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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Колодія Єгора Сергійовича*

академічної групи *125-16-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства «Лата»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.ф-м.н., Гусєв О.Ю.			
розділів:				
спеціальний	ас. Ковальова Ю.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Лізунова Т.Л.			

Дніпро
2020

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Колодію Єгору Сергійовичу* **академічної групи** *125-16-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Політика безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства «Лата»***

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

Розділ	Зміст	Термін виконання
Розділ 1	Зазначена актуальність забезпечення безпеки інформації, розглянуті нормативно-правові документи, обґрунтовано необхідність створення КСЗІ, проведено обстеження на ОІД, розроблено модель порушника та модель загроз.	29.03.2020
Розділ 2	Розроблено політики безпеки приватного підприємства «Лата».	24.05.2020
Розділ 3	Розгянуто питання чи є діяльність приватного підприємства «Лата» економічно доцільною.	14.06.2020

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

Дата видачі: 08.01.2020р.

Дата подання до екзаменаційної комісії: 15.06.2020р.

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

РЕФЕРАТ

Пояснювальна записка: _103_ с., _10_ рис., _19_ табл., _4_ додатка, _10_ джерел.

Об’єкт розробки: інформаційно-телекомунікаційна система (ІТС) ПП «Лата».

Предмет дослідження: політика безпеки інформації об’єкта інформаційної діяльності (ОІД) ПП «Лата»

Мета роботи (проекту): підвищення рівня захисту інформації в ІТС ПП «Лата»

Методи розробки: спостереження, порівняння, аналіз, опис.

У першому розділі визначається сучасний стан інформаційної безпеки в цілому, проведено аналіз кібератак в останні роки, визначена актуальність проблеми захисту інформації в інформаційно-телекомунікаційних системах(ІТС) комерційних підприємств. Проведено аналіз нормативно-правової бази у сфері захисту інформації, виписані терміни, які стосуються безпеки інформації та встановлені задачі на розробку комплексної системи захисту інформації (КСЗІ), на об’єкті інформаційної діяльності (ОІД), де циркулює інформація. Проведено обстеження об’єкту інформаційної діяльності (ОІД): проаналізовані відомості про підприємство, описано середовище функціонування об’єкту інформаційної діяльності, приведена класифікація інформації, що обробляється у інформаційно-телекомунікаційній системі (ІТС). Також було побудовано модель порушника, модель загроз та обрано функціональний профіль захищеності для системи.

У другому розділі (спеціальній частині) було розроблено політики безпеки для приватного підприємства «Лата».

В третьому розділі визначено економічну діяльність підприємства.

ПОЛІТИКА БЕЗПЕКИ, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА

РЕФЕРАТ

Пояснительная записка: _103_ с., _10_ рис., _19_ табл., _4_ приложения, _10_ источников.

Объект разработки: информационно-телекоммуникационная система (ИТС) ООО «Лата».

Предмет исследования: политика безопасности информации объекта информационной деятельности (ОИД) ЧП «Лата»

Цель работы (проекта): повышение уровня защиты информации в ИТС ЧП «Лата»

Методы разработки: наблюдение, сравнение, анализ, описание.

В первом разделе определяется современное состояние информационной безопасности в целом, проведен анализ кибератак в последние годы, определена актуальность проблемы защиты информации в информационно-телекоммуникационных системах (ИТС) коммерческих предприятий. Проведен анализ нормативно-правовой базы в сфере защиты информации, выписаны термины, относящиеся к безопасности информации и установленные задачи на разработку комплексной системы защиты информации (КСЗИ), на объекте информационной деятельности (ОИД), где циркулирует информация. Проведено обследование объекта информационной деятельности (ОИД): проанализированы сведения о предприятии, описано среду функционирования объекта информационной деятельности, приведена классификация информации, обрабатываемой в информационно-телекоммуникационной системе (ИТС). Также была построена модель нарушителя, модель угроз и избран функциональный профиль защищенности для системы.

Во втором разделе (специальной части) был разработан политики безопасности для частного предприятия «Лата».

В третьем разделе определена экономическая деятельность предприятия.

ПОЛИТИКА БЕЗОПАСНОСТИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ІНФОРМАЦИОННО-ТЕЛЕКОМУНІКАЦИОНАЯ СИСТЕМА, ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ

ABSTRACT

Explanatory note: _103_ pp., _10_ fig., _19_ tab., _4_ applications, _10_ sources.

Object of development: information and telecommunication system (ITS) software "Lata".

Subject of research: information security policy of the information activity object (OID) of the Lata PP

Purpose of the work (project): increasing the level of information security in the ITS of Lata LLC

Development methods: observation, comparison, analysis, description.

The first section defines the current state of information security as a whole, analyzes cyber attacks in recent years, identifies the relevance of the problem of information security in information and telecommunication systems (ITS) of commercial enterprises. The analysis of the regulatory framework in the field of information protection is carried out, the terms relating to information security and the established tasks for the development of an integrated information protection system are written out at the information activity object where information is circulated. A survey of the object of information activity has been carried out: information about the enterprise has been analyzed, the operating environment of the object of information activity has been described, a classification of information processed in the information and telecommunication system has been given. An intruder model, a threat model, and a functional security profile for the system were also selected.

In the second section (special part), a security policy was developed for the Lata private enterprise.

The third section defines the economic activity of the enterprise.

SECURITY POLICY, INFORMATION SECURITY, INFORMATION-TELECOMMUNICATION SYSTEM, OBJECT OF INFORMATION ACTIVITY, THREAT MODEL, INTRUDER MODEL

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС - автоматизована система

ЕОТ - електронно-обчислювальна техніка;

ЗУ - закон України;

ІБ - інформаційна безпека;

ІТС - інформаційно-телекомунікаційна система;

КСЗІ - комплексна система захисту інформації;

НСД - несанкціонований доступ;

ОІД - об'єкт інформаційної діяльності;

ОС - операційна система;

ПП – приватне підприємство;

ПЗ - програмне забезпечення;

ТЗІ - технічні засоби інформації;

ЗМІСТ

ВСТУП

Сучасний розвиток інформаційних технологій набув нові цілі та вимоги до зберігання інформації. Усе частіше підприємства та приватні особи переходять зі звичайних носіїв інформації до дистанційних, тож за умови зберігання даних в мережі необхідно будувати ефективну систему захисту цих даних.

У наш час рівень безпеки захищеності інформації відіграє значну роль у ведені бізнесу. Так, кібербезпека є одним з ключових елементів для функціонування компаній, які займаються розробкою незалежних технологій корпоративного рівня та дозволяють клієнтам виконувати інвестиційні рішення з підвищеною швидкістю і контролем. Такі компанії існують завдяки клієнтам, які користуються платформами для виконанням операцій з акціями, опціонами, ф'ючерсами, форекс, фіксованим доходом, процентними свопами з функціональністю, що залежить від активів. Перш за все, клієнтів цікавить безперебійність роботи придбаних програм та безпека коштів, які залучаються для торгівлі, а також безпека особистих даних.

В останні роки світ зіштовхнувся з масовими кібератаками, від яких постраждали чи не всі галузі економіки, а особливо фінансовий сектор (банки, інвестиційні фонди тощо.) та урядові структури. Так, у 2017-му вірус-здирник «WannaCry» вразив пів-мільйона комп'ютерів по всьому світу, а серед найбільш постраждалих країн присутня Україна.

Кількість інцидентів, пов'язаних з замахом на інформаційну безпеку комп'ютерних систем, зростає с кожним роком. За даними компанії Positive Technologies, яка займається аналізом захищеності і відповідності стандартам, в 2019 році було зафіксовано більш ніж 1500 кібератак (що на 19% більше ніж у

попередньому 2018 році) (див. Рисунок 1). Тож не дивно, що зараз кваліфіковані спеціалісти з кібербезпеки користуються попитом на ринку праці.

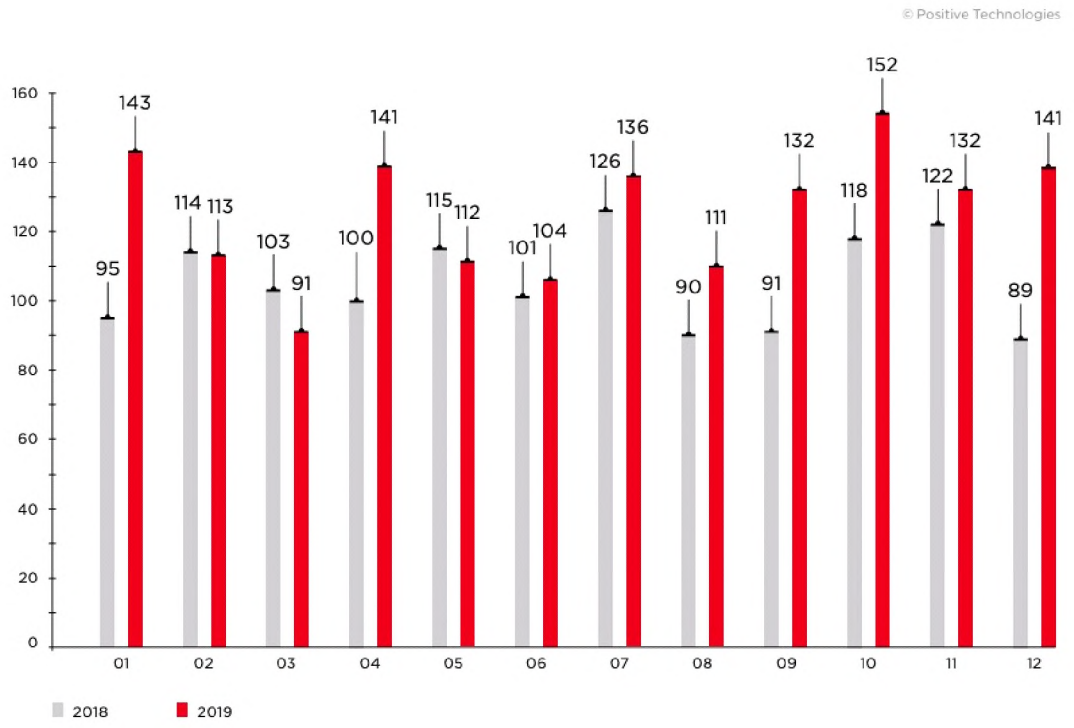


Рисунок 1. Кількість кібератак в 2018 і 2019 роках (по місяцях)

9 травня 2018 року набув чинності закон № 2163-VIII «Про основні засади забезпечення кібербезпеки України». Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Події останніх років стимулювали розвиток кібербезпеки в Україні та вдосконалення КСЗІ у цілому на всіх об’єктах інформаційної діяльності, у тому числі і на підприємствах, які займаються розробкою програм для інвестиційної торгівлі. Одним з найважливіших етапів побудови КСЗІ є розробка політики

безпеки. Правильно розроблена політика безпеки – це запорука успішного захисту у разі спроби атаки на інформаційну систему.

Нижче будуть наведені матеріали, які будуть спрямовані на виявлення та усунення недоліків інформаційної системи розглянутого підприємства.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

На сьогодні суспільство залежить від стабільності роботи інформаційних систем. Найважливішою умовою для підтримки економічної стабільності держави та її функціонування є безпечна й надійна робота мереж передачі даних, комп'ютерних систем та мобільних пристроїв. Кібератаки, людська халатність та помилки, фізичні порушення, вихід з ладу програмного та апаратного забезпечення тощо. - усе це має неабиякий вплив на безпеку роботи основних інформаційних систем загального користування.

Чимало коштів витрачається на забезпечення інформаційної безпеки. Це пов’язано з тим, що рівень кіберзлочинців щороку зростає, а кількість кібератак збільшується.

Так за даними Positive Technologies: 81% жертв кіберзлочинців становлять юридичні особи. Серед них держустанови, промисловість, медицина, сфера науки і освіти, фінансова галузь становлять 54% від усіх кібератак на юридичні особи. (див. Рисунок 2)

Об'єктами атак на юридичні особи виступають комп'ютери , сервери. мережеве обладання (71%). А об'єктами атак на фізичні особи найчастіше виступають комп'ютери , сервери. мережеве обладання (32%), самі ж люди (31%) та мобільні пристрої (26%). (див. Рисунок 3)

Рисунок 2. Категорії юридичних осіб, які зазнали кібератак

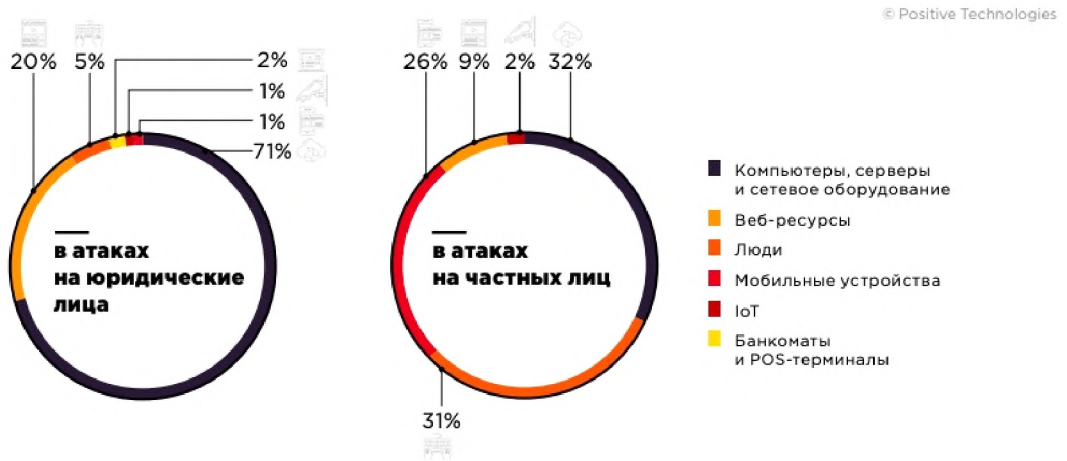


Рисунок 3. Об'єкти атак

Щодо того, яка саме інформація цікавила кіберзлочинців найбільше при здійсненні ними атак на юридичні особи у 2019 році, можна стверджувати, що персональні данні є найпопулярнішим видом викраденої інформації (27%). Також для юридичних осіб 22% викраденої інформаціїї становлять облікові данні, а для

фізичних аж 40%. (див. Рисунок 4)

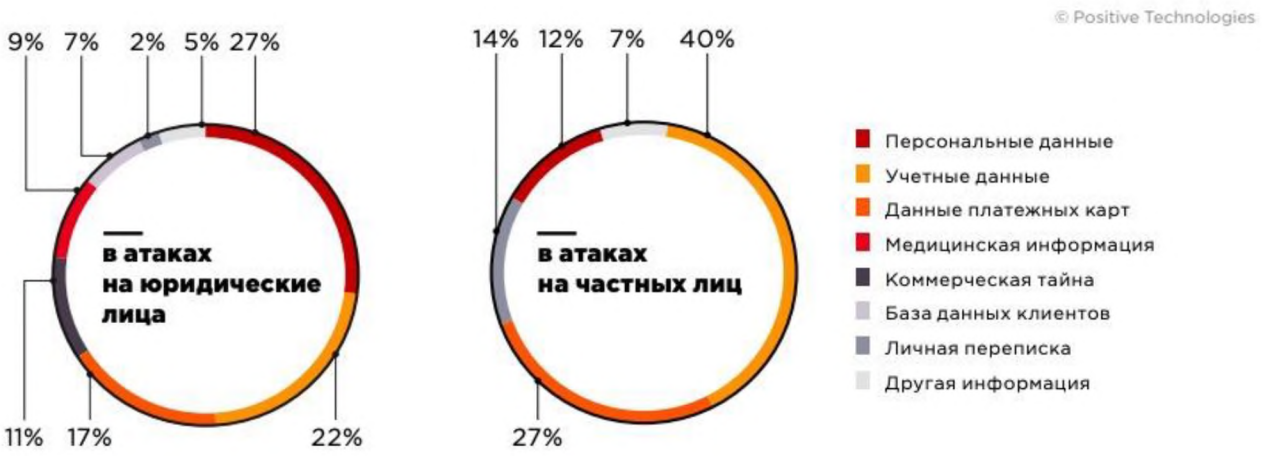


Рисунок 4. Типи вкрадених данних

Станом на початок 2020 року кількість хакерських атак продовжує збільшуватись. Облікові, персональні та дані платіжних карток – найбільше цікавлять кіберзлочинців.

Порівняно з попередніми роками, стан забезпечення безпеки інформації продовжує погіршуватись. Так, в останній чверті 2019 року кількість унікальних інцидентів піднялася на 12% порівняно з попереднім кварталом. При цьому частка цілеспрямованих атак зросла на 2 %, досягнувши 67 % (згідно даних компанії Positive Technologies).

Інформаційні технології відіграють дедалі більшу роль у діяльності підприємств. Зі збільшенням інформатизації у функціонуванні підприємства, збільшується кількість загроз та можливих ризиків.

Загрозу для компанії становлять не лише зловмисники, мотивом яких виступає отримання матеріальної вигоди, а також і конкуренти, які прагнуть заволодіти конфіденційною інформацією або саботувати процес діяльності

підприємства. Сюди ж можна віднести навмисні та ненавмисні дії персоналу, які є загрозою для оброблювальної інформації на підприємстві.

Щоб мінімізувати ризики виникнення загроз на підприємстві слід розробити політику безпеки ОІД, яка є важливою частиною створення КСЗІ.

Метою дипломної роботи є знаходження вразливостей в інформаційній системі ОІД та їх мінімізація шляхом розробки якісної політики безпеки.

1.2 Аналіз нормативно-правової бази у сфері захисту інформації

Згідно ЗУ «Про інформацію» будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Збереження, цілісність та порядок доступу до інформації забезпечує захист інформації, що являє собою сукупність правових, адміністративних, організаційних, технічних та інших заходів.

Згідно цього ж закону, за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

До інформації з обмеженим доступом належить конфіденційна, службова та таємна інформація. Конфіденційна інформація – це інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Згідно ЗУ «Про захист інформації в інформаційнотелекомунікаційних системах» умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не передбачено

законодавством. Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації. Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Беручи до уваги додаток до постанови № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення. Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження. Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

Під час обробки конфіденційної і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

Доступ до конфіденційної інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися. У системі забезпечується можливість надання користувачеві права на виконання однієї або кількох операцій з обробки конфіденційної інформації або позбавлення його такого права.

1.2.1 Терміни

Інформація з обмеженим доступом – інформація, що становить державну або іншу передбачену законом таємницю, а також службова інформація, а також конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України “Про доступ до публічної інформації”, та інша конфіденційна інформація, вимога щодо захисту якої встановлена законом.

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

Цілісність інформації – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем або процесом. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації та видалення.

Доступність інформації – властивість інформаційного ресурсу, яка полягає в тому, що користувач та/або процес, який володіє відповідними повноваженнями, може використовувати цей ресурс відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного) інтервалу часу.

Комплекс ТЗІ – сукупність організаційних, інженерних і технічних заходів та засобів, призначених для захисту від витоку інформації з обмеженим доступом технічними каналами на об’єктах інформаційної діяльності.

Об’єкт інформаційної діяльності – будівлі, приміщення, транспортні засоби чи інші інженерно-технічні споруди, функціональне призначення яких передбачає обіг інформації з обмеженим доступом.

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

Комплексна система захисту інформації; КСЗІ - сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Комплекс засобів захисту; КЗЗ - сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

АС Клас «3» - розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Істотна відміна від попереднього класу — необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. Якщо існують вимоги щодо обмеження можливості модифікації інформації, то відповідні послуги треба шукати в розділі ―Критерії цілісності‖. В цьому розділі описані такі послуги: довірча цілісність, адміністративна цілісність, відкат і цілісність при обміні.

Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то відповідні послуги треба шукати в розділі ―Критерії доступності‖. В цьому розділі описані такі послуги: використання ресурсів, стійкість до відмов, горяча заміна, відновлення після збоїв.

Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні послуги треба шукати у розділі ―Критерії спостереженості‖. В цьому розділі описані такі послуги: реєстрація, ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, автентифікація при обміні, автентифікація відправника (невідмова від авторства), автентифікація одержувача Реєстрація — це процес розпізнавання, фіксування і аналізу дій і подій, що пов'язані з дотриманням політики безпеки інформації. Використання засобів перегляду і аналізу журналів, а особливо засобів налагодження механізмів фіксування подій, має бути прерогативою спеціально авторизованих користувачів.

1.2.2 Підстави для створення КСЗІ

Згідно НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» встановлений цим НД ТЗІ порядок є обов’язковим для всіх суб’єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІТС яких обробляється інформація, яка є власністю держави, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством. Якщо в ІТС обробляються інші види інформації, то вимоги цього нормативного документа суб’єкти системи ТЗІ можуть використовувати як рекомендації.

Роботи зі створення КСЗІ виконуються організацією-власником (розпорядником) ІТС з дотриманням вимог нормативно-правових актів щодо провадження господарської діяльності у сфері захисту інформації.

1.2.3 Процеси створення КСЗІ

Створення комплексу ТЗІ передбачає проведення організаційних, інженерних і технічних заходів на ОІД, а саме:

- озвучення ІзОД (при проведенні нарад, під час показів зі звуковим супроводженням кіно- і відеофільмів тощо);

- здійснення обробки ІзОД технічними засобами (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання ІзОД тощо);

- обіг іншої ІзОД при проектуванні, будівництві, експлуатації об'єктів, виробництві технічних засобів тощо.

У створенні комплексу ТЗІ беруть участь:

– установа, яка є замовником створення комплексу ТЗІ (далі – замовник або установа-замовник);

– виконавець робіт зі створення комплексу ТЗІ (далі – виконавець робіт з ТЗІ);

– виконавець проведення випробувань щодо створення комплексу ТЗІ (далі – виконавець випробувань);

– виконавець проведення атестації комплексу ТЗІ (далі – виконавець атестації).

Установа-замовник може бути виконавцем робіт з ТЗІ і виконавцем випробувань або може залучати до виконання таких робіт і випробувань суб'єктів господарської діяльності, що мають ліцензії на провадження діяльності у сфері ТЗІ.

Атестацію комплексу ТЗІ здійснює виконавець, що має відповідну ліцензію або дозвіл на провадження діяльності у сфері ТЗІ.

У створенні комплексу ТЗІ (залежно від характеру, складності та обсягу робіт) можуть брати участь один або декілька виконавців. У цьому разі замовник визначає головного виконавця.

Установа-замовник для створення комплексу ТЗІ також залучає:

– свої структурні підрозділи, діяльність яких пов'язана з ІзОД та які обґрунтовують необхідність і заявляють про створення комплексу ТЗІ (підрозділи-заявники створення комплексу ТЗІ);

– призначену за необхідністю посадову особу з відповідною фаховою підготовкою для організації та координації робіт на всіх етапах створення комплексу ТЗІ, а також для організації експлуатації цього комплексу;

– підрозділ або посадові особи з відповідною фаховою підготовкою, яким доручено супроводження робіт з ТЗІ в установі (далі – підрозділ ТЗІ), службу захисту інформації в ІТС;

– інші підрозділи установи, які залучаються для формування положень щодо використання в інформаційній діяльності ІзОД, проведення обстеження, категорування об'єктів тощо.

Рішення щодо необхідності створення (модернізації) комплексу ТЗІ готує замовник на стадіях проектування, нового будівництва, розширення, реконструкції (далі – будівництво) ОІД, а також у разі змін умов функціонування ОІД.

Будівництво ОІД може виконуватися за відповідною проектно-кошторисною документацією. При цьому повинні бути враховані вимоги ДБН А.2.2-2 і ДБН А.2.2-3.

Комплекс ТЗІ повинен створюватися виходячи із перспектив модернізації і розвитку інших комплексів ТЗІ установи, охоронних, протипожежних чи загальних систем безпеки установи, спеціальних систем енергоживлення, життєзабезпечення тощо, а також забезпечувати виконання норм ефективності захищеності інформації, відповідати експлуатаційним вимогам щодо необхідності та періодичності перевірок цієї захищеності.

Засоби забезпечення захисту інформації застосовують у складі комплексу ТЗІ за наявності сертифіката відповідності Системи УкрСЕПРО вимогам НД з питань ТЗІ або позитивного висновку державної експертизи у сфері ТЗІ.

Застосування імпортних засобів забезпечення захисту інформації можливе лише за умови відсутності вітчизняних аналогів при наявності відповідних техніко-економічних обґрунтувань і проведення їх сертифікації або одержання позитивного експертного висновку.

Джерела фінансування робіт зі створення комплексу ТЗІ визначає замовник.

Витрати на проектування, будівельно-монтажні роботи, проведення випробувань щодо ТЗІ, атестації комплексу ТЗІ вносяться до кошторису на будівництво та експлуатацію (утримання) ОІД.

1.3 Постановка задачі

На об`єктах інформаційної діяльності, де циркулює інформація з обмеженим доступом повинна бути реалізована система захисту інформації.

Згідно НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" необхідність у створенні комплексів технічного захисту інформації від витоку технічними каналами визначається власником системи. Також він визначає потребу в КСЗІ.

Розробка КСЗІ починається з обстеження на ОІД. Під час виконання обстеження ІТС розглядається як організаційнотехнічна система, яка поєднує:

- обчислювальну систему;

- фізичне середовище;

- середовище користувачів;

- оброблювану інформацію і технологію її обробки.

При обстеженні обчислювальної системи ІТС повинні бути проаналізовані й описані:

- загальна характеристика ОІД;

- загальна структурна схема і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо);

- особливості взаємодії окремих компонентів, їх взаємний вплив один на одного;

- можливі обмеження щодо використання засобів та ін.

Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІТС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

При обстеженні інформаційного середовища аналізу підлягає вся інформація, що обробляється, а також зберігається в ІТС (дані і програмне забезпечення). Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, визначені й описані види (в термінах об’єктів КС) її представлення в ІТС. Для кожного виду інформації і типу об’єкта,

в якому вона міститься, ставляться у відповідність властивості захищеності інформації (конфіденційність, цілісність, доступність).

При обстеженні фізичного середовища здійснюється аналіз взаємного розміщення засобів обробки інформації ІТС на об'єктах інформаційної діяльності, комунікацій, систем життєзабезпечення і зв'язку, а також режим функціонування цих об'єктів.

Аналізу підлягають такі характеристики фізичного середовища:

- територіальне розміщення компонентів ІТС (генеральний план, ситуаційний план); - наявність охорони території та перепускний режим; - наявність категорійованих приміщень, в яких мають розміщуватися компоненти ІТС;

- режим доступу до компонентів фізичного середовища ІТС;

- вплив чинників навколишнього середовища, захищеність від засобів технічної розвідки;

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

- наявність та технічні характеристики систем заземлення;

- умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації;

- наявність проектної та експлуатаційної документації на компоненти фізичного середовища.

При обстеженні середовища користувачів здійснюється аналіз:

- функціонального та кількісного складу користувачів, їхніх

функціональних обов'язків та рівня кваліфікації;

- повноважень користувачів щодо допуску до відомостей, які обробляються в ІТС, доступу до ІТС та її окремих компонентів;

- повноважень користувачів щодо управління КСЗІ;

- рівня можливостей різних категорій користувачів, що надаються (можуть бути доступними) їм засобами ІТС.

Після виконання обстеження ІТС можна приступати до формування завдання на створення КСЗІ:

- визначаються завдання захисту інформації в ІТС, мета створення КСЗІ, варіант вирішення задач захисту (відповідно до ДСТУ 3396.1), основні напрями забезпечення захисту (відповідно до п. 5.8);

- здійснюється аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначається перелік суттєвих загроз;

- визначаються загальна структура та склад КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, допустимі обмеження щодо застосування певних заходів і засобів захисту, інші обмеження щодо середовищ функціонування ІТС, обмеження щодо використання ресурсів ІТС для реалізації задач захисту, припустимі витрати на створення КСЗІ, умови створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальні вимоги до співвідношення та меж застосування в ІТС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ.

1.4 Загальні відомості про підприємство

Повна назва підприємства: ПП «Лата». Юридична адреса: Україна, 49005, м. Дніпро, вул. Писаржевського 1-А. Вид власності – Приватне Підприємство (ПП). Підприємство створено в 1998 році. ПП «Лата» - є дочірнім підприємством американської компанії «Inforeach», головний офіс якої знаходиться у м. Чікаго та є постачальником програмних продуктів для електронної торгівлі, включаючи OMS та EMS платформи для глобальних акцій, фьючерсів, опціонів та фіксованого доходу.

1.4.1 Загальна характеристика підприємства

1.	Назва підприємства	Лата
2.	Форма власності	Приватне підприємство
3.	Тип організації, наявність структурних підрозділів	Приватне підприємство без структурних підрозділів
4.	Рід діяльності підприємства	Постачальник програмних продуктів для електронної торгівлі, включаючи OMS та EMS платформи для глобальних акцій, фьючерсів, опціонів та фіксованого доходу
5.	Розміщення підприємства	2 поверх 9-ти поверхової будівлі
6.	Контрольована зона	Обмежена стінами приміщень
7.	Наявність розгалуженої ІС	-
8.	Персонал підприємства	Директор, бухгалтер, тестувальники, системний адміністратор, розробники, технічна підтримка
9.	Персонал, який відповідає за роботу ІС	Системний адміністратор
10.	Персонал, який використовує ІС	Директор, бухгалтер, тестувальники, системний адміністратор, розробники, технічна підтримка
11.	Тип циркулюючої інформації	Відкрита, конфіденційна, комерційна таємниця
12.	Види циркулюючої інформації	Акустичний, паперовий, електронний
13.	Головні інформаційні потоки підприємства	Бухгалтерський облік, вихідний код ПО, документація по розробці, релізам
14.	Реалізуються за рахунок:	Сервера
15.	Другорядні інформаційні потоки підприємства	Контактні і особисті дані співробітників, логіни та паролі в паперовому вигляді (видаються кожному), договори з працівниками, відомості про клієнтів, бухгалтерський звіт, копії документів тощо
16.	Реалізуються за рахунок:	ПК директора, бухгалтера, розробників, тестувальників, тех.підтримки

1.4.2 Ситуаційний план

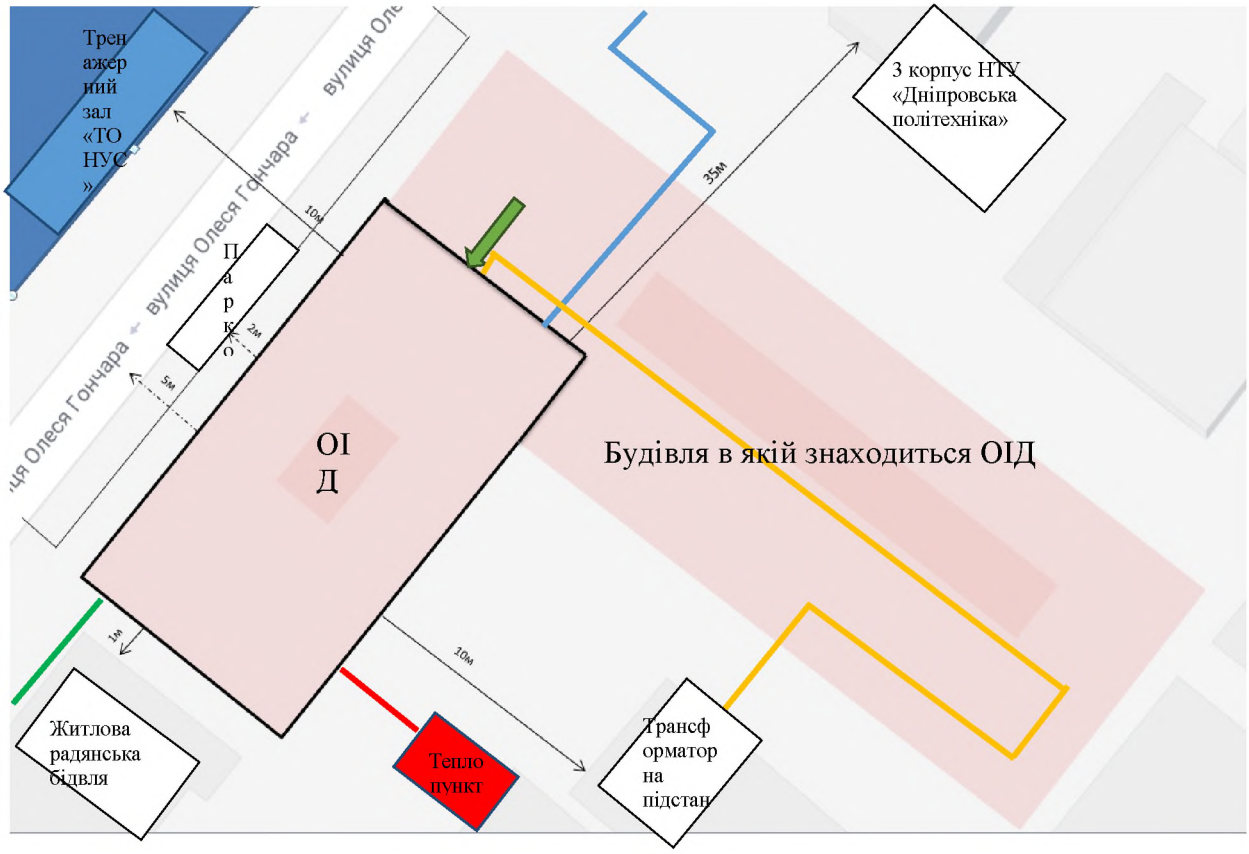


Рисунок 5. Ситуаційний план ОІД

- кордони КЗ та місцезнаходження ОІД

- відстань до споруд

- відстань до дороги

- відстань до парковки

- лінія електроживл

- лінія мережі інтернет

- водопостачання

 - вхід до ОІД з будівлі — - лінія теплопостачання

Відомості про споруди, що оточують будівлю в якій знаходиться ОІД та які знаходяться за КЗ наведені у таблиці 1:

Таблиця 1

№	Розташування відносно ОІД	Характеристика об'єкта	Відстань від ОІД, м
1	З півночі	Будівля 3го корпусу НТУ «Дніпровська політехніка »	35
2	Зі сходу	Трансформаторна підстанція	10
3	З заходу	Тренажерний зал «ТОНУС»	10
4	З заходу	Проїжджа частина	5
5	З заходу	Парковка	2
6	З півдня	Житлова радянська будівля	1

Кількість поверхів будівлі, в якій знаходиться ОІД: 9

1.4.3 Опис будівлі ОІД

- Приміщення знаходиться в бетонній будівлі, перекриття виконані з залізобетонних плит, які спираються на зовнішні стіни;
- Загальна площа ОІД – 345 м^2;
- Товщина несучих стін – 50 см;
- Товщина перегородок – 50 см;
- Висота стель приміщення – 2,75 м;
- Централізоване автономне опалення;

- Електроживлення -централізоване автономне. Контури заземлені;
- Матеріал вікон – металопластикові;
- Вхід в приміщення обладнаний металевими дверима з електричним замком;
- Приміщення, в якому циркулює інформація з обмеженим доступом знаходиться на другому поверсі. Вірогідність несанкціонованого чи випадкового проникнення в приміщення дуже мала, оскільки за для входу потрібно використати спеціальну ключ-карту
- На підприємстві встановлена проводка ще з радянських часів.
- В офісі встановлені на стелі встановлені дешеві, легкозаймисті ПВХ панелі

1.4.4 Розміри приміщень ОІД

- Кабінет тех.підтримки – 44.5 м^2
- Кабінет розробників – 42.5 м^2
- Кабінет системного адміністратора – 40 м^2
- Кабінет тестувальників – 38 м^2
- Конференц-зал – 38 м^2
- Кухня –34 м^2
- Кабінет директора - 32 м^2
- Кабінет бухгалтера - 28 м^2
- Зала відпочинку – 22 м^2
- Службове приміщення №1 – 18 м^2
- Службове приміщення №2 – 18 м^2

1.4.5 Задіяні лінії комунікації

- Електрична мережа – спільна на всю будівлю, входить в межі КЗ і виходить в інші приміщення будівлі (інші офісні приміщення, які розташовані на кожному поверсі 9-поверхової будівлі);
- Джерело електроенергії - трансформаторна підстанція, знаходиться за межами КЗ, але на території будівлі, в якій знаходиться офіс компанії;
- Мережа інтернет - оптоволоконний кабель, виходить за межі КЗ;
- Телефонна лінія, знаходиться в межах КЗ;
- Локальна мережа - кручена пара, яка прокладена в КЗ і не виходить за його межу;
- Вентиляційна система - знаходиться в межах КЗ і виходить в інші приміщення будівлі;
- Опалення і водопровід - спільні на всю будівлю, проходять через КЗ і виходять в інші приміщення (інші офісні приміщення, які розташовані на кожному поверсі 9-поверхової будівлі)

2.1.7 Опис ситуаційного плану

Офіс компанії знаходиться за адресою вул. Пісаржевського 1А. об’єкт розташований на 2-му поверсі 9-поверхової офісної будівлі. К будівлі підведені електро-, газо- та водосполучення. На в'їзді знаходиться пункт охорони і шлагбаум, біля входів розташовані камери спостереження, спостереження ведеться цілодобово. Для того щоб потрапити у будівлю необхідно пройти цілодобовий пункт охорони, який знаходиться на першому поверсі – для цього необхідно мати при собі ключ-карту, яка ідентифікує цю людину. Режим контрольованої зони забезпечується за рахунок дверей на електронному замку, який також вимагає особисту ключ-карту. На вхідних дверях є звукова сигналізація. По відкриттю дверей завжди видається характерний звук, який інформує інших, що людина зайшла або покинула контрольовану зону (офіс).

1.5 Обстеження об’єкту

1.5.1. Генеральний план

Схема генерального плану підприємства приведена нижче:

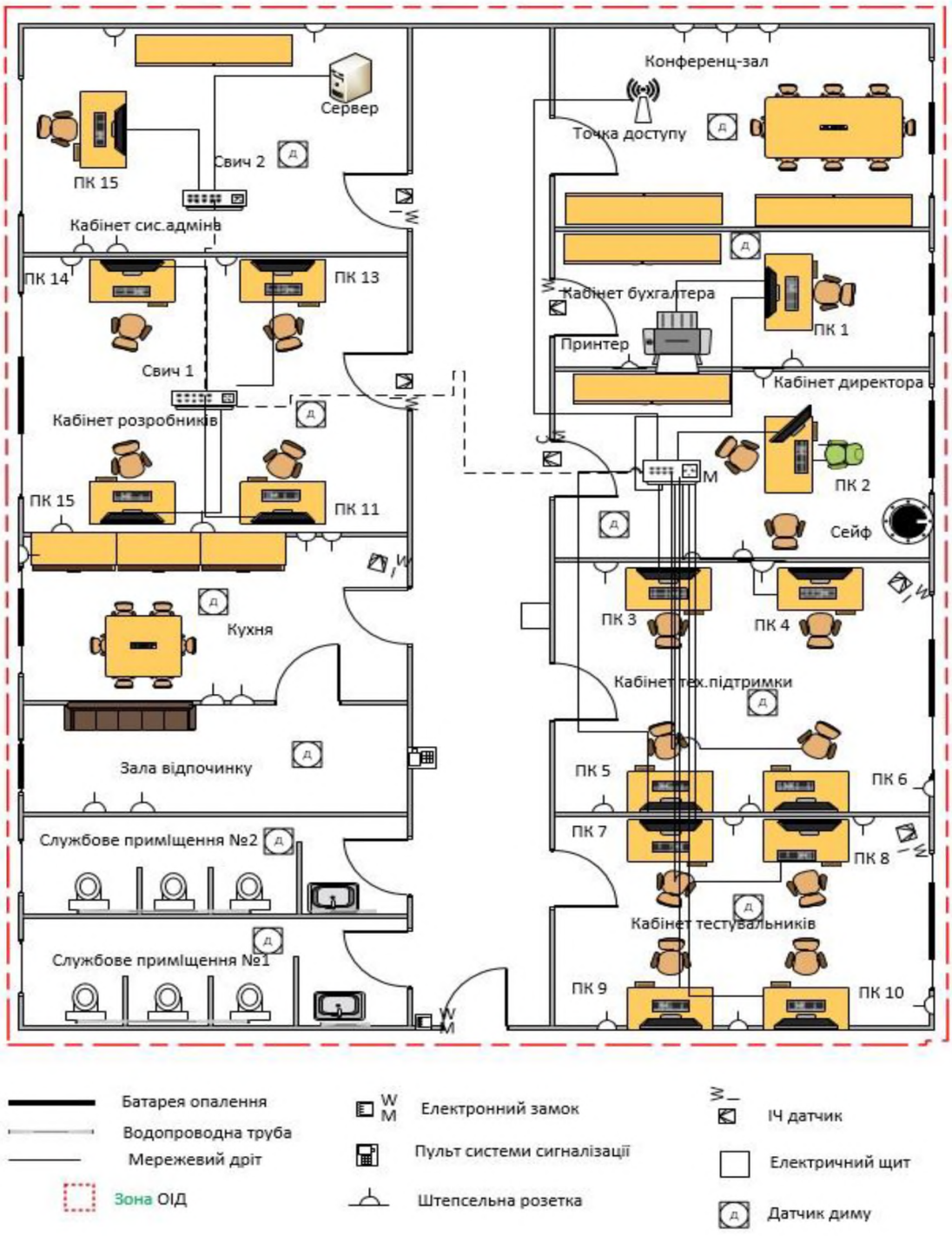


Рисунок 6. Генеральний план ОІД

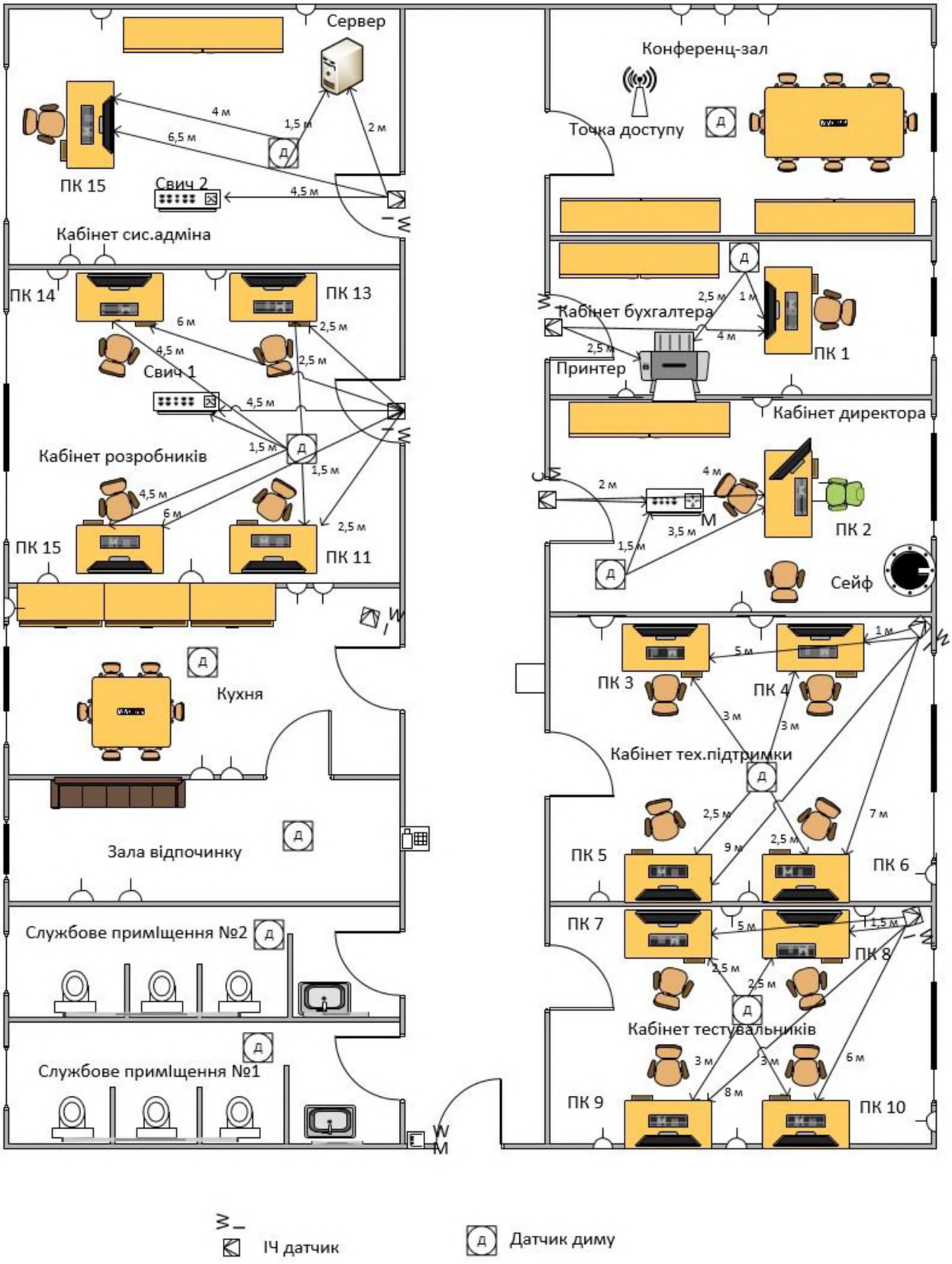


Рисунок 7. План ОІД з відстанню від ТЗПІ до ДТЗС (ВТСС рос.)

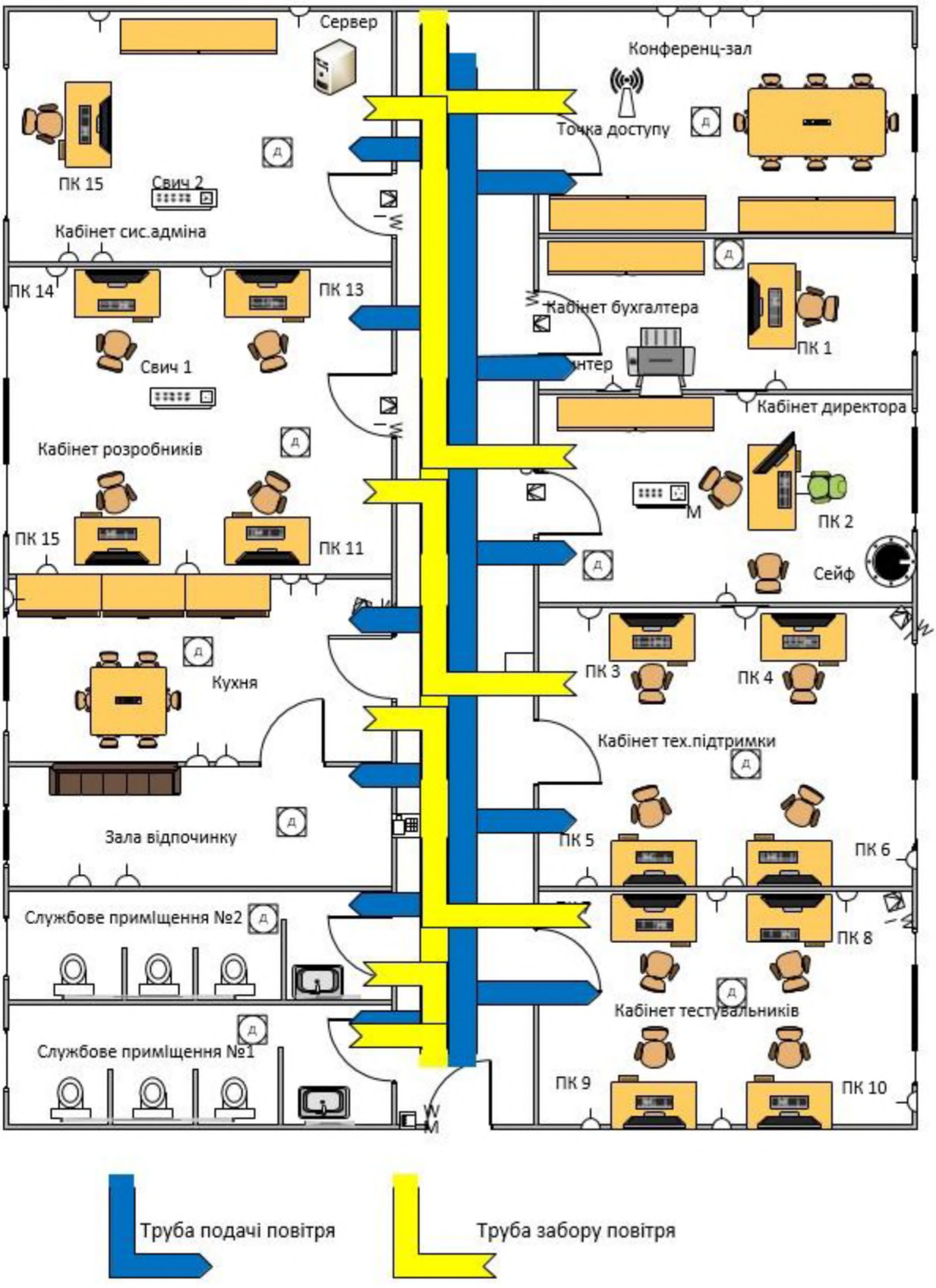


Рисунок 8. Система вентиляції ОІД

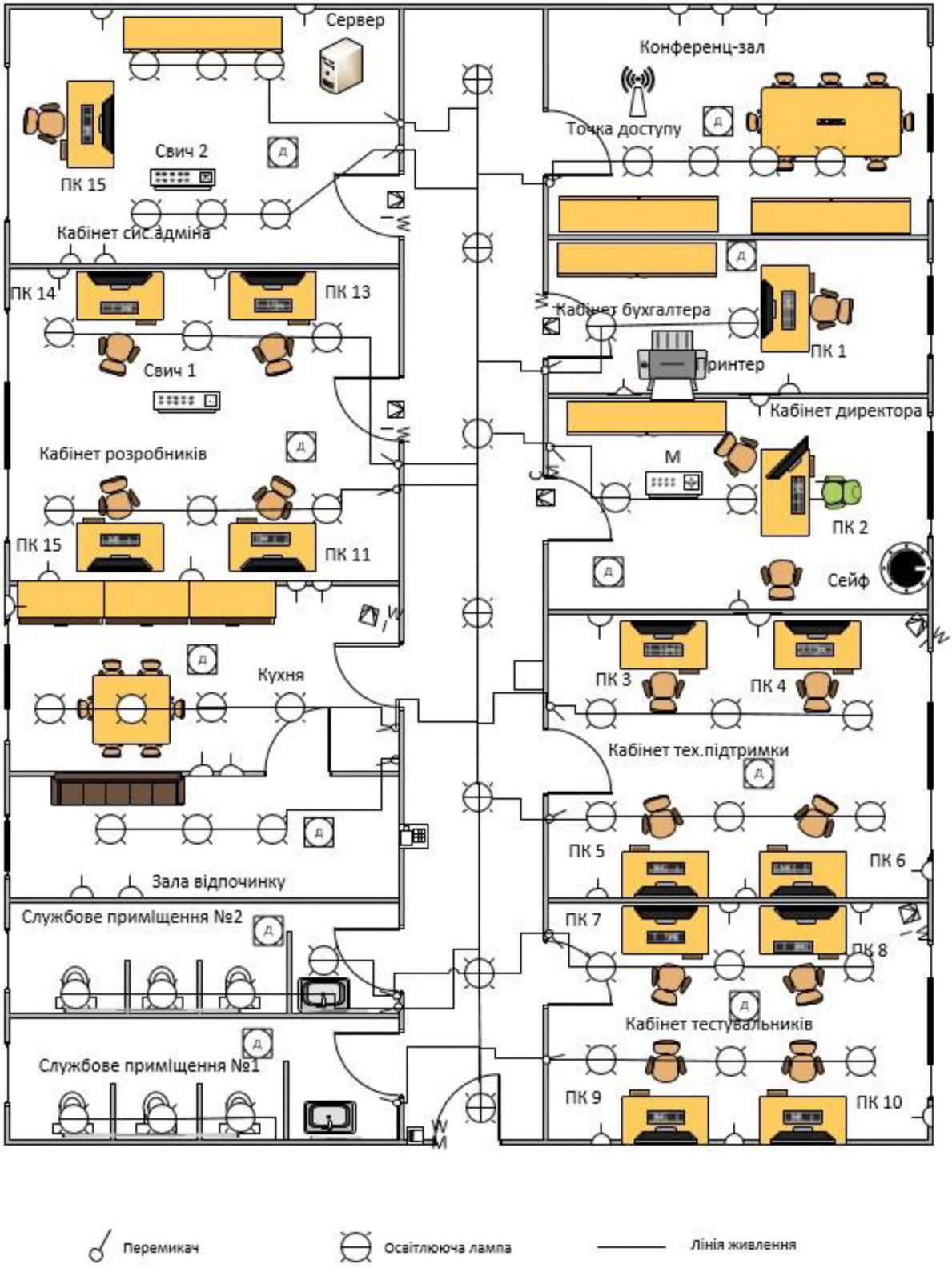


Рисунок 9. План освітлення ОІД

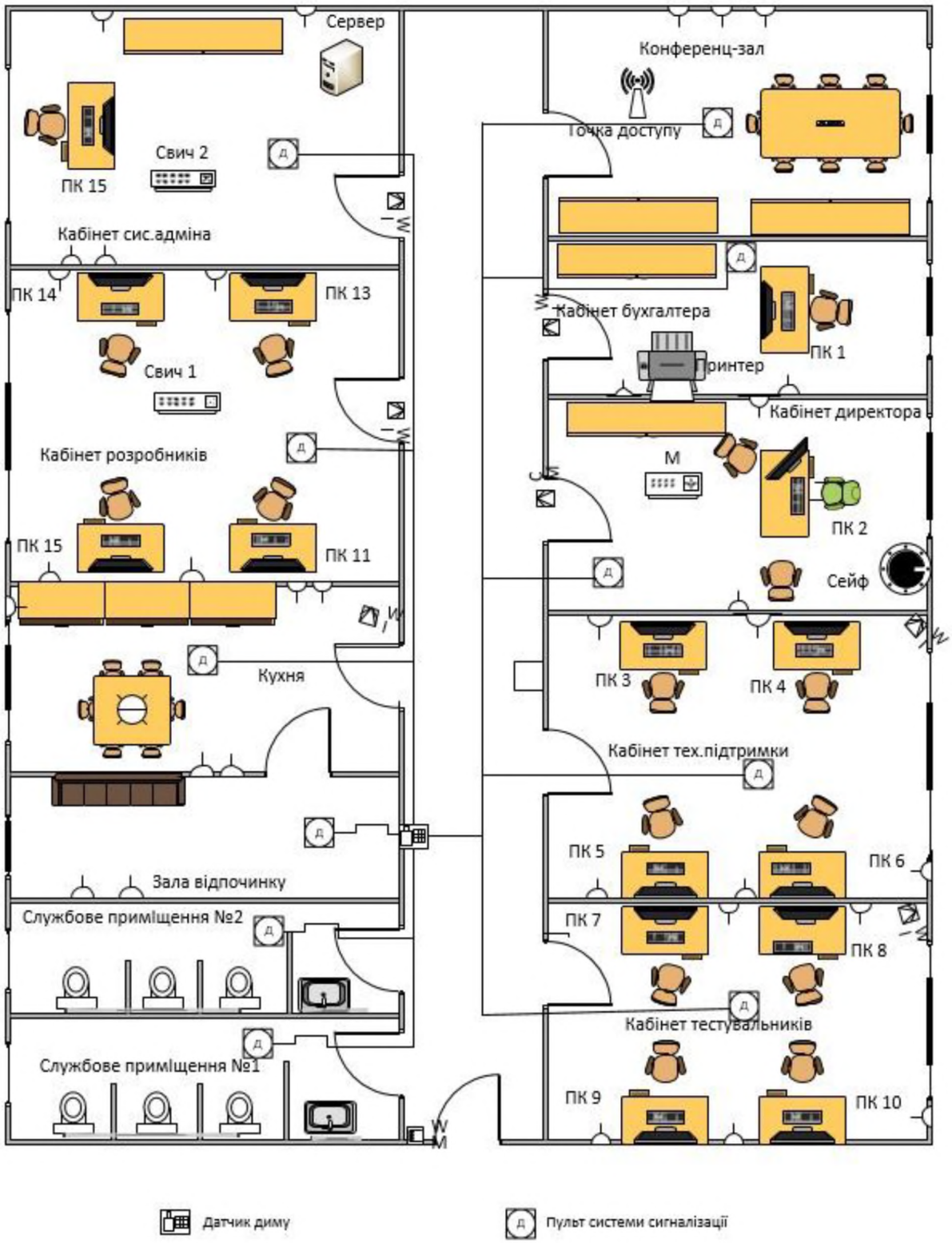


Рисунок 10. План пожарної сигналізації

1.6 Опис основних тех.засобів

Таблиця 2

№	Найменування	Специфікація	Ім'я в ІС	Приміщення	Відповідальна особа	Серійний номер
1	2	3	4	5	6	7
1	Персональний комп'ютер	Intel Core i7-9700F (3.0 - 4.7 ГГц) / RAM 16 ГБ / HDD 1 ТБ + SSD 250 ГБ / nVidia GeForce GTX 1050 Ti, 4 ГБ	ПК1	Кабінет бухгалтера	Бухгалтер	KLS333441
			ПК2	Кабінет директора	Директор	KLS333442
			ПК3	Кабінет працівників тех.підтримки	Працівник тех.підтримки	KLS333443
			ПК4		Працівник тех.підтримки	KLS333444
			ПК5		Працівник тех.підтримки	KLS333445
			ПК6		Працівник тех.підтримки	KLS333446
			ПК7	Кабінет тестувальників	Тестувальник	KLS333447
			ПК8		Тестувальник	KLS333448
			ПК9		Тестувальник	KLS333449
			ПК10		Тестувальник	KLS333410
			ПК11	Кабінет розробників	Розробник	KLS333411
			ПК12		Розробник	KLS333412
			ПК13		Розробник	KLS333413
			ПК14		Розробник	KLS333414

Продовження таблиці 2

1	2	3	4	5	6	7
2	Персональний комп'ютер	AMD Opteron X3216/ HDD 1 ТБ/ 8GB DDR4 2400 MHz/ HPE Embedded Broadcom BCM5720 Dual Port/ 200W/	ПК15	Кабінет системного адміністратора	Системний адміністратор	KLS333415
3	Сервер	Intel Xeon Quad-Core E3-1225 v5 (3.3 - 3.7 ГГц)/ ECC DDR4-2133 MHz/ Intel Rapid Storage Support Raid/ HDD: 2 x 1 ТБ SSD: 2 x 250 ГБ/ PowerEdge T30	Сервер	Кабінет системного адміністратора	Системний адміністратор	KBB333401
4	Комутатор x2	TP-Link TL-SF1008D (8 портов Ethernet)	Світч 1	Кабінет розробників	Системний адміністратор, розробники	KKK333111
			Світч 2	Кабінет системного адміністратора	Системний адміністратор	KKK333112
5	Маршрутизатор	TP-Link WR841n (4 порта LAN)	M	Кабінет директора	Системний адміністратор	KMM333881
6	Принтер	HP LaserJet 1022	Принтер	Кабінет бухгалтера	Бухгалтер	KPP333331

1.6.1 Користувачі системи

Таблиця 3

№	Посада	Роль в ІС	Приміщення	Оцінка кваліфікації
1	Директор	Користувач, має доступ до всієї інформації на підприємстві	Кабінет директора	Кваліфікований (досвід 10+ років)
2	Системний адміністратор	Системний адміністратор	Кабінет сис. адміна	Кваліфікований (досвід 5+ років)
3	Бухгалтер	Користувач, має доступ до бухгалтерської інформації	Кабінет бухгалтера	Кваліфікований (досвід 5+ років)
4	Тех.підтримка	Користувач, має доступ до даних клієнтів, програмного коду	Кабінет тех.підтримки	Кваліфікований (досвід 5+ років)
5				Кваліфікований (досвід 3+ років)
6				Кваліфікований (досвід 3+ років)
7				Кваліфікований (досвід 1+ років)
8	Розробники	Користувач має доступ до вихідного програмного коду, його документацію та опис, а також до даних клієнта	Кабінет розробників	Кваліфікований (досвід 5+ років)
9				Кваліфікований (досвід 5+ років)
10				Кваліфікований (досвід 3+ років)
11				Кваліфікований (досвід 1+ років)
12	Тестувальники	Користувач, має доступ до даних клієнтів, програмного коду	Кабінет тестувальників	Кваліфікований (досвід 3+ років)
13				Кваліфікований (досвід 3+ років)
14				Кваліфікований (досвід 3+ років)
15				Кваліфікований (досвід 3+ років)

1.6.2 Опис допоміжних тех.засобів

Таблиця № 4

№	Назва	Тип	Розташування	Серійний номер
1	Артон ASD-10 (11 штук)	Автономний датчик диму	Усі приміщення ОІД, крім коридору (на стелі)	3BGK100001
				3BGK100002
				3BGK100003
				33BGK100004
				3BGK100005
				3BGK100006
				3BGK100007
				3BGK100008
				3BGK100009
				3BGK100010
2	Pyronix KX10DP (7 штук)	ІЧ датчик	На стіні під стелею в: 1. Кабінеті бухгалтера 2. Кабінеті директора 3. Кабінеті тех.підтримки 4. Кабінеті тестувальників 5. Кабінеті розробників 6. Кабінеті сис.адміна 7. Кухні	1BCA567001
				1BCA567002
				1BCA567003
				1BCA567004
				1BCA567005
				1BCA567006
				1BCA567007

1.6.3 Опис допоміжних технічних засобів і системи

Таблиця 5

№	Назва	Тип	Розташування
1	Лінії локальної та інтернет мережі	Кручена пара (рос. витая пара)	Підведено до усіх ПК на ОІД
2	Линия сигнализации	Кабель КПКВнг-FRLS	Підведено до усіх датчиків сигналізації
3	Освітлення	Кабель ВВГ	Підведено до всіх стельових світильників ОІД
4	Вентиляційна система	Алюмінієва припливно-витяжна установка	Проведена до кожного приміщення
5	Опалювальна система	Біметалічні радіатори і пластикові труби	Встановлена в кожному приміщені, окрім коридору

1.6.4 Обстеження обчислювальної системи ІТС

Склад: 15 ПК, 1 сервер, 1 маршрутизатор, 2 комутатори, 1 точка доступу.

1.6.5 Опис ІТС

ПК – використовуються у робочих цілях для написання, перевірки, завантаження коду;

Сервер – використовується для зберігання інформації і обслуговування баз даних;

Маршрутизатор – використовується для встановлення з'єднання з мережею інтернет та ділиться ним з усіма підключеними до нього пристроями, а також для об'єднання всіх пристроїв у локальну мережу (з можливістю виходу в інтернет);

Комутатори – використовуються для прийому сигналу від маршрутизатора, який встановлює підключення до мережі інтернет, і передачі сигналу на ПК №11-15 та сервер;

Точка доступу – використовується для надання доступу в інтернет персоналу або «гостям» офісу у неробочих цілях

1.6.6 Опис програмного забезпечення

Таблиця 6

№	Найменування	Тип ліцензії	Строк дії	Де встановлено	Відповідальна особа
1	Windows 10 18362.418 (version 1903)	Volume license	-	ПК1-15	Сис. адміністратор
2	Office 365 корпоративний E3 (build 11001.20074)	Volume license	-	ПК1-15	Сис. адміністратор
3	Windows Security Antivirus	Volume license	-	ПК1-15	Сис. адміністратор
4	Ubuntu Server 16.04	General Public License	-	Сервер	Сис. адміністратор
5	1С Підприємство 8.2 Бухгалтерія для України. Базова версія	Клієнтська ліцензія на 1 робоче місце	-	ПК1	Сис. адміністратор
6	IRD Client (власна програма, яка сортує надходження логів та тікетів від різних інсталяцій та клієнтів)	Для індивідуального використання	-	ПК1-15	Сис. адміністратор
7	Google Chrome 70.0.3865.120	General Public License	-	ПК1-15	Сис. адміністратор
8	3CX	Volume license	-	ПК1-15	Сис. адміністратор
9	IDEA/Microsoft Visual Studio Code	License	-	ПК1-15	Сис. адміністратор
10	OpenVPN	License	-	ПК1-15	Сис. адміністратор
11	Microsoft Outlook 2010/2017	Volume license	-	ПК1-15	Сис. адміністратор

1.6.7 Опис каналів зв’язку

Таблиця 7

№	Тип	Характеристики	Обмеження	Средства защиты
1	Мережа інтернет	До 100 Мб/с	Обмеження на вхідні підключення за	Зв'язок з головним американським

		(провідний), до 20 Мб/с (безпровідний)	допомогою Firewall.	офісом організований за допомогою VPN, передані дані захищені IPSec
2	Мобільна мережа	Звичайний зв'язок	немає	немає

1.7 Класифікація інформації

Таблиця 8

№	Назва	За режимом доступу	По правовому режиму	Вид інформації	Вимоги
1	Інформація про активи, доходи та витрати	З обмеженим доступом	Конфіденційна	Електронний, паперовий	Конфіденційність
2	Внутрішні і міжнародні розрахунки	З обмеженим доступом	Конфіденційна	Електронний, паперовий	Конфіденційність та цілістність
3	Вихідний код	З обмеженим доступом	Конфіденційна	Електронний	Конфіденційність та цілістність
4	Документація по релізам, тестам, клієнтам	З обмеженим доступом	Конфіденційна	Електронний	Конфіденційність
5	Інформація про компанію та які послуги надає	Відкритий доступ	З відкритим доступом	Електронний	Доступність

1.7.1 Технологія обробки інформації

Вид інформації №3 - створюються на підприємстві розробниками, далі цей код тестується і результати тестування передаються назад розробникам (що треба виправити тощо). №4 - Згодом ці результати входять у документацію по релізу продукту (що є багом, а що є фічею) клієнту, дані якого включені в цю документацію. Доступ до цієї інформації має весь персонал, крім бухгалтера.

Вид інформації №1 та №2 пов’язані з бухгалтерською діяльністю і доступ до такої інформації має тільки бухгалтер та директор. Кожен квартал бухгалтером робиться звіт про активи, доходи і витрати. Ця інформація надається директору підприємства, який приймає рішення по використанню активів, нарощенню доходу та зменшенню витрат. Внутрішні та міжнародні розрахунки робляться бухгалтером, ці данні записуються у відповідний документ, доступ до якого має і директор.

Вид інформації №5 можна побачити на сайті компанії, туди вона вноситься представниками тех. підтримки або самим директором (уся інформація, яка має бути додана на сайт спочатку погоджується с директором підприємства).

На підприємстві не ведеться реєстр з журналу подій (немає спільної бази усіх записаних дій користувачів при використанні ПК), тобто якщо хтось з персоналу передав конфіденційну інформацію людині, яка не повинна мати доступ до цих даних, то ця дія може залишитися непоміченою.

Кожен співробітник може працювати віддалено (наприклад у період карантину). Доступ до робочого ПК здійснюється через OpenVPN канал. Щоб підключитися, треба завантажити конфіг з Confluence wiki (системи для внутрішнього використання організаціями з метою створення єдиної бази знань) і за допомогою імені ПК або айпі та логіну/паролю підключитися.

1.7.2 Характеристика умов зберігання та використання інформації

Дані по архітектурі ПЗ, вихідний код і т.д. зберігаються на сервері компанії або на приватних хмарних сховищах. За збереження і цілісність даних відповідає системний адміністратор. Персональні дані співробітників зберігаються в електронному вигляді на комп'ютері бухгалтера та директора. Вони несуть відповідальність за збереження цих даних. Юридична інформація та дані для

підприємницької діяльності зберігаються в паперовому вигляді в сейфі в кабінеті директора під його особисту відповідальність.

На робочих ПК розробників міститься інформація, яка стосується конкретного проекту (код), над яким вони працюють. На ПК тестувальників міститься інформація про результати тестувань програм або які тести необхідно ще зробити. На ПК тех.підтримки міститься інформація, яка надходить з різних інсталяцій клієнтів і стосується правильності роботи коду (логи), з якими вони взаємодіють (розмова з клієнтами чому це сталося, як це можна вирішити тощо).

Весь персонал підписує договір о нерозголошенні та в залежності від завданого збитку від розкриття інформації виплачують штраф. На всіх ПК стоять паролі, але немає ніяких інструкцій по зміні, зберіганню та оновленню паролів. Не вжито жодних заходів щодо контролю USB-флеш-носіїв. Працівники несуть відповідальність за розкриття всієї конфіденційної інформації.

1.8 Опис АС

АС 3 класу використовується для розробки ПЗ. Зв'язок з мережею інтернет здійснюється за допомогою роутера, наданим інтернет провайдером. В АС присутня точка доступу wi-fi вона використовується для неробочих цілей.

Розробники отримують код з репозиторію локального сервера. Після закінчення робіт вони завантажують свій код в репозиторій, де потім додатки запускаються в локальній мережі для можливості тестування і перевірки - цим в основному займаються тестувальники, також вони (розробники та тестувальники) завантажують на сервер документацію щодо проекту. Доступ до сервера надається за ip та mac адресою.

Після закінчення циклу розробки старший розробник переносить код на сервер головного офісу і запускає додаток в робочому режимі. Головний офіс знаходиться у м. Чікаго, зв'язок з ним здійснюється за допомогою каналу

OpenVPN поверх мережі інтернет. Також туди дублюється вихідний код по досягненню встановлених етапів розробки. На стороні головного офісу піднято VPN сервер, який дозволяє встановлювати захищений канал. Авторизація проходить по паролю і логіну.

Тех.підтримка використовує мережу інтернет для надання допомоги клієнтам в користуванні продуктом компанії та вирішення проблемних ситуацій, які можуть трапитись при роботі тієї чи іншої програми компанії.

Системний адміністратор відповідальний за підтримку роботи мережі.

Бухгалтер використовує мережу інтернет для подачі електронної бухгалтерської звітності.

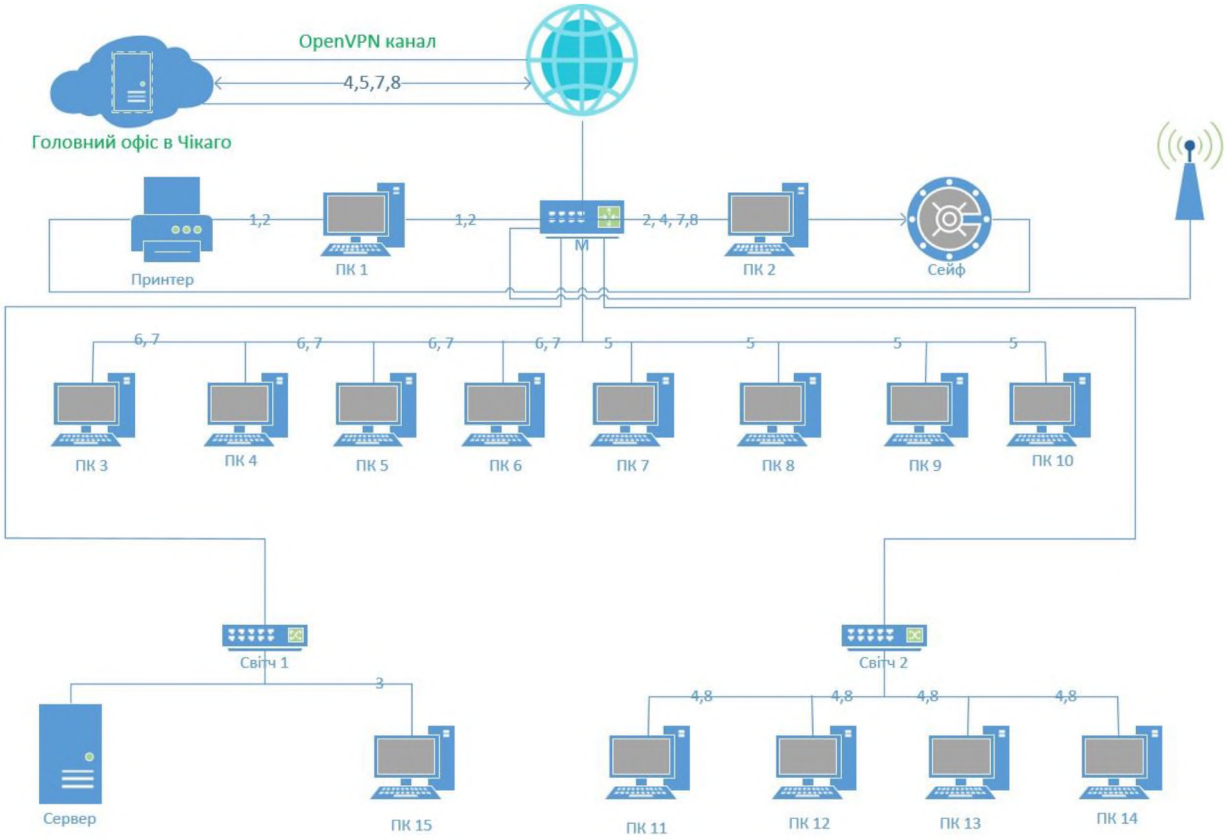
1.8.1 Класифікація інформаційних потоків

Таблиця 9

Номер інформаційного потоку	Назва	Участники

1	Визначення та облік основних фінансових складових частин організації, таких, як активи, доходи та витрати	Директор, Бухгалтер
2	Складання внутрішніх і міжнародних розрахунків	Бухгалтер
3	Стеження за станом ІС -забезпечення мережевої безпеки, стеження за станом комп'ютерів і комп'ютерних програм, їх оновлення тощо	Системний адміністратор
4	Написання коду та завантаження його у внутрішній репозиторій на сервері або завантаження з серверу	Директор, розробники
5	Перевірка та тестування коду	Тестувальники
6	Підтримка вже випущеного продукту	Тех.підтримка
7	Оновлення інформації на сайті компанії	Директор, тех. підтримка
8	Завантаження коду з внутрішнього репозиторію на сервер головного офісу	Директор, розробники

1.8.2 Схема мережі з інформаційними потоками



1.9 Модель порушника

Таблиця 1. Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загроз
	Внутрішні по відношенню до ІТС	
ПВ1	Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІТС	1
ПВ2	Персонал, який обслуговує технічні засоби ІТС (інженери, техніки)	2
ПВ3	Користувачі (оператори) ІТС	2
ПВ4	Адміністратори ІТС, співробітники служби захисту інформації	3
ПВ5	Співробітники служби безпеки установи та керівники різних рівнів	4
	Зовнішні по відношенню до ІТС	
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	2
ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів або закордонних спецслужб «під прикриттям»	4

Таблиця 2. Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов'язок (ПЗ4)	4

Таблиця 3. Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Таблиця 4. Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесено крізь охорону	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4

Таблиця 5. Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час повної бездіяльності ІТС з метою відновлення та ремонту	1
Ч2	Під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації	2
Ч3	Під час функціонування ІТС (або компонентів системи)	3
Ч4	Як у процесі функціонування ІТС, так і під час призупинки компонентів системи	4

Таблиця 6. Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
Д1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів (операторів) ІТС	2
Д3	З доступом у зону зберігання баз даних, архівів тощо	3
Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

Внутрішній порушник «ПВ» - варіант мінімальних загроз з причини безвідповідального ставлення до виконання своїх посадових обов'язків;

Зовнішній порушник «ПЗ4» (агент конкурентів або закордонних спецслужб «під прикриттям») - варіант максимальних загроз з причини цілеспрямованих несанкціонованих дій з метою модифікації або викрадення інформації.

1.10 Сумарний рівень загроз для внутрішніх та зовнішніх порушників

Таблиця 10

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Прибиральник	ПВ1	М1	К1	З1	Ч4	Д1	9
	1	1	1	1	4	1	
	ПЗ4	М4	К4	З4	Ч4	Д1	21
	4	4	4	4	4	1	
Користувач	ПВ3	М1	К2	З1	Ч3	Д2	11
	2	1	2	1	3	2	
	ПЗ4	М4	К4	З1	Ч3	Д2	21
	4	4	4	4	3	2	
Адміністратор ІТС (сис.адмін)	ПВ4	М1	К4	З1	Ч4	Д4	17
	3	1	4	1	4	4	
	ПЗ4	М4	К4	З1	Ч4	Д4	24
	4	4	4	4	4	4	
Служба безпеки	ПВ5	М1	Л1	З1	Ч4	Д3	14
	4	1	1	1	4	3	
	ПЗ4	М4	К4	З4	Ч4	Д3	23
	4	4	4	4	4	3	
Електрик	ПВ1	М1	К1	З1	Ч1	Д1	8
	1	1	1	1	3	1	
	ПЗ4	М4	К4	З4	Ч1	Д1	20
	4	4	4	4	3	1	

Висновок: з останньої таблиці видно, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становить адміністратор ІТС. Тому організація роботи цієї особи повинна бути найбільш контрольованою, оскільки вона є основним потенційним порушником безпеки інформації.

1.11 Модель загроз для інформації на підприємстві

Таблиця 11

№	Загроза	Джерело	Вразливість	Наслідок реалізації загрози	Що порушує	Коефіцієнт можливості реалізації	Критичність наслідку
1	2	3	4	5	6	7	8
1	Зараження ПЗ комп'ютерними вірусами	Персонал підприємства (внутрішнє)	Халатність з боку персоналу щодо забезпечення власної безпеки при роботі в мережі та/або підключення заражених usb носіїв	Уповільнення роботи підприємства, що може призвести до фінансових втрат та порушення репутації (якщо компанія не виконає вчасно умови договору з клієнтами)	К, Ц, Д, С	3	5
2	Несанкціоноване копіювання на зовнішні носії	Персонал підприємства (внутрішнє)	Відсутность обліку зовнішніх носіїв інформації та відсутність протоколювання операції копіювання в журналі подій *[стр.20 «Характеристика умов зберігання та використання інформації»]*	Витік ІзОД, що циркулює в підприємстві та потрапляння її конкурентам – шкода репутації компанії та понесення фінансових втрат	К	4	5

Продовження таблиці 11

1	2	3	4	5	6	7	8
3	Неналежне зберігання паролів/логінів, які були видані у паперовому вигляді	Персонал підприємства (внутрішнє)	Логіни/паролі видаються співробітникам у паперовому вигляді, які частина персоналу залишає на своєму робочому місці не приховуючи *[«Характеристика умов зберігання та використання інформації»]*	У разі проникнення до офісу зловмисника, він може використати ці данні, щоб отримати несанкціонований доступ до ІзОД, яка зберігається на ПК «жертви»	К	5	5
4	Слабкі паролі на ПК працівників	Персонал підприємства (внутрішнє)	Персонал ,в основному, на міняє паролі, які були видані сис.адміном або змінює їх на занадто примітивні, які легко можна підібрати (приклад дата народження і т.д.) *[«Характеристика умов зберігання та використання інформації»]*	Отримавши доступ до ПК працівника зловмисник може легко підібрати пароль та увійти до облікового запису співробітника, у якому зберігаються данні клієнтів та/або вихідний код програм	К	4	5

Продовження таблиці 11

1	2	3	4	5	6	7	8

5	Конфіг підключення до віддаленого робочого столу через OpenVPN не змінюється	Персонал підприємства (внутрішнє) та колишні співробітники (зовнішнє)	Конфіг підключення [*«Технологія обробки інформації»*] до віддаленого робочого столу через OpenVPN канал не змінюється і знаючи айпі або і'мя ПК та підібравши логін/ пароль можна підключитися до цього ПК	Реалізувавши цю загрозу зловмисник може отримати доступ до даних клієнтів та коду програм. В свою чергу це може призвести до значних фінансових втрат та втрати репутації серед клієнтів	К	5	5
6	Підкуп працівників конкурентами підприємства	Персонал підприємства (внутрішнє)	Витік інформації співробіником може залишитися непоміченим, оскільки на підприємстві не контролюється зовнішній канал зв'язку [*«Технологія обробки інформації»*]	Витік ІзОД, що циркулює в підприємстві та потрапляння її конкурентам – шкода репутації компанії та понесення фінансових втрат	К	3	3

Продовження таблиці 11

1	2	3	4	5	6	7	8
7	Крадіжка засобів обробки та носіїв інформації, що зберігаються на підприємстві	Представниками кримінальних структур (зовнішнє)	Крадіжка можлива оскільки на вікнах офісу немає решіток *[рисунок А.1, на якому можна побачити їх відсутність]*	Ця загроза може привести до тимчасового призупинення роботи організації та понесення фінансових втрат	К, Ц, Д	2	4
8	Встановлення технічних пристроїв запису і обробки інформації на території ОІД	Зовнішнє	Зловмисник може проникнути на територію ОІД через вікна офісу, на яких не встановленні решітки *[рисунок А.1, на якому можна побачити їх відсутність]* та встановити технічні пристрої запису і обробки інформації. Наприклад, у ПК персоналу	Витік ІзОД, що циркулює в підприємстві та потрапляння її конкурентам – шкода репутації компанії та понесення фінансових втрат	К	2	4

Продовження таблиці 11

1	2	3	4	5	6	7	8
9	Порушення цілісності інформації або повне її знищення	Слабка протипожежна система	Оскільки датчики диму не встановлені у коридорі, то у разі виникнення пожежі (наприклад, спричиненої коротким замиканням лінії живлення), джерело якої знаходиться у коридорі (стара проводка) *[«Опис будівлі ОІД»]* та легкозаймисті ПВХ панелі, які встановлені на стелі *[«Опис будівлі ОІД»]*, може призвести до несвоєчасного реагування на цю подію.	Понесення значних фінансових втрат	Ц, Д, С	1	3
10	Надходження фішінгових листів на електронну почту працівникам підприємства	Зовнішнє	Неуважність персоналу	Отримання зловмисником паролей/логінів «жертви» (працівника підприємства) та/або встановлення шкідливе ПЗ на ПК неуважного співробітника	К, Ц	2	2

Продовження таблиці 11

1	2	3	4	5	6	7	8

11	Виведення з ладу сервера за допомогою DDoS атак	Зовнішнє	Відсутність проксі серверу nginx, який підсулює Ubuntu, беручи на себе обробку статичного контенту	Зупинення роботи підприємства та понесення фінансових втрат	Д	3	5
12	Встановлення та використання стороннього ПЗ на робочому ПК (ігри, торренти тощо)	Внутрішнє	Недбалість персоналу	Ненавмисне зараження ПК шкідливим ПЗ	К, Ц, Д	1	2
13	Ненавмисне зараження ПК шкідливим ПЗ	Внутрішнє	Неякісний антивірус *[Опис програмного забезпечення]* та необізнаність працівників	Уповільнення роботи працівника, що може призвести до невчасного виконання забов'язань перед клієнтами (понесення фінансових втрат та шкода репутації)	К, Ц, Д, С	3	4
14	Відсутність ЕЦП для обміну документами з головним офісом та клієнтами з використанням поштового сервісу	Внутрішнє	У документообізі підприємства не використовується ЕЦП (електронно-цифровий підпис)	При отримані документа неможливо впевнитись, що лист надійшов саме від відправника (немає гарантії авторства)	К	5	5

Таблиця 12

Коефіцієнт можливості реалізації загрози	Характеристика
1	Практично неможливо

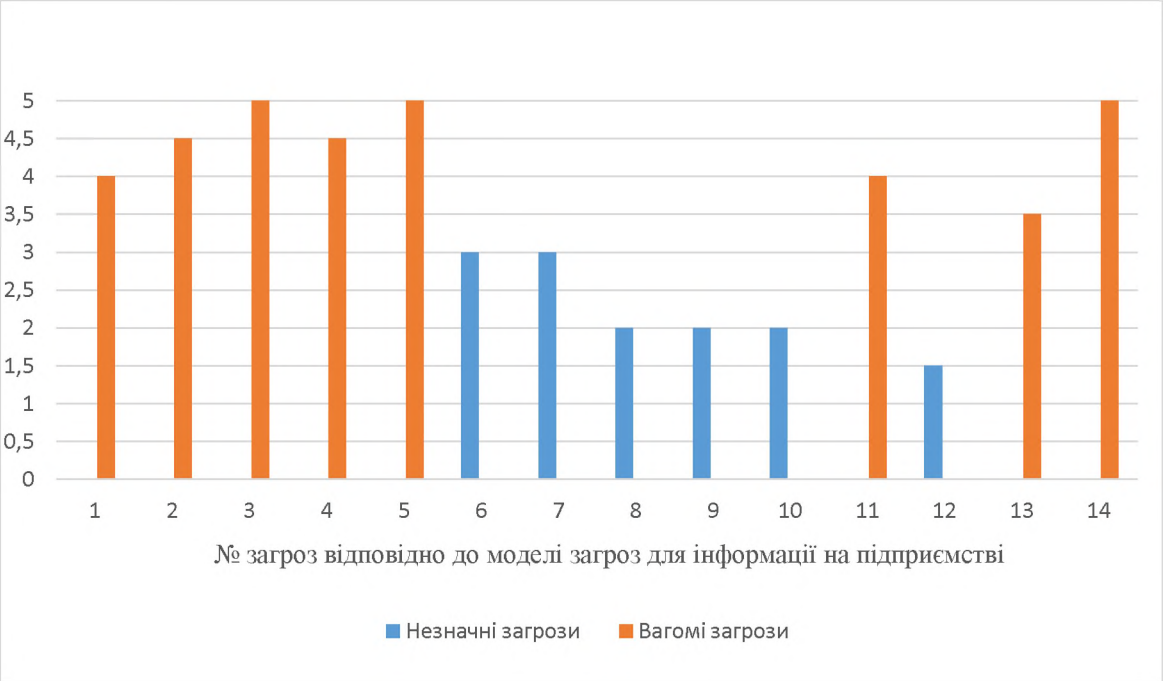
2	Реалізація загрози малоймовірна
3	Реалізація загрози можлива, але недоцільна
4	Реалізація загрози можлива та доцільна
5	Висока ймовірність реалізації загрози

Таблиця 13

Оцінка критичності наслідків	Характеристика
1	Не критичні
2	Низька критичність
3	Середня критичність
4	Вагома критичність
5	Неприпустимо висока критичність

Таблиця 14

№ загрози	Оцінка загрози
1	4
2	4.5
3	5
4	4.5
5	5
6	3
7	3
8	3
9	2
10	2
11	4
12	1.5
13	3.5
14	5



Актуальними загрозами для ОІД вважаються:

- Зараження ПЗ комп'ютерними вірусами
- Несанкціоноване копіювання на зовнішні носії
- Неналежне зберігання паролів/логінів, які були видані у паперовому вигляді
- Слабкі паролі на ПК працівників
- Конфіг підключення до віддаленого робочого столу через OpenVPN не змінюється
- Виведення з ладу сервера за допомогою DDoS атак
- Ненавмисне зараження ПК шкідливим ПЗ
- Відсутність ЕЦП (електронно-цифрового підпису) для обміну документами з головним офісом та клієнтами з використанням поштового сервісу

Для оцінки ризиків використані такі шкали:

1.12 Шкала оцінювання впливу реалізації загрози на конфіденційність

Таблиця 15

Оцінка рівня наслідків	Характеристика
1	Практично не призводить до розкриття конфіденційної інформації
2	Призводить до розкриття окремих документів, які відносяться до ІзОД та/або персональних даних і не призводить до фінансових втрат
3	Призводить до розкриття окремих документів, які відносяться до ІзОД та/або персональних даних і призводить до незначних фінансових втрат
4	Призводить до розкриття окремих документів, які відносяться до ІзОД та/або персональних даних і призводить до значних фінансових втрат
5	Призводить до зупинки роботи системи підприємства

1.13 Шкала оцінювання впливу реалізації загрози на доступність

Таблиця 16

Оцінка рівня наслідків	Характеристика
1	Практично не впливає на доступність
2	Незначний вплив на доступність
3	Середній вплив на доступність
4	Значний вплив на доступність
5	Зупинка роботи системи підприємства на неприпустимо тривалий час

1.14 Шкала оцінювання впливу реалізації загрози на спостережність

Таблиця 17

Оцінка рівня наслідків	Характеристика
1	Практично не впливає на спостережність
2	Незначний вплив на спостережність
3	Призводить до неможливості відстежити частину дій користувачів в системі
4	Призводить до неможливості відстежити дії користувачів і адміністраторів системи
5	Призводить до неможливості відстежити дії всіх кроситувачів і адміністратора системи, може призвести до зупинки роботи системи підприємства на неприпустимо тривалий час

1.15 Шкала оцінювання впливу реалізації загрози на цілісність

Таблиця 18

Оцінка рівня наслідків	Характеристика
1	Практично не призводить до фінансових втрат
2	Призводить до незначних фінансових втрат
3	Призводить до середніх фінансових втрат
4	Призводить до значних фінансових втрат
5	Призводить до зупинки роботи системи підприємства

Внаслідок реалізації загроз, що можуть бути нанесені організації, виконується оцінка збитків з урахуванням очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від втрати керованості ІТС внаслідок реалізації загрози.

Величина можливих збитків визначається розміром фінансових втрат або, у разі неможливості визначення цього, за якісною шкалою (наприклад, величина

збитків - відсутня, низька, середня, висока, неприпустимо висока).

Щоб розрахувати доцільність впровадження політики безпеки, необхідно врахувати той факт, що вартість впровадження заходів безпеки не має перевищувати фінансові втрати понесенні організацією в разі реалізації загрози інформаційної безпеки. Тому для оцінки ризиків використовується комбінація кількісних та якісних методів.

1.16 Функціональний профіль захищеності для системи

Враховуючи характеристики існуючої ІТС та вимог до властивостей інформації, відповідно до НД ТЗІ 2.5-005 -99, обрано такий функціональний профіль захищеності для системи:

3.КЦД.2 = { КД-2, КА-2, КО-1, КВ-2,

ЦД-1, ЦА-1, ЦО-1, ЦВ-1,

ДР-2, ДВ-1,

НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

КД-2 (Базова довірча конфіденційність)

Користувач має можливість керувати доступом інших користувачів до своїх файлів.

КА-2 (Базова адміністративна конфіденційність)

Ця послуга надає можливість управління доступом користувачів до системних ресурсів (процеси, файли тощо)

КО-1 (Повторне використання об'єктів)

Дозволяє забезпечити коректність повторного використання розділюваних об'єктів, тобто таких, які почергово виділяються різним користувачам та/або процесам, а також гарантує, що коли розділюваний об'єкт виділяється новому

користувачу або процесу, він не містить інформації, яка залишилась від попереднього користувача або процесу.

КВ-2 (Мінімальна конфіденційність при обміні)

Забезпечується шифруванням мережевих каналів.

ЦД-1 (Мінімальна довірча цілісність)

У системі присутнє розділення на користувачів та групи користувачів, у яких є ряд повноважень пов'язаних з можливістю модифікації об'єкту.

ЦО-1 (Обмежений відкат)

Забезпечує можливість відновлення останніх збережених налаштувань системи після сбою або ненавмисного видалення.

У операційній системі Windows 10 є функція «Історія файлів» - спосіб відновлення попередньої версії файлів та повнофункціональний інструмент резервування даних. За допомогою точки відновлення можна відновити системні файли Windows 10, а також працездатність операційної системи, виправити раптово виниклі помилки або повернути систему в стан на момент створення точки відновлення.

ЦА-1 (Мінімальна адміністративна цілісність)

Ця послуга надає можливість надавати право на зміну системних файлів іншими користувачами.

ЦВ-1 (Мінімальна цілісність при обміні)

Цілісність при мережевому обміні інформацією забезпечується протоколами шифрування.

ДР-2 (Недопущення захоплення ресурсів)

Реалізація розподілу користувачів в системі дозволяє накладати обмеження на кількість виділених ресурсів в залежності від користувача, який на даний момент авторизований в системі. Обмеження можна накладати на об'єм жорсткого диску, використання інтернет трафіку, встановлення ПЗ, обмеження доступу до переліку сайтів, доступ до налаштувань операційної системи, блокування USB-портів.

ДВ-1 (Автоматизоване відновлення)

Є можливість відновлення системи в разі збою. Наприклад, сбій сектору жорсткого диску.

НР-2 (Захищений журнал)

В системі є журнал подій, в якому зберігаються події, в тому числі пов'язані з безпекою.

НИ-2 (Одиночна ідентифікація і автентифікація)

Для входу у систему користувач повинен ввести логін та пароль, які повинні співпадати з існуючими у системі.

НК-1 (Однонаправлений достовірний канал)

Послуга дозволяє гарантувати, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається). Рівні даної послуги визначені в залежності від того, чи має КЗЗ можливість ініціювати захищений обмін, чи це є прерогативою користувача.

НО-2 (Виділення адміністратора)

Система має розділення на адміністратора та звичайного користувача. Для входу до облікового запису потрібно пройти авторизацію.

НЦ-2 (КЗЗ з контролем цілісності)

У разі виникнення події пов'язаної з порушенням цілісності, відбувається інформування користувача про цю подію, а сама подія реєструється в журналі подій. Для контролю цілісності об'єкту використовується перевірка хеш-сум.

НТ-2 (Самотестування за запитом)

Дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС

Існує можливість тестування елементів системи за запитом користувача з відповідними повноваженнями.

НВ-1 (Автентифікація вузла)

Дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжуються на підставі повноти реалізації.

ВИСНОВКИ ДО РОЗДЛУ І

У цьому розділі були розглянуті та проаналізовані випадки порушення інформаційної безпеки у попередніх роках. Була виявлена тенденція росту кількості кібератак з кожним роком та зазначена актуальність забезпечення безпеки інформації.

Приведені терміни з нормативно-правових документів, які є основою забезпечення безпеки інформації, а саме Законів України та НД ТЗІ. Було зазначено основні положення цих документів, а також обґрунтована потреба у створенні КСЗІ на об’єкті інформаційної діяльності задля упередження несанкціонованого доступу до інформації, яка оброблюється на підприємстві. Зазначені етапи створення КСЗІ та формування завдань.

Відповідно до нормативно-правової документації до етапів створення КСЗІ відноситься обґрунтування необхідності створення, обстеження ОІД, аналіз та виявлення вразливостей і ризиків, розробка політики безпеки.

Було надано загальні відомості про підприємство, його фізичне розташування, апаратний склад, інформаційні потоки, ПЗ, що використовується

на підприємстві, характеристика умов зберігання та використання інформації, опис АС.

Також була розроблена модель порушника, модель загроз та визначено оптимальний функціональний профіль захищеності для системи, що має бути впроваджений на даному підприємстві.

У наступному розділі буде вибраний необхідний функціональний профіль захищеності для системи та розроблена політика безпеки, яка буде визначати основні ризики та мінімізувати збитки, які можуть бути спричинені у разі спроби реалізації вразливостей інформаційної системи підприємства.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Розробка політики безпеки для підприємства

Розробка політики безпеки відіграє значну роль у життєдіяльності підприємства, адже її відсутність чи недбалий підхід до її створення може призвести до припинення діяльності організації.

В АС можуть бути реалізовані декілька відмінних одна від одної політик. Під час розробки необхідно врахувати особливості ІТС, розташування ОІД, опис технічних засобів, опис ПО, класифікувати інформацію, яка циркулює на підприємстві, розробити модель порушника та модель загроз тощо.

Політика безпеки АС має забезпечувати цілісність, доступність, конфіденційність оброблювальної інформації.

Метою політики безпеки є:

- мінімізація ризиків інформаційної безпеки;
- забезпечення безперебійної роботи підприємства;
- захист інформації, яка циркулює в компанії від зовнішніх та внутрішніх загроз

2.1.1 Політика безпеки поштового сервісу

1) Опис

Задля спілкування з клієнтами та між співробітниками підприємства використовується електронна пошта. Неправильне її використання може формувати багато ризиків, що стосуються інформаційної безпеки підприємства, тому необхідно, щоб персонал був ознайомлений з правилами користування електронною поштою та розумів її значення у роботі організації та відносився відповідно.

2) Призначення

Метою цієї політики є забезпечення відповідального користування електронною поштою персоналом ПП «Лата» та проведення інформативних заходів всередині компанії щодо того, як правильно користуватися поштовими сервісами.

Політика безпеки поштового сервісу визначає вимоги до користування електронною поштою працівниками організації.

3) Область застосування

Політика безпеки поштового сервісу застосовується для всіх вхідних та вихідних електронних листів, надісланих за допомогою поштового сервісу та для всіх співробітників ПП «Лата».

4) Положення даної політики

4.1 Регулярно проводити інструктаж для персоналу з приводу безпеки роботи в мережі та інформувати про актуальні загрози.

4.2 Відкривати додатки та переходити за посиланням з електронного листа можна лише у разі відомості та надійності джерела.

4.3 Забороняється використовувати акаунти електронної пошти, які не належать підприємству (Gmail, Yahoo, Hotmail тощо), у робочих цілях. Лище поштовій сервіс Microsoft Outlook та акаунт, який був виданий працівникові як службовий, можна використовувати для ведення робочих справ.

4.4 Якщо на почту користувача прийшов лист, який має явні ознаки спаму, то необхідно відмітити цей лист як спам. Завдяки цьому антиспам-фільтр буде краще розпізнавати спамові листи та блокувати потрапляння таких до електронної пошти користувача.

4.5 Відповідальне користування електронною поштою: не треба спамити інших користувачів або надсилати листи, які суперечать діловим відносинам.

4.6 Постійне оновлення поштового сервісу. Таким чином зловмисник не зможе використати вже відомі вразливості, які постійно з'являються з часом та публікуються на хакерських форумах.

4.7 Налаштування надходжень від різних клієнтів або співробітників компанії: співробітник має створити окрему папку у робочому поштовому сервісі для кожного з клієнтів та інших працівників підприємства, куди будуть надходити листи від них. Наприклад, листи від співробітників клієнта «X» мають потрапляти до папки «X».

Таким чином можна оптимізувати роботу працівника, який не буде витрачати багато часу, щоб знайти той чи інший лист.

4.8 Створити окрему сторінку на Wiki Confluence (доступ до якої матимуть лише працівники компанії), де будуть виписані контакти співробітників (робоча пошта, номер 3CX та номер мобільного телефону).

4.9 Відправляючи електронний лист, співробітник має підписувати його. Наприклад,

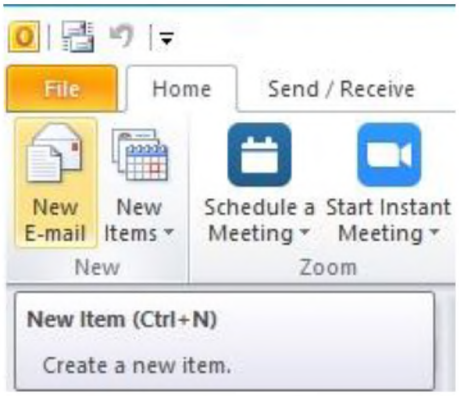
Regards,
Egor Kolodiy

InfoReach, Inc. 77 South Clark Street, Suite 7777, Chicago, IL 60603 Office:+ 1 234 332-4444 ext. 1 |Direct: +1 234 332-4444 egor.kolodiy@inforeachinc.com | www.inforeachinc.com

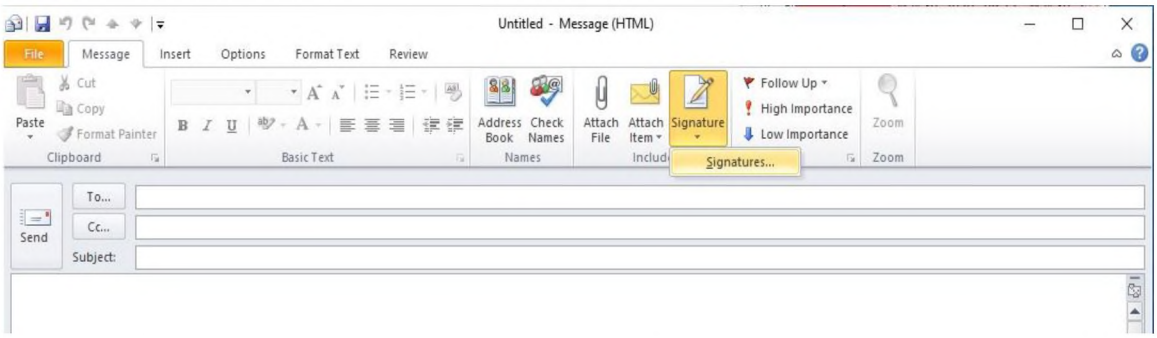
Це необхідно для того, щоб отримувач електронного листа розумів, що відправник – співробітник компанії.

Щоб створити підпис, на прикладі поштового сервісу Microsoft Outlook 2010/2017, який використовується у компанії необхідно:

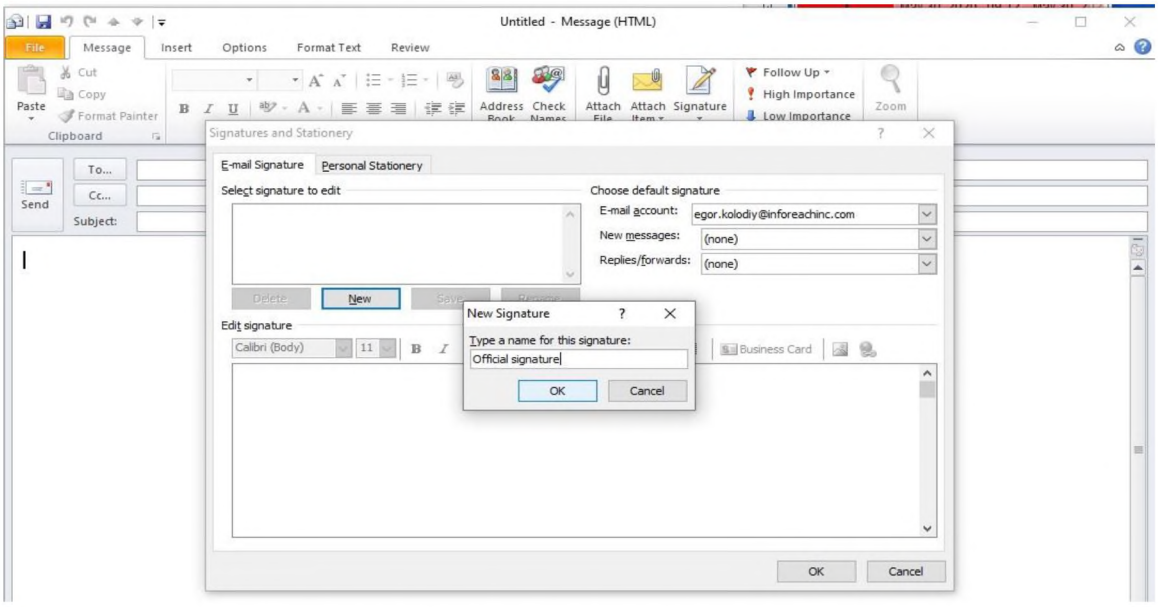
- Відкрити нове повідомлення Microsoft Outlook



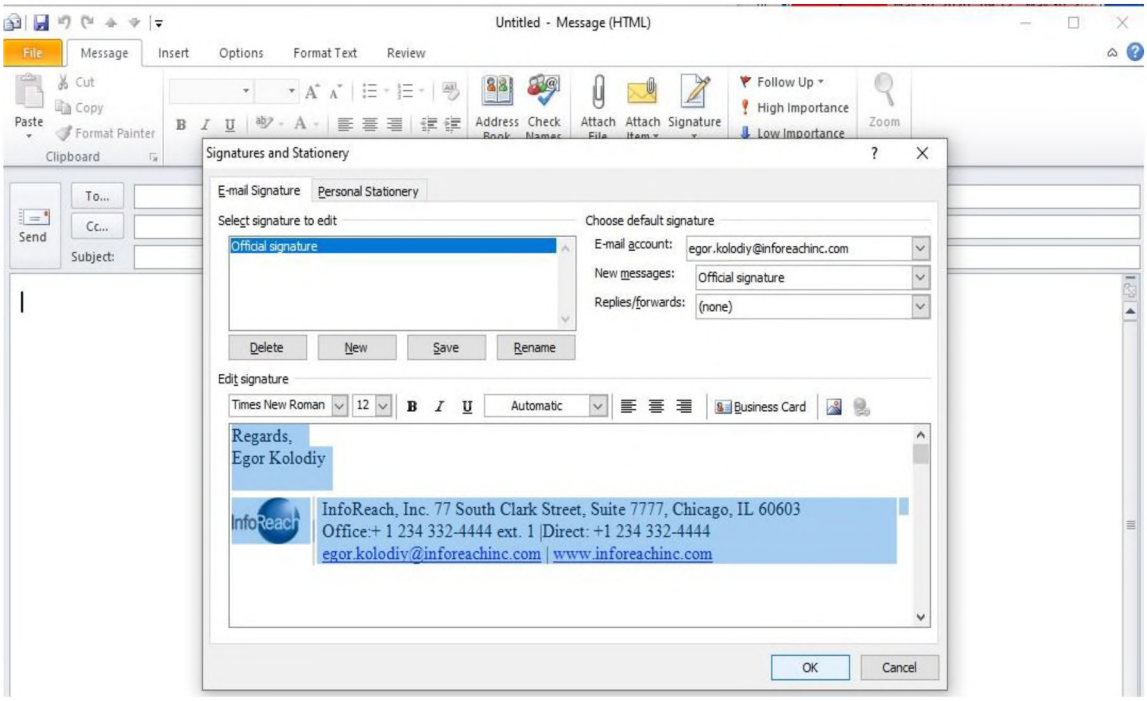
- У самому повідомленні вибрати вкладку «Підпис»



- Відкривши вкладку потрібно створити (додати) новий підпис та нажати ОК



- Потім необхідно додати текст підпису співробітника, в якому буде вказано від кого саме лист, а також назва компанії, її фізична адреса, поштовий індекс, сайт тощо



- Перед тим як нажати ОК необхідно зберегти підпис, нажавши Save
- Тепер при створенні нового електронного листа, автоматично буде створюватися підпис працівника компанії

2.1.2 Політика чистого робочого столу

1) Опис

Політика чистого робочого столу визначає, в якому стані персонал має залишати свої робочі місця.

2) Призначення

Метою цієї політики є запобігання витоку та/або втрати інформації з обмеженим доступом.

3) Область застосування

Політика чистого робочого столу поширюється на весь персонал ПП «Лата».

4) Положення даної політики

4.1 У разі покидання працівником підприємства свого робочого місця, він повинен блокувати або вимикати свій ПК.

4.2 Забороняється видача та зберігання логінів/паролів співробітникам у паперовому вигляді. Замість цього пропонується передача логінів/паролів за допомогою робочого поштового сервісу (від системного адміністратора до працівника, якому видаються ці дані).

4.3 В кінці робочого дня працівник підприємства має забирати з собою усі власні технічні засоби (ноутбук, USB-носій, планшет, телефон тощо).

4.4 Інформація, що підлягає утилізації, повинна бути знищена якнайскоріше за допомогою шредера.

4.5 Документи, які мають інформацію з обмеженим доступом повинні негайно видалятися з принтера.

4.6 В кінці робочого дня працівник підприємства має залишати своє робоче місце у чистоті та ховати всі документи, що зберігаються на робочому столі цього співробітника, у ящик або шафу, які зачиняються на замок.

4.7 Робочі носії інформації з обмеженим доступом мають бути замкнені у сейфі по завершенню роботи з ними.

4.8 Забороняється доступ та користування ПК працівника стороннім особам (наприклад, дітям співробітників)

2.1.3 Політика паролей

1) Опис

Паролі - один з найважливіших складових забезпечення інформаційної безпеки, оскільки слабкий пароль підвищує потенційний ризик несанкціонованого доступу до інформаційної системи підприємства.

2) Призначення

Метою цієї політики є встановлення стандартів створення сильних паролів, їх захист, зберігання і частоту зміни.

3) Область застосування

Політика паролей поширюється на весь персонал ПП «Лата».

4) Положення даної політики

4.1 Працівники підприємства мають зберігати свої паролі у таємниці.

4.2 Після видачі системним адміністратором паролю, працівник, якому призначений цей пароль, має негайно (при першому вході у систему) змінити його на новий, який має задовольняти таким вимогам:

- Довжина паролю має бути не менше восьми символів
- Пароль має складатися з цифр, символів, літер малого та великого реєстру
- Пароль має бути унікальним (не слід використовувати вже створені паролі)

Приклад сильного паролю: J1s$_rtY

4.3 Періодично варто змінювати пароль на новий, який має відповідати політиці паролей приватного підприємства «Лата». Рекомендований інтервал використання паролю три місяці.

4.4 Пароль не повинен містити персональну інформацію працівника (прізвище, ім'я, дата народження, ім'я дружини або матері тощо). Приклад «поганого» паролю: K01od!iY (пароль відповідає вимогам створення паролю, але містить персональну інформацію).

2.1.4 Політика антивірусного захисту

1) Опис

Політика антивірусного захисту визначає вимоги щодо користування антивірусним ПЗ та захисту ІТС ПП «Лата» від загроз інформаційній безпеці компанії, які пов'язані з розповсюдженням шкідливого ПЗ (віруси, майнери тощо).

2) Призначення

Метою цієї політики є запобігання зараження ІТС підприємства шкідливим ПЗ.

3) Область застосування

Політика антивірусного захисту поширюється на весь персонал ПП «Лата».

4) Положення даної політики

4.1 Антивірусне ПЗ повинно бути оновлено на більш якісне. Рекомендовано встановити платний антивірус, оскільки безкоштовний надає тільки базовий функціонал та початковий рівень захисту.
Наприклад, Norton Antivirus *https://us.norton.com/products/norton-360-lifelock-ultimate-plus*, який забезпечує надійний антивірусний захист і надає набір додаткових функцій, включаючи менеджер паролів, VPN, хмарне резервне копіювання тощо.

4.2 Сканування на пошук вірусів потрібно проводити щоденно на кожному робочому ПК.

4.3 Необхідно оновлювати усі програми, з якими працює персонал підприємства щотижня (на вихідних).

4.4 При використанні сторонніх носіїв інформації, слід перевіряти їх антивірусом на наявність шкідливого ПЗ.

4.5 У разі необхідності запуску програми, яка конфліктує з антивірусом, слід виконати повну перевірку на наявність стороннього шкідливого ПЗ та переконатись у його відсутності. Також необхідно бути впевненим, що конфліктуюча програма не призведе до негативних наслідків. Лише у цьому разі дозволяється запуск програми. Під час роботи з запущеною програмою забороняється запускати та користуватися будь-якими додатками, які можуть піддати ризику зараження системи стороннім шкідливим ПЗ Після користування програмою, слід обов'язково відновити роботу антивірусного ПЗ.

4.6 Забороняється завантажувати інформацію з невідомих та підозрілих джерел.

2.1.5 Серверна політика

1) Опис

Серверна політика – це опис методів адміністрування, які мають мінімізувати ризики при роботі з сервером.

2) Призначення

Мета полягає в тому, щоб захистити сервер від загроз його інформаційній безпеці.

3) Область застосування

Серверна політика поширюється на власника системи (директора) та системного адміністратора ПП «Лата»

4) Положення даної політики

4.1 Всі пов'язані з безпекою події в системі повинні реєструватися в журналі подій.

4.2 ОС, яка встановлена на сервері необхідно використовувати разом з

проксі-сервером nginx. Нижче буде наведено інструкції щодо встановлення:

До операційної системи, яка встановлена на сервері (Ubuntu 16.04), слід додатково встановити проксі-сервер nginx. Таким чином nginx буде обробляти увесь статичний контент, який надходить на сервер. Щоб встановити nginx потрібно:

- Відкрити термінал та ввести команду apt-get install nginx
- Обмежити максимальний розмір тіла запиту шляхом використання команди *client_max_body_size* та встановити розмір у 24 МБ
- Використовуючи команду *client_body_buffer_size* визначити розмір буфера для читання тіла запиту від клієнта (від 16 КБ)
- Використовуючи команду *client_header_timeout* обмежити час передачі повного заголовка запиту в межах 15 секунд
- Використовуючи команду *client_body_timeout* визначити час передачі тіла запиту (встановлюється таке ж значення, як для параметра client_header_timeout)
- Встановити тривалість з'єднання клієнта з сервером командою *keepalive_timeout* у 20 секунд
- Встановити час, який буде виділяється клієнту на прийняття відповіді командою *send_timeout* у 5 секунд

Додатково можна встановити модуль mod_security, налаштувавши необхідні фільтри, які будуть забезпечувати захист від DDoS-атак. Для цього потрібно:

- Відкрити термінал та ввести команду *apt-get install libapache2-modsecurity*
- Далі потрібно завершити установку модуля, переіменувавши конфігураційний файл *mv /etc/modsecurity/ modsecurity.conf{-recommended,}*
- По завершенню налаштування, слід перезапустити систему

- Тепер можна переходити до налаштування mod_security: до modsecurity.conf необхідно внести зміни, оскільки спочатку він налаштований лише на відстеження логів запросів та не блокує знайдені вразливості. Тому в modsecurity.conf в строчці SecRuleEngine потрібно змінити значення «Detection Only» на «On»
- Далі потрібно змінити значення в *SecRequestBodyLimit*, *SecRequestBodyNoFilesLimit* та *SecRequestBodyInMemoryLimit* на менші. Базово встановленні такі значення: 12.5 МБ, 128 КБ та 128 КБ відповідно
- Також необхідно ввести базові правила фільтрації Core Rule Set. Для цього слід відредагувати дані в */etc/apache2/mods-enabled/mod-security.conf*. В директорію з модулем security2_module додаються такі каталоги з правилами: *<IfModule security2_module>*
Include«/usr/share/modsecurity-crs/.conf»*
Include«/usr/share/modsecurity-crs/activated_rules/.conf»*
</IfModule>

Ці правила знаходяться у каталогах:
/usr/share/modsecurity-crs/base_rules
/usr/share/modsecurity-crs/optional_rules
/usr/share/modsecurity-crs/experimental_rules

- В каталозі activated_rules потрібно створити посилання для активації потрібних правил: *cd /usr/share/modsecurity-crs/activated_rules*
- Далі потрібно задати правило для захисту від введення SQL-коду, таким чином зловмисник не зможе отримати доступ до баз даних MySQL через фіктивні логін та пароль: *In –s /usr/share/modsecurity-crs/base_rules/modsecurity_crs_41_sql_injection_attacks.conf*
- Для активації внесених змін, слід перезапустити систему

4.3 Системному адміністратору забороняється працювати під обліковим записом root. Під root може заходити лише власник системи (директор

підприємства).

4.4 Обов'язки адміністратора безпеки (у разі його відсутності) повинен брати на себе власник системи (директор).

2.1.6 Політика підключення до віддаленого робочого столу

1) Опис

Політика підключення та використання віддаленого робочого столу визначає вимоги щодо дистанційної роботи на ПК.

2) Призначення

Метою цієї політики є забезпечення безпечного дистанційного підключення та використання віддаленого робочого столу.

3) Область застосування

Політика підключення та використання віддаленого робочого столу поширюється на весь персонал ПП «Лата».

4) Положення даної політики

4.1 Конфіг підключення до віддаленого робочого столу через OpenVPN повинен змінюватися щомісячно або у разі звільнення когось з персоналу ПП «Лата».

4.2 При підключенні до віддаленого робочого столу слід встановити двофакторну авторизацію використовуючи додатки (Authy, Google Authenticator), які дають можливість отримувати тимчасові паролі.

4.3 Забороняється використання будь-яких додатків (наприклад TeamViewer), завдяки яким можно підключитися до свого ПК віддалено, окрім підключення через OpenVPN канал.

4.4 Забороняється передавати логін та пароль будь-кому, навіть членам родини.

2.1.7 Політика використання VPN

1) Опис

Політика використання VPN визначає вимоги щодо користування VPN у ПП «Лата».

2) Призначення

Метою цієї політики є визначення правил для VPN-підключень до корпоративної мережі ПП «Лата».

3) Область застосування

Політика використання VPN поширюється на весь персонал ПП «Лата».

4) Положення даної політики

4.1 Користувачі VPN не повинні допускати несанкціонованого доступу інших користувачів до внутрішніх мережевих ресурсів підприємства.

4.2 Коли VPN-підключення активно, весь вихідний і вхідний трафік комп'ютера має йти через OpenVPN канал; інший трафік скидається.

4.3 Заборонено використання подвійного тунелювання; дозволено тільки одне підключення до мережі.

4.4 VPN-шлюзи мають налаштовуватися і обслуговуватися системним адміністратором та власником системи (директор підприємства).

4.5 Всі комп'ютери, підключені до локальної мережі підприємства через OpenVPN канал, повинні використовувати найактуальніше антивірусне ПЗ (*https://us.norton.com/products/norton-360-lifelock-ultimate-plus*).

4.6 Якщо OpenVPN канал не використовується, то його необхідно відключити.

2.1.8 Політика забезпечення збереженості засобів та носіїв інформації від викрадення або руйнування

1) Опис

Політика забезпечення збереженості засобів та носіїв інформації від викрадення або руйнування визначає правила щодо забезпечення безпеки цілісності інформації на ПП «Лата».

2) Призначення

Метою цієї політики є забезпечення цілісності інформації на ПП «Лата».

3) Область застосування

Політика забезпечення збереженості засобів та носіїв інформації від викрадення або руйнування поширюється на весь персонал ПП «Лата» та на всю КЗ.

4) Положення даної політики

4.1 У кожному приміщені офісу підприємства має бути встановлений робочий датчик диму, який у разі раптового загоряння надішле сигнал на пульт сигналізації, проінформувавши о пожежі.
Таким чином вдасться оперативно зреагувати на інцидент та мінімізувати збитки.

4.2 На вікнах офісу підприємства повинні бути встановлені решітки. Таким чином зловмисник практично не зможе потрапити до офісу компанії через вікна.

4.3 У разі втрати ключ-картки, співробітник має негайно повідомити про це директора підприємства та з його згоди отримати нову ключ-картку на пункті охорони.

4.4 Доступ до офісу підприємства можливий лише у разі наявності ключ-картки, яка ідентифікує працівника компанії або у разі отримання тимчасового пропуску на пункті охорони.

2.1.9 Політика резервного копіювання

1) Опис

Політика резервного копіювання задає основні цілі і завдання резервного копіювання, вимоги до нього та обгрунтовує його необхідність.

2) Призначення

Метою цієї політики є забезпечення безпеки процедури резервного копіювання даних та їх збереження. А також розмежування доступу до збережених даних та забезпечення контролю системи та процесу резервного копіювання.

3) Область застосування

Політика резервного копіювання поширюється на всю інформацію, яка циркулює у ПП «Лата».

4) Положення даної політики

4.1 При роботі з даними необхідно їх збереження у три резервні копії, в двох форматах зберігання, з яких, мінімум одна повинна зберігатися в фізично окремому місці.

4.2 Перед тим, як щось копіювати, необхідно це перевіряти через процес відновлення.

4.3 Усі оброблювальні данні повинні копіюватися.

4.4 Всі канали повинні бути зашифровані. Зберігатися можуть чутливі дані (дані авторизації тощо).

4.5 Повинно бути забезпечено резервування даних, як мінімум 1 раз на добу.

4.6 Повинна бути можливість шифрувати призначені для користувача резервні копії секретним ключем на робочому ПК співробітника, без можливості розшифровки на сервері.

4.7 Повинна бути можливість реплікації копій для конкретного хмарного сховища з шифруванням бекапів.

4.8 Резервне копіювання повинно виконуватись за розкладом та за запитом.

2.1.10 Політика розмежування прав доступу

1) Опис

Політика розмежування прав доступу встановлює правила доступу користувачів системи (персоналу ПП «Лата») до інформації, яка циркулює у компанії.

2) Призначення

Метою цієї політики є надання прав доступу до інформації.

3) Область застосування

Політика резервного копіювання поширюється на весь персонал ПП «Лата».

4) Положення даної політики

4.1 Кожен працівник підприємства має свій унікальний логін та пароль. Право видачі логіну/паролю надається системному адміністратору (зі згоди власника системи, тобто директора компанії).

4.2 Скомпрометовані або застарілі атрибути користувачів повинні негайно видалятися та змінюватися на нові.

4.3 За всі зміни ПЗ, створення резервних і архівних копій несе

відповідальність системний адміністратор, але його робота повинна бути контрольована з боку власника системи (директора).

4.4 Для кожного співробітника повинно бути робоче місце, який несе відповідальність за працездатність свого ПК та дотримується вимог щодо захисту обробки інформації. Співробітник підприємства повинен бути ознайомлений з усіма відповідними інструкціями, який повинен надавати системний адміністратор (у разі відсутності адміністратора безпеки).

5) Розробка матриці керування доступом

При створенні матриці кервування доступом виділюються об'єкти та суб'єкти доступу. Суб'єктами доступу є персонал ПП «Лата», об'єктами доступу вважається інформація, шо циркулює в ІТС.

Суб'єкти доступу:

- S1 – директор
- S2 – системний адміністратор
- S3 – бухгалтер
- S4 – розробники
- S5 – працівники тех.підтримки
- S6 – тестувальники

Об'єкти доступу:

- O1 – Організаційно-розпорядча документація
- O2 – Облік внутрішніх документів (накази, службові записки, інструкції)
- O3 – Інформація про надання послуг та контактна інформація підприємства
- O4 – Інформація про персонал підприємства

- О5 – Документи на дозвіл ведення підприємницької діяльності
- О6 – Облік та реєстрація вхідних та вихідних документів організації
- О7 – Трудові договори працівників
- О8 – Договори з клієнтами по наданню послуг
- О9 – База даних клієнтів
- О10 – Дані про рахунки клієнтів (номера банківських рахунків тощо)
- О11 – Заявки на розірвання договору по наданню послуг
- О12 – Фінансові звіти підприємства
- О13 – Відомості постачальників послуг (постачання питної води, тарифи за газ/воду/інтернет тощо)
- О14 – Плани закупівель
- О15 – Вихідні коди програм, які розроблюються на підприємстві
- О16 – Повна характеристика комп'ютерної техніки (характеристики, серійний номер тощо)
- О17 – Зміст та характер договорів, контрактів однією із сторін яких виступає підприємство
- О18 – База вхідних цін
- О19 – Інформація по ліцензійне ПО
- О20 – Звіт про виконання ремонтних послуг офісної техніки
- О21 – Відомості про створення сертифіката клієнта
- О22 – Формування та відправка пакетів звітності в електронному вигляді по електронній пошті з використання криптографічного захисту
- О23 – Відомості про генерацію ключів ЕЦП
- О24 – Формування та ведення реєстру форм звітних документів

- О25 – Відомості щодо тестування програм, що розробляються на підприємстві (результати тестування, виявленні баги/фічі, план тестування тощо)
- О26 – Інструкції щодо використання VPN, забезпечення захисту інформації на підприємстві, відомості про віддалене підключення до робочого столу тощо
- О27 – Відомості про підтримку вже випущеного продукту

Операції з файлами:

- Ч – читання
- З – зберігання
- Д – друкування
- К - копіювання
- ЗН – знищення
- М – модифікація

Таблиця 19

	О1	О2	О3	О4	О5	О6	О7	О8	О9
S1	Ч,З,Д,М,З Н,К	Ч,З,Д	Ч,З,Д,М,З Н,К	Ч,З,Д,З Н, М	Ч,З,Д,К, ЗН, М	Ч,З,Д,К, М, ЗН	Ч,З,Д,К, М	Ч,З,Д,К, ЗН, М	Ч,З,Д,К, ЗН, М
S2	Ч,К,З	Ч,З,Д	Ч,З,Д	Ч,З,Д	Ч	-	-	Ч,З,Д	Ч,З,Д
S3	Ч,К,З	Ч,З,Д	Ч,З,Д	Ч,З,Д, К, М	Ч,З,Д,К	Ч,З,Д	Ч,З,Д,К, ЗН, М	Ч,З,Д,К, ЗН, М	Ч,З,Д,К
S4	Ч,К,З	Ч,З,Д	Ч,З,Д	Ч,З,Д	Ч	-	-	Ч,З,Д	Ч,З,Д
S5	Ч,К,З	Ч,З,Д	Ч,З,Д	Ч,З,Д	Ч	-	-	Ч,З,Д	Ч,З,Д
S6	Ч,К,З	Ч,З,Д	Ч,З,Д	Ч,З,Д	Ч	-	-	Ч,З,Д	Ч,З,Д
	О10	О11	О12	О13	О14	О15	О16	О17	О18
S1	Ч,З,Д,К, М, ЗН	Ч,З,Д,К,М, ЗН	Ч,З,Д,К,М, ЗН	Ч,З,Д,К, М, ЗН	Ч,З,Д,К, М, ЗН	Ч,З,Д,К, М, ЗН	Ч,З,Д,К, М, ЗН	Ч,З,Д,К, М, ЗН	Ч,З,Д,К, М, ЗН
S2	-	Ч	-	Ч,З,Д	Ч,М,З	Ч,З,Д,К	Ч,З,Д,К, М	Ч,З,Д	-
S3	Ч,З,Д,К, М, ЗН	Ч,З,Д,К	Ч,З,Д,К,М, ЗН	Ч,З,Д,К	Ч,З,Д,К, М	-	Ч,З,Д	Ч,З,Д,М, К	Ч,З,Д,К, М, ЗН
S4	-	Ч	-	Ч,З,Д	Ч	Ч,З,Д,К, М, ЗН	Ч,З,Д	Ч,З,Д	-
S5	-	Ч	-	Ч,З,Д	Ч	Ч,З,Д,К, М	Ч,З,Д	Ч,З	-
S6	-	Ч	-	Ч,З,Д	Ч	Ч,З,Д,К	Ч,З,Д	Ч,З	-
	О19	020	021	022	023	024	025	026	027
S1	Ч,З,Д,К, М, ЗН	Ч,З,Д,К,М, ЗН	Ч,З,Д,К,М, ЗН	Ч,З,Д,К, М, ЗН	Ч,З,Д,К, М, ЗН	Ч,З,Д,К, М, ЗН	Ч,З,Д,К, М, ЗН	Ч,З,Д,К, М, ЗН	Ч,З,Д,К, М, ЗН
S2	Ч,З,Д,К, М	Ч,З,Д,К	Ч,З,Д,	Ч,З,Д,К, М, ЗН	Ч,З,Д,К, М, ЗН	Ч,З,Д,К	Ч,З	Ч,З,Д,К, М	Ч,З,Д
S3	Ч,З,Д,К	Ч,З,Д,К,М,	Ч,З,Д,К	-	Ч,З,Д	Ч,З,Д,К, М, ЗН	-	-	Ч,З,Д
S4	Ч,З,Д,К	Ч,З	Ч,З,Д	Ч,З,Д,К, М, ЗН	Ч,З,Д	Ч,З,Д,К	Ч,З,Д,К	Ч,З	Ч,З,Д,К, М
S5	Ч,З,Д,К	Ч,З	Ч,З,Д	Ч,З,Д,К, М, ЗН	Ч,З,Д	Ч,З,Д,К	Ч,З,Д,К, М, ЗН	Ч,З	Ч,З,Д,К, М
S6	Ч,З,Д,К	Ч,З	Ч,З,Д	Ч,З,Д,К, М, ЗН	Ч,З,Д	Ч,З,Д,К	Ч,З	Ч,З	Ч,З,Д,К, М, ЗН

2.1.11 Політика електронного документообігу

1) Опис

ЕЦП (електронно-цифровий підпис) – це інформація в електронній формі, яка поєднана до іншої інформації в електронній формі або іншим чином пов'язана з такою інформацією і яка використовується для визначення особи, яка підписує інформацію.

2) Призначення

Метою цієї політики є забезпечення авторства та гарантії того, що документ не був змінений.

3) Область застосування

Політика електронного документообігу поширюється на весь персонал ПП «Лата».

4) Положення даної політики

4.1 Всі співробітники повинні ознайомитись з політикою електронного документообігу та підписати її прийняття своїм підписом (у письмовому вигляді).

4.2 Регулярно (раз на місяць) проводити збори серед персоналу, які будуть присвячені сучасному документообігу. Відповідальним за проведення зборів назначається директор підприємства.

4.3 Для роботи ЕЦП потрібен центр сертифікації, який буде виконувати функцію по створенню та видачі сертифікатів ключей перевірки електронних підписів. Рекомендований центр сертифікації *https://shop.yt.ua/uk/page/acsk*

ВИСНОВКИ ДО РОЗДІЛУ ІІ

Отримані результати з першого розділу були використані у розробці політик безпеки для ПП «Лата», які мусять забезпечити мінімізацію загроз системи та ризики завдання збитків компанії.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Застосування концепції безпеки програмних продуктів для електронної торгівлі, включаючи OMS та EMS платформи для глобальних акцій, фьючерсів, опціонів та фіксованого доходу потребує обґрунтування економічної її доцільності, виходячи з аналізу витрат на розробку та впровадження. Тому метою економічного розділу є аналіз економічної ефективності розробки програмних продуктів для електронної торгівлі, включаючи OMS та EMS платформи для глобальних акцій, фьючерсів, опціонів та фіксованого доходу приватного підприємства «Лата». Для цього необхідно здійснити розрахунок:

– капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення;

– річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування;

– річного економічного ефекту;

– показників економічної ефективності розробки та впровадження розробки сертифікованого підключення мобільних користувачів до інтрамережі підприємства.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

До капітальних витрат належать витрати на розробку політики безпеки інформації, які визначаються виходячи з трудомісткості розробки політики безпеки інформації.

Визначення трудомісткості розробки політики безпеки інформації

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

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

де $tmз$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$tв$ – тривалість розробки концепції безпеки інформації у організації;

ta – тривалість процесу аналізу ризиків;

$tвз$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$tозб$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$tовр$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$tд$ – тривалість документального оформлення політики безпеки.

Визначено, що відповідно до етапів розробки політики безпеки інформації, тривалість операцій складає наступні величини: $t_{тз}$=20 годин, $t_{в}$=30 годин, $t_{тз}$=15 годин, $t_{вз}$=10 годин, $t_{озб}$=10 годин, $t_{овр}$=6 годин, $t_{д}$=6 годин.

Отже, t=20+30+15+10+10+6+6= 97 годин,

Розрахунок витрат на створення політики безпеки інформації

Витрати на розробку політики безпеки інформації Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації Змч.

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 55000+ 500= 60000 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 97*610 = 27300 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

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

$$З_{мч}= t*С_{мч}=97*5,15=500 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = 0,8 * 15 * 1,1 + (15600 * 0,3)/1920 + (5770 * 0,1)/1920 = 15,94 \text{ грн.}$$

Відповідно до розроблених рекомендації щодо застосування розробки у інтрамережі підприємства ПП «Лата» планується додатково придбати антивірусне ПЗ Norton 360 Premium, проксі сервер nginx Enterprise, який буде використовуватись з вже наявним Ubuntu Server 16.

Таким чином, капітальні (фіксовані) витрати на створення політики безпеки інформації:

$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = 149385$ грн.

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

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

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

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

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

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

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \text{ грн.}$$

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

$С_{к}$ - витрати на керування системою в цілому;

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

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{ел} + С_{о} + С_{тос}, \text{ грн.}$$

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

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

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

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

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 50000 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо налаштувань інфраструктури безпечних підключень мобільних користувачів до інтрамережі підприємства потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$С_з$ = (50000*12 + 50000*12*0,1)*0,25= 165000 грн.

З 01.01.2019 р. Ставка ЄСВ для всіх категорій платників складає 22%.

$$С_{єв} = 165000 * 0,22 = 36300 \text{ грн.}$$

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

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.,}$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1,4 кВт);

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

$С_е$ – тариф на електроенергію, ($С_е$ = 1,64 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 1,4*1920*1,8 = 4838,4 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1% (Стос = 149385*0,01=1493,85 грн).

Річний фонд амортизаційних відрахувань (Са) за прямолінійним методом для ПЗ склад два роки тобто:

$$Са = 72400/2 = 31200 \text{ грн.}$$

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

$$С_к = 15000+165000+36300+4838,4+1493,85+31200 = 253832,25 \text{ грн.}$$

Отже, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = 320462,25 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 75081 грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

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

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 2 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 1 години;

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

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 18000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 23000 грн./міс.;

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

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 14 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 5000000 грн. у рік;

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

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 30.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

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

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

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

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

$$П_п = (\sum З_с/F) * t_n = (23000 * 12)/176)) * 2 = 3136{,}36 \text{ грн.}$$

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

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

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

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

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

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

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

$$Пви = (\sum З_с/F) * t_{ви} = (23000 * 12)/176)) * 4 = 6272{,}72 \text{ грн.}$$

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

$$Ппв = (\sum З_о/F) * t_в = (18000 * 12)/176)) * 1 = 1227{,}27 \text{ грн.}$$

Витрати на заміни встаткування або запасних частин можуть скласти 1600 грн.

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

$$П_в = 6272,72 + 1227,27 + 5000 = 12499,99 \text{ грн.}$$

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

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

$$V = (5000000/2080) * (2 + 1 + 4) = 16826,92 \text{ грн.}$$

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.

$$U = 3136,36 + 12499,99 + 16826,92 = 32462,28 \text{ грн.}$$

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

$$B = \sum_1 \sum_{30} 32462,28 = 973868,4 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \text{ грн.},$$

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

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (60%);

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 973868,4*0,6 – 320462,25 = 263858,79 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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

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

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

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = 263858,79 /149385 = 1,77 \text{ частки одиниці}$$

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

$$ROSI > (N_{деп} – N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (20%);

$N_{інф}$ – річний рівень інфляції, (15%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$1,77 > (20 – 15)/100 = 1,77 > 0,05.$$

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

$$To = K/E = 1/ROSI = 1/1,77 = 0,56 років$$

ВИСНОВКИ ДО РОЗДІЛУ ІІІ

Розробка програмних продуктів для електронної торгівлі, включаючи OMS та EMS платформи для глобальних акцій, фьючерсів, опціонів та фіксованого доходу приватного підприємства «Лата» є економічно доцільним, оскільки коефіцієнт повернення інвестицій ROSI складає 1,86 грн./грн., що означає отримання 1,86 грн. економічного ефекту на кожну гривню капітальних вкладень на розробку конфігурації налаштувань інфраструктури безпечних підключень мобільних користувачів до інтрамережі підприємства. Отримане значення коефіцієнту повернення інвестицій вище дохідності альтернативного вкладення коштів. Термін окупності при цьому складатиме 0,56 років (біля 5 років 6 місяців). Капітальні витрати складають 149385 грн.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було розглянуто сучасний стан інформаційної безпеки та приведена статистика злочинів, які були скоєні у попередніх роках. Зазначена актуальність розвитку кібербезпеки. Обґрунтовано потребу у створенні КСЗІ на підприємстві для запобігання НСД до важливих ресурсів системи. До етапів створення КСЗІ, що використані в роботі віднесені: обґрунтування необхідності створення, обстеження на ОІД та розробка політики безпеки. В результаті проведеного обстеження ОІД побудовано модель порушника та модель загроз, які присутні у даній ІТС, було класифіковано інформацію, що зберігається і циркулює на підприємстві та виявлено ресурси, які потребують найбільшого рівня інформаційної безпеки, обрано профіль захищенності, який має функціонувати для даного підприємства.

Отримані результати були використані у розробці політик безпеки для приватного підприємства «Лата». Також була проаналізована економічна доцільність діяльності підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

- ЗАКОН УКРАЇНИ Про інформацію [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12
- ЗАКОН УКРАЇНИ Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94%D0%B2%D1%80
- ЗАКОН УКРАЇНИ Про основні засади забезпечення кібербезпеки Украіи [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19
- ЗАКОН УКРАЇНИ Про захист персональних даних [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17
- Данні компанії Positive technologies [Електронний ресурс] – Режим доступу до ресурсу: https://www.ptsecurity.com/ru/research/analytics/cybersecurity-threatscape-2019/
- Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі НД ТЗІ 3.7-003-05 [Електронний ресурс] – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074&cat_id=38835
- Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=15FDA2B2745B1390AC937214804F2E76?showHidden=1&art_id=102089&cat_id=89734&ctime=1344502332348
- Norton 360 with LifeLock Ultimate Plus [Електронний ресурс] – Режим доступу до ресурсу: https://us.norton.com/products/norton-360-lifelock-ultimate-plus
- Как защитить сервер от DDoS-атаки [Електронний ресурс] – Режим доступу до ресурсу: https://vps.ua/wiki/how-to-protect-server-from-ddos/
- Центр сертифікації ключів "Україна" [Електронний ресурс] – Режим доступу до ресурсу: https://shop.yt.ua/uk/page/acsk

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	**Формат**	**Найменування**	**Кількість листів**	**Примітки**
Документація				
1	А4	Реферат	6	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	4	
4	А4	Вступ	3	
5	А4	Стан питання. Постановка задачі	48	
6	А4	Спеціальна частина	21	
7	А4	Економічний розділ	10	
8	А4	Висновки	5	
9	А4	Перелік посилань	10	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація Колодій.ppt

2 Диплом Колодій.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ Пілова Д.П.

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-16-1 Колодія Є.С.

на тему: «*Політика безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства «Лата»*»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 103 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на забезпечення ефективного захисту інформації в АС, методами модифікації вже існуючої системи а також розробкою політики безпеки підприємства.

При виконанні роботи автор продемонстрував достатньо високий рівень теоретичних знань і практичних навичок. На основі обстеження підприємства та аналізу профіля захищеності у ній було сформульовані задачі, вирішенню яких присвячений спеціальний розділ. У ньому було запропоновано ряд рішень які спрямовані на мінімізацію загроз які були виявленні і розроблено політики безпеки.

Практична цінність роботи полягає в тому, що запропоновані рішення можна використати для покращення ефективності захисту інформації в конкретному приватному підприємстві.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Колодій Є.С. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник кваліфікаційної роботи

Керівник спец.розділу