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 *Ткачука Владислава Ігоровича*

академічної групи *125-18-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Створення комплексної системи захисту інформації підприємства "CleverPath"*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. каф. БІТ Сафаров О.О.			
розділів:				
спеціальний	к.т.н., доц. каф. БІТ Сафаров О.О.			
економічний				

Рецензент	к.е.н., доц. Пілова Д.П.			

Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту _____ **академічної групи** _____
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації _____

за освітньо-професійною програмою *Кібербезпека*

на тему *Створення комплексної системи захисту інформації підприємства "CleverPath"*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від _____№ _____

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Обстеження інформаційно-телекомунікаційної системи «CleverPath»	
Розділ 2	Створення КСЗІ.	
Розділ 3	Техніко-економічне обґрунтування доцільності запровадження КСЗІ.	

Завдання видано _____ Сафаров О.О.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Ткачук В.І.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 89 ст., 12 рис., 22 табл., 3 додатків, 14 джерел.

Об’єкт розробки: інформаційно-телекомунікаційна система ТОВ “CleverPath”.

Предмет розробки: створення комплексної системи захисту інформації інформаційно-телекомунікаційної системи ТОВ “CleverPath”.

Мета кваліфікаційної роботи: розробка рішень щодо захисту від загроз інформаційної безпеки в інформаційно-телекомунікаційної системі ТОВ “CleverPath”.

У першому розділі роботи, обґрунтовується створення КСЗІ, надано загальні відомості про об’єкт та його ІТС. Виконано акт обстеження об’єкту та визначено перелік властивостей, джерел загроз та загроз.

У другому розділі, розробляються та наводяться рішення спрямовані на усунення загроз, визначених в першій частині.

В третьому розділі, проводяться розрахунки витрат на розробку, впровадження та експлуатацію КСЗІ. Обчислюється доцільність впровадження створеної КСЗІ.

Практичне значення роботи полягає в розробці та розрахунку доцільності впровадження актуальної комплексної системи захисту інформації для підприємства “CleverPath”.

РЕФЕРАТ

Пояснительная записка: 89 с., 12 рис., 22 табл., 3 приложений, 14 источников.

Объект разработки: информационно-телекоммуникационная система ООО “CleverPath”.

Предмет разработки: создание комплексной системы защиты информации информационно-телекоммуникационной системы ООО “CleverPath”.

Цель квалификационной работы: разработка решений по защите от угроз информационной безопасности в информационно-телекоммуникационной системе ООО “CleverPath”.

В первом разделе роботы, обосновывается создание КСЗИ, надаются общие ведомости про объект и его ИТС. Исполнен акт обследования объекта и определён перечень особенностей, источников угроз и угроз.

Во втором разделе, разрабатываются и приводятся решения, направленные на устранение угроз, определённых в первой части.

В третьем разделе, проводятся расчёты затрат на разработку, введение и эксплуатацию КСЗИ. Рассчитывается целесообразность введения разработанной КСЗИ.

Практическое значение работы состоит в разработке и расчётах целесообразности введения актуальной комплексной системы защиты информации для предприятия “CleverPath”.

ABSTRACT

Explanatory note: 89 p., 12 fig., 22 tables., 3 applications, 14 sources.

Object of study: information and telecommunication system LTD “CleverPath”.

Project Objective: development of a comprehensive system for the protection of information technology and telecommunication systems of LTD “CleverPath”.

The purpose of the qualification work: working out the solution for the threat of information security in the information and telecommunication systems of LTD “CleverPath”.

In the first section of the work, the creation of IISS is justified, general information about the object and its ITS is given. The act of monitoring the facility was drawn up and a list of features, sources of threats and threats was defined.

In the second section, means of preventing the threats defined in the first part are developed and presented.

In the third section, the development cost for the development, implementation and operation of IISS is calculated. The expediency of implementing IISS is calculated.

The practical significance of the work is in the development and calculations of the feasibility of implementation of a relevant integrated information security system for the “CleverPath” enterprise.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АС – Автоматизована система;

ПЗ – Програмне забезпечення;

КСЗІ – Комплексні система захисту інформації;

ОІД – Об’єкт інформаційної діяльності;

КЗ – Контрольована зона;

ПК – Персональний комп’ютер;

ІТС – Інформаційно-телекомунікаційна система;

КСІБ - Комп'ютерної системи інформаційної безпеки;

ТОВ – товариство з обмеженою відповідальністю;

ЗМІСТ

ВСТУП

Збільшення об’ємів оброблюваної інформації, зростання вимог що до її доступності та впровадження цифрових технологій призводить до впровадження АС для зберігання та обробки інформації в усіх галузях. Це в свою чергу призводить до виникнення та поширення нових загроз безпеці інформації.

Згідно з Нормативним документом Систем технічного захисту інформації «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу» : «Захист інформації в АС (information protection, information security, computer system security) — 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.»[1]

Таким чином до захисту інформації входить не лише захист інформації, а й самої АС та збереження доступності інформації.

Через активний і стрімкий розвиток АС і в технічному плані і з огляду на ПЗ, що використовується, так само змінюються і виникають нові загрози. Відповідно виникають та вдосконалюються методи та засоби протидії актуальним загрозам.

Як наслідок виникає ситуація коли загроза може мати різні, ефективні засоби протидії, чи напроти нова загроза не матиме перевірених та перевірених рішень. Саме тому проведення робіт з аналізу КСЗІ, їх оновлення та актуалізація мають проводитися регулярно.

РОЗДІЛ 1. ПРОВЕДЕННЯ ОБСТЕЖЕННЯ ОБ'ЄКТА

1.1 Обґрунтування розробки КСЗІ

Компанія "CleverPath" розробляє та реалізує ПЗ для мобільних пристроїв та веб-сайтів.

Діяльність компанії спрямована на реалізацію ПЗ закордонним споживачам. Як наслідок, переважна кількість договорів, що укладається під час реалізації ПЗ, є договорами, укладеними на відстані[2]. Так само реалізація та розповсюдження продукції відбувається з використанням інформаційно-телекомунікаційних систем.

Згідно із Законом України «Про інформацію»[4], інформація, що зберігається та обробляється в АС компанії поділяється на:

1. Інформацію про фізичну особу або персональні данні;
2. Інформацію про товар;
3. Податкову інформацію;
4. Статистичну інформацію.

Згідно із Законом України «Про інформацію»[4] та внутрішнім статутом компанії про інформацію і документообіг, ця інформація може мати наступні рівні доступу:

1. Інформація з відкритим доступом;
2. Конфіденційна інформація;
3. Комерційна таємниця.

Таким чином, згідно із вимогами діючого законодавства, що затверджують необхідність обмеження доступу, забезпечення цілісності та доступності для певних видів інформації, створення КСЗІ є необхідним.

КСЗІ буде спрямована на забезпечення цілісності та безпеки інформації, унеможливлювати несанкціонований доступ до неї. Система повинна включати в себе організаційні заходи, інженерно-технічні та програмно-технічні заходи за для надання максимально можливого та необхідного рівня захисту.

1.2 Ситуаційний план об’єкта

Об’єктом інформаційної діяльності є будівля в якій знаходиться компанія

"CleverPath". Розташована за адресою Україна, м. Дніпро, площа Вокзальна, 2д.

ОІД це адміністративна триповерхова будівля. Будівля збудована із цегла та бетонних конструкцій. Дах будівлі викладено з металочерепиці, стійкої до температурного та природнього впливу і яка є вогнестійкою.

Будівля є новою і відповідає всім чинним державним будівельним нормам України.

Навколо будівлі, де знаходиться ОІД розташовані наступні об’єкти:

- На півночі, знаходиться парковка для співробітників;
- На півночі, поруч із парковкою, розташована така сама адміністративна триповерхова будівля, позначена як 2;
- За адміністративною будівлею (2), знаходиться двоповерхова адміністративна будівля (15);
- На сході, перед будівлею ОІД, знаходиться пішохідна зона, спільна для ОІД і будівлі 2;
- На сході, знаходиться двоповерхова адміністративна будівля (5), що має одноповерхову прибудову (10);
- На сході, в притулок до прибудови (10) розташована двоповерхова адміністративна будівля (11);
- На сході, південніше, розташована трансформаторна будка (7);
- За трансформаторною будкою (7), розташована двоповерховий господарський комплекс (14);
- Від прибудови (10) до адміністративна будівля (14) розташовано бетонний паркан 2 метри заввишки;

- За господарським комплексом (14), знаходиться адміністративна будівля, що має чотири поверхи (12), та має частину з дев'ятьма поверхами (13);
- На південному сході, розташований двоповерховий господарський корпус (8) із одноповерховою прибудовою (9);
- Від господарського комплексу (14) до господарського корпусу (8) розташовано бетонний паркан 2 метри заввишки;
- За господарським корпусом (8) і його прибудовою (9), продовжується адміністративна будівля (12), і має п'ятиповерхову частину (4)
- На півдні та заході розташовані зелені насадження, що включають в себе високі дерева із пишною кроною;
- На півдні, заході та сході, пішохідна зона обнесена сітчастим парканом заввишки в 2 метри, що проходить по границі із зоною зелених насаджень та парковки;
- На півдні, заході та північному заході, розташована п'ятиповерхова житлова будівля (3) із шестиповерховою частиною (6).

Нижче наведено ситуаційний план рис.1.1 та характеристику споруд табл. 1.1, що оточують ОІД.

На території ОІД проходять наступні системи комунікацій:

- Лінії систем електропостачання;
- Лінії пожежної сигналізації;
- Лінії охоронної сигналізації;
- Лінії комп'ютерної мережі;
- Лінії глобальної мережі інтернет;
- Системи водопостачання.

Рисунок 1.1 - Ситуаційний план об’єкта

Таблиця 1.1 – Характеристика споруд, що оточують ОІД

Позначення на плані	Найменування	Кількість поверхів	Адреса	Відстань до ОІД, м
1	Адміністративна будівля	3	Пл. Вокзальна, 2Д	ОІД
2	Адміністративна будівля	3	Пл. Вокзальна, 2Н	10
3	Житловий будинок	5	Пл. Вокзальна, 2	24
4	Адміністративна будівля	5	Пр-т. Дмитра Яворницького, 108	75
5	Адміністративна будівля	2	Пл. Вокзальна, 15Б	32
6	Житловий будинок	6	Пл. Вокзальна, 2	65
7	Адміністративна будівля	1	-	22
8	Громадський корпус	2	Пл. Вокзальна, 19	48
9	Громадський корпус	1	Пл. Вокзальна, 19	59
10	Адміністративна будівля	1	Пл. Вокзальна, 15Б	32
11	Адміністративна будівля	2	Пр-т. Дмитра Яворницького, 108А	36
12	Адміністративна будівля	4	Пр-т. Дмитра Яворницького, 108	68
13	Адміністративна будівля	9	Пр-т. Дмитра Яворницького, 108	57
14	Громадський корпус	2	-	27
15	Адміністративна будівля	2	Пл. Вокзальна, 15	36

Сітчастий паркан, що оточує ОІД на півдні, заході та сході, див мал. 1.1, має хвіртку, що веде до парковочного майданчику, із замком. Працівники, за бажанням, можуть отримати копію ключа від замку.

Зовнішнє КПП відсутнє, адже КЗ закінчується на межах адміністративної будівлі в якій розташовано ОІД.

Зовнішні камери відеоспостереження відсутні. Вхідні двері мають електронний замок, що відмикається цифровим кодом, відомим працівникам служби безпеки, та магнітними пропусками, що видаються усім співробітникам.

Увійти до ОІД за пропуском можливо лише в часи роботи, з шостої ранку до десятої вечора. В інші часи вхід на територію ОІД можливий за наявності дозволу від керівництвом та домовленості із працівниками служби безпеки.

При проведенні на територію ОІД особи, що не є працівником компанії, співробітник, що її привів несе безпосередню відповідальність за неї, та повинен супроводжувати її до моменту коли та покину об’єкт.

1.3 Опис фізичного середовища ОІД

ОІД, що обстежується знаходиться на першому та другому поверсі будівлі. На третьому поверсі будівлі знаходиться компанія розробник мобільних ігр. Фактично, з початку пандемії Covid 19, ця компанія переведена на дистанційну модель роботи, таким чином офіс на третьому поверсі не експлуатується.

До ОІД надходять лінії електроживлення, водопостачання та мережі інтернет. Лінії електроживлення та водопостачання підключені із західної частини будівлі. Мережа інтернет підключена зі півночі. На ОІД використовуються лише електричні прилади опалення, тому підключення до мережі опалення відсутнє.

Будівля ОІД завдовжки 24 метри та 12 метрів завширшки, і має загальну площу одного поверху в 288 метрів квадратних. Таким чином, загальна територія досліджуваного ОІД складає 576 метрів квадратних.

Товщина зовнішніх стін складених із цегли становить 30 см.

На західній стороні будівля має по чотири вікна на кожному поверсі. На північній та південній частинах розташовується по два вікна на кожному поверсі. На сході будівля має п’ять вікон на першому та по чотири вікна на інших поверхах. Вікна не мають гратів чи сигналізації. Вікна виконані зі стандартного однокамерного склопакету, та мають товщину в 24 мм.

ОІД має єдиний вхід-вихід на східній частині будівлі, та пожежні сходи розташовані на західній стороні. Вони доступні з головних сходів в середині будівлі та мають металеві двері із замком. Ключ знаходиться на пункті охорони.

Вхідні двері виготовлені із прозорого, зміцненого скла та мають металопластикову рамку. Напроти дверей, в фойє будівлі розташовано пункт охорони, де постійно знаходиться працівник служби безпеки. Це забезпечує

можливість спостереження як за входом безпосередньо, так і за невеликою територією поза межами будівля.

Пункт охорони розташовано під сходами на другий поверх. До пункту охорони надходять данні з камер відеоспостереження та датчиків диму встановлених на території ОІД. Працівники служби безпеки працюють в дві зміни, тим самим забезпечують цілодобовий нагляд.

З фойє можливо потрапити до сходів, що ведуть на другий поверх, в північну та південну частини ОІД. До північної та південної частини ведуть офісні двері виготовлені із ДСП матеріалів. На другому поверсі основне приміщення відділено від сходів матовою скляною стіною, з дверима зробленими із відповідного скла.

Усі перелічені двері обладнані магнітними замками аналогічними до встановленого на вхідній двері, проте без можливості вводу цифрового коду для відкриття. Можуть бути відімкнуті за допомогою магнітного пропуску.

На внутрішніх дверях встановлено контролер із вбудованим зчитувачем карт типу SEVEN CR-772M EM- Marin, на вхідних дверях встановлено контролер із вбудованим зчитувачем карт та кодовою клавіатурою типу SEVEN CR-775S EM-Marin.

Стіни фойє складені із цегли та мають товщину в 20 см.

В південній частині першого поверху двері ведуть до великої зали, що використовується для проведення масових заходів, презентацій для співробітників та в якості зони відпочинку. В залі, на стелі, встановлено проектор Epson EB-E10 White. Підключення до проектора відбувається за допомогою USB порту. В залі також встановлено маршрутизатор TP-Link Archer AX10. Розташування надає можливість покриття усієї території ОІД. Зал має чотири вікна, три з яких виходять на схід та одне на південь.

З «Зали для відпочинку» можна потрапити до «Кухні» та «Відділу HR». Обидві кімнати відгороджені скляними стінами з склопакету та мають матове

покриття і декоративні наліпки, для перекриття поля зору. Двері в данні кімнати виготовлені зі скла та металопластику і не мають замків.

В «Відділі HR» працює три співробітники та встановлена відповідна кількість ПК. Данні ПК мають вихід до глобальної мережі інтернет через маршрутизатор, розташований у «Залі для відпочинку». Усі інші ПК та пристрої можуть підключитися до мережі інтернет через даний маршрутизатор після введення паролю, який можна дізнатися у працівників відділу HR. Кімната має два вікна, одне з яких виходить на південь а інше на захід.

«Кухня» має холодильник, підключений рукомийник, два столи і шістнадцять стільців, робочу поверхню та куллер з водою. Тут зберігається набор медичної допомоги. В кімнаті є вікно, що виходить на захід.

В північній частині ОІД, за дверима з фойє знаходиться коридор, що веде до: вбиральні, «Відділу бухгалтерії», «Відділу продаж», складського приміщення, «Кабінету системного адміністратора», звичайної та малої «Переговорної зали». Всі приміщення, окрім вбиральні, відділяються одне від одного скляними стінами і дверима, аналогічними до використаних в південній частині ОІД.

Вбиральня, в свою чергу складена з цегли, має стіни в 20 см та двері з ДСП матеріалів, що можна зачинити чи відчинити з середини. Має встановлений бойлер, що постачає теплу воду для всього ОІД. Вікна відсутні.

В «Відділі бухгалтерії» працює чотири співробітники і встановлена відповідна кількість ПК. Також встановлено принтер HP LaserJet 135w, що під'єднано до всіх ПК в кімнаті через USB порт із використанням USB-хабу. Всі ПК підключені до мережі інтернет через окремі ethernet дроти та комутатор, що знаходиться в «Відділі продаж». В кімнаті є вікно, що виходить на захід.

У «Відділі продаж» працює сім співробітників та встановлена відповідна кількість ПК. Чотири з них додатково обладнані веб камерами та гарнітурою, що підключаються до ПК через USB на пряму. В відділі розташовано маршрутизатор, що надає доступ до мережі інтернет ПК в «Відділі бухгалтерії», «Відділі продаж», «Кабінеті системного адміністратора» та маршрутизатору в «Кімнаті відпочинку». Всі підключення виконані окремими дротами. В кімнаті є два вікна, одне з яких виходить ні захід а інше на північ.

Складське приміщення розташовано в кінці коридору та не має замку на двері. Використовується для зберігання технічних приладів. Побутової хімії та інших речей. Не має вікон.

«Кімната системного адміністратора» обладнана одним ПК відповідно до одного наявного на ОІД системного адміністратора. ПК має підключення до мережі інтернет через ethernet та комутатор в «Відділі продаж». В кімнаті є два вікна, одне з яких виходить на північ а інше на схід.

Обидві зали для переговорів мають лише столи та стільці, і використовуються для проведення співбесід, зустрічей та розмов із керівництвом та клієнтами. Обидві кімнати мають по одному вікну, що виходять на схід.

Скляні перегородки, що використовуються в якості стін мають звукоізоляцію, що не відрізняється від віконних склопакетів. Таким чином вони надають достатній, для комфортної праці та запобігання непомітного перехоплення аудіо інформації, рівень ізоляції звуку. А нанесене матове покриття та наліпки перекривають лінію обзору, що ускладнює візуальне перехоплення даних з моніторів ПК чи інших носіїв інформації.

Всі вікна на першому поверсі можливо відчинити, проте лише для провітрювання. На кожному вікні встановлено вертикальні жалюзі.

Відповідно до пори року, при настанні темного часу доби співробітники зобов’язані закрити жалюзі та ввімкнути штучне світло.

Відстань від полу до стелі в усіх приміщеннях складає 2,8 м. Стеля зроблена зі стандартних офісних металевих конструкцій, що кріпляться до фактичної стелі з бетонних конструкцій товщиною в 15 см. В утвореній порожнині проходить переважна більшість ліній комунікацій та електроживлення. В кімнати та до приладів ці лінії комунікації надходять по стінах, при цьому захищаються пластиковим коробом.

Нижче наведено генеральний план першого поверху ОІД з урахуванням ліній водопостачання, електроживлення, мережі та охоронної системи.

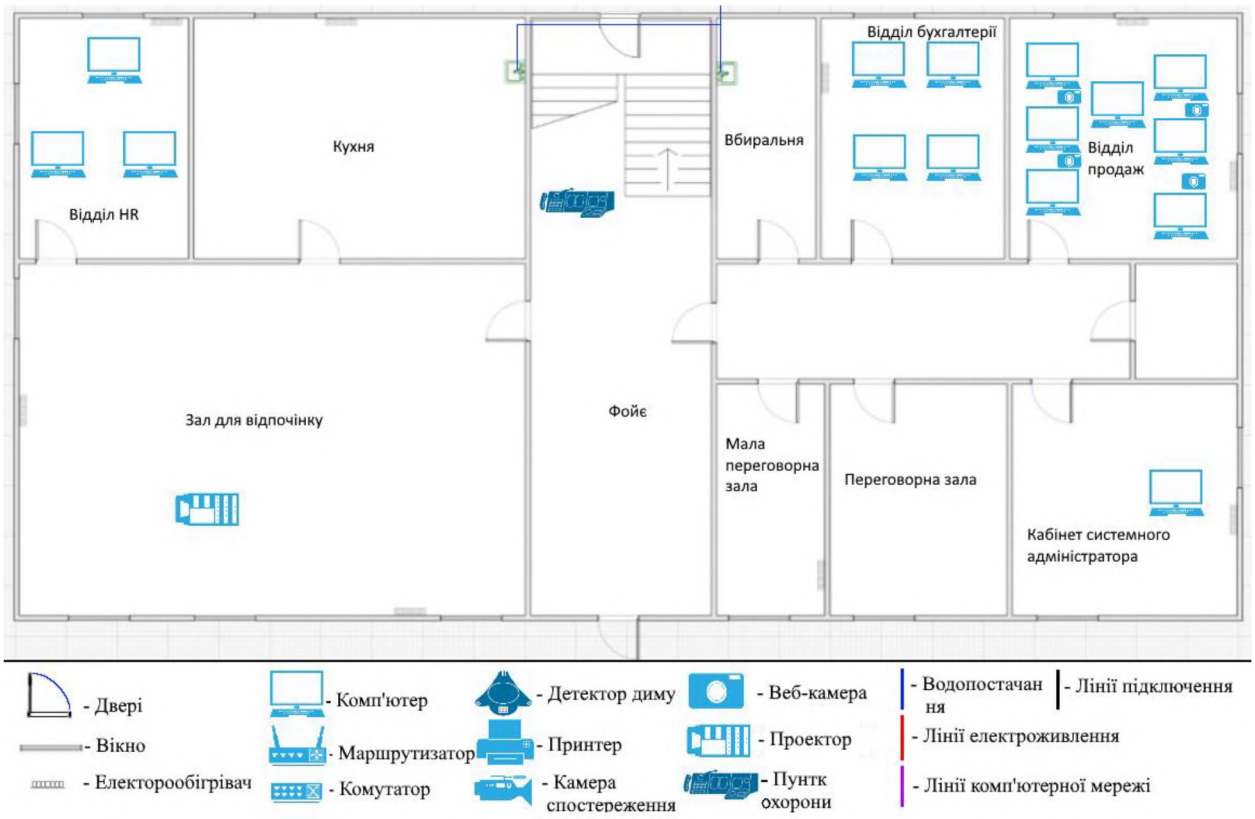

Рисунок 1.2 – Генеральний план першого поверху ОІД із лініями водопостачання

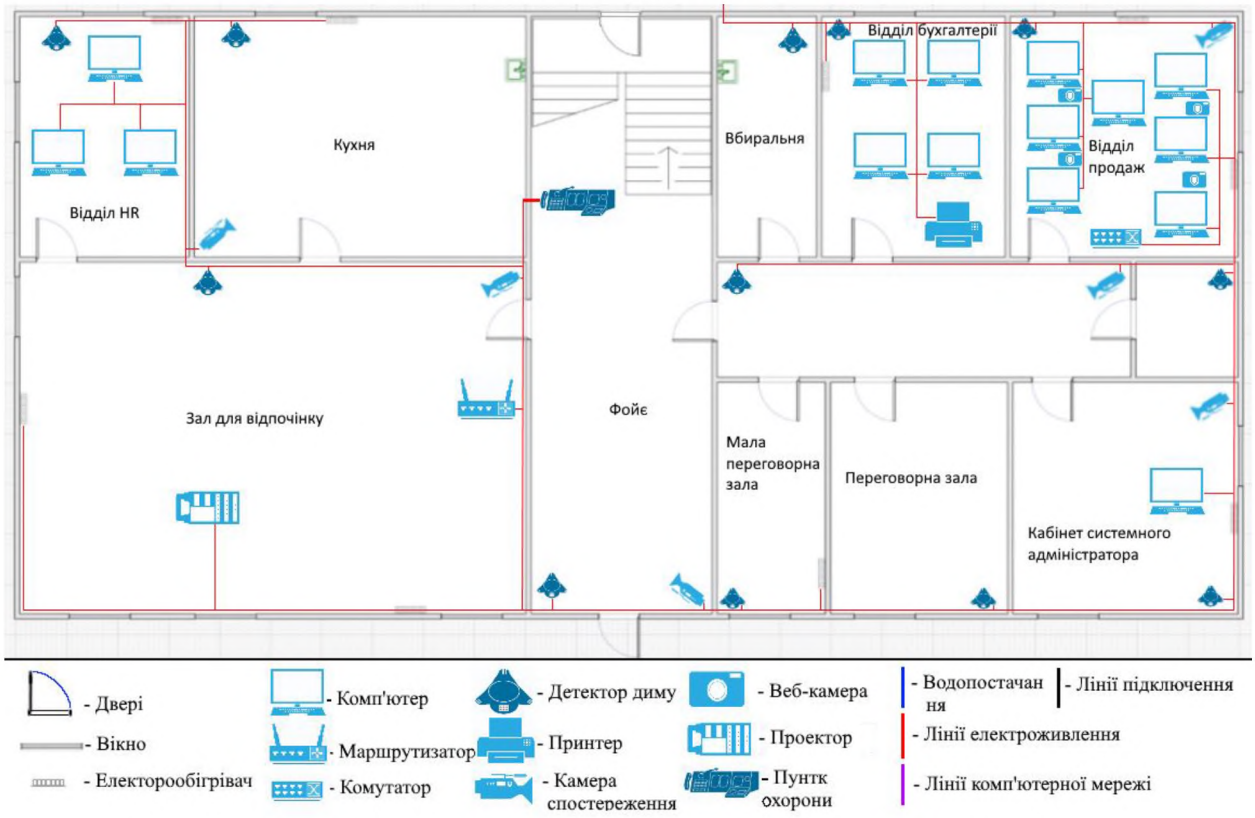

Рисунок 1.3 – Генеральний план першого поверху ОІД із лініями електроживлення

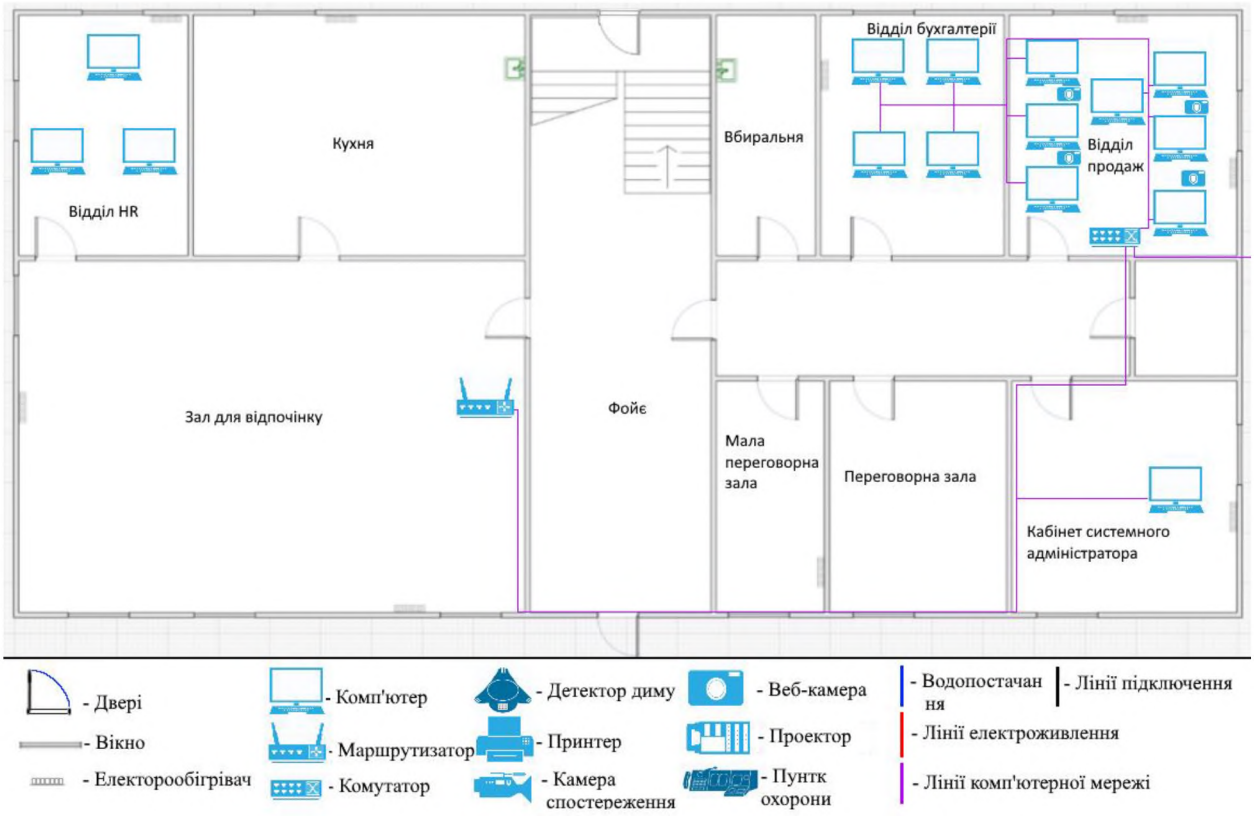

Рисунок 1.4 – Генеральний план першого поверху ОІД із лініями мережі

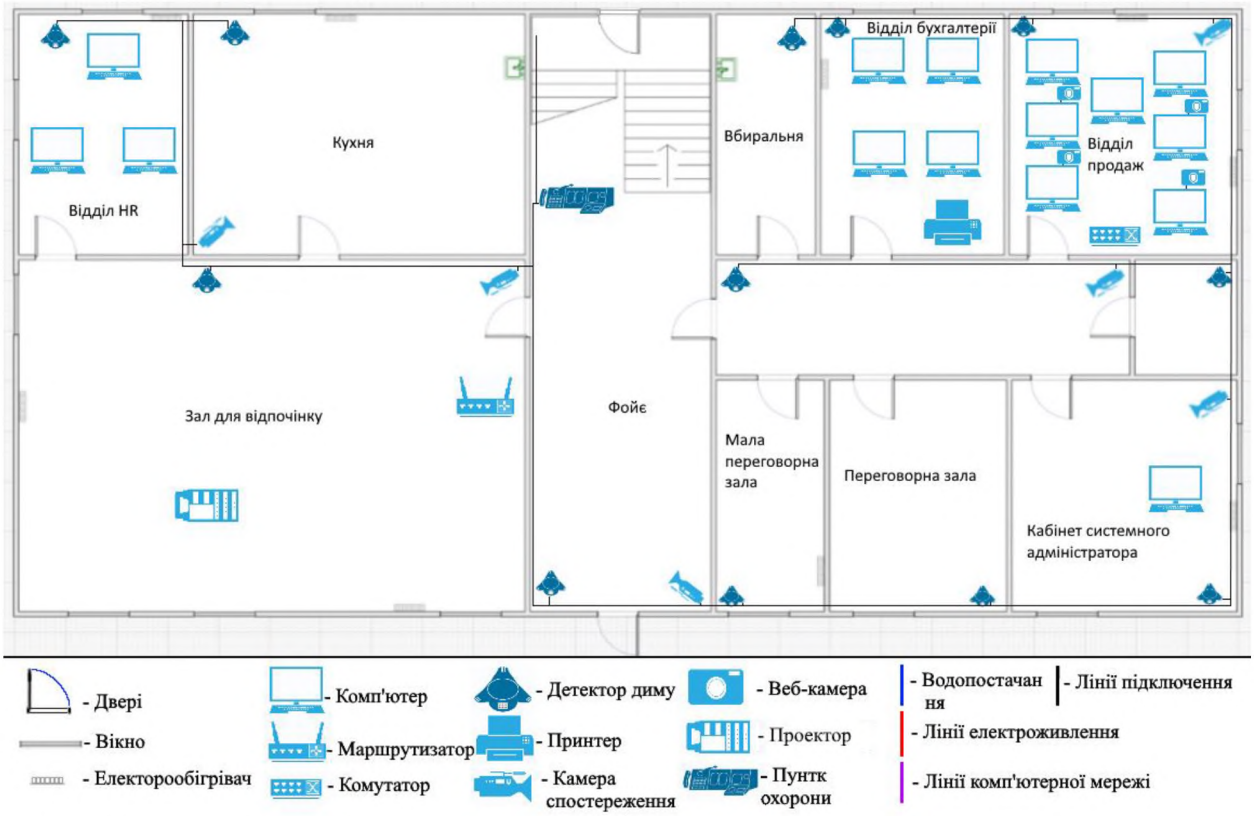

Рисунок 1.5 – Генеральний план першого поверху ОІД із лініями підключення охоронної системи

Згідно із рис. 1.5 в кожній кімнаті ОІД на першому поверсі встановлено детектор диму. Кожен з дванадцяти приладів окремо під'єднаний до панелі на пункті охорони. Також встановлено шість камер відеоспостереження, що окремо під'єднані до пункту охорони. Данні, що збирають камери, зберігаються протягом тижня.

При вході на другий поверх, ми потрапляємо в коридор, що веде до «Відділу .NET розробки», «Серверної», «Відділу Web розробки», «Переговорного залу», «Відділу Android розробки», «Відділу iOS розробки» та вбиральні. Всі кімнати окрім вбиральні, аналогічно першому поверху, розділені одна від одної, матовими скляними стінами.

Вбиральня, аналогічно вбиральні на першому поверсі, складена за цегли і має стіни з товщиною 20 см. Не має бойлер, адже приєднана до бойлера на першому поверсі. Вікна відсутні.

В південному кінці коридору розташовано комутатор, що підключено до відповідного комутатора в «Серверній», див. рис. 1.8. Цей комутатор надає доступ до мережі інтернет та серверу ПК в «Відділі Android розробки» та «Відділі iOS розробки».

В «Відділі .NET розробки» працює три співробітники та встановлена відповідна кількість ПК. Дані ПК мають підключення до мережі інтернет та серверу через відповідний комутатор, що розташовано в «Серверній», див. рис. 1.8. В кімнаті є три вікна, два з яких виходять на захід та одне на північ.

В північному кінці коридору розташована «Серверна» кімната. Двері до кімнати не мають додаткових посилень та замків. В даній кімнаті розташовано сервер Dell PowerEdge T40 v14. Цей сервер має підключення до мережі інтернет та всіх ПК на другому поверсі через комутатори розташовані в «Серверній». Даний сервер використовується для проводження тестів на навантаження для розроблюваного ПЗ. Також в кімнаті встановлено два комутатори, що забезпечують інтернет підключення та підключення до

серверу ПК на поверсі. Один із комутаторів має зовнішнє підключення до мережі інтернет. Вікна в кімнаті відсутні.

В «Відділі Web розробки» працює чотири співробітники та встановлена відповідна кількість ПК. Всі ПК мають підключення до мережі інтернет та серверу, через відповідний комутатор в «Серверній», див. рис. 1.8. В кімнаті є три вікна, одне з яких виходить на північ а два інших схід.

Переговорна зала відповідає аналогам на першому поверсі, проте не використовується для прийому клієнтів, і здебільшого, використовується розробниками для обговорення проектів та брифінгів. Має одне вікно, що виходить на схід.

В «Відділі Android розробки» працює чотири співробітники та встановлена відповідна кількість ПК. ПК мають доступ до мережі інтернет та серверу через підключення до комутатора в коридорі. Кімната має три вікна, два з яких виходять на схід та одне на південь.

В «Відділі iOS розробки» працює три співробітники та встановлена відповідна кількість ПК. ПК мають доступ до мережі інтернет та серверу через підключення до комутатора в коридорі. Кімната має три вікна, два з яких виходять на захід та одне на південь.

Стеля на другому поверху виконана відповідно до стелі на першому поверсі, включно із лініями електроживлення та мережі.

Вікна відповідно до вікон на першому поверсі не здатні відчинитися навстіж. Мають такі самі жалюзі і однакові правила стосовно використання штучного світла.

Нижче наведено генеральний план другого поверху ОІД з урахуванням ліній водопостачання, електроживлення, мережі та охоронної системи.

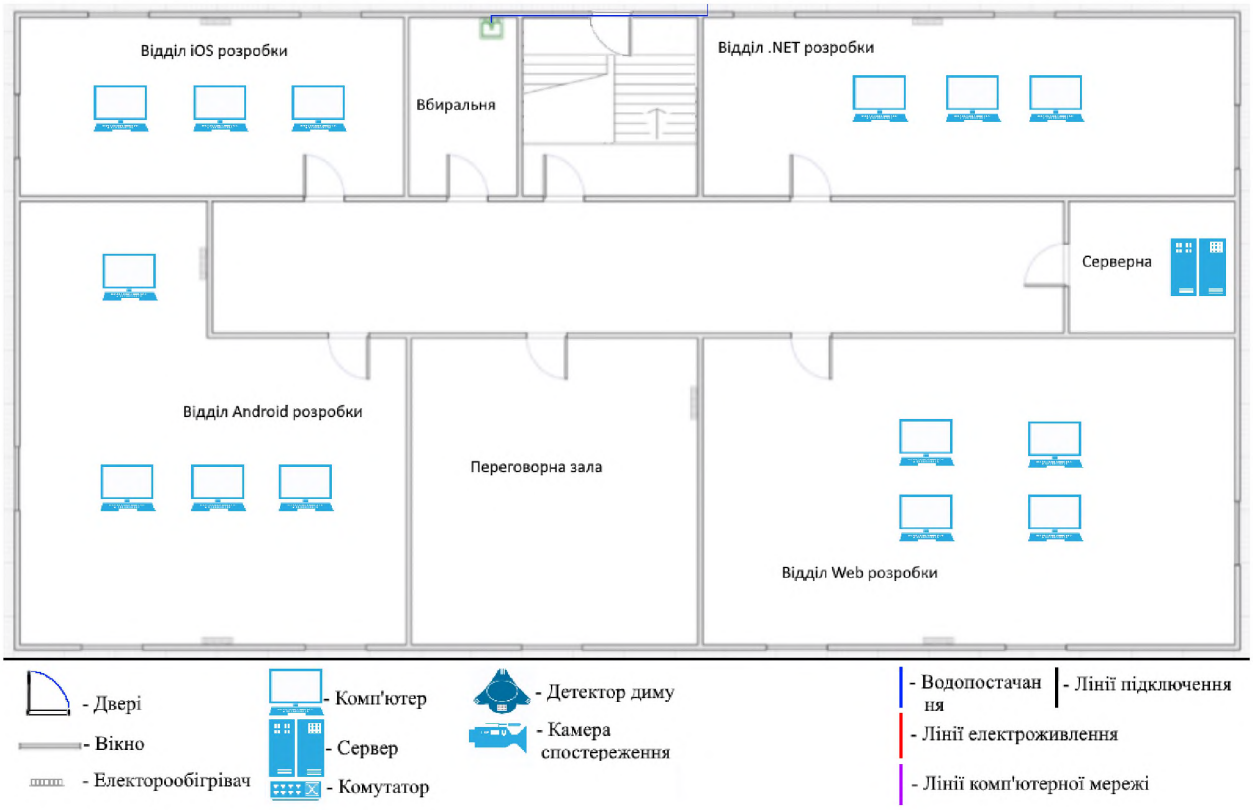

Рисунок 1.6 - Генеральний план другого поверху ОІД із лініями водопостачання

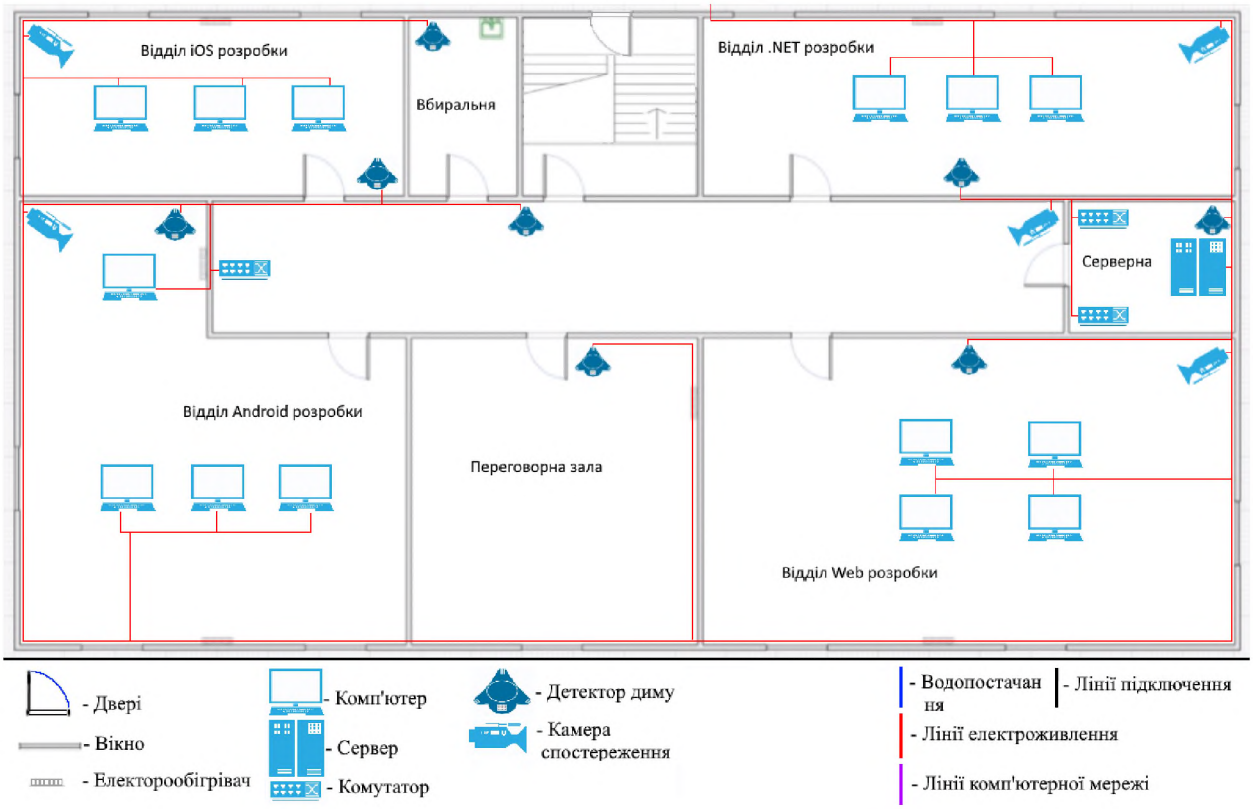

Рисунок 1.7 – Генеральний план другого поверху ОІД із лініями електроживлення

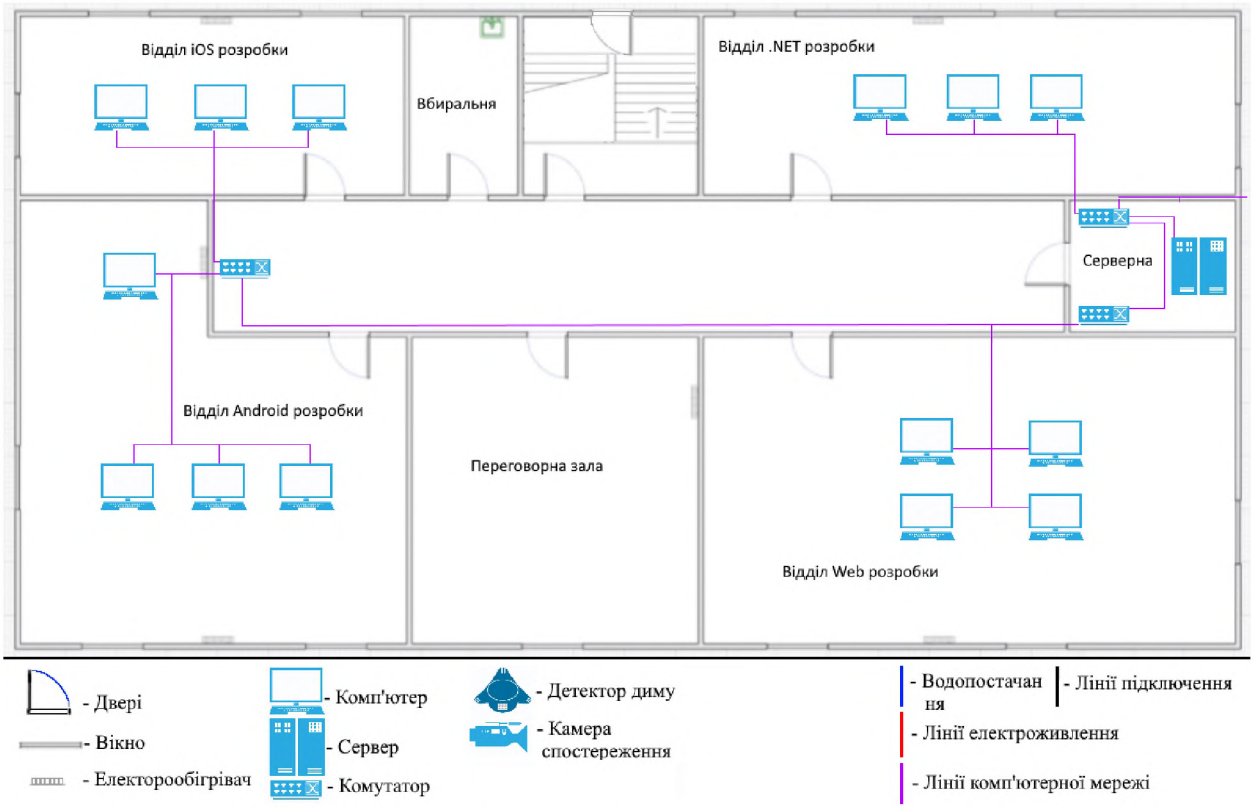

Рисунок 1.8 – Генеральний план другого поверху ОІД із лініями мережі

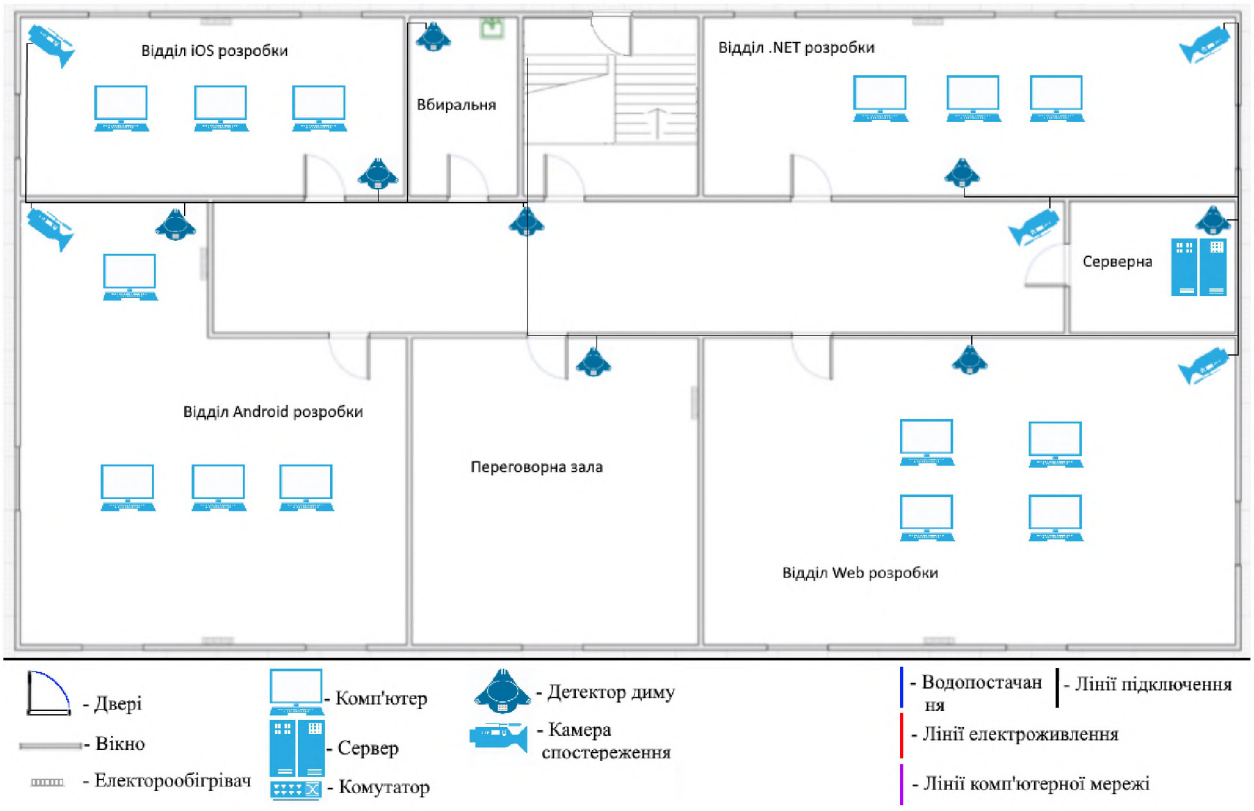

Рисунок 1.9 – Генеральний план другого поверху ОІД із лініями підключення охоронної системи

Відповідно до рис. 1.9 в кожному приміщенні на другому поверсі встановлено детектор диму. Кожен з восьми детекторів окремо підключено до пункту охорони. Загалом на території ОІД встановлено двадцять детекторів диму.

Відповідно до рис. 1.9 на другому поверсі встановлено п’ять камер відеоспостереження. Кожна з камер окремо під’єднана до пункту охорони. Загалом на території ОІД встановлено одинадцять камер відеоспостереження, що передають данні на пункт охорони. Данні з усіх камер зберігаються протягом одного тижня.

1.4 Обстеження обчислювальної системи

Відповідно до рис. 1.4 та 1.8 ПК на першому та другому поверсі об'єднані в окремі комп'ютерні мережі за допомогою комутаторів, маршрутизатору та ethernet кабелів. Головною метою для створення мережі на першому поверсі є надання пристроям доступу до глобальної мережі інтернет. На другому поверсі метою також є надання доступу до серверу компанії.

Доступ до серверу можливий лише з ПК глав відділів розробки, відповідно до мережевих налаштувань.

Всі ПК в ОІД складаються є моноблочними. Мають клавіатури та комп'ютерної миші. Ці компоненти можуть відрізнятися відповідно до відділу, див табл. 1.2.

Чотири з семи ПК в «Відділі продаж» мають встановлені веб-камери та гарнітуру, що підключаються напряму через USB. ПК в «Кабінеті системного адміністратора» та «Відділі HR» так само мають гарнітуру.

Сервер в ОІД використовується лише для проведення тестів на навантаження та автоматизованих перевірок ПЗ, що розробляється.

Нижче наведено таблицю інвентаризації з указаним місцем розташування пристрою та відстанню до границі ОІД.

Таблиця 1.2 – Інвентаризаційна відомість апаратного забезпечення ІТС

Позначення приналежності	Назва	Марка	Модель	Повер х	Розміщення	Відстань до межі ОІД. м
ПК 1	Моноблочний ПК	ARTLINE	Business M61	1	Відділ HR, на столі	0.4
ПК 2	Моноблочний ПК	ARTLINE	Business M61	1	Відділ HR, на столі	0.5
ПК 3	Моноблочний ПК	ARTLINE	Business M61	1	Відділ HR, на столі	1,0
ПК 4	Моноблочний ПК	ARTLINE	Business M61	1	Відділ бухгалтерії, на столі	0,4
ПК 5	Моноблочний ПК	ARTLINE	Business M61	1	Відділ бухгалтерії, на столі	0,4
ПК 6	Моноблочний ПК	ARTLINE	Business M61	1	Відділ бухгалтерії, на столі	1,0
ПК 7	Моноблочний ПК	ARTLINE	Business M61	1	Відділ бухгалтерії, на столі	1,0
ПК 8	Моноблочний ПК	ARTLINE	Business M61	1	Відділ продаж, на столі	0,4
ПК 9	Моноблочний ПК	ARTLINE	Business M61	1	Відділ продаж, на столі	0,7
ПК 10	Моноблочний ПК	ARTLINE	Business M61	1	Відділ продаж, на столі	0,7
ПК 11	Моноблочний ПК	ARTLINE	Business M61	1	Відділ продаж, на столі	1,5
ПК 12	Моноблочний ПК	ARTLINE	Business M61	1	Відділ продаж, на столі	2,0
ПК 13	Моноблочний ПК	ARTLINE	Business M61	1	Відділ продаж, на столі	0,2
ПК 14	Моноблочний ПК	ARTLINE	Business M61	1	Відділ продаж, на столі	0,2

Продовження таблиці 1.2

Позначення приналежності	Назва	Марка	Модель	Поверх	Розміщення	Відстань до межі ОІД. м
ПК 15	Моноблочний ПК	Lenovo	IdeaCentre AIO 3	1	Кабінет системного адміністратора, на столі	0,4
ПК 16	Моноблочний ПК	Lenovo	IdeaCentre AIO 3	2	Відділ .NET, на столі	1,0
ПК 17	Моноблочний ПК	Lenovo	IdeaCentre AIO 3	2	Відділ .NET, на столі	1,0
ПК 18	Моноблочний ПК	Lenovo	IdeaCentre AIO 3	2	Відділ .NET, на столі	1,0
ПК 19	Моноблочний ПК	Lenovo	IdeaCentre AIO 3	2	Відділ Web, на столі	1,2
ПК 20	Моноблочний ПК	Lenovo	IdeaCentre AIO 3	2	Відділ Web, на столі	1,2
ПК 21	Моноблочний ПК	Lenovo	IdeaCentre AIO 3	2	Відділ Web, на столі	1,5
ПК 22	Моноблочний ПК	Lenovo	IdeaCentre AIO 3	2	Відділ Web, на столі	2,0
ПК 23	Моноблочний ПК	Lenovo	IdeaCentre AIO 3	2	Відділ Android, на столі	0,7
ПК 24	Моноблочний ПК	Lenovo	IdeaCentre AIO 3	2	Відділ Android, на столі	0,7
ПК 25	Моноблочний ПК	Lenovo	IdeaCentre AIO 3	2	Відділ Android, на столі	1,4
ПК 26	Моноблочний ПК	Lenovo	IdeaCentre AIO 3	2	Відділ Android, на столі	1,4
ПК 27	Моноблочний ПК	Lenovo	IdeaCentre AIO 3	2	Відділ iOS, на столі	0,5
ПК 28	Моноблочний ПК	Lenovo	IdeaCentre AIO 3	2	Відділ iOS, на столі	1,2

Продовження таблиці 1.2

Позначення приналежності	Назва	Марка	Модель	Поверх	Розміщення	Відстань до межі ОІД. м
ПК 29	Моноблочний ПК	Lenovo	IdeaCentre AIO 3	2	Відділ iOS, на столі	1,2
ПК 1 – ПК 13	Комп'ютерна миш(13)	Logitech	B100	1	Відділ HR, відділ бухгалтерії, відділ продаж, на столі	0,2 – 2,0
ПК 14 – ПК 29	Комп'ютерна миш (16)	Logitech	B110 Silent	1,2	Відділ продаж, кабінет системного адміністратора, відділ .NET, відділ Web, відділ Android, відділ iOS, на столі	0,2 – 2,0
ПК 1 – ПК 29	Клавіатура (29)	Logitech	Corded Keyboard K280e	1	Відділ HR, відділ бухгалтерії, відділ продаж, кабінет системного адміністратора, відділ .NET, відділ Web, відділ Android, відділ iOS, на столі	0,2 – 2,0
П	Принтер	HP	Laser 135w	1	Відділ бухгалтерії, на столі	1,3

Продовження таблиці 1.2

Позначення приналежності	Назва	Марка	Модель	Поверх	Розміщення	Відстань до межі ОІД. м
М 1	Комутатор	TP-Link	TL-SG1024DE	1	Відділ продаж, полиця в столі	1,0
М 2	Комутатор	TP-Link	TL-SG108E	2	Серверна, на стелаж	1,4
М 2	Комутатор	TP-Link	TL-SG108E	2	Серверна, на стелаж	1,4
М 2	Комутатор	TP-Link	TL-SG108E	2	Коридор другого поверху, на тумбочці	2,3
М 1	Маршрутизатор	TP-Link	Archer AX10	1	Зал для відпочинку, на полиці шафи	3,4
М 2	Сервер	Dell	PowerEdge T40 v14	2	Серверна, на спеціалізованому стелажі	0,2
-	Проектор	Epson	EB-E10	1	Зал для відпочинку, кріпиться до стелі	2,2

Продовження таблиці 1.2

Позначення приналежності	Назва	Марка	Модель	Поверх	Розміщення	Відстань до межі ОІД. м
О	Камера відеоспостереження (11)	Dahua	DH-HAC-HDW1200RP-BE	1,2	Фойє, зал для відпочинку, кухня, коридор на першому поверху, відділ продаж, кабінет системного адміністратора, коридор на другому поверху, відділ .NET, відділ Web, відділ Android, відділ iOS,	0,1 – 5,5
П	USB-хаб	RZTK	3	1	Відділ бухгалтерії, на столі	1,3

Продовження таблиці 1.2

Позначення приналежності	Назва	Марка	Модель	Поверх	Розміщення	Відстань до межі ОІД. м
О	Детектор диму (20)	Артон	2П	1,2	Відділ HR, зал для відпочинку, кухня, фойє, коридор на першому поверху, вбиральня на першому поверсі, відділ бухгалтерії, відділ продаж, кабінет системного адміністратора, переговорна зала, мала переговорна зала, коридор на другому поверху, вбиральня на другому поверху, відділ .NET, серверна, відділ Web, переговорна зала на другому поверсі, відділ Android, відділ iOS,	-

Продовження таблиці 1.2

Позначення приналежності	Назва	Марка	Модель	Поверх	Розміщення	Відстань до межі ОІД. м
ПК 11 – ПК 14	Веб-камера (4)	Logitech	HD Pro C920x	1	Відділ продаж, прикріплені до ПК	0,2 – 2,0
ПК 1 - ПК 3, ПК 11 – ПК 15	Гарнітура (8)	Microsoft	LifeChat LX-3000	1	Відділ продаж, відділ HR, кабінет системного адміністратора,	0,2 – 2,0

1.5 Обстеження інформаційної системи

На сервері встановлено серверну операційну систему та ПЗ для тестування мобільного ПЗ та проводження тестів на навантаження для сайтів. Дані з ПК не дублюються та не зберігаються на сервері.

Всі ПК на території ОІД мають встановлену операційну систему Ubuntu. Оновлення та налаштування системи не контролюється та не обмежується.

На всіх ПК по базі існує користувач із правами адміністратора, та створюється новий звичайний користувач для співробітника, що буде за ним працювати. Співробітник отримує згенерований пароль від системного адміністратора, та згодом може змінювати його за своїм бажанням.

Так само співробітники отримують данні від аккаунтів, що створюються для них персонально чи до корпоративних аккаунтів, якщо доступ до них необхідний. У разі особистого акаунту, працівник має можливість та право змінювати пароль.

На кожному ПК є ряд встановлених по базі програм, до них входять браузер, антивірусне забезпечення, програми для роботи з документами, обміну файлами та комунікації.

На ПК, що встановленні на другому поверсі та належать до відділів розробки, встановлено відповідне ПЗ для розробки та дизайну. При розробці ПЗ використовується платформа GitHub, та розподілення задач між працівниками одного чи декількох відділів. Що два тижні, відбувається завантаження даних до репозиторію відповідного проекту.

На ОІД відсутні обмеження та контроль за зовнішніми носіями інформації та способом зберігання даних.

Переважна більшість працівників дублює данні з якими працює в хмарне сховище, що прив’язане до їх корпоративного аккаунту Google, чи використовує його як основне.

Окремо компанія має власний веб-сайт призначений для клієнтів та реклами. Даний сайт зберігається та розташовується на сторонньому хостингу.

Перелік ПЗ, що використовується в ОІД, із зазначенням пристроїв приведено нижче:

Таблиця 1.3 – Інвентаризаційна відомість програмного забезпечення ІТС

Назва	Тип	Опис	Ліцензія	Де встановлено
Ubuntu 21.10 +	Система	Операційна система	GPL General Public License	ПК 1 – ПК 29
Google Chrome	Прикладне	Браузер	Freeware	ПК 1 – ПК 29
Аналог базового пакету Microsoft Office 2019 Professional для Ubuntu	Прикладне	Програмне забезпечення для роботи з документами	Volume License	ПК 1 – ПК 29
ClamAV	Прикладне	Пакет антивірусного ПЗ	GNU General Public License	ПК 1 – ПК 29, Сервер
Slack	Прикладне	Програма для комунікації співробітників	Proprietary software	ПК 1 – ПК 29
Rider	Прикладне	IDE для .NET розробки	GNU General Public License	ПК 16 – ПК 18
IntelliJ IDEA	Прикладне	IDE для Web та Android розробки	GNU General Public License	ПК 19 – ПК 26
AppCode	Прикладне	IDE для iOS розробки	GNU General Public License	ПК 27 – ПК 29

Продовження таблиці 1.3

Назва	Тип	Опис	Ліцензія	Де встановлено
Figma	Прикладне	Програма для створення та редагування дизайну та зображень із функцією колективного створення проектів для веб сайтів та ПЗ	GNU General Public License	ПК 19 – ПК 22
Windows Server	Системне	Серверна операційна система	Full Package Product	Сервер
Apache JMeter	Прикладне	Програмне забезпечення для тестів навантаження сайтів	Apache License 2.0	Сервер
Calabash	Прикладне	Програмне забезпечення для тестування мобільного ПЗ	Freeware	Сервер

Програми наведені в табл. 1.3 є встановленими на відповідних ПК по базі. Проте в компанії не встановлено обмежень та стандартів стосовно ПЗ для оброблення та зберігання інформації, окрім мов програмування та бібліотек, що використовуються для створення ПЗ.

1.6 Обстеження інформації, що циркулює на ОІД

Інформація що циркулює на ОІД поділяється на:

1. Інформацію про фізичну особу або персональні данні;
2. Інформацію про товар;
3. Податкову інформацію;
4. Статистичну інформацію.

Інформація про фізичну особу та персональні данні клієнта та співробітників і може бути представлена у вигляді тексту, графічних зображень, аудіо файлів запису розмов із клієнтом та відеофайлів запису відео дзвінків та презентацій, зроблених за попередньої згоди. Ці дані зберігаються та оброблюються в «Відділі продаж» та «Відділі бухгалтерії».

Персональні данні в ОІД поділяються на данні з закритим доступом та відкритим доступом. Персональні данні клієнтів можуть бути використані на сайті з метою реклами послуг та товарів компанії, з попередньої згоди із клієнтом.

Інформація про товар включає в себе данні, що містять опис ПЗ, безпосередньо ПЗ, дизайн до ПЗ, відеофайли, що демонструють роботу ПЗ. Відповідно можуть бути у вигляді текстових файлів, графічних зображень та відео файлів. Ці дані зберігаються та оброблюються в «Відділі продаж», «Відділі .NET розробки», «Відділі Web розробки», «Відділі Android розробки» та «Відділі iOS розробки».

Інформація про товар поділяється на данні з закритим доступом та відкритим доступом. До відкритої інформації може відноситись обмежена загальна інформація про товар, що використовується в якості реклами послуг та товарів компанії, за попередньої домовленості із клієнтом.

Податкова інформація містить інформацію про фінансову діяльність компанії зберігається у вигляді текстових документів. Ці дані зберігаються та обробляються в «Відділі бухгалтерії»

Податкова інформація має обмежений доступ.

Статистична інформація містить узагальнені данні про клієнтів та їх замовлення, кількість та тип користувачів веб-сайту та статистику про розробку ПЗ. Ці дані зберігаються та обробляються в «Відділі продаж», «Відділі .NET розробки», «Відділі Web розробки», «Відділі Android розробки» та «Відділі iOS розробки».

Статистична інформація має обмежений доступ та поширюється серед співробітників залежно від рішень керівництва.

Нижче наведено таблицю із видами інформації, шо циркулюють на ОІД з відповідними рівнями важливості та таблиця користувацького середовища, що відображає можливості користувачів різного рівня допуску до інформації.

Таблиця 1.4 – Інформація, яка циркулює в ОІД

Вид інформації	Режим доступу	Правовий режим	Вид представлення в ІТС	Вимоги до захисту		
				К	Ц	Д
Інформація про клієнтів компанії	Відкритий доступ	Відкрита	Текстова, графічна, звукова, відео	К1	Ц2	Д2
Інформація про клієнтів компанії	Обмежений доступ	Конфіденційна	Текстова, графічна, звукова, відео	К3	Ц2	Д2
Інформація про товар	Відкритий доступ	Відкрита	Текстова, графічна, відео	К1	Ц2	Д2
Інформація про товар	Обмежений доступ	Конфіденційна	Текстова, графічна,	К3	Ц3	Д2
Бухгалтерські звіти діяльності компанії	Обмежений доступ	Службова	Текстова, графічна,	К2	Ц2	Д2
Статистичні дані	Обмежений доступ	Службова	Текстова, графічна,	К2	Ц2	Д1

Таблиця 1.5 – Рівні важливості конфіденційності

Оцінка рівня наслідків	Опис
К1	Не призводить до розкриття конфіденційної інформації
К2	Призводить до розкриття окремих документів, які відносяться до “комерційної таємниці”, персональних даних і може призвести до незначних фінансових втрат
К3	Призводить до розкриття документів, які відносяться до “комерційної таємниці”, персональних даних і призводить до значних фінансових втрат, має значний вплив на репутацію підприємства

Таблиця 1.6 – Рівні важливості цілісності

Оцінка рівня наслідків	Опис
Ц1	Не призводить до фінансових втрат
Ц2	Призводить до незначних фінансових втрат та має незначний вплив на репутацію підприємства
Ц3	Призводить до великих фінансових втрат, має значний вплив на репутацію підприємства

Таблиця 1.7 – Рівні важливості доступності

Оцінка рівня наслідків	Опис
Д1	Не впливає на доступність
Д2	На деякий час впливає на доступність до ресурсу, що може принести незначні збитки або мати невеликий вплив на репутацію підприємства
Д3	Унеможливлює користування ресурсом на тривалий час і має значний вплив на роботу підприємства

Таблиця 1.8 – Користувацьке середовище

Користувач	Кількість працівників	Роль в ІС	Інформація				Повноваження керувати КСЗІ	Пристрої
			персональна	продукт компанії	бухгалтерська	статистика		
Керівники відділів розробки	4	Системний адміністратор	-	R, W, C, D, M, S	R	R, W, C, D, M, S, P	+	ПК 18, ПК 22, ПК 26, ПК 29
Керівники інших відділів	2	Користувач	R, W, C, D, M, S, P	R	R, W, D, M, S, P	R, W, C, D, M, S, P	-	ПК 14, ПК 7
Системний адміністратор	1	Системний адміністратор	R, C, D, M, S	R, C, D, M, S	R, C, D, M, S	R, W, C, D, M, S, P	+	ПК 15, сервер, комутатори, маршрутизатор
ІТ спеціаліст	10	Користувач	-	R, W, C, D, M, S	-	R	-	ПК 16 - ПК 17, ПК 19 – ПК 21, ПК 23 – ПК25, ПК 27 – ПК 28
Бухгалтер	4	Користувач	R, W, C, P	-	R, W, D, M, S, P	R	-	ПК 4 - ПК 6

Продовження таблиці 1.8

Користувач	Кількість працівників	Роль в ІС	Інформація				Повноваження керувати КСЗІ	Пристрої
			персональна	продукт компанії	бухгалтерська	статистика		
Спеціалісти з роботи з клієнтами	7	Користувач	R, W, C, D, M, S	R	R	R	-	ПК 8 - ПК 13
HR спеціалісти	3	Користувач	R, W, C, D, M, S, P	R	R	R, W, C, D, M, S, P	-	ПК 1 – ПК 3

Примітка до табл. 1.8:

R – читання
W – запис та створення
C – копіювання
D – видалення
M – модифікація
S – зберігання
P – друкування

1.7 Розробка моделі порушника

Проаналізувавши умови обігу інформації та табл. 1.8 можливо розпочати створення моделі потенційного порушника для ІТС. При розробці буде враховуватися позиція потенційного порушника, його приналежність до компанії, мотивація, кваліфікація, засоби які він може використовувати, його можливості впливу відносно часу та місця.

Для кожного імовірного порушника буде наведено два варіанти. Перший відображає найбільш реалістичний рівень загрози, а другий – гіпотетичний максимальний рівень.

Таблиця 1.9 – Модель потенційного порушника

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Керівники відділів розробки	ПВ 2	М 1	К 3	З 3	Ч 1	Д 2	13
	3	1	3	3	1	2	
	ПЗ 4	М 4	К 3	З 4	Ч 3	Д 2	20
	4	4	3	4	3	2	
Керівники інших відділів	ПВ 5	М 1	К 2	З 3	Ч 1	Д 2	11
	2	1	2	3	1	2	
	ПЗ 4	М 4	К 3	З 4	Ч 3	Д 2	20
	4	4	3	4	3	2	
ІТ спеціаліст	ПВ 2	М 3	К 3	З 3	Ч 1	Д 2	13
	3	1	3	3	1	2	
	ПЗ 4	М 4	К 3	З 3	Ч 2	Д 2	18
	4	4	3	3	2	2	
Бухгалтер	ПВ 3	М 1	К 1	З 2	Ч 1	Д 2	10
	2	1	1	3	1	2	
	ПЗ 4	М 4	К 3	З 3	Ч 2	Д 2	18
	4	4	3	3	2	2	
Менеджер продаж	ПВ 3	М 1	К 1	З 2	Ч 1	Д 2	10
	2	1	1	3	1	2	
	ПЗ 4	М 4	К 3	З 3	Ч 2	Д 2	18
	4	4	3	3	2	2	
HR спеціаліст	ПВ 3	М 1	К 1	З 2	Ч 1	Д 2	10
	2	1	1	3	1	2	
	ПЗ 4	М 4	К 3	З 3	Ч 2	Д 2	18
	4	4	3	3	2	2	
Системний адміністратор	ПВ 4	М 1	К 4	З 3	Ч 1	Д 2	15
	4	1	4	3	1	2	
	ПЗ 4	М 4	К 4	З 4	Ч 4	Д 4	24
	4	4	4	4	4	4	

Продовження таблиці 1.9

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Працівник служби безпеки	ПЗ 2	М 1	К 1	З 1	Ч 2	Д 1	7
	1	1	1	1	2	1	
	ПЗ 4	М 4	К 2	З 2	Ч 2	Д 2	17
	4	4	2	3	2	2	
Прибиральник	ПЗ 2	М 1	К 1	З 1	Ч 2	Д 1	7
	1	1	1	1	2	1	
	ПЗ 4	М 4	К 2	З 2	Ч 2	Д 2	
	4	4	2	3	2	2	20

Таблиця 1.10 – Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загроз
Внутрішні по відношенню до ІТС		
ПВ 1	Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІТС	1
ПВ 2	Персонал, який обслуговує технічні засоби ІТС (системний адміністратор, ІТ спеціаліст)	3
ПВ 3	Користувачі ІТС	2
ПВ 4	Адміністратор ІТС(системний адміністратор)	4
ПВ 5	Керівники різних рівнів(директор)	2
Зовнішні по відношенню до ІТС		
ПЗ 1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ 2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання та інше)	1
ПЗ 3	Хакери	3
ПЗ 4	Агенти конкурентів	4

Таблиця 1.11 - Специфікація моделі порушника за мотивами здійснення порушень

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

Таблиця 1.12 - Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

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

Таблиця 1.13 - Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З 1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З 2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	3
З 3	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 та пронесено крізь охорону	3
З 4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4

Таблиця 1.14 - Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч 1	Під час функціонування ІТС	1
Ч 2	Під час бездіяльності компонентів системи (в неробочій час, під час планових перерв у роботі, перерв для обслуговування і ремонту і т.п.)	2
Ч 3	Під час повної бездіяльності ІТС з метою відновлення та ремонту	3
Ч 4	Як у процесі функціонування систем захисту інформації, так і під час зупинки компонентів системи	4

Таблиця 1.15 - Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
Д 1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д 2	З робочих місць користувачів (операторів) ІТС	2
Д 3	З доступом у зону зберігання баз даних, архівів тощо	3

Продовження таблиці 1.15

Позначення	Характеристика місця дії порушника	Рівень загроз
Д 4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

Аналізуючи табл. 1.9, ІТС компанії та обіг інформації в ній можна зробити висновок, що ймовірність зовнішнього втручання від потенційних конкурентів, чи цільова атака хакерів є малоймовірною та спричинені збитки чи потенційний прибуток від них не будуть відповідати затратам. Таким чином для забезпечення достатнього рівня захисту ІТС достатньо розглядати порушників із реалістичним рівнем загрози.

Результатом буде спрощена модель потенційного порушника.

Таблиця 1.16 - Реалістична модель порушника політики безпеки інформації

Категорія порушника «ПВ»	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Керівники відділу розробки	ПВ 2	М 1	К 3	З 3	Ч 1	Д 2	13
Керівники іншого відділу	ПВ 5	М 1	К 2	З 3	Ч 1	Д 2	11
ІТ спеціаліст	ПВ 2	М 3	К 3	З 3	Ч 1	Д 2	13
Бухгалтер	ПВ 3	М 1	К 1	З 2	Ч 1	Д 2	10
Менеджер продаж	ПВ 3	М 1	К 1	З 2	Ч 1	Д 2	10
HR спеціаліст	ПВ 3	М 1	К 1	З 2	Ч 1	Д 2	10
Системний адміністратор	ПВ 4	М 1	К 4	З 3	Ч 1	Д 2	15
Працівник служби безпеки	ПЗ 2	М 1	К 1	З 1	Ч 2	Д 1	7
Прибиральниця	ПЗ 2	М 1	К 1	З 1	Ч 2	Д 1	7

Згідно із табл. 1.16 найбільшої загрози для ІТС потенційно несуть системний адміністратор, керівники відділів розробки та ІТ спеціалісти. Беручі до уваги табл. 1.8 та політику компанії й налаштування серверу, згідно з якими лише керівники мають можливість взаємодіяти з сервером та КСЗІ, стає зрозуміло, що найбільшу потенційну загрозу становлять системний адміністратор та керівники відділів розробки.

1.8 Розробка моделі загроз

Згідно із даними зазначеними в 1.1 та 1.7 частинах можливо розробити відповідну модель загроз для ІТС компанії із подальшим описом та аналізом потенційних збитків.

При аналізі загрози буде враховуватися її ймовірність та рівень збитків, що завдасть її реалізація, відповідно до трьох рівнів:

- високий - якщо реалізація загрози надає великих збитків, у разі ймовірності реалізації відповідає за високу ймовірність (3 бали);
- середній - якщо реалізація загрози надає помірних збитків, у разі ймовірності реалізації відповідає за середню ймовірність (2 бали);
- низький - якщо реалізація загрози надає незначних збитків, у разі ймовірності реалізації відповідає за низьку ймовірність (1 бал).

Таблиця 1.17 - Перелік загроз з визначенням порушень властивостей

Потенційні загрози для інформації в ІТС	Ризики для			
	К	Ц	Д	С
Стихійні явища	-	+	+	-
Відсутність електропостачання	+	+	+	+
Відмова/збій обчислювальної техніки	+	+	+	+
Відмова/збій програмного забезпечення	+	+	+	+
Пошкодження паперової документації	-	-	-	-
Відмова доступу до інтернету	-	+	-	-
Несанкціоноване підключення до технічних засобів	+	+	-	-
Несанкціоноване підключення до мережевих вузлів	+	+	+	-
Читання даних, залишених без нагляду та читання даних, що виводиться на екран	+	-	-	+
Перехоплення даних за допомогою акустичного каналу	+	-	-	+
Несанкціонований перегляд інформації за допомогою візуально-оптичного каналу	+	-	-	+
Зараження системи вірусами	+	+	+	+
Втрата паролів	+	-	+	-
Втрата резервних копій	-	-	-	-
Несанкціоноване внесення змін у технічні засоби	+	+	-	-
Використання недозволеного програмного забезпечення або модифікація компонентів програмного та інформаційного забезпечення	+	+	+	+
Пошкодження носіїв інформації	-	-	+	-
Вхід в систему недопущених осіб (подолання систем захисту)	+	+	+	+
Недоступність до хмарного сховища	-	-	+	-
Неправильне налаштування резервного копіювання	-	+	+	-
Неправильні налаштування прав доступу співробітників	+	-	+	+
Недбале зберігання документів	+	+	+	+
Отримання сторонньою особою інформації у персоналу ІТС	+	+	+	+
Відсутність правильно налагодженої системи сигналізації	+	+	-	+
Відсутність шифрування даних	+	+	-	-
Передача важливих документів в незашифрованому вигляді	+	+	-	+
Хакерська атака	+	+	+	+
Використання заборонених ресурсів Інтернету в своїх цілях	+	+	+	-
DDoS-атака	-	-	+	-

Таблиця 1.18 - Загрози конфіденційності інформації

Механізм реалізації	Рівень		Сума загроз
	ризики	збитки	
Халатність співробітників підприємства	1	2	3
Не дотримання чітких правил безпеки під час користування ПК	1	1	2
Копіювання даних для ознайомлення сторонніми особами	1	3	4
Погана звукоізоляція приміщення	2	2	4
Неправильні умови зберігання паперових документів в архівах	1	1	2
Викрадення носіїв з метою несанкціонованого ознайомлення сторонніх осіб	1	2	3
Відсутність опису використання зовнішніх носіїв	2	2	4
Використання сторонньої інформації з посиланням на авторів	1	1	2

Таблиця 1.19 - Загрози цілісності інформації

Механізм реалізації	Рівень		Сума загроз
	ризики	збитки	
Помилки (ненавмисні) користувачів ІТС, які призвели до модифікації або спотворення інформації на жорсткому диску або зовнішніх носіях	1	2	3
Несанкціонована (навмисне) модифікація або спотворення інформації персоналом ІТС на жорсткому диску або зовнішніх носіях	1	3	4
Відсутність своєчасного резервного копіювання	2	2	4
Відсутність своєчасного копіювання та зберігання важливих документів	2	3	5
Прояви помилок системного ПЗ, внаслідок яких стала можливою модифікація інформації або її спотворення користувачами	1	2	3
Безпосередній доступ до інформації будь-яким способом сторонніми особами	1	3	4
Халатність співробітників щодо пропуску сторонніх осіб	1	3	4
Відсутність підтвердження відправника інформації що надходить на обробку	1	2	3

Таблиця 1.20 - Загрози доступності інформації

Механізм реалізації	Рівень		Сума загроз
	ризики	збитки	
Помилка користувача, яка призвела до знищенню даних	1	3	4
Помилка адміністраторів, яка призвела до віддаленню даних	1	3	4
Пошкодження парольних носіїв персоналом ІТС, що призвело до втрати доступу до інформації	1	3	4
Прояви помилок системного ПЗ, яке призвело до втрати доступу до інформації або ІТС	1	2	3
Прояви помилок системного ПЗ, внаслідок яких стала можливою модифікація інформації або її спотворення користувачами	1	2	3
Безпосередній доступ до інформації будь-яким способом сторонніми особами	1	3	4
Навмисне видалення або деформація інформації	2	3	5
Можливість невчасного оновлення інформації	1	1	2

Таблиця 1.21 - Загрози спостереженості ІТС

Механізм реалізації	Рівень		Сума загроз
	ризики	збитки	
Помилки (ненавмисні) персоналу ІТС, які призвели до втрати спостережності	1	2	3
Помилки (ненавмисні) адміністраторів ІТС, які призвели до втрати спостережності	1	2	3
Некоректне налагодження засобів захисту адміністраторами ІТС, яке призвело до втрати спостережності	1	3	4
Порушення спостережності користувачами ІТС внаслідок навмисних цілей	1	3	3
Порушення спостережності внаслідок пошкодження, у тому числі навмисного, архівів та носіїв з архівами даних	1	2	3
Прояви помилок системного ПЗ, яке призвело до втрати спостережності	1	1	2
Безпосередній доступ до ІТС будь яким способом сторонніх осіб	1	3	4
Можливе спостереження співробітниками охорони	1	2	3

Проаналізувавши таблиці 1.18 – 1.21 можна зробити узагальнення загроз ІТС, що матиме наступний вигляд:

Таблиця 1.22 - Узагальнена таблиця загроз ІТС

Види загроз	1 загроза	2 загроза	3 загроза	4 загроза	5 загроза	6 загроза	7 загроза	8 загроза	Сума загроз
Конфіденційності	3	2	4	4	2	3	4	2	24
Спостережності	3	3	4	3	3	2	4	3	25
Доступності	4	4	4	3	3	4	5	2	33
Цілісності	3	4	4	5	3	4	4	3	34

Згідно із табл. 1.21 ІТС є найбільш вразливою до порушення цілісності та доступності. Враховуючи табл. 1.18 – 1.21 і частину 1.6 можливо зробити висновок, що така ситуація є наслідком легкої реалізації загроз та відсутності необхідних мір протидії й механізмів контролю.

1.9 Висновок

Ознайомившись із матеріалами першого розділу можна робити відповідні висновки стосовно КСЗІ компанії та загроз, що є актуальними для неї.

До важливих недоліків КСЗІ відносяться:

1. Відсутність стандартів, обмежень та контролю за використанням ПЗ для обробки, створення та збереження інформації. На сам перед несе загрозу через можливість встановлення стороннього ПЗ, що в свою чергу може бути шкідливим, мати сторонні модифікації чи прогалини в захисті.
2. Відсутність політики та стандарту обігу даних в відділах не пов'язаних із розробкою. Через відсутність чіткої політики копіювання та зберігання даних з'являється можливість їх ушкодження, втрати або втрати доступу до них.
3. Відсутність політики стосовно використання зовнішніх носіїв інформації. Тісно пов'язана із попереднім пунктом, та становить загрозу як для даних так і для АС через можливість потрапляння до системи шкідливого ПЗ
4. Значний рівень потенційної загрози від системного адміністратора та керівників відділів розробки та відсутність методів по їх контролю. Данні працівники несуть потенційну небезпеку через високий рівень доступу до КСЗІ, що посилюється відсутністю контролю за їх діями в ІТС.

На ряду з цим існують менш критичні недоліки:

1. Відсутність контролю доступу до «Серверної». Оскільки в ній встановлено цінне та критичне обладнання вільний доступ до даної кімнати спричиняє ризики його пошкодження.

2. Відсутність політики та контролю при віддаленій праці. Використання особистого ПК для доступу та обробки інформації ставить під загрозу їх конфіденційність, а у випадку завантаження файлів, що були створені на особистому ПК й загрозу цілісності ІТС.

3. Відсутність автоматичних оновлень операційної системи. Через різницю в версіях потенційно може спричиняти конфлікти між файлами, що обробляться.

4. Відсутність єдиної комп'ютерної мережі. Відсутність єдиної мережі між першим та другим поверхами підвищує ймовірність виникнення неполадок, та змушує системного адміністратора звертатися до серверу через глобальну мережу замість локальної.

5. Недоліки в розташуванні камер відеоспостереження. Через встановлення камер виникають сліпі зони.

6. Відсутність захисту чи датчиків на вікнах першого поверху. Оскільки вікна не є посиленими та не мають гратів виникає можливість швидко потрапити на територію ОІД.

Загалом перелічені недоліки мають програмну, апаратну та організаційну природу. Деякі з них самі по собі несуть загрозу для ІТС та АС, інші не становлять прямої загрози, проте в разі реалізації однієї із загроз розглянутих в частині 1.7 можуть призвести до збитків.

Тому ліквідація даних недоліків є необхідною умовою для забезпечення безпеки ІТС та налагодження КСЗІ.

РОЗДІЛ 2. СТВОРЕННЯ КСЗІ

2.1 Контроль за використанням ПЗ

Відсутність певних стандартів, що до ПЗ яке використовують співробітники та обмежень користувачів в правах для самостійного встановлення ПЗ може спричиняти ряд наслідків, в число яких входить загроза з встановлення шкідливого ПЗ.

Перш за все необхідно зібрати статистику по відділам та розробити відповідні стандарти стосовно використання ПЗ для обробки певних видів інформації.

Наступним кроком буде встановлення на відповідні ПК необхідного ПЗ та їх налаштування.

Оскільки працівники «Відділу HR», «Відділу бухгалтерії» та «Відділу продаж» працюють із стандартними документами, для них головним ПЗ для обробки даних є «Аналог базового пакету Microsoft Office 2019 Professional для Ubuntu» та онлайн версія Microsoft Office, що доступна через корпоративні аккаунти Google.

ПК в «Відділі продаж», що мають підключену веб-камеру та використовуються для спілкування із клієнтами повинні мати ПЗ для проведення відео дзвінків. Оскільки за статистикою, клієнти використовують Zoom та Teams, саме ці дві програми та їх онлайн версії повинні використовуватися.

Для відділів розробки стандартним має стати IDE встановлене по базі, адже данні програми були обрані відповідно до рівня їх якості, та всі працівники використовували їх в якості основних.

До стандартних програм, що встановлюються на всі ПК, відносяться браузери Google Chrome та Firefox, ПЗ для корпоративної комунікації Slack, та пакет антивірусного ПЗ ClamAV.

Слід провести організаційні роботи, стосовно інформування співробітників про нові стандарти.

Системний адміністратор повинен провести відповідні налаштування в операційних системах всіх ПК, що належать співробітникам без прав адміністративного доступу до ПК. Операційна система Ubuntu дозволяє обмежити права користувачів на встановлення стороннього ПЗ та ініціалізацію певних файлів.

Таким чином лише за допомогою організаційних заходів можливо вирішити проблему з відсутністю стандартів та контролю за ПЗ, що використовується.

2.2 Політика обігу інформації

Відсутність норм, що до збереження та передачі даних підвищує ризик для цілісності та доступності даних в ІТС.

Оскільки для кожного співробітника створюється корпоративний акаунт Google, що має хмарне сховище з об'ємом 15 ГБ, то використання його можливо використовувати в якості хмарного сховища для даних. При цьому існує можливість налаштування правд доступу інших співробітників до даного файлу. У разі внесення змін до файлу, данні про користувача та внесені зміни будуть зберігатися в журналі.

Основними перевагами при використанню стане забезпечення доступності, цілісності та конфіденційності інформації.

При цьому з метою підвищення цілісності даних та їх доступності у разі несправності мережі необхідно дублювати дані на ПК користувача.

Таким чином найкращім рішенням буде використовувати хмарне сховище для дублювання критичної інформації та даних які активно використовуються.

Програма для корпоративного спілкування Slack, що використовується в ІТС, здатна до передачі файлів. Таким чином можливо використовувати її для обміну файлами, що не зберігаються в хмарному сховищі.

У разі критичних збоїв в роботі мережі жодний з наведених способів передачі даних працювати не зможе, тому слід використовувати апаратне рішення.

В відділи розробки, «Відділ продаж» та «Відділ бухгалтерії» необхідно купити по два USB накопичувача, враховуючи розміри файлів, що циркулюють в ІТС, достатньо буде об'єму в 8 ГБ. Так само один накопичувач для «Відділу HR» та «Кабінету системного адміністратора». Загально чотирнадцять USB накопичувачів.

На них необхідно нанести відповідні до відділів маркування та вести журнал про їх використання.

Таким чином дана накопичувачі можливо буде використовувати в якості резервного або більш надійного методу передачі та збереження інформації.

2.3 Політика використання зовнішніх носіїв інформації

Беручи до уваги попередній пункт, стає зрозуміло, що використання зовнішніх носіїв інформації окрім USB накопичувачів, що не залишають територію ОІД та є безпечними, не є необхідним.

Таким чином, слід вводити заборону на використання сторонніх носіїв інформації.

З метою реалізації, слід провести організаційні заходи.

Операційна система Ubuntu дозволяє налаштувати розпізнавання та доступ до зовнішніх носіїв інформації та інших пристроїв.

Системний адміністратор повинен провести відповідні налаштування на всіх ПК в ІТС, що унеможливлять підключення сторонніх носіїв інформації та підключення несанкціонованих пристроїв.

2.4 Контроль за діями системного адміністратора та керівників відділів

Для створення ефективного та надійного методу контролю необхідно буде об'єднати дві локальні мережі, на першому та другому поверсі, в одну, адже це спростить моніторинг дій зазначених користувачів, та позбавить системного адміністратора від необхідності звертатися до серверу через глобальну мережу інтернет.

Для цього достатньо з'єднати комутатор в «Серверній» із комутатором в «відділі продаж».

Після створення однієї мережі, на ПК, що належать керівникам відділів розробки та системному адміністратору слід встановити та відповідно налаштувати SysLog.

Дане програмне забезпечення дозволяє створювати журнал дій користувача та надсилати його до іншого пристрою. Має гнучкі налаштування та може збирати данні з декількох пристроїв і надсилати їх на один.

Цю програму слід налаштувати наступним чином:

- Створювати журнал дій, що враховуватиме дії, що стосуються мережі, так дій, що доступні лише системному адміністратору та керівникам відділів, див табл. 1.8
- Надсилати отримані журнали системному адміністратору та керівникам відділів.

Таким чином, ця система не буде діяти, лише в разі критичних збоїв мережі, тобто в момент коли реалізація потенційної загрози з боку зазначених працівників не можлива. Контроль за діями зазначених працівників буде здійснюватися ними самими, таким чином для реалізації потенційної загрози кожному з зазначених співробітників необхідно буде

змовитися або бути підкупленими. Хоча це теоретично можливо, проте затрати на реалізацію подібної загрози не будуть відповідати отриманій вигоді, а тому це не є реальним.

2.5 Контроль доступу до «Серверної»

Оскільки програми встановлені на сервері виконують тестування та перевірки ПЗ автоматично, а право доступу до серверу є лише в системного адміністратора та керівників відділів розробки, доступ до «Серверної» необхідно обмежити.

Найнадійнішим рішенням буде використання магнітного замку з панеллю для введення коду, аналогічного до того, що використовується на вхідних дверях, SEVEN CR-775S EM-Marin. При цьому використовувати лише з кодовим замком.

Таким чином можливо буде обмежити круг співробітників, що мають доступ до «Серверної» та зменшити ризик потрапляння до неї сторонніх людей, шляхом уникання використання фізичного ключа.

2.6 Політика віддаленої праці

Беручі до уваги попередні запропоновані рішення, одним із найбільших джерел загроз залишається використання особистого ПК під час віддаленої роботи.

Оптимальним рішення для забезпечення безпечної віддаленої роботи є використання спеціалізованого ПЗ. Серед ряду можливих програм я надаю перевагу TeamViewer.

Данна програма дозволяє отримувати віддалений доступ до ПК та відрізняється рядом переваг в порівнянні із аналогами. До них входить можливість налаштування доступу до файлів, налаштування та обмеження пристроїв, що можуть підключатися до одного ПК, захист даних та можливість віддаленого ввімкнення та вимикання ПК.

Використання «Корпоративної» версії програми також дозволить використовувати її в якості ПЗ для моніторингу дій користувачів.

Таким чином, системному адміністратору необхідно встановити та відповідно налаштувати TeamViewer на всі ПК в ІТС. А саме налаштувати обмежений доступ до фалів та програм які використовуються співробітниками під час роботи, налаштувати моніторинг дій в мережі та можливість віддаленого вимкнення та вмикання ПК.

Для працівників необхідно буде провести організаційні заходи із інформування про нову політику віддаленої роботи та для надання знань, що до особливостей її використання.

2.7 Налаштування операційної системи

Відсутність своєчасного оновлення операційної системи чи ряду ПЗ може спричиняти конфлікти версій оброблюваних файлів, чим загрожує їх цілісності. На ряду із цим відсутність оновлень загрожує цілісності АС та ІТС в цілому, адже прогалини в безпеці застарілих версій операційних систем та ПЗ становлять для неї загрозу.

Для налаштування автоматичного оновлення в операційній системі Ubuntu необхідно встановити та налаштувати відповідній пакет ПЗ.

Системному адміністратору необхідно виконати інсталяцію та налаштування цього пакету для оновлення операційних систем та ПЗ, що встановлено на ПК. Оптимальним часом для оновлення ПЗ буде обідня перерва з 12:00 до 13:00, а для оновлення системи при закінчені роботи.

Для додаткового візуального захисту інформації на ПК, рекомендовано налаштувати таймер автоматичного блокування на 5 хвилин, та позбавити користувачів можливості зміни даного часу.

2.8 Корегування розташування відеокамер

Через актуальне розміщення камер відеоспостереження на ОІД виникають сліпі зони, частина яких є потенційно небезпечною

На першому поверсі в «Відділі HR» слід встановити камеру так, щоб вона була спрямована на кут будівлі та охоплювала покриттям всю кімнату та обидва вікна, що в ній розташовані.

На першому поверсі в «Відділі бухгалтерії» слід встановити камеру так, щоб вона могла спостерігати всю кімнату та вікно в ній.

На першому поверху в «Відділі продаж» камеру необхідно переставити в діагонально протилежний кут так, щоб вона могла спостерігати всю кімнату і обидва вікна в ній.

На першому поверху в «Кабінеті системного адміністратора» камеру слід переставити в кут біля дверей так, щоб вона спостерігала всю кімнату та обидва вікна.

Оскільки висота вікна на другому поверсі приблизно становить 3,4 м, немає необхідності спрямовувати камери до віко. Таким чином, лише камеру в «Відділ Android розробки» необхідно представити в кут будівлі, щоб позбутися невеликої сліпої зони де розташовані двері.

Загалом необхідно встановити дві додаткові камери та переставити три камери.

Нижче наведено генеральні плани першого та другого поверху із запропонованими змінами.

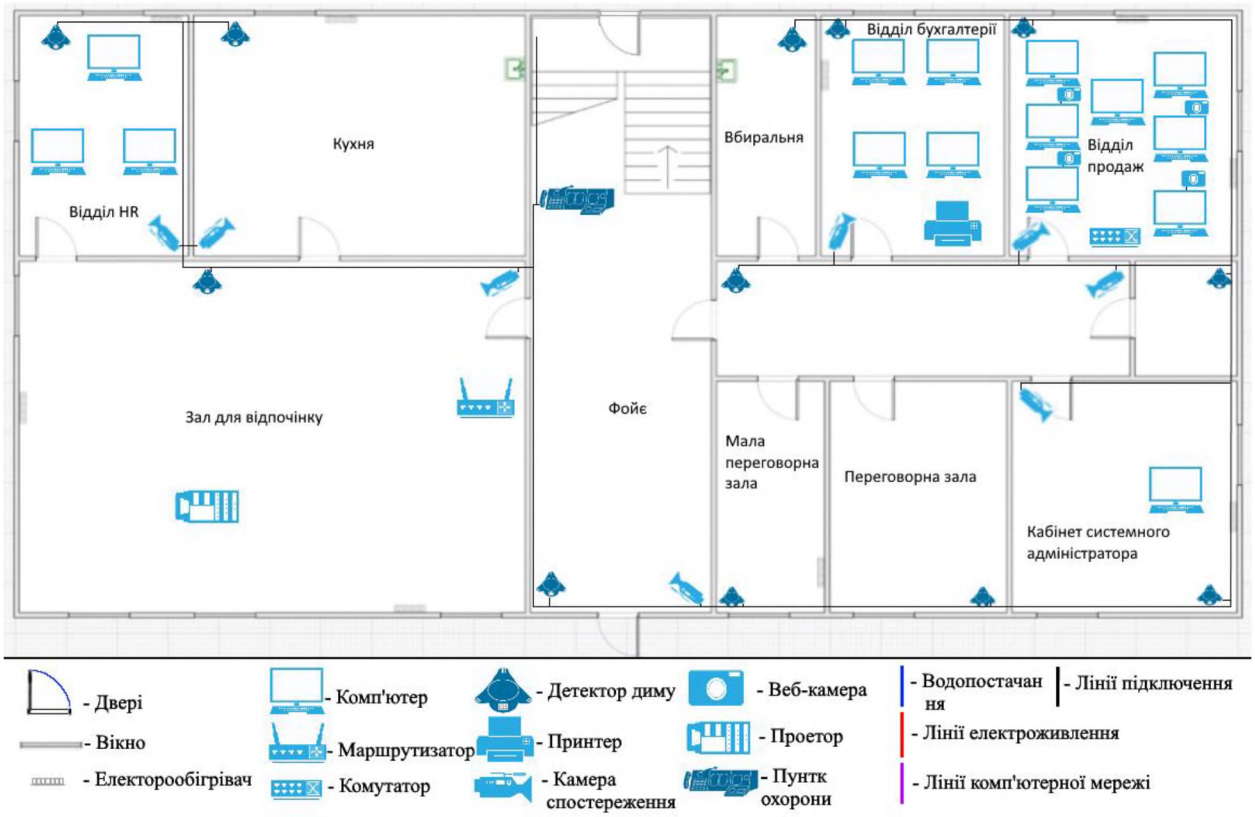

Рисунок 2.1 - Генеральний план першого поверху ОІД із лініями підключення охоронної системи

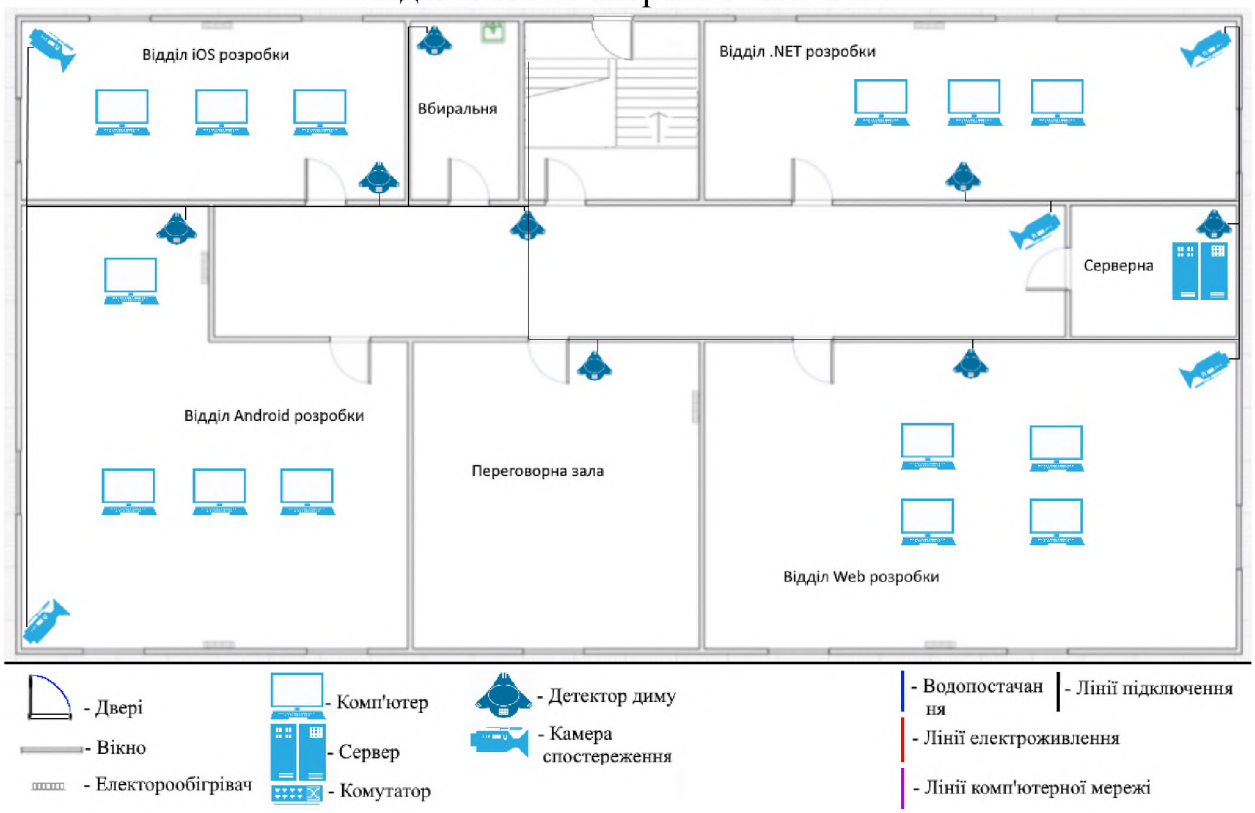

Рисунок 2.2 - Генеральний план другого поверху ОІД із лініями підключення охоронної системи

2.9 Встановлення захисту для вікон

Враховуючи кількість вікон на першому поверсі, їх розташування та можливість спостереження через них за розташуванням приладів та камер, необхідно встановити засоби протидії або сповіщення про проникнення.

Для запобігання проникненню, найкращім рішенням є встановлення гратів. В такому разі всього необхідно буде встановити чотирнадцять гратів.

Оскільки на об'єкті вже цілодобово присутні співробітники служби безпеки, пристрої про сповіщення будуть так само ефективні в разі проникнення на територію ОІД.

Беручі до уваги, що вікна неможливо відчинити навстіж, зрозуміло, що для проникнення через них необхідно розбити скло. В такому випадку для сповіщення можливо використовувати датчик розбиття скла.

Для внутрішнього встановлення та для підключення до посту охорони гарним рішенням стане Crow GBD-plus. Необхідно буде встановити та приєднати всі чотирнадцять датчиків до пункту охорони.

Нижче наведено генеральний план першого поверху із урахуванням встановлених датчиків.

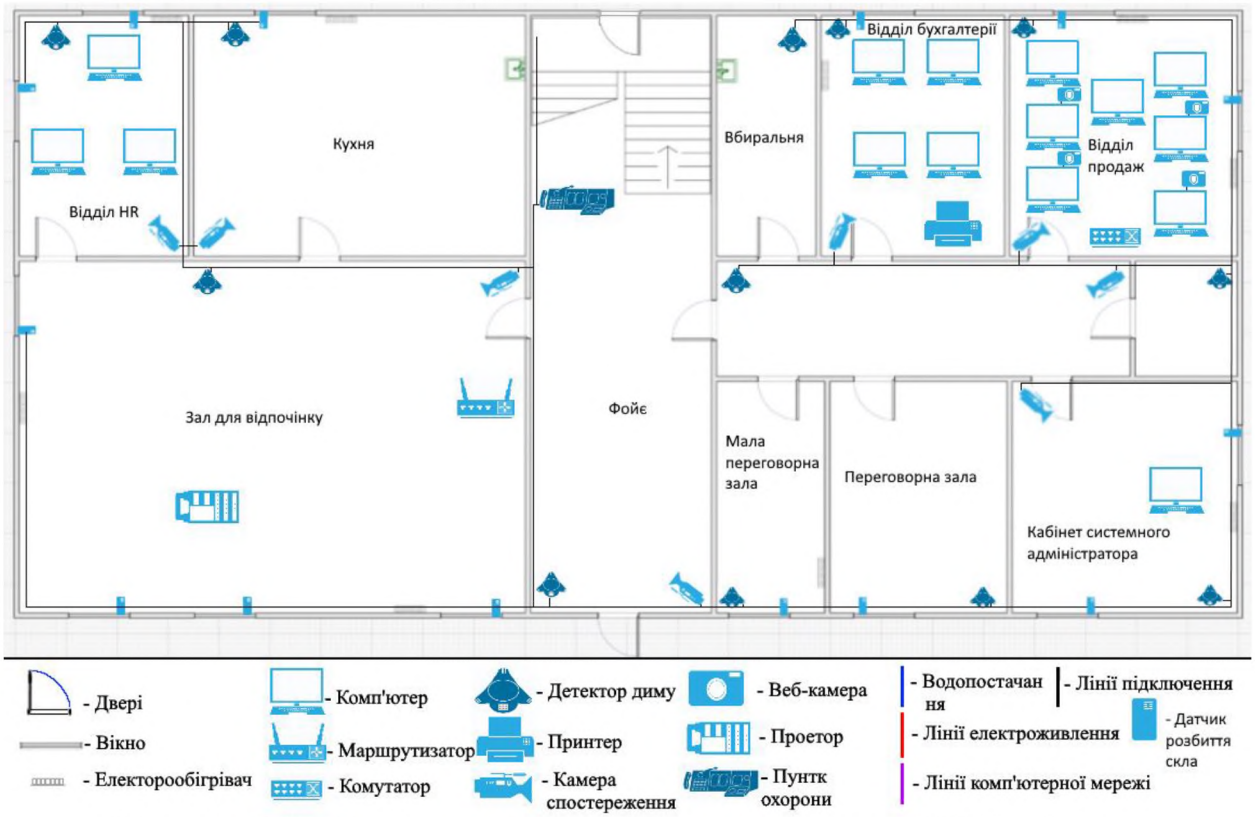

Рисунок 2.3 - Генеральний план першого поверху ОІД із лініями підключення охоронної системи

2.10 Висновки

Приведені рішення, здебільшого, є організаційними заходами та використовують мінімальну кількість ресурсів на впровадження програмних та апаратних рішень. Головними чинниками цього є специфіка роботи компанії та використання операційної системи Ubuntu.

Використання цієї системи дозволяє гнучко й ефективно налаштовувати як мережу взагалі, так і можливості та права доступу конкретних її користувачів. Це в свою чергу дозволяє ефективніше будувати ІТС та використовувати ресурси.

РОЗДІЛ 3. ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ

3.1 Розрахунок витрат

В даній частині буде розрахована і обґрунтована економічна доцільність впровадження комплексної системи захисту інформації для компанії.

З цією метою необхідно розрахувати капітальні витрати, термін окупності інвестицій та їх коефіцієнт.

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

Відповідно до Gartner Group до капітальних витрат відносяться наступні:

- Витрати на розробку проекту КСЗІ;
- Витрати на закупівлю апаратного забезпечення;
- Витрати на закупівлю ліцензованого ПЗ;
- Витрати на встановлення апаратного та програмного забезпечення;
- Витрати на навчання працівників та обслуговуючого персоналу.

Вартість розробки КСЗІ складається з двох показників:

- Трудомісткість розробки КСЗІ;
- Витрати на розробку КСЗІ.

3.2 Трудомісткість розробки КСЗІ

Формула розрахунку трудомісткості розробки КСЗІ:

$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}$, годин

де $t_{тз}$ – тривалість складання технічного завдання на розробку КСЗІ – складає 8 год.;

$t_{в}$ - тривалість розробки концепції безпеки інформації у організації – складає 17 год.;

$t_{а}$ – тривалість процесу аналізу ризиків – складає 8 год.;

tвз – тривалість визначення вимог до заходів, методів та засобів захисту – складає 6 год.;

tозб – тривалість вибору основних рішень з забезпечення безпеки інформації – складає 6 год.;

товр – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації – складає 8 год.;

tд – тривалість документального оформлення політики безпеки – складає 6 год.;

Враховуючи зазначені данні формула має наступний вигляд:

t = 8 + 17 + 8 + 6 + 6 + 8 + 6 = 59 годин

Таким чином трудомісткість розробки КСЗІ складатиме 59 годин.

3.3 Витрати на створення елементів КСЗІ

Формула розрахунку витрат на створення елементів КСЗІ:

Крп = Ззп + Змч грн.

де Ззп – витрати на заробітну плату спеціаліста з інформаційної безпеки;

Змч – вартість машинного часу для розробки КСЗІ.

Формула витрат на заробітну плату спеціаліста з інформаційної безпеки:

Ззп = t * Зіб грн.

де t - загальна тривалість розробки політики безпеки, або трудомісткість розробки КЗСІ – складає 59 год.;

Зіб - средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину – складає 160 грн/год.;

Враховуючи зазначені данні формула має наступний вигляд:

Ззп = 59 * 160 = 9440 грн/год.

Таким чином, витрати на заробітну плату спеціаліста з інформаційної безпеки складатимуть

Формула вартості машинного часу для розробки КСЗІ:

Змч = t * Смч, грн.

де t - загальна тривалість розробки політики безпеки, або трудомісткість розробки КЗСІ – складає 59 год.;

Смч - вартість 1 години машинного часу ПК, грн./год.

Формула вартості 1 години машинного часу ПК:

Смч = Р * tнал * Се + (Фзал * На)/Fр + (Клпз * Напз)/Fр, грн.

де Р - встановлена потужність ПК – складає 0,09 кВт;

tнал – кількість задіяних робочих станцій при створенні КСЗІ – складає 1;

Се – тариф на електричну енергію – складає 1,68 грн/кВт*год;

Фзал – залишкова вартість ПК на поточний рік – складає 24 грн.;

На – річна норма амортизації на ПК – складає 0,4;

Напз – річна норма амортизації на ліцензійне програмне забезпечення – складає 0,5;

Клпз – вартість ліцензійного програмного забезпечення – складає 0 грн.;

Fр – річний фонд робочого часу – складає 1920 год.

Враховуючі зазначені данні формула матиме наступний вигляд:

Смч = 0,09 * 1 * 1,68 + (24 * 0,4)/1920 + (0 * 0.5)/1920 = 0,1562 грн/год.

Таким чином, вартість 1 години машинного часу складає 0,1562 грн/год., тоді формула вартості машинного часу для розробки КСЗІ матиме наступний вигляд:

Змч = 59 * 0,1562 = 9,22 грн

Таким чином, вартість машинного часу для розробки КСЗІ складає 9,22 грн., а формула розрахунку витрат на створення елементів КСЗІ має наступний вигляд:

Крп = 9440 + 9,22 = 9449,22 грн.

Таким чином, витрати на створення елементів КСЗІ складають 9449,22 грн.

3.4 Капітальні витрати

Формула капітальних витрат на проектування та впровадження проектного варіанту КСЗІ:

К = Кпр + Кзпз + Каз + Кнавч + Кн, грн

де Кпр – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, оскільки зовнішніх консультантів не залучали – замінюється на Крп і складає 9449,22 грн.;

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення – складає 55322,63 грн., що складається з вартості річної корпоративної ліцензії TeamViewer;

Каз – вартість закупівлі апаратного забезпечення та допоміжних матеріалів – складає 11972 грн., що складається з магнітного замка з контролером доступу SEVEN CR-775S EM-Marin, двох камер Dahua DH-HAC-HDW1200RP-BE, чотирнадцяти USB накопичувачів Mibrand Panther 8GB та чотирнадцяти датчиків розбиття скла Crow GBD-plus;

Кнавч – витрати на навчання технічних фахівців і обслуговуючого персоналу – складає 0;

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки – складає 4350 грн.

Враховуючи зазначені данні формула матиме наступний вигляд:

К = 9449,22 + 55322,63 + 11972 + 0 + 4350 = 81093,85 грн.

Таким чином, капітальні витрати складатимуть 81093,85 грн.

3.5 Експлуатаційні витрати

Експлуатаційні витрати - це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період, що виражені у грошовій формі. В данному випадку обрано річний період.

Формула річних експлуатаційних витрат:

С = Св + Ск + Сак, грн.

де Св – upgrade-відновлення системи інформаційної безпеки – складає 55322,63 грн.;

Сак - витрати, викликані активністю користувачів системи інформаційної безпеки – складає 0;

Ск - витрати на керування системою в цілому;

Формула витрат на керування системою:

Ск = Сн + Са + Сз + Сєв + Сел + Со + Стос, грн.

де Сн – витрати на навчання адміністративного персоналу й кінцевих користувачів – складає 1000 грн.;

Са – річний фонд амортизаційних відрахувань – складає 9750 грн.;

Со – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування – складає 0 грн.;

Стос – витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки, визначається у відсотках від вартості капітальних витрат (1-3%) – складає 1621,88 грн.;

Сз - річний фонд заробітної плати інженерно-технічного персоналу

Формула річного фонду заробітної плати інженерно-технічного персоналу:

Сз = Зосн + Здод, грн.

де Зосн – основна заробітна плата відповідно, грн. на рік – складає 120000 грн.;

Здод - додаткова заробітна плата відповідно, грн. на рік – складає 12000 грн.

Враховуючі зазначені данні, формула річного фонду заробітної плати інженерно-технічного персоналу матиме наступний вигляд:

Сз = 120000 + 12000 = 132000 грн.

Таким чином, річний фонд заробітної плати інженерно-технічного персоналу, або Сз – складає 132000 грн.;

Сєв – єдиний внесок на загальнообов'язкове державне соціальне страхування – складає 29040 грн.;

Сел – вартість електроенергії;

Формула вартості електроенергії:

Сел = Р * Fр * Це, грн.

де Р – потужність апаратури інформаційної безпеки – складає 0,192 кВт.;

Fр – річний фонд робочого часу системи інформаційної безпеки – складає 8760 год.;

Це – тариф на електроенергію – складає 1,68 грн/кВт*год

Враховуючі зазначені данні, формула вартості електроенергії матиме наступний вигляд:

Сел = 0,192 * 8760 * 1,68 = 2825,63 грн.

Таким чином, річна вартість електроенергії складає 2825,63 грн. , тоді формула витрат на керування системою матиме наступний вигляд:

Ск = 1000 + 9750 + 132000 + 29040 + 2825,63 + 0 + 1621,88 = 176237,51 грн

Таким чином, річні витрати на керування системою складають 176237,51 грн, тоді формула річних експлуатаційних витрат матиме наступний вигляд:

С = 55322,63 + 176237,51 + 0 = 231560,14 грн.

Таким чином, експлуатаційні витрати складають 231560,14 грн.

3.6 Величина збитків

До збитків, що впливають на ефективність КСІБ відносяться наступні:

- порушення конфіденційності ресурсів КСІ;
- порушення доступності ресурсів КСІБ;
- порушення цілісності ресурсів КСІБ;
- порушення автентичності ресурсів КСІБ.

Формула упущеної вигоди від простою атакованого вузлу або сегмента корпоративної мережі:

$U = Пп + Пв + V,$ грн.

де Пп - оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі;

Формула оплачуваних втрат робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі:

$Пп = (\Sigma Зс/F)*tп,$ грн.

де Зс – загальна кількість витрат на заробітну плату співробітників за місяць – складає 14000 грн.;

F – місячний фонд робочого часу – складає 160 год.;

tп – час простою внаслідок атак – складає 12 год.

Враховуючи зазначені данні, формула оплачуваних втрат робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі матиме наступний вигляд:

$Пп = (14000/160)*12 = 1050$ грн.

Таким чином, оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, або Пп, складають 1050 грн.;

Пв - вартість відновлення працездатності вузла або сегмента корпоративної мережі;

Формула вартості відновлення працездатності вузла або сегмента корпоративної мережі:

Пв = Пви + Ппв + Пзч, грн.

де Пви – витрати на повторне уведення інформації;

Формула витрат на повторне уведення інформації:

Пви = (ΣЗс/F)*tви, грн.

де tви – час необхідний для повторного внесення інформації – складає 45 хв.;

Враховуючи зазначені данні, формула витрат на повторне уведення інформації матиме наступний вигляд:

Пви = (14000/160) * 45 = 3937,5 грн.

Таким чином, витрати на повторне уведення інформації, або Пви, складають 3937,5 грн.;

Ппв – витрати на відновлення вузла або сегмента корпоративної мережі;

Формула витрат на відновлення вузла або сегмента корпоративної мережі:

Ппв = (ΣЗо/F)*tв, грн.

де Зо – заробітна плата системного адміністратора – складає 12000 грн.;

F – місячний фонд робочого часу – складає 160 год.;

tв – час на введення загубленої інформації унаслідок атаки – складає 20 год.

Враховуючи зазначені данні, формула витрат на відновлення вузла або сегмента корпоративної мережі матиме наступний вигляд:

Ппв = (12000/160)*20 = 1500 грн.

Таким чином, витрати на відновлення вузла або сегмента корпоративної мережі складають 1500 грн.;

Пзч – вартість заміни устаткування або запасних частин – складає 21500 грн.

В Враховуючи зазначені данні, формула вартості відновлення працездатності вузла або сегмента корпоративної мережі матиме наступний вигляд:

Пв = 3937,5 + 1500 + 21500 = 26937,5 грн.

Таким чином, вартість відновлення працездатності вузла або сегмента корпоративної мережі, вона ж Пв, складає 26937,5 грн.

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

Формула втрат від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі:

V = (O/Fr) * (tп +tв+tви), грн.

де О – обсяг продажів атакованого вузла або сегмента корпоративної мережі – складає приблизно 14178460,80 грн.;

Fг – річний фонд часу роботи організації – складає 1920 год.;

tп – час простою вузла унаслідок атаки – складає 12 год.;

tв = час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі – складає 20 год.;

tви = час відновлення після атаки персоналу, що обслуговує корпоративну мережу – складає 24 год.

Враховуючи зазначені данні, формула втрат від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі матиме наступний вигляд:

V = (14178460,80 / 1920) * (12 + 20 + 24) = 413 538,44 грн.

Таким чином, втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі складають 413 538,44

грн., тоді формула упущеної вигоди від простою атакованого вузлу або сегмента корпоративної мережі матиме наступний вигляд:

U = 1050 + 26937,5 + 413 538,44 = 441 525,94 грн.

Таким чином, упущена вигода від простою атакованого вузлу або сегмента корпоративної мережі складає 441 525,94 грн.

Формула загальних збитків від атаки:

B= Σi Σn*U, грн.

де i - кількість атакованих вузлів – складає 3;

n – кількість прогнозованих атак – складає 2.

Враховуючи наведені данні, формула загальних збитків від атаки матиме наступний вигляд:

B= 3 * 2 * 441 525,94 = 2 649 155,64 грн.

Таким чином, загальні збитки від атак за рік складатимуть 2 649 155,64 грн.

3.7 Ефект від впровадження КСЗІ

Загальний ефект від впровадження КСЗІ розраховується враховуючи ризики порушення інформаційної безпеки.

Формула ефекту від впровадження КСЗІ:

E = B * R - C, грн.

де B – загальний збиток від атаки у разі перехоплення інформації – складає 2 649 155,64 грн.;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі – складає 0.5;

C – щорічні витрати на експлуатацію системи інформаційної безпеки – складає 231560,14 грн.

Враховуючи зазначені данні, формула ефекту від впровадження КСЗІ матиме наступний вигляд:

E = 2 649 155,64 * 0.5 - 231560,14 = 1 093 017,68 грн.

Таким чином, ефект від впровадження КСЗІ складатиме 1 093 017,68 грн.

3.8 Економічна ефективність КСЗІ

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

Формула коефіцієнт повернення інвестицій:

ROSI = E/K,

де E – загальний ефект від впровадження системи інформаційної безпеки – складає 1 093 017,68 грн.;

K – капітальні інвестиції – складає 81093,85 грн.

Враховуючи наведені данні, формула коефіцієнт повернення інвестицій матиме наступний вигляд:

ROSI = 1 093 017,68 / 81093,85 = 13,48

Таким чино, коефіцієнт повернення інвестицій складає 13,48.

Термін окупності капітальних інвестицій відображає, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження КСЗІ.

Формула терміну окупності:

To = 1/ ROSI

Враховуючи попередні розрахунки, формула терміну окупності матиме наступний вигляд:

To = 1/ 13,48 = 0,074

Таким чином, термін окупності складатиме 27 діб.

3.9 Висновок

Згідно за даними отриманими в 3 частині, капітальні затрати на впровадження КСЗІ, складають 81093,85 грн., експлуатаційні - 231560,14 грн. Загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складає 2 649 155,64 грн. Загальний ефект від впровадження КСЗІ складає 1 093 017,68 грн. Коефіцієнт ROSI склав 13,48.

Отже створення та впровадження елементів політики безпеки є цілком доцільним, а термін окупності елементів політики безпеки становить 27 днів.

ВИСНОВКИ

Під час проведення кваліфікаційної роботи було обґрунтовано необхідність створення комплексної системи захисту інформації для підприємства “CleverPath”, проведено обстеження об’єкту інформаційної діяльності та його інформаційно-телекомунікаційної системи відповідно до НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». На підставі отриманих даних були розроблені модель загроз, модель порушника та визначені вразливості і актуальні загрози відповідно до НД ТЗІ 3.1-001-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Перед проектні роботи».

Обрано профіль захищеності відповідно до НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу» та НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу». З метою захисту та мінімізації збитків від визначених загроз були розроблені наступні проектні та організаційні рішення: введення контролю за використанням ПЗ, розробка політики обігу інформації та використання зовнішніх носіїв інформації, впровадження контролю за діями системного адміністратора та керівників відділів розробки, обмеження доступу до «Серверної», розроблення політики віддаленої праці, налаштування операційної системи працівників, зміна кількості та розташування відеокамер та встановлення датчиків розбиття скла на вікна першого поверху.

Доцільність впровадження зазначених рішень було доведено в економічній частині кваліфікаційної роботи.

ПЕРЕЛІК ПСИЛАНЬ

1. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».
2. Закон України «Про захист прав споживачів» від 12.05.91.
3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5.07.94.
4. Закон України «Про інформацію» від 2.10.92.
5. Закон України «Про доступ до публічної інформації» від 13.01.11.
6. НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці».
7. НД ТЗІ 3.7-001-99 « Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі».
8. НД ТЗІ 1.1-005-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення».
9. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».
10. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу».
11. НД ТЗІ 3.1-001-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Перед проектні роботи».

12.НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».
13.НД ТЗІ 2.6-001-11 «Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах»
14.НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ ДИПЛОМНОЇ РОБОТИ

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	59	
6	А4	2 Розділ	10	
7	А4	3 Розділ	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	2	

ДОДАТОК Б. ПЕРЕЛІК МАТЕРІАЛІВ НА ОПТИЧНОМУ НОСІЇ

- Ткачук В.І. 125-18-3.doc
- Ткачук В.І. 125-18-3.pp
- Ткачук В.І. 125-18-3.pdf
- Підпис.p7s

ДОДАТОК В. ВІДГУК

ВІДГУК

на кваліфікаційну роботу студента групи 125-18-3

Ткачука Владислава Ігоровича

на тему: «Створення комплексної системи захисту інформації підприємства "CleverPath"»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 85 сторінках.

Метою кваліфікаційної роботи є розробка рішень щодо захисту від загроз інформаційної безпеки в інформаційно-телекомунікаційної системі ТОВ “CleverPath”.

Тема кваліфікаційної роботи безпосередньо пов’язана з об’єктом діяльності бакалавра спеціальності 125 “Кібербезпека”. Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз нормативно-правової бази у сфері забезпечення кібербезпеки, виконання акту обстеження ІТС, визначення переліку актуальних загроз.

Розроблено організаційні і проектні рішення щодо захисту підприємства від актуальних загроз, створено відповідні розділи політики безпеки.

Практичне значення результатів кваліфікаційної роботи полягає у розробленій комплексній системі захисту інформації для підприємства та обґрунтуванні економічного ефекту від її впровадження.

За час дипломування Ткачук В.І. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Рівень запозичень у кваліфікаційній роботі не перевищує вимог “Положення про систему виявлення та запобігання плагіату”.

Кваліфікаційна робота заслуговує оцінки «_____».

Керівник
кваліфікаційної роботи доц. каф. БІТ, к.т.н. Сафаров О.О.

Керівник спец. розділу доц. каф. БІТ, к.т.н. Сафаров О.О.