ступінь фатальності.

Для визначення ступеня доступності до об'єкта К1 використовують ранги:

5 - джерело має повний доступ до технічних засобів;

4 - джерело має можливість опосередкованого доступу до системи та й компонентів за необхідності;

З - джерело має обмежену можливість доступу до системи та її компонентів;

2 - джерело дуже обмежено у можливостях;

1 - повна відсутність доступу.

Для визначення рівня кваліфікаці К2:

5 - максимальний рівень прав.

4 - може впреити змити;

З - середній рівсть прав;

2 - обмежені права;

1 - повна відсутність прав.

Для визначення ступеня фатальності КЗ:

5 - велика проблема, для вирішення якої треба призупиняти функціонування системи або її компонентів;

4 - проблема, яка потребує негайного вирішення;

3 - проблема, яка не потребує негайного вирішення;

2 - незначні проблеми;

1 - проблеми не виникали.

Техногенними джерелами виступають технічні засоби, які так само можуть бути зовнішніми (Т.З) та внутрішніми (Т.В):

Т.З.1 - телекомунікаційні мережі;

Т.З.2 - мережі інженерних комунікацій (водопостачання, каналізаці);

Т.В.1 - технічні засоби обробки інформації;

Т.В.2 - програмні засоби обробки інформації;

Т.В.3 - допоміжні засоби (охорони, сигналізаці).

Для ранжування техногенних джеред загроз використовуються наступні коефішієнти:

К1 - визначає ступінь віддаленості джерела загрози від об'єкту;

К2 - необхідні умови готовності джерела загрози;

К3 - визначає ступінь фатальності.

Для визначення ступеня віддаленості джерела загрози від об'єкту, що закишається використовують наступні значення:

5 - співпалаючі об'єкти;

4 - джерело знаходиться поруч;

3 - джерело знаходиться на деякій невеликій відстані;

2 - джерело знаходиться на дсякій великій відстані;

1 - джерело знаходиться дуже далеко.

Для визначення необхідних умов готовності джерела загрози використовують значення:

5 - загроза може бути успішно реалізована;

4 - загроза може бути реалізована;

3 - загроза може бути помірно реалізована;

2 - загроза слабко реалізується;

1 - загроза не може бути реалізована.

Ступінь фатальності визначають слідуючим чином:

5 - велика проблема, для вирішення якої треба призупиняти функціонування системи або її компонентів;

4 - проблема, яка потребує негайного вирішення;

3 - проблема, яка не потребує негайного вирішення;

2 - незначні проблеми;

1 - проблеми не виникали.

Стихійні лиха, як джерела загроз інформаційній безпеці, як правило, є зовнішніми по відношенню до об'єкту, що захищається і під ними розуміються насамперед природні катаклізми (С.3):

С.3.1 – пожежа;

С.3.2 - землетруси, повені, урагани;

С.3.3 – епідемії;

С.3.4 - масові заворушення.

Для ранжування стихійних лих, як джерел загроз використовуються наступні коефішенти:

КІ - визначає особливості місцезнаходження об екту, що захищається;

К2 - необхідні умови готовності джерела;

КЗ - визначає ступінь фатальності.

Для визначення особливостей місцезнаходження об'єкту, що захищається К1 використовують наступні значення:

5 - зона захисту знаходиться у зоні стихійного лиха;

4 - стихійне лихо часто відбувається у зоні захисту;

3 - інколи трапляється стихійне лихо у зоні захисту;

2 - мала ймовірність виникнення стихійного лиха у зоні захисту;

1 - виникнення стихійного лиха у зоні захисту майже неможливо.

Необхідні умови готовності джерела К2 визначаються виходячи з можливості реалізації загрози в конкретних умовах розташування об'єкта:

5 - загроза може бути успішно реалізована;

4 - загроза може бути реалізована;

3 - загроза може бути помірно реалізована;

2 - загроза слабко реалізується;

1 - загроза не може бути реалізована.

Ступінь фатальності визначається слідуючими рангами:

5 - велика проблема, для вирішення якої треба призупиняти функціонування системи або її компонентів;

4 - проблема, яка потребує негайного вирішення;

3 - проблема, яка не потребує негайного вирішення;

2 - незначні проблеми;

1 - проблеми не виникали.

За допомогою ранжування усіх джерел загроз, можна провести їх кількісну оцінку використовуючи формулу:

$$К_Н = \frac{К_1 * К_2 * К_3}{125}, \quad (2.1)$$

де Кн - загальний коефіцієнт небезпеки;

К1, К2, К3 - коефіцієнти для ранжування джерел загроз.

Враховуючи проведене ранизвання розрахуємо загальний коефіцієнт небезпеки для кожного з визначених джерел (таблиця 2.8)

Таблиця 2.8. – Джерела загроз

Умовне позначення	К1	К2	К3	$К_Н$
А.З.1	3	3	5	0,36
А.З.2	2	3	3	0,14
А.З.3	4	2	4	0,26
А.В.1	5	4	4	0,64
А.В.2	4	3	4	0,38
Т.З.1	4	3	4	0,38
Т.З.2	4	3	4	0,38
Т.В.1	5	3	4	0,64
Т.В.2	5	4	4	0,64
Т.В.3	4	3	4	0,38
С.З.1	2	2	5	0,16
С.З.2	3	2	3	0,14
С.З.3	2	2	3	0,1
С.З.4	2	2	2	0,06

Найбільш небезпечними можна назвати джерела загроз, загальні коефіцієнти небезпеки яких більше за 0,3.

Згідно проведеного аналізу це:

А.3.1 - конкуренти (0,36);

А.В. - директор (0,64);

А.В.2 - персонал (співробітники) (0,38);

Т.3.1 - телекомунікаційні мережі (0,38);

Т.3.2 - мережі інженерних комунікацій (водопостачання, каналізації (0,38);

Т.В. 1 - технічні засоби обробки інформації (0,64);

Т. В. 2 - програмні засоби обробки інформації (0,64);

Т.В.3 - допоміжні засоби (охорони, сигналізаші) (0,58).

Зважаючи на результати ранжування джерел загроз, визначимо загрози безпеці інформації для підприємства «Vodafone Україна Першотравенськ» та вразливості які вони використовують.

Побудована модель загроз представлена в таблиці 2.9.

Таблиця 2.9 – Список загроз з описом порушень властивостей інформації та ІКС

Джерело загроз	Вразливість	Загроза	Значення наслідків	Йомовірність ревлизації	Показник ризику	К	Ц	Д
Конкуренти	Неконтрольоване копіювання	Перехоплення конкурентами інформації	5	3	15	x		
	Встановлення апаратних закладок у приміщені		5	2	10	x		
Директор	Неправильний розподіл прав доступу	Зловживання правами	5	3	15	x	x	x
	Відсутність регулярних аудитів		5	3	15	x	x	x
Адміністратор безпеки	Помилки при експлуатації програмного забезпечення	Зараження комп’ютерів вірусами	4	5	20	x	x	x
	Відсутність механізма моніторінга	Незаконе оброблення даних	4	4	16	x	x	x
Основний персонал	Відсутня обережність під час розміщення	Читання/викрадання документів	4	3	12	x		
	Неналежна обізнаність щодо безпеки	Помилка під час використання	4	5	20	x	x	

Продовження таблиці 2.9 – Список загроз з описом порушень властивостей інформації та ІКС

Джерело загроз	Вразливість	Загроза	Значення наслідків	Йомовірність ревлизації	Показник ризику	К	Ц	Д
Комунікаційні мережі	Одна точка відмови	Аварія комунікаційного обладнення	4	3	12			х
Мережі інженерних комунікацій	Ушкодження електро-, водо-, теплопостачання, каналізації	Призупинення роботи на деякий час через аварію інженерних систем	2	3	6			х
Технічні засоби обробки інформації	Чутливість до змін напруги	Втрата електроживлення	2	3	6			х
	Відсутній ефективний контроль змін конфігурації	Помилка під час використання	3	5	15			х
Програмні засоби обробки інформації	Відсутній журнал подій	Зловживання правами	4	4	16	х	х	х
Допоміжні засоби (охорони, сигналізації)	Ушкодження системи охорони та/або сигналізації	Призупинення роботина деякий час	2	3	6			х

Значення наслідків: 1 – незначний (дуже низький), 2 – низький, 3- середній, 4 – вищий за середній, 5 – значний.

Імовірність реалізації загрози: 1 – дуже низька, 2 – низька, 3 – середня, 4 – висока, 5- дуже висока.

Побудована модель загроз пов’язує чинники наслідків та імовірності реалізації загрози (враховуючи аспекти вразливостей). Таким чином, остаточно загрози можуть бути ранжовані в порядку їх пов’язаного показника ризику.

В подальшому, для розробки заходів безпеки до урахування будемо брати загрози показник ризику яких більше, або дорівнює 15, а саме:

- зараження комп’ютерів вірусами;
- помилки під час використання;
- незаконне оброблення даних;
- зловживання правами;
- перехоплення конкурентами інформації.

2.3 Профіль захищеності

Під час створення КСЗІ оцінюється здатність системи забезпечувати захист інформації. Розглядається захист оброблюваної інформації як від несанкціонованого доступу, так і від витоку через технічні канали. Критерії комп'ютерної системи включають набір функціональних послуг і функцій, які забезпечують захист від визначених загроз [8, с. 4].

Автоматизована система є організаційно-технічною системою, що включає персонал, оброблювану інформацію, операційні системи та фізичне середовище. Для нашого об'єкта інформаційної діяльності обрана АС класу «3». Відповідно до НД ТЗІ 2.5-005-99 [9, с. 16], це розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу. Відмінною рисою від попереднього класу є необхідність передачі інформації через незахищене середовище або, у загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

В автоматизованій системі класу «3» обрані стандартні функціональні профілі захищеності комп'ютерної системи з підвищеними вимогами до забезпечення конфіденційності, цілісності та 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, ДВ-1 НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1, НА-1}.

Згідно з НД ТЗІ 2.5.004-99:

К1-2 – Базова довірча конфіденційність. Стандартна система вибіркового керування доступу дозволяє резлізувати базовий рівень даної послуги. У поточній конфітурації системи, послута реалізована завдяки спискам контролю доступу. Необхідні умови: КО-1, НИ-1.

КА-2 - Базова адміністративна конфіденційність. Ця послуга дозволяє адміністратору або спешально авторизованому користувачу розпоряджатися потоками інформації від захищених об'єктів до користувачів. Реалізована завдяки системним адміністраторам, які надають рівні доступу до об'єктів та мають журнал доступу користувачів різних рівнів до інформації. Необхідні умови: КО-1, НО-1,НИ-1.

КО-1 - Повторне використання об'єктів. Реалізована. Ця послуга гарантує вірне повторне застосування загальних об'єктів, гарантуючи, те що в разі якщо загальний об'єкт призначений новому користувачеві або процссу, він не стане включати ніякої інформації. Через систему розмежування доступу до облікових записів.

КВ-2 - Базова конфіденційність при обхіні. Не реалізована. Дана послуга дозволяє захистити об'єкти від несанкціонованого доступу, що міститься в них, при їх експорті/імпорті через незахищену середу.

КВ-1 - Мінімальна конфіденційність при обміні. Реалізована. Стандартними послугами операційної снетеми Microsoft Windows 11.

ЦД-1 - Мінімальна довірча цілісність. Резлізована. Дана послуга дає можливість користувачеві регулювати інформаційні потоки від імені інших користувачів до захищених об'єктів, що належать його домену. У системі присутня можливість надавати різні рівні доступу. Необхідні умови: НИ-1.

ЦА-2 - Базова адміністративна цілісність. Реалізована. Дана послуга дас можливість адміністратору або особливо уповноваженому користувачу регулювати потоком даних від користувачів до захищених об'єктів. В системі

присутні уповноважені особи (системні адміністратори), які можуть керувати потоками інформації.

ЦО-1 - Обмежений відкат. Резлізована. Ця послуга дає можливість уберегти об'єкти від несанкціонованої модифікації інформації, що міститься в них, в період їх експорту/імпорту за допомогою незахищеного середовиша. У системі наявна можливість відміни останніх дій (від 30 до 100 у різних програмах) у таких програмах як Mictosoft World. Необхідні умови: НИ-1.

ДР-1 - Квоти. Не реалізована. Ця послуга дозволяс користувачам керувати використанням послут та ресурсів.

ДВ-1 - Ручне відновлення. Реалізована. Ця послуга дозволяс повернути КС у відомий захищенний стан після відмови або переривання обсуговування, або іншими непередбачуваними ситуаціями. Відновлення у відомий захищений стан відбувається завляки системним адміністраторам. Необхідні умови: НО- 1.

НР-2 - Захищений журнал. Реєстранія у журналі подій дає моживість здійснювати контроль за діями, небезпечними для КС. К33 повинен бути здатним здійснювати реєстрацію подій, що мають безпосередне відношення до безпеки. Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу або об'єкта, що мали відношення до кожної зареєстрованої події. К33 повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, молифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

Необкілні у мови: НИ-1, НО-1.

НИ-2 - Одиночна ідентифікація і автентифікація. Реалізована. Ідентифікація та автентифікація дозволяють К33 ілентнфікувати та перевірити особистість користувача, що намагається отримати доступ до КС. Необхідні умови: НК-1.

НК-1 - Однонаправлений достовірний канал. Ця послуга дає можливість

забезпечувати користувачеві можливість безпосередньої взаємодії з КЗЗ. Реалізована, за рахунок вбудованих функцій операційної системи Microsoft Windows 11.

НО-2 - Розподіл обов'язків адміністраторів. Дана послуга зменшує можливість навмисних або помилкових несанкціонованих дій користувача або адміністратора, а також обсяг потенційного збитку від полібних операцій. У мовно реалізована. АС має три особи, що виконують ролі адміністраторів системи. За бажанням власника ІТС можливе розподілення ролей адміністраторів. Необхідні умови: НИ-1.

НЦ-2 - КЗЗ з гарантованою цілісністю. Дана послуга визначає ступінь можливості КЗЗ захищатися та гарантувати свою здатність ксрувати захищеними об'єктами. Жодна КС не може вважатися захищеною, якщо засоби захисту с об'єктом для несанкціонованого впливу. В зв'язку з цим рівень НЦ-1 даної послути є необхідною умовою для абсолютно всіх рівнів усіх інших послуг. Реалізована, за рахунок вбудованих функцій операційної снетеми Microsoft Windows 11.

НТ-2 - Самотестування при старті, КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження при ініціалізації КЗЗ. Реалізована, за рахунок вбудованих функцій операційної системи Microsoft Windows 1, а також за допомогою антивирусного забезпечення. Необхідні умови: НО-1.

НВ-1 – Автентифікація вузла. Дана послуга дає можливість КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, ідентифікувати і автентифікувати цей КЗЗ з використанням захищеного механізму і підтвердження ідентичності. Мас виконуватися на підставі затвердженого протоколу автентифікації. Резлізована, за рахунок вбудованих функцій операційної системи Microsoft Windows 11.

НА-1 - Базова автентифікація відправника. Реалізована. Ця послуга дозволяє однозначно встановити відносини між певним обектом та певним користувачем, тобто той факт, що об'єкт був створений або відправлений цим

користувачем. Кожнен облікови запис містить інформацію щодо прізвища та ім’я користувача.

НП-1 — Базова автентифікація отримувача. Резлізована. Дана послуга дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Кожна облікова запис містить інформацію щодо прізвища та ім’якористувача.

2.4 Визначення методів та засобів захисту

Основним критерієм вибору методів захисту було:

– використовувати методи захисту відповідно до п. 17 Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27 вересня 1999 р. № 1229. Перелік призначений для використання суб’єктами системи технічного захисту інформації (ТЗ) під час розроблення, модернізації та впровадження комплексів КЗІ на об’єктах інформаційної діяльності (ОД) та комплексних систем захисту інформації (КСЗІ) в автоматизованих системах (АС);

– використовувати економічно обгрунтовані методи захисту;

– дотримуватись принципів логічності.

Проаналізувавши основні загрози та вразливості підприємства «Vodafone Україна Першотравенськ», що надані в таблиці 2.9, було запропоновано наступне:

1. Вимоги з інформаційної безпеки, які під час роботи забороняють:

– користуватись мобільними пристроями зв’язку (телефон, смартфон тощо) в торгівельному залі;

– підключати до комп’ютерів, що знаходяться в торгівельному залі будь-які зовнішні накопичувачі інформації (USB Flash, SD-карти, телефони/смартфони тощо);

– приносити та підключати до робочих комп'ютерів та/або локальної комп'ютерної мережі будь-яке стороннє обладнання/пристрої використовувати для входу в інформаційну систему облікові дані іншого співробітника;

– ремонтувати робочий комп'ютер, вносити зміни у склад його апаратних та програмних засобів (завантажувати інтерфейс керування системним ПЗ BIOS, вносити зміни або знищувати системні/конфігураційні файли операційної системи/мережевих пристроїв, самостійно встановлювати програмне забезпечення, самостійно підключати або відключати периферійне обладнання, порушувати цілісність корпусу робочого комп'ютера (крім випадків обумовлених використанням посадових/договірних обов'язків);

– залишати на робочому місці робочі записи/чернетки після закінчення робочого часу (в електронному вигляді - видаляти, в паперовому - знищувати у пристроях утилізації паперу);

– залишати ввімкненим робочий комп'ютер по закінченню робочого часу, за винятком випадків коли його подальша робота викликана технологічними вимогами;

– намагатись та/або вчиняти дії щодо отримання несанкціонованого доступу до робочих комп'ютерів мережевого обладнання та сервера, а також втручатись в роботу системи антивірусного захисту;

– використовувати Internet для обміну інформацією розважального характеру, зокрема відвідувати файл обмінні сервіси, соціальні мережі, сайти знайомств, чати, відео-/аудіо-ресурси та ін.

– відправляти повідомлення електронною поштою. Особам, які не мають відношення до інформації, що пересилається (спам в електронній пошті);

– поширювати електронні повідомлення, що містять підозрілі вкладення, посилання на сторонні ресурси Намагатись переглянути вкладення підозрілих електронних повідомлень;

– завантажувати з мережі Internet зберігати та/або використовувати на робочому комп'ютерів програмне забезпечення та/або інформацію, що не має відношення до виконання посадових обов'язків;

– використовувати мережеві та обчислювальні ресурси для отримання або спроби отримання несанкціонованого доступу, участі у мережевих атаках та будь-яких деструктивних діях по відношенню до будь-якої мережі через Internet.

2. Впровадити технології DLP

Технологія DLP (Data Leak Prevention) запобігає витоку конфіденційної інформації з інформаційної системи. DLP-системи будуються на аналізі потоків даних, які перетинають периметр інформаційної системи. Якщо була знайдена після аналізу потоків конфіденційна інформація - спрацьовує активна компонента системи, і передача повідомлення (пакета, потоку, сесії) блокується.

Для запровадження була обрана DL.P-система з переліку засобів КЗІ, які мають експертний висновок про відповідність до вимог технічного захисту інформації, що сформовано відповідно до п. 17 Положення про технічний захист інформації в Україні, а саме Trellix Complete EndPoint Protection – Business версії 9х, виробництва компанії Trellix (США).

Trellix Complete EndPoint Protection – Business є комплексним засобом захисту від внутрішнього порушника, яке забезпечує зв'язок між декількома засобами захисту від загроз для виявлення, здавалося б, не пов'язаних між собою подій, що пов'язані і є частиною цілеспрямованої атаки. Виявляє, очищає та блокує шкідливі програми з серверів Microsoft Exchange та Lotus Domino за допомогою McAfee Security for Email Servers. Захист від невідомих загроз нульового дня та нових вразливостей, зниження терміновості виправлень. Захист конфіденційних даних на ПК, комп'ютерах Mac, ноутбуках, мережевих серверах, знімних носіях та хмарних сховищах..

Trellix Complete EndPoint Protection – Business дозволить закрити основні канали витоку інформації, що дозволить захистити конфіденційні дані компанії

не тільки від несанкціонованого доступу, а й від потенційно шкідливої активності співробітників, наділених правом працювати з такими відомостями.

Завдання розпізнавання нестандартної діяльності співробітників вирішується завдяки звітам з діяльності співробітника, а саме:

- підрахунку згенерованого і одержаного мережевого трафіку;
- контролю використання додатків і пристроїв;
- відвідування веб-сайтів;
- контроль друку, роботи з файлами і електронною поштою.

3. Впровадити новий програмний продукт антивірусного захисту, що обрано з переліку засобів КЗІ, які мають експертний висновок про відповідність до вимог технічного захисту інформації, що сформовано відповідно до п. 17 Положення про технічний захист інформації в Україні, а саме ESET Endpoint Security для Windows (EES) з системою централізованого керування ESET Remote Administrator, виробництва компанії ESET (Словаччина).

Endpoint Security виявляє та знешкоджує загрози, спрямовані на операційну систему Windows, забезпечує управління змінними носіями, запобігає вторгненням (HIPS), дозволяє створювати завантажувальний образ операційної системи з встановленим антивірусним сканером для очищення заражених ПК.

4. Створення політики або впровадження в існуючу політику розділів, щодо розмежування доступу та ведення журнала реєстрації подій.

В таблиці 2.10 наведені основні положення, що повинні включати запропоновані політики безпеки.

Таблиця 2.10 - Основні положення, що повинні включати запропоновані політики безпеки.

Назва	Опис
Політика розмежування прав доступу	Політика розмежування прав доступу регламентує правила доступу користувачів і процесів до пасивних об'єктів. Відповідно до НД ТЗІ 1,4-001.2000, мають виконуватися наступні дії: – кожне робоче місце повинно мати свого користувача, який несе відповідальність за його працездатність; – для попередження неавторизованого доступу до даних, ПЗ, інших ресурсів, керсування механізмами захисту здійснюється адміністратором системи; – за всі зміни ПЗ, створення резервних та архівних копій несе відповідальність адміністратор системи; – кожний користувач має свій ідентифікатор та пароль. Атрибути для адміністратора системи надає адміністратор безпеки. Видача атрибутів доступу дозволяється тільки після документальної реєстрації користувача; – користувачі проходять процедуру автентифікації для отримання ресурсів ІКС; – атрибути користувачів змінюються двічі на рік, а невикористовування і скомпроментовані - видаляються.
Політика ведення журнала реєстрації подій	Журнал реєстрації призначений для зберігання подій, що виникають в процесі роботи користувачів з інформаційною базою. Усі системи, які обробляють конфіденційну інформацію, мають підключення до мережі або приймають рішення щодо контролю доступу (автентифікація та авторизація), повинні фіксувати та зберігати інформацію про реєстрацію події, достатню для відповіді на наступні запитання: – Яку діяльність виконували? – Хто або що виконував діяльність, включаючи те, звідки чи за якою системою діяльність здійснювалась (суб'єкт)? – З якою діяльністю виконувались (об'єкт)? – Коли виконувалася діяльність? – Яким інструментом (інструментами) виконувалась діяльність? – Яким був статує (наприклад, успіх проти невдачі), результат чи результат діяльності?

Продовження таблиці 2.10 - Основні положення, що повинні включати запропоновані політики безпеки.

Назва	Опис
Політика ведення журнала реєстрації подій	Журнал повинен створюватися шоразу, коли система вимагає виконання будь-якої з наступних дій: – створювати, читати, оновлювати або видаляти конфіденційну інформацію, включаючи конфіденційну інформацію про автентифікацію, таку як паролі; – створювати, оновлювати або видаляти інформацію, не висвітлену в N°1; – ініціювати підключення до мережі; – прийняти підключення до мережі; – аутентифікація та авторизація користувачів для дій, описаних в N°l або N°2, таких як вхід та вихід користувача; – надати, змінити або скасувати права доступу, включаючи додавання нового користувача або групи, зміну рівнів привілеїв користувача, зміну дозволів файлів, зміну дозволів об'єктів бази даних, зміну правил брандмауера та зміну пароля користувача. – зміни конфігурації системи, мережі чи послут, включаючи встановлення виправлень та оновлень програмного забезпечення, або інші встановлені зміни програмного забезпечення, – запуск, призулинення або перезапуск процесу застосування; – переривання, відмова або аномальне завершення процесу програми, особливо через вичерпання ресурсів або досягнення обмеження або порогу ресурсу відмови мережі послуги, такі як DHCP або DNS, або несправність обладнання; - виявлення підозрілих / шкідливих дій, таких як система виявлення або запобігання вторгненню (IDS / IPS), антивірусна система чи система захисту від шпигунського програмного забезпечення.

6. Запровадити організаційні методи, що направлені на підвищення обізнаності щодо інформаційної безпеки у співробітників.

Основною метою підвищення обізнаності працівників організації з питань інформаційної безпеки є зменшення втрат (матеріальних, фінансових,

іміджевих), що виникають внаслідок загроз, пов'язаних з недостатнім знанням працівників або нерозумінням основних принципів інформаційної безпеки, у тому числі при роботі в інформаційній системі організації.

Таким чином необхідно:

– розробити зобов'язання про нерозголошення конфіденційної інформації, яке співробітник повинен підписувати до того, як йому буде повідомлено склад конфіденційних відомостей;
– інформувати працівників про існуючі загрози (вразливості) та питання безпеки, які можуть виникнути під час їх повсякденної роботи;
– забезпечити працівників основними вимогами, обмеженнями та правилами політики інформаційної безпеки організації.
– проводити регулярні тренінги, спрямовані на підвищення обізнаності користувачів в питаннях інформаційної безпеки.

2.5 Аналіз загроз після впровадження програмно-організаційних рішень

В таблиці 2.11 наведено перелік загроз з визначенням порушень властивостей інформації ІКС після впровадження запропонованих програмно-організаційних рішень «Vodafone Україна Першотравенськ»

Таблиця 2.11. - Перелік загроз з визначенням порушень властивостей інформації ІКС після впровадження програмно-організаціних рішень

Джерело загроз	Вразливість	Загроза	Значення наслідків	Йомовірність ревлизації	Показник ризику	К	Ц	Д
Конкуренти	Неконтрольоване копіювання	Перехоплення конкурентами інформації	5	2	10	x		
	Встановлення апаратних закладок у приміщені		5	2	10	x		
Директор	Неправильний розподіл прав доступу	Зловживання правами	5	2	10	x	x	x
	Відсутність регулярних аудитів		5	2	10	x	x	x
Адміністратор безпеки	Помилки при експлуатації програмного забезпечення	Зараження комп'ютерів вірусами	4	3	12	x	x	x
	Відсутність механізма моніторінга	Незаконе оброблення даних	4	2	8	x	x	x
Основний персонал	Відсутня обережність під час розміщення	Читання/викрадання документів	4	3	12	x		
	Неналежна обізнаність щодо безпеки	Помилка під час використання	4	3	12	x	x	

Продовження таблиці 2.11 – Перелік загроз з визначенням порушень властивостей інформації ІКС після впровадження програмно-організаціних рішень

Джерело загроз	Вразливість	Загроза	Значення наслідків	Йомовірність ревлизації	Показник ризику	К	Ц	Д
Комунікаційні мережі	Одна точка відмови	Аварія комунікаційного обладнення	4	3	12			х
Мережі інженерних комунікацій	Ушкодження електро-, водо-, теплопостачання, каналізації	Призупинення роботи на деякий час через аварію інженерних систем	2	3	6			х
Технічні засоби обробки інформації	Чутливість до змін напруги	Втрата електроживлення	2	3	6			х
	Відсутній ефективний контроль змін конфігурації	Помилка під час використання	3	4	12			х
Програмні засоби обробки інформації	Відсутній журнал подій	Зловживання правами	4	3	12	х	х	х
Допоміжні засоби (охорони, сигналізації)	Ушкодження системи охорони та/або сигналізації	Призупинення роботи на деякий час	2	3	6			х

Проаналізувавши таблицю 2.11, можна визначити, що після запровадження рекомендацій показник ризику зменшився до прийнятого рівня (менше 15), а саме:

– ризик зараження комп'ютерів вірусами через помилки при експлуатації програмного забезпечення знизився з 20 до 12;
– ризик помилки під час використання через неналежну обізнаність щодо питань безпеки знизився з 20 до 12;
– ризик незаконного оброблення даних через відсутність механізму моніторингу знизився з 20/16 до 8;
– ризик зловживання правами через відсутній журнал подій знизився з 16 до 12;
– ризик перехоплення конкурентами інформації через неконтрольоване копіювання знизився з 15 до 10.

2.6 Висновки до другого розділу

Ігнорування загроз і вразливостей інформаційно-телекомунікаційної системи може призвести до значних фінансових втрат та витоку інформації підприємства "Vodafone Україна Першотравенськ". В рамках другого розділу розроблено модель порушника і модель загроз для "Vodafone Україна Першотравенськ", а також обрано стандартний профіль захищеності, який використовується на підприємстві. Виявлено найбільш актуальні загрози та запропоновано організаційні та програмні рішення для їх мінімізації:

- сформульовано вимоги щодо інформаційної безпеки;
- впроваджено Trellix Complete EndPoint Protection - Business (США);
- впроваджено новий антивірусний продукт ESET Endpoint Security для Windows (EES) з системою централізованого керування ESET Remote Administrator від компанії ESET (Словаччина);

- проведено розмежування ролей адміністратора мережі та адміністратора безпеки “Vodafone Україна Першотравенськ”;
- розроблено елементи політики щодо розмежування доступу та ведення журналу реєстрації подій;
- запроваджено організаційні методи, спрямовані на підвищення обізнаності співробітників щодо інформаційної безпеки.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Метою економічного розділу є підтвердження економічної доцільності впровадження комплексної системи захисту інформації інформаційно-комунікаційної системи «Vodafone Україна Першотравенськ» [19, с. 21]. До розрахунків включаються оцінка капітальних витрат на придбання та налагодження компонентів системи інформаційної безпеки або витрат, пов'язаних з розробкою апаратури, пристроїв, програмного забезпечення; розрахунок щорічних експлуатаційних витрат на утримання і обслуговування проектованого об'єкта; визначення щорічного економічного ефекту від впровадження проектованого об'єкта; аналіз показників економічної ефективності запропонованого проектного рішення; формулювання висновків щодо доцільності такого проектного рішення.

3.1 Розрахунок капітальних (фіксованих) витрат

У цьому розділі виконаємо розрахунок капітальних затрат [20, с. 23].

В процесі аналізу собівартості впровадження удосконалень системи захисту ІКС «Vodafone Україна Першотравенськ» слід виконати розрахунок сукупної вартості володіння [21, с. 23].

Таблиця 3.1 - Сукупна вартість володіння містить наступні статті витрат їх вагові частки

№ п/п	Назва статті затрат	Відсоток
1	Фіксовані (капітальні) вкладення	19%
2	Поточні витрати, у тому числі	81%
3	Керування системою	14%
4	Технічна підтримка і відновлення	19%
5	Активність користувача	46%

3.1.1 Визначення трудомісткості розробки політики безпеки інформації

Трудомісткість розробки політики може бути розрахована на основі трудомісткості робіт, які виконуються [22, с. 24].

$$t = t_{тз} + t_в + t_а + t_{вз} + t_{озб} + t_{овр} + t_д, \text{ годин,} \quad (3.1)$$

де $t_{тз}$ – тривалість складання ТЗ на розробку політики;

$t_{тз}$ = 24 годин;

$t_в$ – тривалість розробки концепції безпеки інформації в організації;

$t_в$ = 13 годин;

$t_а$ – тривалість процесу аналізу ризиків;

$t_а$ = 9 годин;

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

$t_{вз}$ = 11 годин;

$t_{озб}$ – тривалість виробу основних рішень з забезепечення безпеки інформації;

$t_{озб}$ = 21 годин;

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

$t_{овр}$ = 12 годин;

$t_д$ – тривалість документального оформлення політики безпеки;

$t_д$ = 7 годин.

t=24+13+9+21+11+12+7 = 97 годин.

3.1.2 Розрахунок витрат на створення політики безпеки інформації.

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

Де $К_{рп}$ – витрати на розробку політики безпеки інформації [23, с. 25];

$З_{зп}$ – витрати на заробітну плату спеціалісту з інформаційної безпеки;

$З_{мч}$ – вартость витрат машинного часу, що необхідний для розробки політики.

$К_{рп}$ = 17196 +288= 17484 грн.

Заробітна плата виконавця враховує основну і додаткову ЗП, відрахування на соціальні потреби.

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

де t – загальна тривалість розробки політики безпеки, годин;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину [24, с. 26].

$З_{зп} = 97*177 = 17169$ грн.

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

де t – трудомісткість розробки політики на ПК, годин;

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

$З_{мч} = 97*2,97 = 288,09$ грн.

$$С_{мч} = P \times t_{нал} \times С_е + \frac{Ф_{зал} \times Н_а}{F_p} + \frac{K_{лпз} \times Н_{апз}}{F_p}, \text{грн} \quad (3.5)$$

Де Р – встановлена потужність ПК, кВт;

$t_{нал}$ – кількість задіяних робочих станцій пр написані політики;

$С_е$ – тариф на електроенергію, грн./кВт*година;

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

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

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

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

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

$С_{мч} = 0,7*2*4,32 + ((6634*0,3)/1920) + ((10000*0,1)/1920) = 7,6$ грн.

На підприємстві «Vodafone Україна Першотравенськ» планується додатково використовувати програмні засоби наведені в таблиці 3.2 [25, с. 28].

Таблиця 3.2 – Додаткові програмні засоби

Програмний засіб	Вартість, грн
Avast Business Premium Business Security	2500
Ідентифікатор Microsoft Entra	1960
Закупівля та ліцензування програмного забезпечення	10000
Всього	14460

Відповідно до прийнятих проектних рішень, на впровадження апаратних рішень витрати не виникають [26, с. 28].

Капітальні (фіксовані) витрати на створення політики безпеки інформації:

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_{н}, \quad (3.6)$$

де $К_{пр}$ – вартість розробки проєкту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн [27, с. 21];

$К_{пр} = 0$.

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

$К_{зпз} = 14460$ грн.

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

$К_{рп} = 17484$ грн.

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

$К_{аз} = 0$.

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;

$К_{навч} = 2000$ грн.

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

$К_{н} = 0$.

$К = 0 + 14460 + 17484 + 0 + 2000 + 0 = 33944$ грн.

3.2 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – поточні витрати на обслуговування об'єкта проектування за визначений період [28, с. 21].

Річні поточні витрати на функціонування системи інформаційної безпеки:

$$С = С_в + С_к + С_{ак}, \text{ грн}, \quad (3.7)$$

де $С_в$ – вартість відновлення й модернізації системи;

$С_в$ = 785 грн.

$С_к$ – витрати на керування системою в цілому;

$С_{ак}$ – витрати, викликані активністю користувачів системи інформаційної безпеки.

$С_{ак}$ = 0.

Витрати на керування системою інформаційної безпеки ($С_к$) складають [29, с. 18]:

$$С_к = С_н + С_а + С_з + С_{єв} + С_{ел} + С_о + С_{тос}, \text{ грн}, \quad (3.8)$$

де $С_н$ – це витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації;

$С_н$ = 2000 грн.

$С_а$ – це річний фонд амортизаційних відрахувань визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів ($П_з$);

Вартість ПК, яка складає 31535 грн., ділимо на термін корисного використання, який складає 10 років, і отримаємо 3154 грн.

$С_а$ = 3154 грн [30, с. 20].

$С_З$ – це річний фонд заробітної плати інженерно–технічного персоналу, що обслуговує систему інформаційної безпеки;

$$С_з = З_{осн} + З_{дод}, \text{ грн.}, \quad (3.9)$$

Де основна заробітна плата ($З_{осн}$) визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата ($З_{дод}$) – в розмірі 8-10% від основної заробітної плати [31, с. 20].

Основна заробітна плата спеціаліста з інформаційної безпеки – 17484 грн./місяць.

Виконання робіт вимагає залучення спеціаліста з інформаційної безпеки на 0,25 ставки [32, с. 26].

$С_з$ = (17484*12 + 17484*12*0,1)*0,25= 57697 грн.

З 01.12.2021 р. ставка ЄСВ (єдиний соціальний внесок) складає 22%.

$С_{єв}$ = 33944 * 0,22 = 7468 грн.

$С_{ел}$ – вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року [33, с. 29];

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.}, \quad (3.10)$$

де Р – встановлена потужність апаратури інформаційної безпеки;

Р = 0,7 кВт.

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

$F_р$ = 1920 год.

$Ц_е$ – тариф на електроенергію;

$Ц_е$ = 4,32 грн./кВт за годину.

$С_{ел}$ = 0,7*1920*4,32 = 5806 грн.

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1% [34, с. 25].

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

$С_о$ = 0.

$С_{тос}$ = 33944 *0,01 = 339 грн.

$С_к$ = 2000 + 3154 + 57697 + 7468 + 5806 + 339 = 76464 грн.

Річні поточні витрати на функціонування системи інформаційної безпеки складають 76464 грн [35, с. 12].

3.3 Оцінка можливого збитку від атаки (взлому) на вузол або сегмент корпоративної мережі

3.3.1 Оцінка величини збитку

Вихідні дані для розрахунку:

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

$t_п$ = 3 години;

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

$t_в$ = 5 години;

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

$t_{ви}$ = 1.5 години [36, с. 22];

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.);

$З_о$ = 15200 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі;

$З_с$ = 14000 грн./міс.;

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

$Ч_о$ = 1 особа;

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

$Ч_с$ = 2 осіб;

О – обсяг збитку атакованого вузла або сегмента корпоративної мережі;

О = 500 000;

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

I – число атакованих сегментів корпоративної мережі;

I = 1;

N – середнє число атак на рік,

N = 5.

Упущена вигода від простою атакованого сегмента корпоративної мережі [37, с. 24]:

$$U = П_п + П_в + V, \quad (3.11)$$

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

$$П_п = \frac{\sum З_c}{F} t_п, \quad (3.12)$$

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

$П_п$ = ((14000 * 23)/176)*3 = 5489 грн,

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн [38, с. 22];

$$П_в = П_{ви} + П_{пв} + П_{зч}, \quad (3.13)$$

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.

$$П_{ви} = \frac{\sum З_с}{F} t_{ви}, \quad (3.14)$$

$П_{ви}$ = ((14000 *23)/176) *1,5 = 2744 грн.

$$П_{пв} = \frac{\sum З_о}{F} t_в, \quad (3.15)$$

$П_{пв}$ = ((15200 *1)/176) *5 = 432 грн.

$П_в$ = 2744 + 432 = 3176 грн.

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн [39, с. 21].

$$V = \frac{O}{F_г}(t_п + t_в + t_{ви}), \quad (3.16)$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год [40,

с. 24].

V = (500000/2080) * (3+5+1,5) = 22836 грн.

U = 5489 + 3003 + 22836 = 31328 грн.

Загальний збиток від атаки на сегмент корпоративної мережі організації:

$$B = \sum_i \sum_n U, \quad (3.17)$$

B = 1 * 5 * 31328 = 156640 грн.

3.3.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки [41, с. 14]:

$$E = B \times R - C, \quad (3.18)$$

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

B = 156640 грн.;

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

R = 60 %;

C – щорічні витрати на експлуатацію системи інформаційної безпеки;

C = 785 + 76464 + 0 = 77249 грн.

E = 156640 * 0,6 – 77249 = 16735 грн.

3.4 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки [42, с. 12]:

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \quad (3.19)$$

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

E = 16735 грн.

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

К = 33944 грн.

ROSI = 16735 / 33944 = 0,5

Проект визначається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції [43, с. 12]:

$$ROSI > (N_{деп} – N_{інф})/100), \quad (3.20)$$

де $N_{деп}$ – річна депозитна ставка;

$N_{деп}$ = 8 %.

$N_{інф}$ – річний рівень інфляції;

$N_{інф}$ = 5 %.

Розрахункове значення коефіцієнта повернення інвестицій:

0,5 > (8 – 5)/100

0,5 > 0,03

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки [44, с. 15]:

T = 1/0,5 = 2 роки.

3.5 Висновки до економічного розділу

В цьому розділі проведено розрахунки капітальних (фіксованих) витрат на створення політики безпеки інформації, які складають 33944 грн.; розрахунки поточних (експлуатаційних) витрат на функціонування системи інформаційної безпеки, які складають 77249 грн.. Провели оцінювання можливого збитку від атаки (взлому) на вузол або сегмент корпоративної мережі, де визначили, що загальний збиток від атаки на сегмент корпоративної мережі організації складає 156640 грн. Розрахували загальний ефект від впровадження системи інформаційної безпеки, який складає 16735 грн.

В результаті виконання розрахунків отримали період окупності вдосконалень системи захисту «Vodafone Україна Першотравенськ» становить

2 роки.

Згідно з коефіцієнтом повернення інвестицій ROSI, який показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки, який складає 0,5 на 1 грн., а також з терміном окупності капітальних інвестицій, який складає 2 роки, можемо зробити висновок, що проектне рішення, яке прийняте на підприємстві «Vodafone Україна Першотравенськ» економічно доцільне.

ВИСНОВКИ

В роботі було виконано дослідження напрямків підвищення безпеки даних, які циркулюють в інормаційно-комунікаційної системи підприємства «Vodafone Україна Першотравенськ».

Мета роботи полягала в розробці рекомендацій щодо підвищення рівня захисту інформації в інформаційно-комунікаційній системі підприємства «Vodafone Україна Першотравенськ».

Під час проведення дослідження застосовувалися такі методи, як спостереження, порівняння, аналіз, опис, вивчення фахової літератури.

В першому розділі кваліфікаційної роботи надано загальний опис підприємства «Vodafone Україна Першотравенськ», наведена його структура, проведено аналіз нормативно-правової бази.

В другій частині кваліфікаційної роботи розроблено модель загроз та порушника, проаналізовані актуальні загрози та вразливості, обрано профіль захищеності та рішення для захисту інформації у «Vodafone Україна Першотравенськ». Проведено аналіз ефективності рішень, які спрямовані на підвищення ступеню захиста даних.

В економічному розділі кваліфікаційної роботи розраховано капітальні та поточні витрати, проведено оцінку можливого збитку від атаки та виконано аналіз економічної доцільності запропонованих рішень.

Практичне значення роботи полягає у підвищенні рівня захисту інформації в інформаційно-комунікаційній системі «Vodafone Україна Першотравенськ», за рахунок розробки рекомендацій щодо впровадження проектних рішень.

ПЕРЕЛІК ПОСИЛАНЬ

1. Розумний маркетинг [Електронний ресурс] Режим доступу до ресурсу: https://martech.org/smart-marketing-still-hinges-on-humanity-not-technology/.
2. Як технології змінюють маркетинг [Електронний ресурс] Режим доступу до ресурсу: https://www.theguardian.com/media-network/media-network-blog/2014/sep/29/technology-changing-marketing-digital-media.
3. Створення комплексних систем захисту інформації [Електронний ресурс] Режим доступу до ресурсу: https://tzi.com.ua/stvorennya-kompleksnix-sistem-zaxistu-nformacz.html.
4. Закон України «Про інформацію» від 02.10.1992 No2657-XII // Відомості Верховної Ради України-1992-No 48. [Електронний ресурс] Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12.
5. Закон України «Про захист персональних даних» від 01.06.2010 No 2297-VI // Відомості Верховної Ради України-2010-No 5. [Електронний ресурс] Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17.
6. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 No80-VI // Відомості Верховної Ради України-1994-No 80. [Електронний ресурс] Режим доступу до ресурсу: http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 .
7. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі. [Чинний від 08.11.2005] - К.: ДССЗЗІ, 2005-No125(Нормативний документ системи технічного захисту інформації).
8. НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в

комп'ютерних системах від несанкціонованого доступу.[Чинний від 28.04.1999] - К.: ДСТСЗІ СБУ, 1999- No22 (Нормативний документ системи технічного захисту інформації).

9. НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. [Чинний від 28.04.2000] - К.: ДСТСЗІ СБУ, 2000- No22 (Нормативний документ системи технічного захисту інформації).
10. НД ТЗІ 1.6-005 - Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. [Чинний від 15.04.2013] - К.: ДССЗЗІ, 2013-No125 (Нормативний документ системи технічного захисту інформації).
11. Етапи побудови КСЗІ [Електронний ресурс] Режим доступу до ресурсу: http://altersign.com.ua/korysna-informacija/pobudova-kszi/etapy-pobudovy-kszi.
12. Вадим Гребенніков «Комплексні системи захисту інформації. Проектування, впровадження, супровід» [Електронний ресурс] Режим доступу до ресурсу: https://ru.bookmate.com/books/dqaXNzVz?dscvr=top_result.
13. Aarsand, P. and Aronsson, K. (2009) 'Gaming and Territorial Negotiations in Family Life', Childhood, 16(4):497–517.
14. Abelman, R. (2007) 'Fighting the War on Independency: Mediating TV, Internet, and Videogame Usage among Achieving and Underachieving Gifted Children', Roeper Review, 29, 100-12.
15. Anderson, B. (2001) e-Living: State of the Art Review, report for the e-Living project.
16. Anderson, M. & Perri, A. (2017) Tech Adoption Climbs Among Older Adults, https://www.pewinternet.org/2017/05/17/technology-use-among-seniors/

17. Apple, L., Dadina, P., Dwyer, M., Hampton, K., Kitzie, V., Matni, Z., Moore, P. and Teodoro, R. (2014) 'Testing the validity of social capital measures in the study of information and communication technologies', Information, Communication and Society, 17(4), 398-416.
18. Aroldi, P. and Colombo, F. (2016) 'The elderly, IT and the public discourse. Representations of exclusion and inclusion', in Zhou, J. and Salvendy, G. (eds) ITAP 2016, Part II, LNCS 9755, pp.176-185.
19. Aroldi, P., Colombo, F. and Carlo, S. (2014, "Stay tuned": The role of ICTs in elderly life, in Riva, G., Ajmone, P. and Grassi, C. (Eds.) Active Ageing and Healthy Living, IOS Press, Amsterdam, pp.145-156.
20. Aroldi, P., Colombo, F. and Carlo, S. (2015) 'New Elders, old Divides: ICTs, Inequalities and Well Being amongst Young Elderly Italians', Comunicar, 45.
21. Bar, L., Elias, N. and Levy, S. (2018) 'Development of infants' media habits in the age of digital parnting, in Mascheroni, G., Ponte, C. and Jorge, A. (eds) Digital Parenting: The Challenges for Families in the Digital Age, Nordicom, Göteborg, 103-112.
22. Berg, A-J (1994) The Domestication of Telematics in Everyday Life. Paper presented at Cost248 meeting, Lund, 13th-14th April
23. Berg, A-J. (1997) 'Karoline and the Cyborgs: The Naturalisation of a Technical Object', in Frissen, V. (Ed.) Gender, ITCs and Everyday Life: Mutual Shaping Processes, COSTA4, Brussels, pp.7-35.
24. Bergman, S. (1994) 'Communication Technology in the Household: The Gendering of Artefacts and Practices', in Frissen, V. (Ed.) Gender, ITCs and Everyday Life: Mutual Shaping Processes, COSTA4, Brussels, pp.135-153.
25. Berker, T., Hartmann, M., Punie, Y. and Ward, K. (eds) (2006) Domestication of Media and Technologies, Open University Press, Maidenhead.
26. Bittman, M., et al. (2011). 'Digital Natives? New and Old Media and

Children's Outcomes', Australian Journal of Education 55(2), 161-175

27. Blaschke, C., Freddolino, P. and Mullen, E. (2009) 'Ageing and Technology: A Review of the literature', British Journal of Social Work, 39, 641-656.
28. Bonfadelli, H., Bucher, P. and Piga, A. (2007) 'Use of old and new media by ethnic minority youth in Europe with a special emphasis on Switzerland', Communications 32(2), 141–170.
29. Bovill, M. and Livingstone, S. (2001) 'Bedroom Culture and the Privatization of Media Use', in Livingstone, S. and Bovill, M. (eds) Children and their Changing Media Environment. A European Comparative Study, Mahwah, New Jersey: Lawrence Erlbaum Associates, 179-200.
30. Buckingham, D. (2000) After the Death of Childhood. Growing up in the Age if Electronic Media, Polity Press, Cambridge.
31. Buckingham, D. (2008) Youth, Identity, and Digital Media. The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning. Cambridge, MA: The MIT Press.
32. Buckingham, D. and Willet, R. (eds) (2006) Digital Generations: Children, Young People, and the New Media. New York: Routledge
33. Bury, R. and Li, J. (2015) 'Is it live or is it timeshifted, streamed or downloaded? Watching television in the era of multiple screens', New Media & Society, 17(4), 592–610.
34. Buse, C. (2009) 'When You Retire, does Everything become Leisure? Information and Communication Technology Use and the Work/Leisure Boundary in Retirement', New Media and Society, 11, No (7), 1143-61.
35. Caradec, V. (1999) 'Vieillissment et Usage des Technologies. Une Perspective Idenitaire et Relationnelle', Réseaux, 17, 96.
36. Carlo, S. and Vergani, M. (2016) Risk and Benefit Perceptions: Resistance, Adoption and Use of ICT among the Italian Elderly, in Zhu, J and Salvendy, G. (eds) ITAP 2016, Part 1, Springer, pp.155-166.

37. Caron, A. (2000) New Communication Technologies in the Home: A Qualitative Study of the Introduction, Appropriation and Uses of Media in the Family, Young People and the Media, Sydney: International Forum of Researchers.

38. Caron, A. (2008) 'New Screens and Young People: Crossing Times and Boundaries. What Roles do they Play in their Everyday Life', Observatorio, 2(3), 53-68, available at http://obs.obercom.pt/index.php/obs/issue/view/12

39. Carvalho, J., & Francisco, R., & Relvas, A. (2014) 'Family functioning and information and communication technologies: How do they relate? A literature review', Computers in Human Behavior, 45, 99-108.

40. Charness, N. & Boot, W. (2009) 'Aging and information technology use: potential and barriers', Current Directions in Psychological Science, 18(5), 253–258.

41. Chen, Y. R. R., & Schulz, P. J. (2016) 'The effect of information communication technology interventions on reducing social isolation in the elderly: A systematic review', Journal of Medical Internet Research, 18(1), e18.

42. Chiaro, M and Fortunati, L. (1999) 'Nouvelles Technologies et Compétence des Usagers', Réseaux, 17(96).

43. Choi YK, Kim J and McMillan SJ (2009) 'Motivators for the intention to use mobile TV: A comparison of South Korean males and females', International Journal of Advertising 28(1): 147–167.

44. Church, K., Weight, J., Berry, M. and MacDonald, H. (2010) 'At Home with Media Technology', Home Cultures, 7(3), 263-286.

45. Colombo, F. and Vittadini, N. (eds) (2006) Digitising TV. Theoretical Issues and Comparative Studies across Europe, Vita Pensiero, Milano.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	6	
5	А4	1 Розділ	10	
6	А4	2 Розділ	26	
7	А4	3 Розділ	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	5	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

Пояснювальна записка Димарьова.docx

Презентація Димарьова.pptx

ДОДАТОК В. Відгуки керівників розділів

Комплексна система захисту інформації інформаційно - комунікаційної системи підприємства «Vodafone Україна Першотравенськ»

студента групи 125-20-3

Димарьової Марії Костянтинівни

Відгук керівника економічного розділу:

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку __90__ б. («___відмінно_____»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
Комплексна система захисту інформації інформаційно - комунікаційної системи підприємства «Vodafone Україна Першотравенськ»
студента групи 125-20-3
Димарьової Марії Костянтинівни

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 75 сторінках та містить 18 таблиць, 2 рисунки, 45 джерел та 4 додатків.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою, відповідає вимогам положення про систему запобігання та виявлення плагіату у Національному технічному університеті «Дніпровська політехніка». Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник спец. розділу
ас. кафедри БІТ Юлія МІЛІНЧУК