**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** Чумака Владислава Івановича

**академічної групи** 125-19-2

**спеціальності** 125 Кібербезпека

**спеціалізації** _____

**за освітньо-професійною програмою** Кібербезпека

**на тему** Політика безпеки інформації інформаційно-комунікаційної системи закладу ресторанного господарства «KFC»

| Керівники | Прізвище ініціали | Оцінка за шкалою | | Підпис |
|---|---|---|---|---|
| | | рейтинговою | інститутною | |
| Кваліфікаційної роботи | к.т.н., доц. Сафаров О.О | | | |
| Розділів | | | | |
| Спеціальний | ст. в. Тимофєєв Д.С. | | | |
| Економічний | к.е.н., доц. Пілова Д.П. | | | |
| **Рецензент** | | | | |
| **Нормоконтролер** | | | | |

**Дніпро**
**2023**

**ЗАТВЕРДЖЕНО:**
завідувач
кафедрибезпеки інформації та
телекомунікацій
_____д.т.н., проф.
Корнієнко В.І.

«_____»_____20___року

# ЗАВДАННЯ
## на кваліфікаційну роботу ступеня бакалавра

**Студенту** **Чумаку В.І.** **академічної групи** **125-19-2**
(прізвище та ініціали) (шифр)

**спеціальності** **125 Кібербезпека**

**спеціалізації**

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

**на тему** **Політика безпеки інформації інформаційно-комунікаційної системи закладу ресторанного господарства «KFC»**

Затверджену наказом ректора НТУ «Дніпровська політехніка» від_____№ _____

| Розділ | Зміст | Термін виконання |
|---|---|---|
| Розділ 1 | Визначається стан питання, для побудови КСЗІ | 15.05.2023 |
| Розділ 2 | Визначаються основні відомості про підприємство на базі ОІД | 30.05.2023 |
| Розділ 3 | Розрахувати економічну частину | 05.06.2023 |

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

Дата видачі завдання: 01.05.2023

Дата подання до екзаменаційної комісії: 19.06.2023

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

# РЕФЕРАТ

Пояснювальна записка: __с., __ рис., __ табл., __ додатки, __ джерела.

Предмет розробки: Політика безпеки інформації інформаційно-комунікаційних систем закладу ресторанного господарства «KFC»

Об'єкт розробки: Компанія ТОВ «Тесті фуд». Заклади ресторанного господарства «KFC», компанія займається наданням харчових товарів та послуг у сфері обслуговування.

Мета роботи: Підвищення рівня захисту інформації з обмеженим доступом, приватної компанії ТОВ «Тесті Фуд» у закладах ресторанного господарства «KFC».

У першому розділі кваліфікаційної роботи визначається стан питання, розповідається про підстави створення КСЗІ та ПБ, види різних загроз для великих підприємств у сфері надання послуг.

У другому розділі визначаються основні відомості про підприємство. Досліджено інформаційну систему, обстежено фізичне середовище, середовище покупців, середовище співробітників, Проаналізовано метод обробки інформації, сукупність методів захисту інформації. Структуровано внутрішню інформацію підприємства, знайдено основні вразливості, їх причини, створено модель порушника. Створено головні методи запобігання нанесення шкоди підприємству та інформації підприємства.

У третьому розділі було розраховано всі витрати на впровадження методів запобігання нанесення шкоди підприємству та інформації підприємства, також щорічні витрати на підтримку методів запобігання шкоди. Також було розраховано затрати на впровадження захисту інформації підприємства та захисту підприємства.

ІНФОРМАЦІЙНА БЕЗПЕКА, ПОЛІТИКА БЕЗПЕКИ, ЗАХИСТ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНИЙ АКТИВ, ВРАЗЛИВОСТІ, ПРОФІЛЬ ЗАХИЩЕННОСТІ ІНФОРМАЦІЇ

ABSTRACT

Explanatory note: __p., __fig., __table, __appendices, __sources.

Development subject: The information security policy of the information and communication system of the «KFC» restaurant establichment.

Object of development: "Testy Food" LLC. "KFC" restaurant establishments, the company is engaged in the provision of food products and services in the field of service.

The purpose of the work: Increasing the level of protection of information with limited access, private company "Testy Food" LLC in "KFC" restaurants.

In the first section of the qualification work, the state of the issue is defined, the reasons for the creation of KSZI and PB, types of various threats to large enterprises in the field of service provision are discussed.

The second section defines basic information about the enterprise. The information system was studied, the physical environment, the environment of customers, the environment of employees was examined, the method of information processing, the set of information protection methods were analyzed. The company's internal information was structured, the main vulnerabilities and their causes were found, and a model of the offender was created. The main methods of preventing damage to the enterprise and enterprise information have been created.

In the third section, all the costs of implementing methods of preventing damage to the enterprise and information of the enterprise, as well as the annual costs of maintaining the methods of preventing damage, were calculated. The costs of implementing enterprise information protection and enterprise protection were also calculated

INFORMATION SECURITY, SECURITY POLICY, INFORMATION PROTECTION, INFORMATION ASSETS, VULNERABILITIES, INFORMATION SECURITY PROFILE

# СПИСОК УМОВНИХ СКОРОЧЕНЬ

АЗ – антивірусний захист

АС – автоматизована система

ДСТУ – державний стандарт України

ІБ – інформаційна безпека

ІзОД – інформація з обмеженим доступом

ІТС – інформаційно-телекомунікаційна система

КЗЗ –

КСЗІ – комплексна система захисту інформації

КЦД – конфеденційність, цілісність, доступність

НД ТЗІ – нормативний документ в галузі технічного захисту інформації

НСД – несанкціонований доступ

ОІД – об’єкт інформаційної діяльності

ПБ – політика безпеки

ПБІ – політика безпеки інформації

ПВ – програми вимагачі

ПЗ – програмне забезпечення

ПІП – прізвище, ім’я, по батькові

ТОВ – товариство з обмеженою відповідальністю

ТЦ – торгівельний центр

ЗМІСТ

# ВСТУП

На фоні нинішніх реалій все біль і більше люди віддають перевагу автоматизованим системам в яких використання комп'ютерних технологій та програмного забезпечення дозволяє автоматизувати виконання завдань, процесів та операцій у межах певної діяльності.

Процеси в автоматизованій системі відносяться до послідовності дій або операцій, що виконуються в рамках системи для досягнення певних цілей. Процеси можуть бути зумовлені і стандартизовані, а також можуть включати різні етапи, кроки, ролі і взаємодії між різними компонентами системи. Автоматизовані системи мають багато перевах, наприклад: збільшення продуктивності, автоматизовані системи можуть допомогати у зниженні помилок, пов'язаних з людським фактором, та підвищенні якості виконання операцій, автоматизація дозволяє більш точно контролювати та відстежувати виконання процесів, а також надавати деталізовану інформацію про виконані операції та результати, автоматизовані системи можуть скоротити необхідність вручну виконувати завдання, що дозволяє заощадити час та ресурси організації.

Сфера інформаційних технологій постійно розвивається та зазнає значних змін відповідно до технологічних, соціальних та економічних тенденцій. Інтернет  охоплює мережу фізичних пристроїв, які можуть взаємодіяти та обмінюватися даними через Інтернет. Розвиток IoT технологій дозволяє підключати все більше пристроїв до мережі від побутової техніки до промислового обладнання, створюючи таким чином мережу взаємопов'язаних пристроїв і систем. Зростання інформаційних технологій також спричинило збільшення загроз у сфері кібербезпеки. Розвиток технологій у сфері кібербезпеки спрямовано захист інформаційних систем від зовнішніх загроз, включаючи зловмисницькі атаки, крадіжку даних та інші види шахрайства.

Об’єктом кваліфікаційної роботи є безпека інформації інформаційно -

телекомунікаційних систем ресторанного господарства «КФС» - велике підприємство є ресторанною компанією, що пропонує широкий асортимент курячих страв, працює над розширенням своєї мережі та прагне надати своїм клієнтам якісний досвід харчування швидким шляхом.

Предметом кваліфікаційної роботи є політика безпеки інформації.

Метою кваліфікаційної роботи є розробка політики безпеки інформації у закладах ресторанного господарства. Політика безпеки інформації є актуальною та невід'ємною частиною діяльності будь-якої організації чи підприємства. Політика безпеки інформації допомагає захистити конфіденційність інформації, включаючи персональні дані клієнтів, бізнес-секрети, фінансову інформацію та іншу конфіденційну інформацію, щоб запобігти несанкціонованому доступу або витоку даних. У сучасному цифровому світі організації стикаються з різними кіберзагрозами, такими як шкідливі програми, атаки хакерів, фішинг та інші форми кіберзлочинності. Політика безпеки інформації визначає заходи та процедури для захисту від цих загроз та мінімізації можливих уразливостей. Витік інформації або порушення безпеки може завдати серйозної шкоди репутації організації. Політика безпеки інформації допомагає запобігти таким інцидентам та забезпечує захист репутації, збереження довіри клієнтів, партнерів та зацікавлених сторін.

# 1. ЗМІСТ ПИТАННЯ. ВСТАНОВЛЕННЯ ЗАДАЧІ.

## 1.1 Зміст питання

За статистикою кібератак за 2022 рік можна поспостерігати, що щодня відбувається 2200 кібератак, в середньому на кожні 39 секунд відбувається одна кібератака. Кібербезпека розвивається, але наразі під час воєнного часу кількість кіберзлочинів збільшується все більше і більше. Забезпечення впевненного захисту від кібератак стає все важче. Під час війни ми можемо бачити збільшення хактивізму: коли хакери та кіберактивісти спрямовують свої атаки на організації чи країни, пов'язані з конкретними подіями під час війни. Вони можуть використовувати кібератаки як висловлювання своєї політичної позиції чи створення хаосу. Також велике значення мають кібератаки на критичну інфраструктуру військовий конфлікт може спровокувати кібератаки на критичну інфраструктуру, такі як енергетичні системи, телекомунікації, транспортні системи та інші. Метою таких атак може бути паралізація супротивника чи створення хаосу у суспільстві.

Щодня створюється близько трьохсот тисяч шкідливих програм, близько 92% всіх загроз від шкідливого програмного забезпечення пересилаються поштою і можуть бути виявлені та активовані користувачем протягом 49 днів. За спостереженнями STATISTA до 2026 року ми можемо стати свідками того, що глобальний ринок безпеки як послуг досягне понад 22 мільярдів доларів США.

У 2022 році 71% підприємств стали жертвами атак програм-вимагачів, дані програми стали дуже поширені з Q2 2021 в цей період було скоїно 188,9 мільйонів кібератак. На даний момент программи - вимагачі є найпопулярнішою серед шкідливих програм. Программи - вимагачі набули популярності за рахунок здатності вимагати великі суми грошей, не даючи кіберзлочинцям великих ризиків бути виявленими.

Також велику популярність набув фішинг - крадіжка особистих даних. Виділяючи результати журналу SECURITY MAGAZINE на Q1 і Q2 2022

року було 236 мільйонів замахів програм - вимагачів. За статистикою STATISTA 42% атак були ненавмисно викликані діями користувачів, переходячи по спам посиланням.

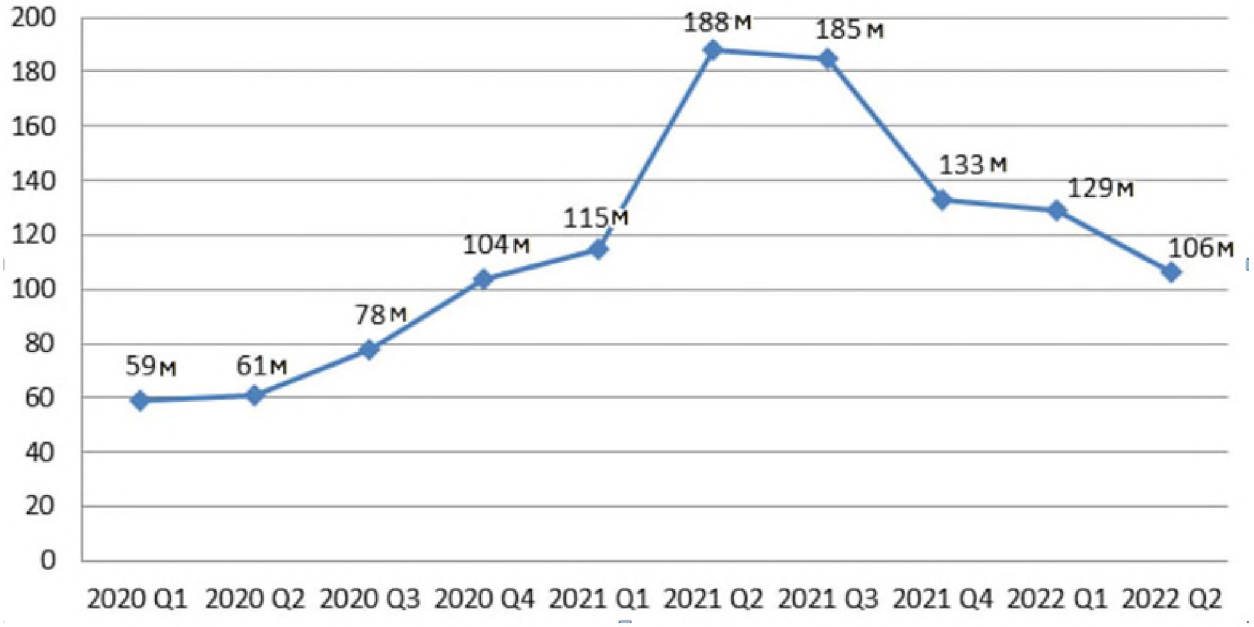


Рисунок 1.1 – Масштаб кібератак програм – вимагачів

Поспостерігавши за Q3 і Q4 2022 року кількість DDos атак збільшилася на 60%, таким чином багато підприємств стали вразливі для збоїв своїх систем, більшість кібератак націлені на перевантаження серверів трафіком що в результаті призводить до збоїв.

На діаграмі 1.2 можемо детальніше роздивитись порівняння різних країн щодо витоку інформації на Q4 2022

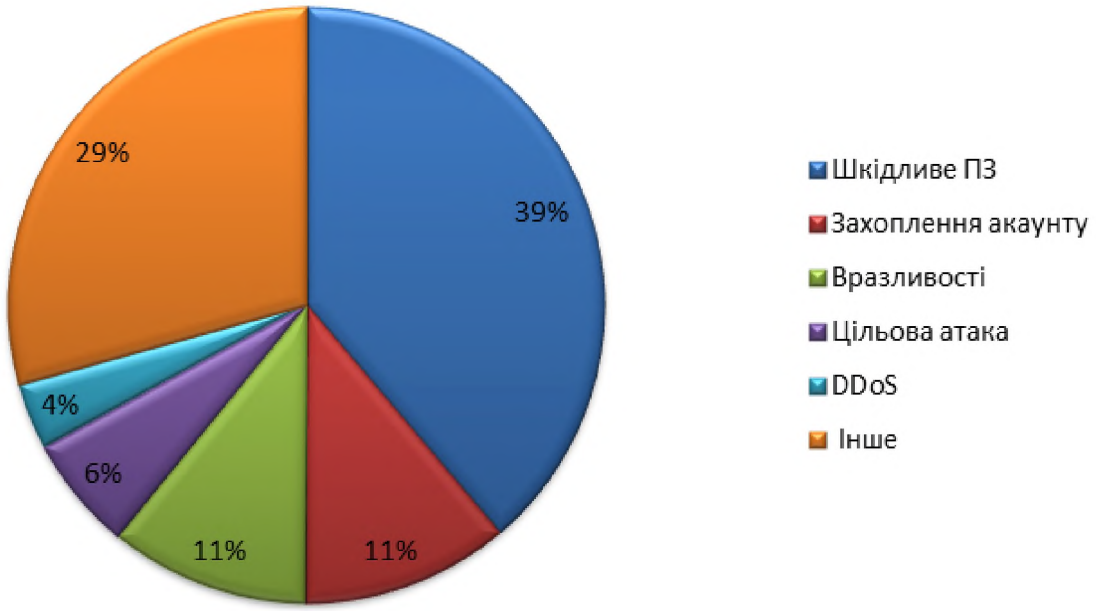


Рисунок 1.2 – Статистика кібератак 2023

Якщо ми роздивимось останні великі кібератаки які були нанесено за останні роки на думку надходить одна з майже недавніх масштабних кібератак, кібератака на SolarWinds 2020 року ця кібератака була однією з найсерйозніших та наймасштабніших. Атака розпочалася зі злому мережі компанії SolarWinds, яка спеціалізується на розробці програмного забезпечення для моніторингу мереж. Зловмисники впровадили шкідливий код в оновлення програмного забезпечення під назвою SolarWinds Orion. Атака почалася щонайменше навесні 2020 року і тривала непоміченою протягом декількох місяців. Зловмисники використовували хитрі методи для приховання своєї присутності та уникали виявлення. Після успішного впровадження шкідливого коду в системи SolarWinds зловмисники отримали доступ до мереж клієнтів, які використовували це програмне забезпечення. Вони перейшли до етапу розвідки, переміщення мережами і виконували додаткові кібератаки. Це призвело до компрометації тисяч організацій, включаючи урядові агенції та великі компанії.

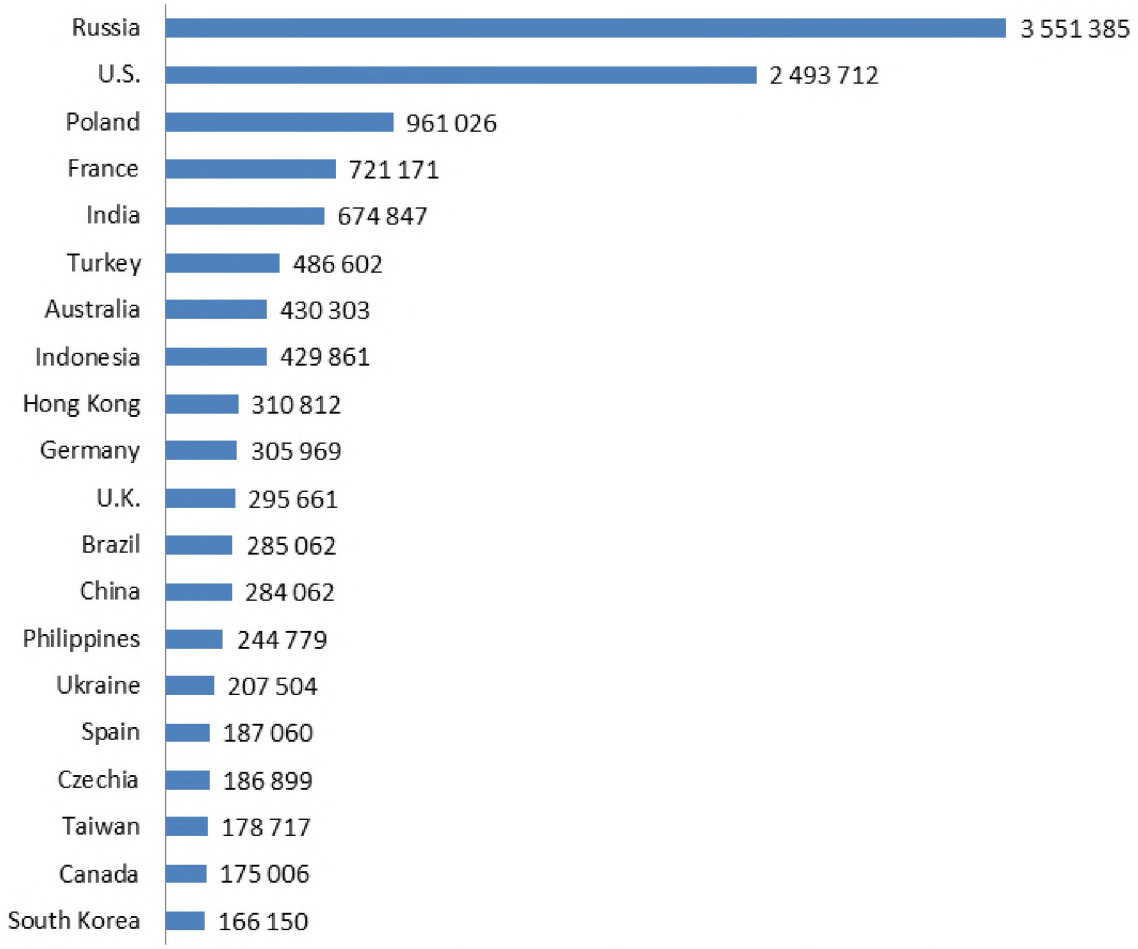


Рисунок 1.3 – Статистика витоку інформації за Q4 2022

В цілому, ресторани та інші підприємства у сфері обслуговування їжею схильні до ризиків кібератак, кібератаки на ресторани стають все більш поширеним явищем у сучасному цифровому світі. Ресторани та кафе часто стають метою хакерів, які можуть прагнути вкрадених даних платіжних карток, особистої інформації клієнтів або навіть завдати шкоди діловій репутації закладу. Кібератаки на ресторани можуть мати різні цілі, включаючи крадіжку фінансових даних, порушення операцій, шантаж та отримання доступу до особистої інформації клієнтів. Ось кілька поширених видів кібератак, які можуть бути спрямовані на ресторани:

— Фішингові атаки: Зловмисники можуть надсилати підроблені електронні листи або повідомлення, вдаючись представниками ресторану або відомих постачальників, щоб зібрати особисті дані, такі як паролі або номери кредитних карток.

— Атаки на POS-термінали: Шкідливе програмне забезпечення може бути встановлене на термінали обробки платежів у ресторані для збору фінансових даних клієнтів.

— DDoS-атаки: Напади відмовою в обслуговуванні (DDoS) можуть бути спрямовані на веб-сайт ресторану, що призведе до перевантаження сервера та тимчасової недоступності для клієнтів. Використання таких методів атак може порушити роботу сайту ресторану, зловмисники можуть залишити негативні відгуки або навіть поширювати неправдиву інформацію про продукти чи послуги закладу.

— Шкідливе програмне забезпечення: Зловмисники можуть впроваджувати зловмисне програмне забезпечення на комп'ютери та системи ресторану, щоб отримати доступ до конфіденційної інформації або нашкодити операціям.

— Соціальна інженерія: Атакуючі можуть використовувати методи соціальної інженерії, щоб обдурити співробітників ресторану та отримати доступ до систем чи інформації, наприклад, через підроблені дзвінки, електронні листи або фальшиві ідентифікаційні дані.

Крім того, ресторани можуть бути атаковані через мережі Wi-Fi, які надаються для зручності гостей. Незахищені або недостатньо захищені Wi-Fi-мережі можуть становити загрозу, що дозволяє хакерам перехоплювати дані клієнтів, такі як імена, адреси, електронні пошти та телефонні номери.

Важливо, що методи кібератак постійно еволюціонують і нові загрози можуть виникати з часом. Ресторани повинні вживати заходів для захисту своїх систем, таких як регулярне оновлення програмного забезпечення.

Також загрози для ресторанів є не тільки з зовні але і у самих закладах, а саме - співробітники ресторанів, у деяких випадках, можуть завдати шкоди закладу, як у сфері інформаційної безпеки, так і здійснюючи різні недобросовісні дії або порушуючи політики та процедури роботи. Наведу декілька прикладів, як співробітники можуть завдати шкоди ресторану:

— Крадіжка: Співробітники можуть красти готівку з каси, алкогольні напої, продукти чи інші цінні предмети з ресторану. Вони можуть також ухилятися від оплати за свої замовлення або надавати хибні знижки своїм знайомим.

— Службові секрети: Співробітники, які мають доступ до конфіденційної інформації, можуть вкрасти або розкрити комерційні секрети ресторану, такі як секретні рецепти, дані про клієнтів або процеси виробництва, завдаючи тим самим шкоди репутації та конкурентоспроможності ресторану.

— Саботаж: Деякі співробітники можуть свідомо шкодити операціям ресторану. Наприклад, вони можуть скидати обслуговування клієнтів, уповільнювати процеси приготування їжі, неправильно пакувати замовлення або пошкоджувати обладнання.

— Несумлінне обслуговування: Співробітники, які не виконують своїх обов'язків належним чином, можуть надавати погане обслуговування клієнтам, що може позначитися на репутації ресторану та збитковості бізнесу.

— Витік конфіденційної інформації: Співробітники, які мають доступ до конфіденційних даних, таких як дані про клієнтів, платіжні реквізити або комерційні секрети, можуть вкрасти, скопіювати або розкрити цю інформацію третім особам. Це може призвести до витоку даних, порушення конфіденційності клієнтів та репутації ресторану.

— Несанкціонований доступ: Співробітники можуть зловживати своїми привілеями доступу до систем ресторану та отримувати доступ до даних або ресурсів, до яких вони не мають повноважень. Це може включати перегляд, зміну або видалення даних, а також порушення системної безпеки.

— Вразливість паролів: Співробітники можуть використовувати слабкі паролі або повторно використовувати їх для різних облікових записів, що робить їх вразливими до злому. Компрометовані паролі можуть відкрити

доступ до систем та інформації ресторану.

— Фішинг та соціальна інженерія: Співробітники можуть стати жертвами фішингових атак або бути ошуканими у наданні доступу до систем чи інформації третім особам. Це може призвести до компрометації облікових записів або доступу до чутливої інформації.

— Несанкціоноване використання ресурсів: Співробітники можуть зловживати доступом до комп'ютерів, мереж або інших ресурсів ресторану, наприклад, встановлення забороненого програмного забезпечення, відвідування шкідливих веб-сайтів або зловживання електронною поштою для надсилання небажаної інформації.

Для захисту інформаційної безпеки ресторану рекомендується вживати таких заходів:

— Реалізувати суворі політики доступу та авторизації для персоналу.

— Навчити співробітників основ інформаційної безпеки та проводити регулярні оновлення навчальних програм.

— Використовувати багатофакторну аутентифікацію та складні паролі для доступу до систем.

— Встановити системи моніторингу та аудиту для виявлення несанкціонованих дій працівників.

— Регулярно оновлювати та забезпечувати безпеку програмного забезпечення та систем ресторану.

— Створити політики безпеки даних, які включають шифрування, резервне копіювання та обмеження доступу до конфіденційної інформації.

Поінформованість та пильність співробітників, а також встановлення відповідних контрольних механізмів відіграють важливу роль у захисті інформаційної безпеки ресторану.

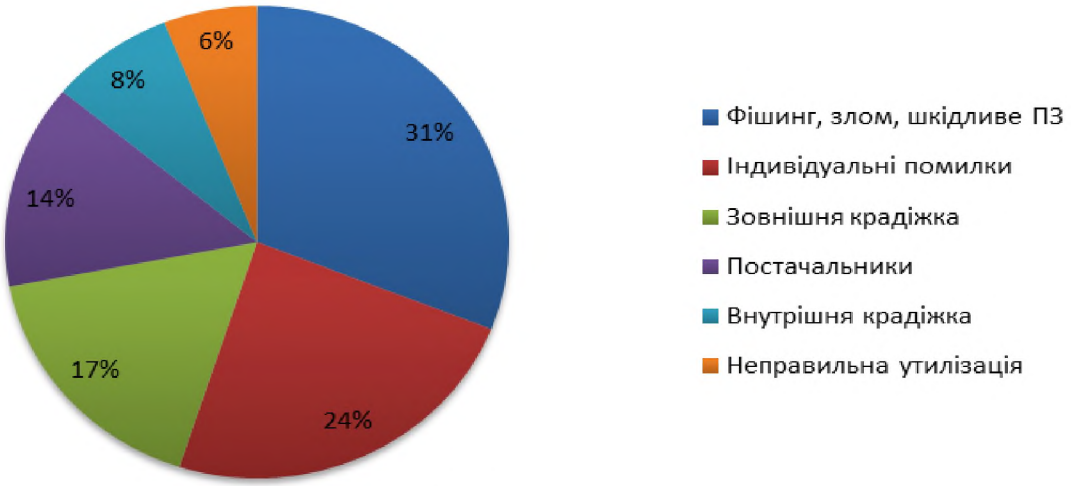


Рисунок 1.4 – Види порушень

1.2 Нормативно – правова база. Забезпечення захисту інформації у сфері кібербезпеки на території України.

В Україні кібербезпека регулюється кількома нормативно-правовими актами. Нижче наведено основні з них:

— Закон України "Про базові засади кібербезпеки" № 2163-VIII. Цей закон було прийнято у 2017 році та визначає основні засади та підходи до забезпечення кібербезпеки в Україні. Він також встановлює механізми для реагування на кібератаки та запобігання інцидентам у сфері інформаційної безпеки.

— Закон України "Про захист персональних даних" №2297-VI. Цей закон регулює збирання, зберігання та обробку персональних даних в Україні. Він встановлює вимоги до організацій із забезпечення безпеки персональних даних та права громадян на захист своєї особистої інформації.

— Кримінальний кодекс України: Кримінальний кодекс містить набір норм, що регулюють злочини у сфері кібербезпеки, такі як несанкціонований доступ до комп'ютерних систем, створення та використання шкідливого програмного забезпечення, шахрайство у сфері інформаційних технологій.

Наведу декілька статей із криминального кодексу України:

Стаття 361 "Незаконне вторгнення до комп'ютерних програм, баз

даних, інформаційних систем або їх частин". Ця стаття встановлює кримінальну відповідальність за незаконне вторгнення до комп'ютерних програм, баз даних, інформаційних систем або їх частин без згоди власника. Це включає такі дії, як несанкціонований доступ до комп'ютерної інформації, шкідливе програмне забезпечення та інші аналогічні дії.

Стаття 361-1 "Створення, використання чи розповсюдження шкідливих програмних комплексів (шкідливого програмного забезпечення)". Ця стаття визначає кримінальну відповідальність за створення, використання або розповсюдження шкідливих програмних комплексів або шкідливого програмного забезпечення. Такі дії можуть завдати серйозної шкоди інформаційним системам та даним.

Стаття 362 "Шахрайство у сфері інформаційних технологій". Ця стаття стосується злочинів, пов'язаних із шахрайством у сфері інформаційних технологій. Зокрема, вона встановлює кримінальну відповідальність за незаконне отримання доступу до коштів або майна шляхом використання інформаційних технологій, включаючи комп'ютерні системи.

Стаття 363 "Порушення правил поводження з інформацією, що зберігається на комп'ютерах, комп'ютерних системах або комп'ютерних мережах". У цій статті розглядається кримінальна відповідальність за порушення правил поводження з інформацією, що зберігається у комп'ютерах, комп'ютерних системах чи комп'ютерних мережах. Це включає такі дії, як знищення, блокування, зміна або копіювання інформації без відповідних дозволів.

Стаття 361-2. "Неправомірний доступ до комп'ютерної інформації". У цій статті встановлюється відповідальність за неправомірний доступ до комп'ютерної інформації шляхом подолання або обходу технічних засобів захисту або порушення правил доступу.

— Закон України "Про телекомунікації" №1280-IX. Цей закон визначає правила та вимоги у сфері телекомунікацій, які також мають пряме

відношення до кібербезпеки. Він містить положення про захист мереж та інформаційних систем від кіберзагроз, про вимоги до операторів зв'язку та провайдерів інтернет-послуг.

Національна стратегія кібербезпеки України. Це стратегічний документ, який встановлює пріоритети та завдання у сфері кібербезпеки національного рівня. Він визначає заходи щодо зміцнення кіберзахисту, співпраці з міжнародними партнерами та підвищення поінформованості про кіберзагрози. Стратегія розробляється з метою забезпечення захисту інформаційних систем, критично важливих об'єктів інфраструктури, персональних даних та забезпечення кібербезпеки в цілому.

Основними принципами Національної стратегії кібербезпеки України є:

Захист національних інтересів: Стратегія спрямована на захист національних інтересів України у кіберпросторі, включаючи національну безпеку, економічну стійкість, правопорядок та демократичні цінності.

Комплексний підхід: Стратегія передбачає комплексний підхід до кібербезпеки, включаючи технічні, правові, організаційні та освітні аспекти.

Міжнародне співробітництво: Стратегія призвана підтримувати та розвивати міжнародне співробітництво з іншими країнами, міжнародними організаціями та приватним сектором для спільного вирішення кіберзагроз.

Розробка кадрів: Стратегія визнає важливість підготовки висококваліфікованих фахівців у галузі кібербезпеки та сприяє розвитку національної кадрової бази.

Основні напрямки діяльності Національної стратегії кібербезпеки України включають:

— Забезпечення стійкості критично важливих об'єктів інфраструктури: Стратегія передбачає заходи щодо захисту критично важливих об'єктів інфраструктури, таких як енергетика, транспорт, фінанси, телекомунікації тощо.

— Захист персональних даних: Стратегія спрямована на забезпечення

конфіденційності, цілісності та доступності персональних даних громадян.

— Запобігання кіберзлочинності: Стратегія включає заходи для запобігання та припинення кіберзлочинності, виявлення та розслідування кіберпорушень.

— Розвиток національної кіберекосистеми: Стратегія спрямована на розвиток національної кіберекосистеми, включаючи створення потужностей для виявлення, відповіді та відновлення після кібератак.

— Підвищення освіти та свідомості: Стратегія підтримує розвиток освіти та підвищення свідомості громадян, бізнесу та державних службовців щодо кібербезпеки.

— Національна стратегія кібербезпеки України регулярно оновлюється для врахування змін у кіберзагрозах та технологічному розвитку. Вона є важливим інструментом для забезпечення стійкості кіберпростору та захисту інформаційної безпеки в Україні.

Термін "політика безпеки" стосується набору принципів, стратегій, процедур та практик, які визначаються організацією або державою для забезпечення безпеки своїх ресурсів, інформації, систем та активів. Політика безпеки є основним документом або набором документів, які визначають загальні принципи та цілі організації в галузі безпеки та встановлюють рамки для прийняття рішень та розробки заходів щодо забезпечення безпеки.

Політика безпеки описує принципи та цілі організації в галузі безпеки, включаючи управління вразливістю, захист від загроз і ризиків, контроль доступу, забезпечення конфіденційності та цілісності даних, забезпечення бізнес-тривалості та відновлення після інцидентів, а також відповідність нормативним вимогам та законодавству.

Політика безпеки повинна відповідати контексту та потребам організації. Вона зазвичай розробляється з урахуванням унікальних аспектів та ризиків, пов'язаних із конкретною організацією, її інфраструктурою та операціями. Важливими аспектами політики безпеки є ясність, зрозумілість

та доступність для всіх співробітників організації, а також постійне оновлення та адаптація у відповідь на нові загрози та зміни у технологічному середовищі.

Ефективна політика безпеки допомагає організації знизити ризики та вразливості, захистити важливі дані та активи, а також забезпечити довіру та конфіденційність клієнтів та партнерів. Вона також є основою для розробки відповідних заходів безпеки, стандартів, процедур та практик, які будуть застосовуватися в організації для забезпечення безпеки та захисту від загроз.

Політика безпеки заснована на різних ресурсах, які допомагають організації визначити та реалізувати свої цілі та стратегії у сфері безпеки. Розбиремося з чого саме складається політика безпеки:

Людські ресурси: людські ресурси є ключовим аспектом безпекової політики. Це включає навчання та підвищення поінформованості співробітників про безпеку, а також встановлення ролей, обов'язків та відповідальності у сфері безпеки. Крім того, важливо мати кваліфікованих фахівців у галузі кібербезпеки, які можуть розробляти та реалізовувати заходи безпеки.

Використання відповідних технологій та інструментів є важливим аспектом політики безпеки. Це може включати системи контролю доступу, антивірусні програми, міжмережеві екрани, системи виявлення вторгнень та інші технічні рішення, які допомагають захистити інформацію та ресурси організації.

Встановлення чітких процесів та процедур є невід'ємною частиною безпекової політики. Це включає розробку правил доступу, процедур контролю, резервного копіювання даних, управління змінами, обробки інцидентів безпеки та інших процесів, які допомагають ефективно керувати безпекою.

Доступ до актуальної інформації про нові загрози, уразливості та найкращі практики є важливим ресурсом для розробки політики безпеки.

Організації повинні стежити за оновленнями безпеки, обмінюватися інформацією з іншими організаціями та звертатися до надійних джерел, щоб залишатися в курсі останніх тенденцій і подій у кібербезпеці.

Забезпечення фінансування для реалізації безпекової політики є важливим чинником. Організації повинні виділяти достатні ресурси для впровадження та підтримки заходів безпеки, включаючи придбання необхідних технологій, навчання персоналу та аудит безпеки.

Облік відповідного законодавства та нормативних вимог є важливим аспектом політики безпеки. Організації повинні дотримуватись застосовних правових та регуляторних вимог, пов'язаних з безпекою та захистом інформації.

Ресурси політики безпеки можуть змінюватись в залежності від конкретних потреб та характеристик організації, але ці основні аспекти зазвичай враховуються для створення комплексного та ефективного підходу до забезпечення безпеки.

КСЗІ (Комплексна система захисту інформації) – це сукупність технічних, організаційних та процедурних заходів, які вживаються для забезпечення безпеки інформації в інформаційних системах. Вона включає різні компоненти і методи захисту, спрямовані на запобігання несанкціонованого доступу до інформації, її зміну, знищення або розкриття.

КСЗІ використовується для захисту різних типів інформаційних систем, включаючи комп'ютерні мережі, бази даних, електронні документи та інші цифрові ресурси. Вона допомагає забезпечити конфіденційність, цілісність та доступність інформації, а також захистити її від зовнішніх та внутрішніх загроз. Основні компоненти КСЗІ включають:

— Ідентифікація та аутентифікація КСЗІ може надати механізми та технології для перевірки справжності користувачів та пристроїв, таких як паролі, біометричні дані або апаратні аутентифікатори. Це допомагає запобігти несанкціонованому доступу до інформації.

— Шифрування даних, за допомогою КСЗІ маємо можливість зашифрувати конфіденційні дані при їх передачі або зберіганні. Шифрування дозволяє уявити дані в зашифрованому вигляді, який може бути розшифрований тільки за допомогою правильного ключа. Це допомагає захистити дані від несанкціонованого доступу чи перегляду.

— Контроль доступу має засоби для встановлення політик та правил контролю доступу до інформаційних ресурсів. Механізми контролю доступу дозволяють визначити, хто має право отримати доступ до яких даних або функцій системи. Це включає управління привілеями, рольові моделі та механізми авторизації.

— Аудит та моніторинг - надає можливість вести аудит та моніторинг системи для виявлення потенційних інцидентів безпеки. Ведення журналів подій, моніторинг мережного трафіку та інші механізми дозволяють виявляти підозрілу активність та швидко реагувати на погрози.

— Управління вразливістю - включає процеси та практики з ідентифікації, оцінки та усунення вразливостей в інформаційній системі. Це включає регулярне оновлення програмного забезпечення, застосування виправлень та патчів безпеки, а також проведення тестування на проникнення для виявлення слабких місць.

— Навчання та обізнаність - передбачає навчання співробітників та підвищення їх поінформованості щодо безпеки інформації. Це допомагає створити культуру безпеки в організації та зменшити ризик людського фактора, який може бути використаний зловмисниками.

— Фізична безпека - включає заходи щодо забезпечення фізичної безпеки інформаційних ресурсів. Це може включати контроль доступу до серверних приміщень, захист від пожежі та повені, використання систем відеоспостереження тощо. Комплексність: КСЗІ є системою, що складається з різних компонентів і заходів, які взаємодіють і взаємодоповнюють один одного. Вона охоплює різні аспекти безпеки інформації, включаючи технічні,

організаційні та процедурні заходи.

— Захист інформації - Основна мета КСЗІ полягає у забезпеченні безпеки інформації, включає захист від несанкціонованого доступу до інформації, її модифікації, знищення чи розкриття. КСЗІ допомагає запобігти витоку конфіденційної інформації, зберегти цілісність даних та забезпечити доступність інформації лише авторизованим користувачам.

— Комплексний підхід - КСЗІ застосовує комплексний підхід до безпеки інформації. Вона враховує не лише технічні аспекти, такі як шифрування та контроль доступу, а й організаційні та процедурні заходи. Це означає, що КСЗІ включає навчання співробітників, розробку політик безпеки, аудит і моніторинг, управління вразливістю та інші заходи для забезпечення повної безпеки інформації.

—

КСЗІ вимагає постійного вдосконалення та оновлення. Оскільки загрози та атаки постійно еволюціонують, КСЗІ має бути гнучкою та адаптивною, щоб ефективно боротися з новими загрозами. Організації повинні регулярно аналізувати свої системи безпеки, проводити аудити та впроваджувати покращення, щоб підтримувати високий рівень захисту інформації.

КСЗІ є ключовим інструментом забезпечення безпеки інформації в сучасному інформаційному суспільстві. Її реалізація допомагає організаціям захистити конфіденційність та цілісність інформації, а також забезпечити Безпеку за допомогою КСЗІ потребує комплексного та систематичного підходу. Важливо адаптувати КСЗІ до конкретних потреб і загроз організації, а також регулярно оновлювати та вдосконалювати заходи безпеки відповідно до загрозової ситуації, що змінюється.

Закон України "Про захист персональних даних" є одним із основних нормативних актів, що регулюють питання захисту персональних даних в Україні. Він регулює збирання, зберігання, використання та передачу

персональних даних у різних сферах діяльності.

Закон визначає поняття, пов'язані з персональними даними, такі як суб'єкт персональних даних, оператор та обробка персональних даних. Закон встановлює принципи, якими оператори повинні керуватися під час обробки персональних даних. До них відносяться принципи законності, справедливості, прозорості, обмеження цілей, мінімізації даних, збереження точності та ін.

Закон гарантує певні права суб'єктів персональних даних, включаючи право на інформацію про свої персональні дані, доступ до них, їх виправлення, блокування або видалення при порушенні закону. Закон визначає обов'язки операторів щодо обробки персональних даних, включаючи забезпечення безпеки та конфіденційності даних, інформування суб'єктів про цілі обробки та отримання їх згоди, забезпечення прав суб'єктів персональних даних та інші.

Закон містить положення про міжнародну передачу персональних даних, включаючи вимоги щодо захисту даних при передачі за межі України. Законом передбачено механізми контролю за дотриманням вимог щодо захисту персональних даних, включаючи повноваження органів державного контролю та відповідальність за порушення закону.

Закон України "Про захист персональних даних" спрямований на забезпечення захисту прав і свобод суб'єктів персональних даних та регулювання обробки персональних даних відповідно до принципів законності та справедливості

У сфері інформаційних відносин виділяються дві основні сторони: суб'єкти та об'єкти інформаційних відносин. Розглянемо їх детальніше:

Суб'єкти - це учасники інформаційних відносин, які здійснюють дії у галузі обробки, передачі та отримання інформації. Основними суб'єктами інформаційних відносин є:

— Фізичні особи: Люди, які здійснюють обробку, передачу або

отримання інформації. Вони можуть бути авторами, споживачами чи передавачами інформації.

— Юридичні особи: Організації, такі як компанії, установи, урядові органи тощо, які здійснюють обробку, передачу або отримання інформації в межах своєї діяльності.

— Державні органи: Включають урядові установи, міністерства, комітети, агенції тощо, які займаються обробкою, передачею або отриманням інформації у межах своїх повноважень.

Об'єкти - це сама інформація, яка обробляється, передається чи отримується суб'єктами інформаційних відносин. Об'єктами інформаційних відносин можуть бути:

— Документи: Паперові чи електронні документи, які містять інформацію, що передається чи обробляється.

— Дані: Сукупність фактів, цифр, тексту, зображень, звуку тощо, які містяться у документах чи інших носіях інформації.

— Інформаційні системи: Комп'ютерні системи, бази даних, мережі тощо, які забезпечують зберігання, обробку та передачу інформації.

— Комунікаційні канали: Засоби передачі інформації, такі як телефонні лінії, інтернет, пошта тощо, які забезпечують передачу інформації між суб'єктами.

Взаємодія між суб'єктами та об'єктами інформаційних відносин відбувається через процеси обробки, передачі, зберігання, отримання та використання інформації. Законодавство про інформацію визначає права та обов'язки суб'єктів, а також регулює взаємодію між ними у цій сфері.

Політика безпеки інформації (ПБІ) в інформаційних системах (АС) є набором правил, процедур, практик і заходів, розроблених для забезпечення конфіденційності, цілісності та доступності інформації, а також захисту від загроз інформаційної безпеки.

Основна мета ПБІ в АС полягає в тому, щоб встановити рамки та принципи, якими повинні керуватися організації та їхні співробітники при обробці, передачі та зберіганні інформації. Це включає визначення ролей та відповідальності, встановлення процедур контролю та моніторингу, а також застосування технічних та організаційних заходів для забезпечення безпеки.

У політиці безпеки інформації в АС зазвичай містяться такі аспекти

— Визначення цілей та принципів: ПБІ має визначити цілі безпеки інформації, такі як захист від несанкціонованого доступу, запобігання витоку інформації, забезпечення цілісності даних та інші. Вона також має встановити принципи, якими керуються під час розробки заходів безпеки.

— Ролі та відповідальність: ПБІ має визначити ролі та відповідальність різних стейкхолдерів, включаючи адміністраторів системи, користувачів та інших учасників процесу обробки інформації. Кожна сторона повинна знати свої обов'язки та виконувати їх належним чином.

— Управління доступом: ПБІ має містити політику управління доступом, яка визначає права та привілеї користувачів, процедури автентифікації та авторизації, а також контроль доступу до інформації залежно від ролей та необхідності.

— Захист від загроз: ПБІ має включати заходи щодо захисту від різних загроз інформаційній безпеці, таких як віруси, атаки хакерів, фізичні крадіжки або пошкодження обладнання. Це може включати використання антивірусних програм, брандмауерів, шифрування даних та інших технічних заходів.

— Навчання та обізнаність: ПБІ має передбачати навчання співробітників з питань безпеки інформації, підвищення їх поінформованості про потенційні загрози та правила безпечного поводження з інформацією.

Регулярний аудит та огляд ПБІ має передбачати проведення регулярних аудитів та оглядів безпеки інформаційної системи для виявлення вразливостей та перевірки відповідності безпеці. Важливо, що ПБІ має бути

розроблена та застосована з урахуванням специфічних потреб та вимог кожної конкретної АС та організації. Вона має бути документована та регулярно оновлюватися для врахування нових загроз та технологій.

1.3 Постановка задачі

Проблема захисту інформації на великих підприємствах являється актуальною на данний час і в майбутньому, виходячі з аналізу розвитку великих ризиків та загроз у світі за останні роки важаю доречним забезпечити високий рівень захищеності інформації. Виходячи з нормативно – правової бази для того щоб досягти бездоганного рівня захищеності інформації на великих підприємствах вважаю доречним створення захисту інформації за допомогую КСЗІ.

Під час створення та розробки політики безпеки за допомогою КСЗІ необхідно надати:

— Сфера діяльності підприємства;

— Фізичне середовище підприємства;

— Інформаційну систему на підприєстві;

— Побудувати модель порушника і модель загроз;

— Виявити проблеми та вразливості;

— Розробити елементи політики безпеки інформації;

Висновок:

Проаналізувавши перший розділ кваліфікаційної роботи було виявлено темпи росту кіберзлочинності, загальні відомості про кібератаки у світі. Було розглянуто перелік загроз для великих підприємств і закладів ресторанного господарства. Було проаналізовано нормативно – правову базу та основні закони України стосовно інформації.

# 2 СПЕЦІАЛЬНИЙ РОЗДІЛ

## 2.1 Інформація стосовно діяльності підприємств швидкого харчування «КФС»

Мережа ресторанів KFC (Kentucky Fried Chicken) – це міжнародна мережа фаст-фуд ресторанів, що спеціалізується на приготуванні та продажу курки, особливо смаженого курячого м'яса. Основними аспектами діяльності ресторанів мережі KFC є гастрономічна пропозиція: KFC пропонує широкий вибір страв на основі курки, включаючи смажені шматочки курячого м'яса, крильця, нагетси та бургери з курячою начинкою. Однією з відомих страв KFC є "Оригінальний рецепт" (Original Recipe) - спеціальний секретний рецепт приправ для смаження курки.

Кампанії мережі мають різноманітні формати ресторанів, включаючи фудкорти, ресторани швидкого обслуговування (QSR) та ресторани з обслуговуванням за столиками. Вони зазвичай пропонують як внутрішній зал для посадки, і послуги " на винос " чи доставку.

KFC є глобальною мережею ресторанів та має присутність у багатьох країнах світу. Кожна країна може мати деякі адаптації меню та пропонувати місцеві варіанти страв, щоб відповідати місцевим уподобанням та культурі. Багато ресторанів KFC працюють на основі франчайзингової моделі, де франчайзі (незалежний підприємець) отримує право використовувати торгову марку KFC і дотримуватися встановлених стандартів та процедур. KFC активно працює над розвитком своїх корпоративних ініціатив, включаючи забезпечення продуктової якості, екологічну відповідальність, соціальні програми та ініціативи сталого розвитку. Загалом ресторани мережі KFC пропонують курячу продукцію та фаст-фуд послуги, прагнучи задовольнити потреби своїх клієнтів та надати їм унікальний досвід.

На території України мережею закладів ресторанного господарства (франчайзі) володіє декілька великих кампаній: ТОВ «Тесті Фуд», «ГРГ», «ДТС» , у кваліфікаційній роботі мова піде про ТОВ «Тесті Фуд». Ця

кампанія налічує 22 заклади на всій території України та головний офіс у м.Дніпрі. Кожен ресторан мережі має штат персоналу в залежності від маштабу закладів та виручок мінімальний штат персоналу налічує 18 людей: 1 директор, 1 заступник керівника, 2 менеджера, 1 інструктор з виробничого навчання, та 13 членів бригади. Максимальний штат персоналу налічує до 50 співробітників: 1-2 директора, 3-4 заступника керівника, 4-6 менеджерів, 3-5 молодших менеджерів, мінімум 2 інструктори з виробничого навчання - максимум за потреби закладу та 30 членів бригади. Кампанія ТОВ «Тесті Фуд» має свій веб сайт на якому кожен з відвідувачів закладів може залишити відгук про сам заклад, обслуговування, смак їжі, та загальне враження. Діяльніть кампанії на пряму пов'язана як з юридичними особами так і фізичнми особами. Кампанія ТОВ «Тесті Фуд» обробляє різні типи інформації своєї діяльності. Наприклад: збирають та обробляють персональні дані своїх клієнтів, такі як імена, контактна інформація (адреса, телефон, електронна пошта), дати народження та переваги клієнтів. Це може бути необхідним для обробки замовлень, програм лояльності, розсилки інформації та зворотного зв'язку з клієнтами. Ресторани можуть опрацьовувати фінансову інформацію, пов'язану з оплатою замовлень клієнтів. Це може включати номери банківських карток, дані транзакцій, інформацію про платіжні системи тощо. Кампанія обробляє інформацію про замовлення та продажі, включаючи деталі замовлень клієнтів, склад страв, вартість, дата та час замовлення. Ця інформація може використовуватися для обліку продажів, планування постачання, управління запасами та аналізу бізнесу. Також обробляється інформація про своїх співробітників, включаючи персональні дані, дані про зайнятість, оплату праці, податкову та соціальну інформацію, інформацію про професійні навички та навчання. Це необхідно для управління персоналом, виплати заробітної плати, оподаткування та інших адміністративних процесів. Для управління поставками, укладання та виконання контрактів та підтримки ділових відносин обробляється інформація про своїх постачальників, контрагентів та інших ділових партнерів. Це може

включати контактні дані, договірні відносини, інформацію про товари та послуги, фінансову інформацію тощо.

Заклади кампанії мають різний час роботи: заклади які знаходяться у ТЦ працюють з 07:00 до 21:30 при цьому з 07:00 до 10:00 в закладах відбувається прибирання та підготовка до відкриття, о 10 вони відчиняються для відвідувачів та 21:00 зачиняються, після 21:00 до 21:30 починается підготовка до прибирання, зачинення кассових аппаратів і внесценя всіх данних у бази данних такі як «1С» та, «BITRIX». Самостійні заклади які мають окрему територію і не від кого не залежать працюють цілодобово: з 08:00 вони відчиняються для  відвідувачів, о 22:00 зачиняється основний зал закладу, та працює тільке вікно на замовлення з собою, після 22:00 в закладах починається прибирання, внесення всіх данних до баз данних, та підготовка до вікриття.

Співробітники закладів мають обід протягом 30 хвилин. Вихід на 5 хвилин для того щоб перепочити кожні 2 години. Вихід на обід або на 5 хвилинний відпочинок відбувається після дозволу старшого менеджера зміни. Кожен співробітник може вийти на обід у будь-який зручний час або за вказівкою старшого менеджера.

Кампанія ТОВ «Тесті Фуд» має трьох системних адміністраторів для безпереривної роботи закладів та підтримки бізнес процесів, кожен з системних адміністраторів допомагає всім закладам мережі з поточними проблемами такими як: не працюючі монітори, помилки касових апаратів, принтерів, програм, баз данних, тощо. Системні адміністратори в загальному працюють з закладами віддалено через відповідні группи у соцмережах таких як Viber та telegram. Якщо проблема віддалено не вирішується, то адміністратори виїзджають на локації ресторанів. Також в кампанії є IT – спеціаліст який відповідає за встановлення, налаштування та оновлення комп'ютерів, серверів, мережного обладнання та програмного забезпечення, щоб забезпечити їх правильне функціонування та сумісність. IT – спеціаліст керує операційними системами, встановлює патчі та оновлення, налаштовує

безпеку, контролює доступ та забезпечує надійність та стабільність роботи операційних систем, створює та налаштовує локальні мережі (LAN) та розподілені мережі (WAN), встановлює та підтримують маршрутизатори, комутатори, брандмауери та інше мережеве обладнання. Він також відповідає за безпеку мереж та контроль доступу до ресурсів, стежать за працездатністю та продуктивністю систем, проводять моніторинг мереж та серверів, аналізують журнали подій та роблять налагодження та усунення несправностей, також відповідає за резервне копіювання даних та відновлення систем у разі збоїв.

2.2 Причини для створення КСЗІ

Для внутрішньої та зовнішньої безпеки кампанії було визначено підстави для стоворення КСЗІ. Директором підприємства було виданно акт про категоріювання (ДОДАТОК 1). Також директром підприємства було виданно наказ про створення КСЗІ (ДОДАТОК 2) для забезпечення цілісністі даних, тобто запобіганю їх несанкціонованій зміні або пошкодженню, включаючи механізми контролю цілісності даних, резервне копіювання і відновлення, а також захист від шкідливих програм і кібератак, зниження ризиків та врат пов'язаних з порушенням безпеки інформації та крадіжками. Це включає запобігання витоку даних, фінансових втрат, пошкодження репутації організації та інших негативних наслідків, пов'язаних з порушенням безпеки інформації.

2.3 Розгляд фізичного середовища на базі ОІД

Головний сервер кампанії розташований на першому поверсі двухповерхневого будинку за адресою вул. Князя Володимира 21Б.

Фундамент будівлі виконаний з бетону. Наружні стіни будинку виконані з пінобетону, внутрішні стіни та перегородки виконані з гіпсокартону.

Дах будівлі плоский має на собі лінію громо відведення.

Будівля оснащена ситемою вентиляції яка керується через окремий

пульт управління.

Вікна металопластикові. Будівля має 1 центральну металопластикову дверь з 1 звичайним замком зі звичайними ключами та 1 металеву дверь на пожежний вихід яка оснащена 2-ма замками: 1 звичайний замок зі звичайним клюем; 1 механічний кодовий замок.

Будівля має електро та водопостачання підведене під землею.

Будівля розділена на гостьову частину, частину для персоналу, має особисту ситему коридорів та переходів в середині, має складські приміщення, виробничі приміщення, окрему серверну.

Будівля мєжує з іншим рестораним закладом через пінобетонну стіну.

На першому поверсі розташована власна щитова.

У ресторану «КФС» за адресою вул. Князя Володимирв 21Б заключений договір з охороною кампанією поліції, наряд поліції приїзджає за 5 хвилин після виклику через 1-канальний комплект управління (U1HS, U1HSD, U1HSL, U1HR – приймачі).

Будівля оснащена камерами відеофіксації як з внутрішньої частини так і з зовнішньої частини будівлі.

Комунікації будівлі:

До будинку проведено лінії інтернет провайдерів. Заклад користується послугами двох провайдерів. Лінії інтерне під'єднання проходять по оптоволоконному кабелю, кабелі проходять через дах будівлі, надземно. Один роутер встановлений на першому поверсі у спеціально відведеному місці, а інший знаходится на даху та керується супутником «Starlink».

Електропостачання комплекне проходить по всій будівлі. Трансформаторна підстанція знаходится поза будинком. Електропостачання проходить під землею , заклад оснащено власним електрощитком який знаходиться спец приміщені. Біля будівлі стоїть дизельний генератор на 300Вт, під'єднаний надземно до основної щитової, при вимкнені живленя від

міста, підключається самостійно.

Водопровід та каналізація проходить через району водонапірну станцію, та проходить по всій будівлі. В будівлі знаходяться числені стоки до каналізації, та крани для обмеження води

— Біля будівлі знаходяться також і інші споруди:

— 50м - 2-х поверхневий торгівельний комплекс, на другому поверсі якого знаходится розважальний комплекс з виходом на терасу яка дивится у сторону нашого закладу №1.

— 100м – одноповерхневий магазин №2.

— 150м – 2-х поверхнева будівля, розділена на 2 частини цегляною стіною з лівої сторони №3.1 житловий будинок з правої сторони №3.2 офісний центр та парковкою №3.3

— Через пінобетону стіну межує з іншим рестораним закладом №4.

— 350м – будівля знахлдится біля місцевої парковки №5.

— На задній частині є внутрішній двір №6.

— Окремий в’їзд та виїзд з парковни до внутрішнього двору №7.

— 100м – 2х поверхневий офісний будинок №8.

— 50м – котельна №9

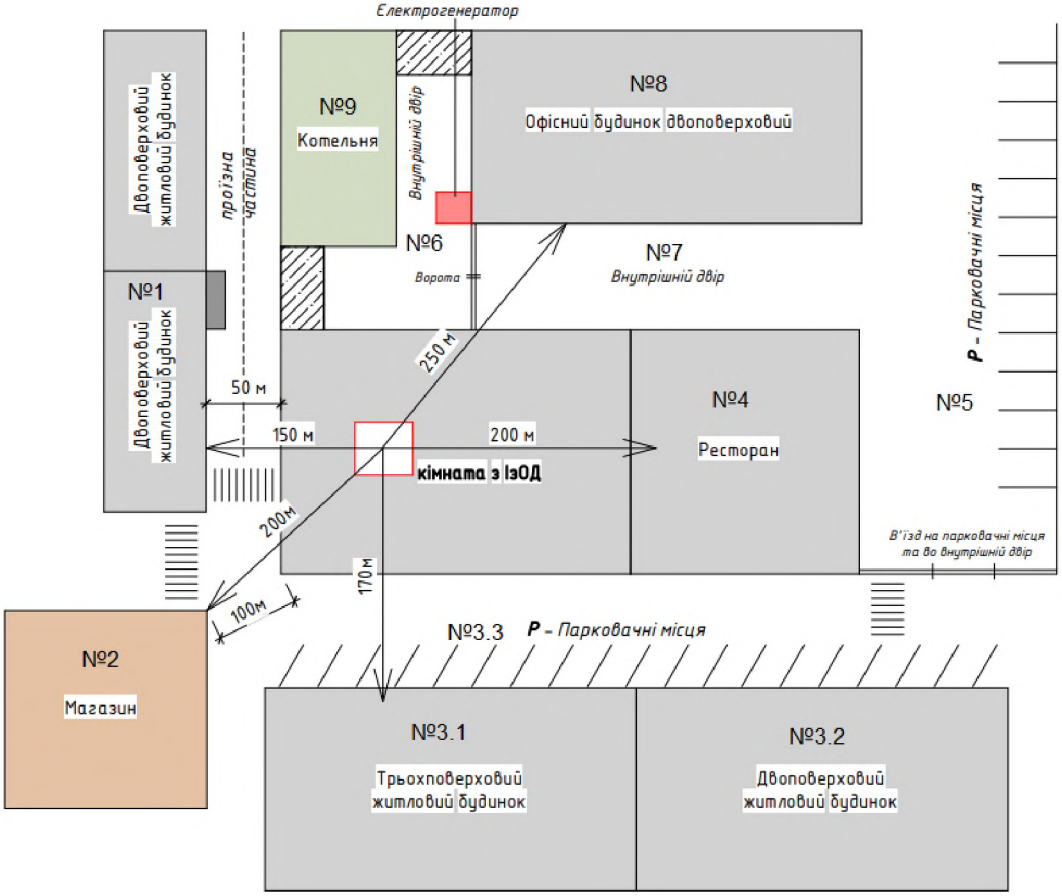


Рисунок 2.1 – Ситуаційний план ресторану

Таблиця 2.1 Перелік споруд та будівель біля об'єкту з циркуляцією ІзОД

| № | Призначення бцдівлі | Адреса | Кіл-кість поверхів | Мінімальна відстань до ІзОД, м |
|---|---|---|---|---|
| 1 | Магазин | Князя Володимира 21 | 1 | 200 |
| 2 | Двоповерховий житловий будинок | Князя Володимира 20 | 2 | 150 |
| 3 | Котельна | Князя Володимира 19 | 2 | 200 |
| 4 | Офісна будівля | Князя Володимира 19Б | 2 | 250 |
| 5 | Ресторан | Князя Володимира 21А | 2 | 200 |

Продовженя таблиці 2.1

| № | Призначення бцдівлі | Адреса | Кіл-кість поверхів | Мінімальна відстань до ІзОД, м |
|---|---|---|---|---|
| 6 | Житловий будинок | Князя Володимира 22 | 3 | 170 |
| 7 | Житловий будинок | Князя Володимира 21Б | 2 | 300 |

Будівля в якій циркулює ІзОД розташована на першому поверсі двохповерхневого будинку, на території першого повеху знаходится зала для відвідувачів, 3 зони робочих приміщень, 4 складські приміщення та кімната менеджерів та директора. У приміщені використані металопластикові вікна.

Площа ресторанного закладу складає 400м$^2$, товщина стін з пінобетону складає 200см, товщина перегородок з гіпсокартону 100см, висота стелі 3м.

Вентиляція виповнена приточною системою з нержавіючої сталі.


Рисунок 2.2 – Генеральний план будівлі

| Найменування | Площа | Примітка |
|---|---|---|
| Площа технології (з урахуванням перегородок та оздоблення) | 140м$^2$ | |
| Загальна площа зала 1 та 2 поверхи | 50м$^2$+187м$^2$=237м$^2$ | |
| Загальна площа WC + МОП зала 1 та 2 поверхи | 0,8м$^2$+22,2м$^2$=23м$^2$ | |
| Загальна площа ресторану 1 та 2 поверхи | 400м$^2$ | |

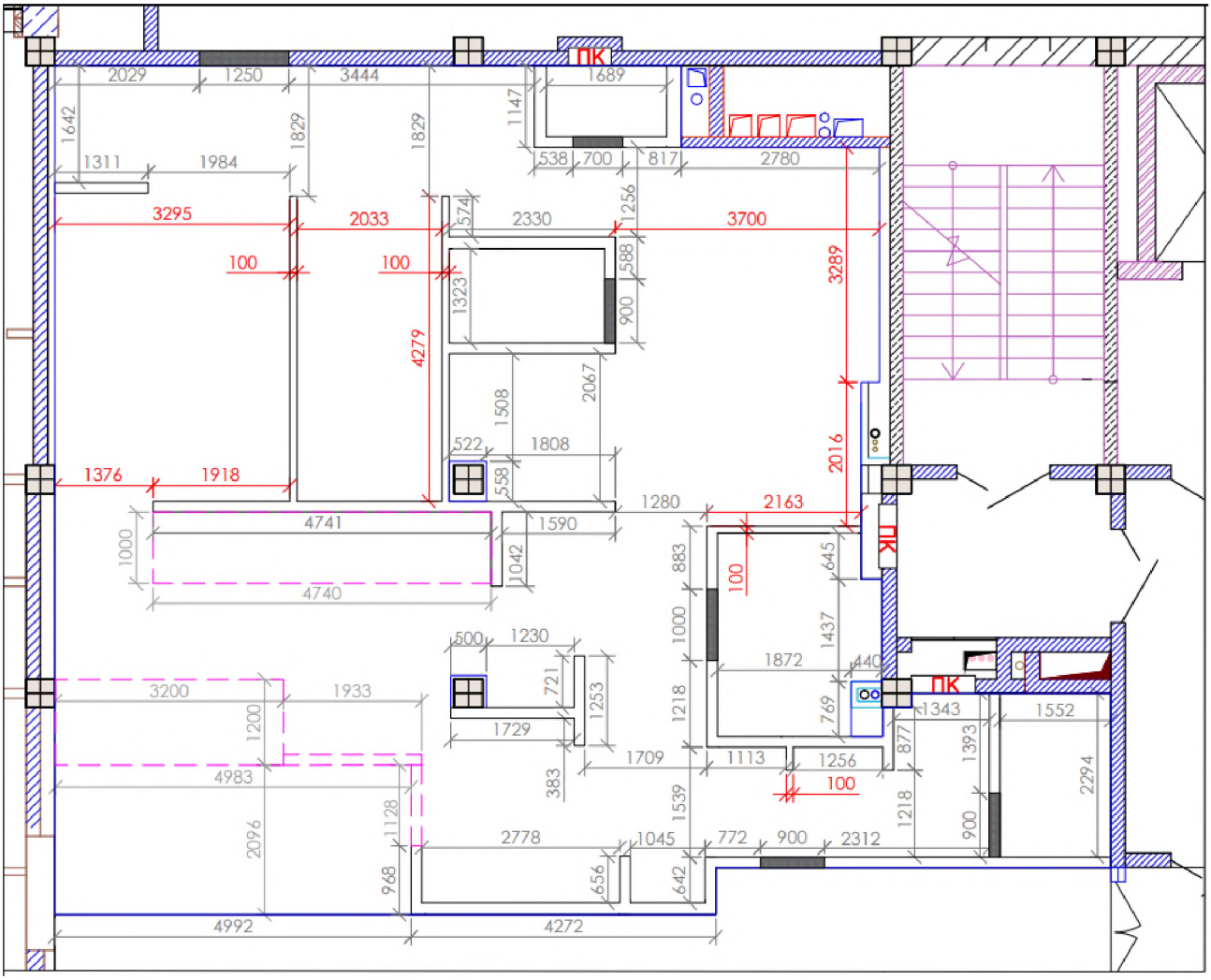


Рисунок 2.3 – План стін будівлі

| | |
|---|---|
| | існуючі стіни, колони, будівельні конструкції будівлі. |
| | перегородки з гіпсокартону, товщина не більше 150мм. |
| | лінія чистового оздоблення стін. |
| | Дверні отвори. |
| | двері виконані у вигляді вертикальних роль-ставень із замком. |
| | антресольні полиці. |
| | рама без полиці. |

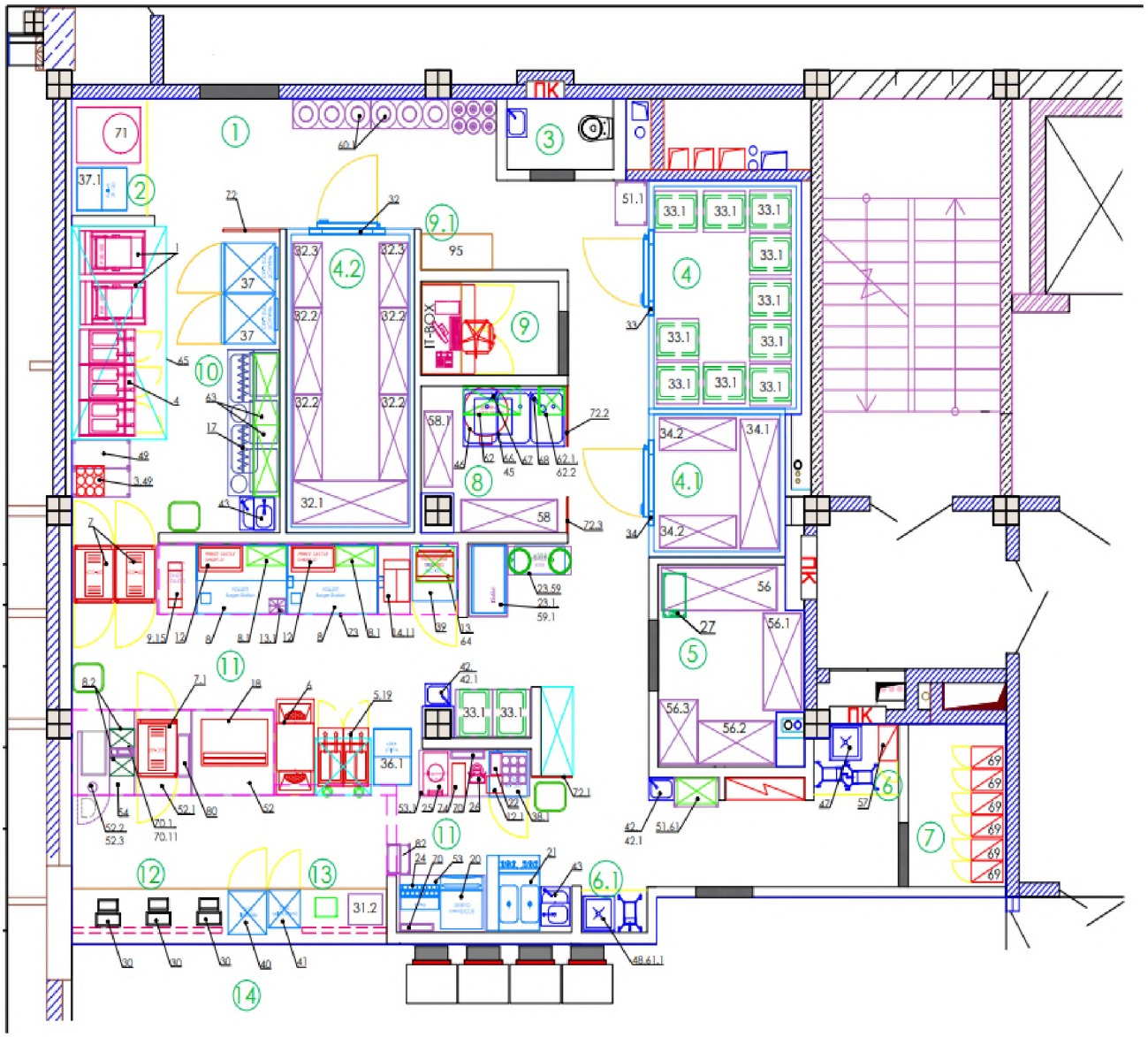


Рисунок 2.4 - експлікація приміщення KFC

Таблиця 2.1 Опис генерального плану ОІД

| Номер | Назва | Площа кв.м |
|---|---|---|
| 1 | Коридор | |
| 2 | Компакторна | 2 |
| 3 | Санвузол для персоналу | 1.7 |
| 4 | Холодильна камера | 7.1 |
| 4.1 | Холодильна камера №2 | 3.9 |
| 4.2 | Морозильна камера | 7.7 |
| 5 | Склад | 6.2 |
| 6 | МОП | 1.3 |
| 6.1 | МОП зал 1 поверх | 0.8 |
| 7 | Роздягальня | 3.6 |
| 8 | Мийка | 4.6 |
| 9 | Офіс | 2.9 |
| 9.1 | Зона навчання персоналу | |
| 10 | Гарячий цех | 14.2 |
| 11 | Роздавальня | |
| 12 | Зона прийому замовлень | |
| 13 | Зона видачі замовлень | |
| 14 | Зал для гостей 1 поверх | 50 |
| 14.1 | Зал для гостей 2 поверх | 187 |
| 15 | МОП зал 2 поверх | 22.2 |
| Загальна площа | | 400 |

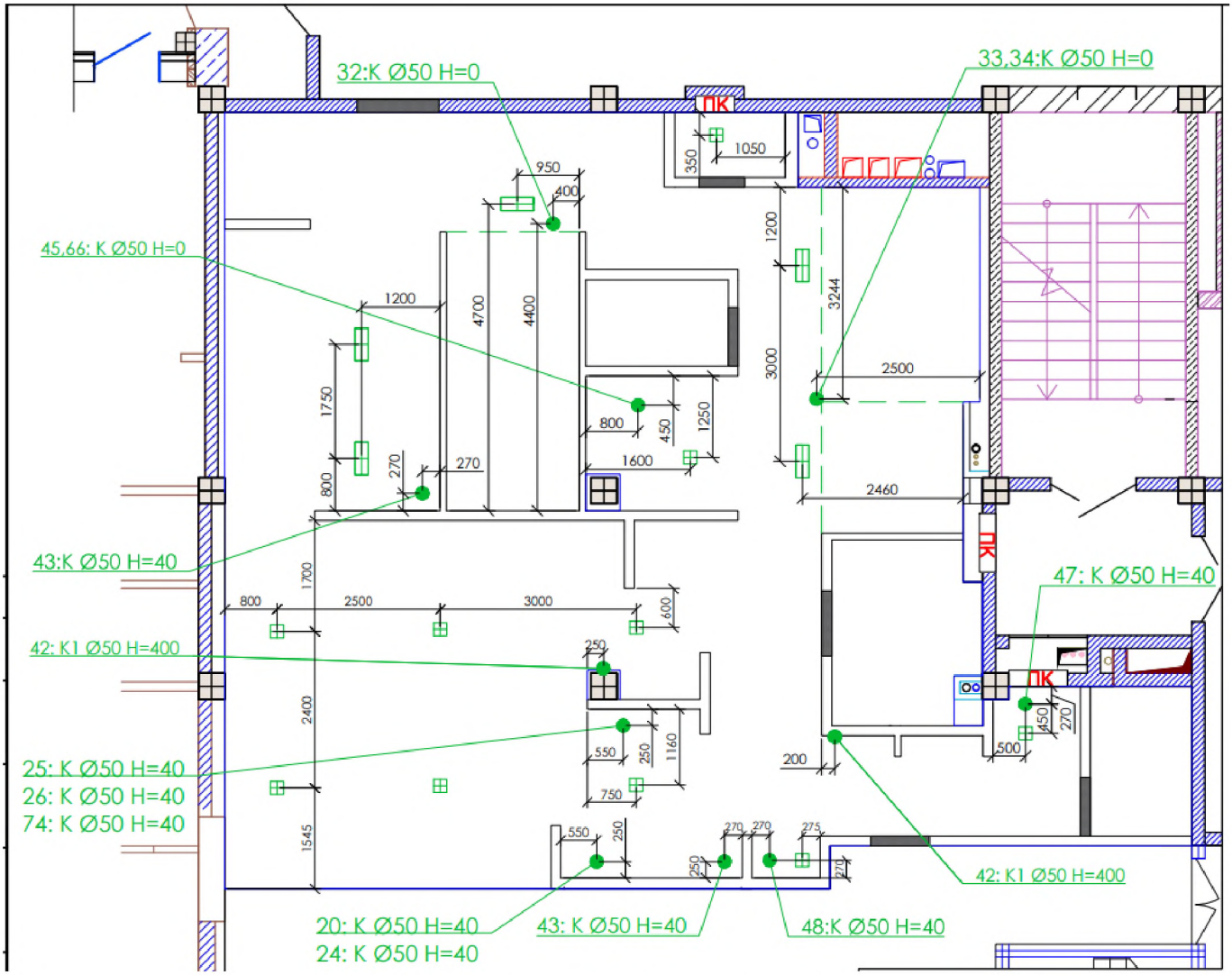


Рисунок 2.5 – Вивід каналізації

K - Каналізація вівід з під полу

K1 - Каналізація вивід з стіни

Ø - Діаметр підведення у мм

H - Висота підведення у мм від рівня полу

17 - Номер обладнення

- Евроканал (500x200), Ø 50

- Трап (200x200), Ø 50

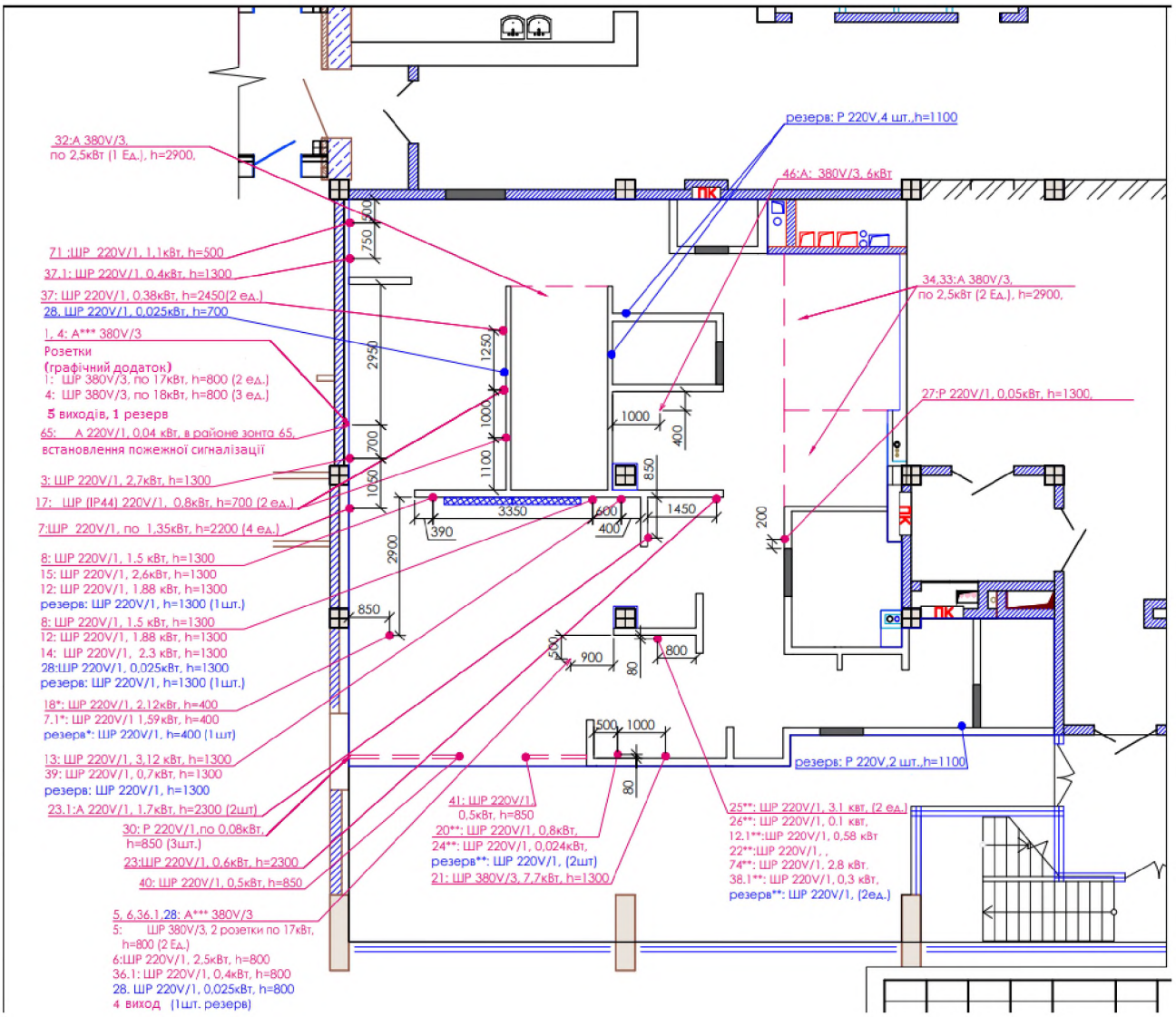


Рисунок 2.6 – Електро під’єднання

** - Розетки встановлюються на торці короба над столом не менше 1300мм від підлоги.

*** - Розетки встановлюються у нижньому торці стіни.

Короб під стільницею касової стійки.

Зона, де розетки встановлювати НЕ МОЖНА

UPS- Пристрій бесперебійного живлення

ШР - Штепсельний роз'єм

Р - Євророзетка

h - Висота підведення у мм

А - Виведення гнучкого кабелю зі стелі, довжина кабелю не меньше 2мм

20 - Номер позиції

* - Комунікації підводяться зі стелі в спеціальних коробах. Розетки встановлюються в коробах для електричних розеток.

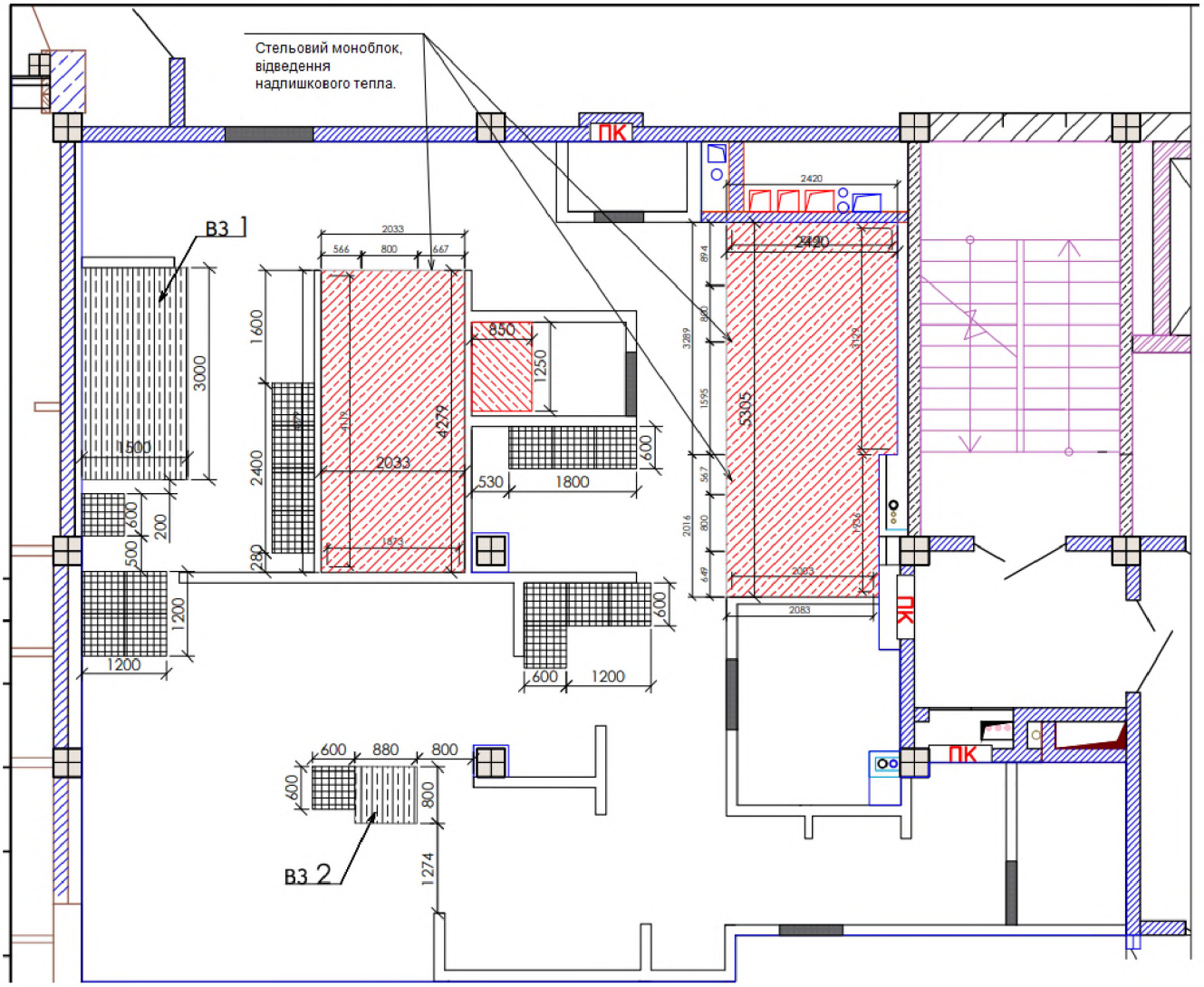


Рисунок 2.7 – Сиситема вентиляції

- Зони надлишкового виділення тепла

- Вентиляційний зонт над технологічним обладнанням

- Вентиляційні грати - 600х600

ВЗ - Витяжний зонт

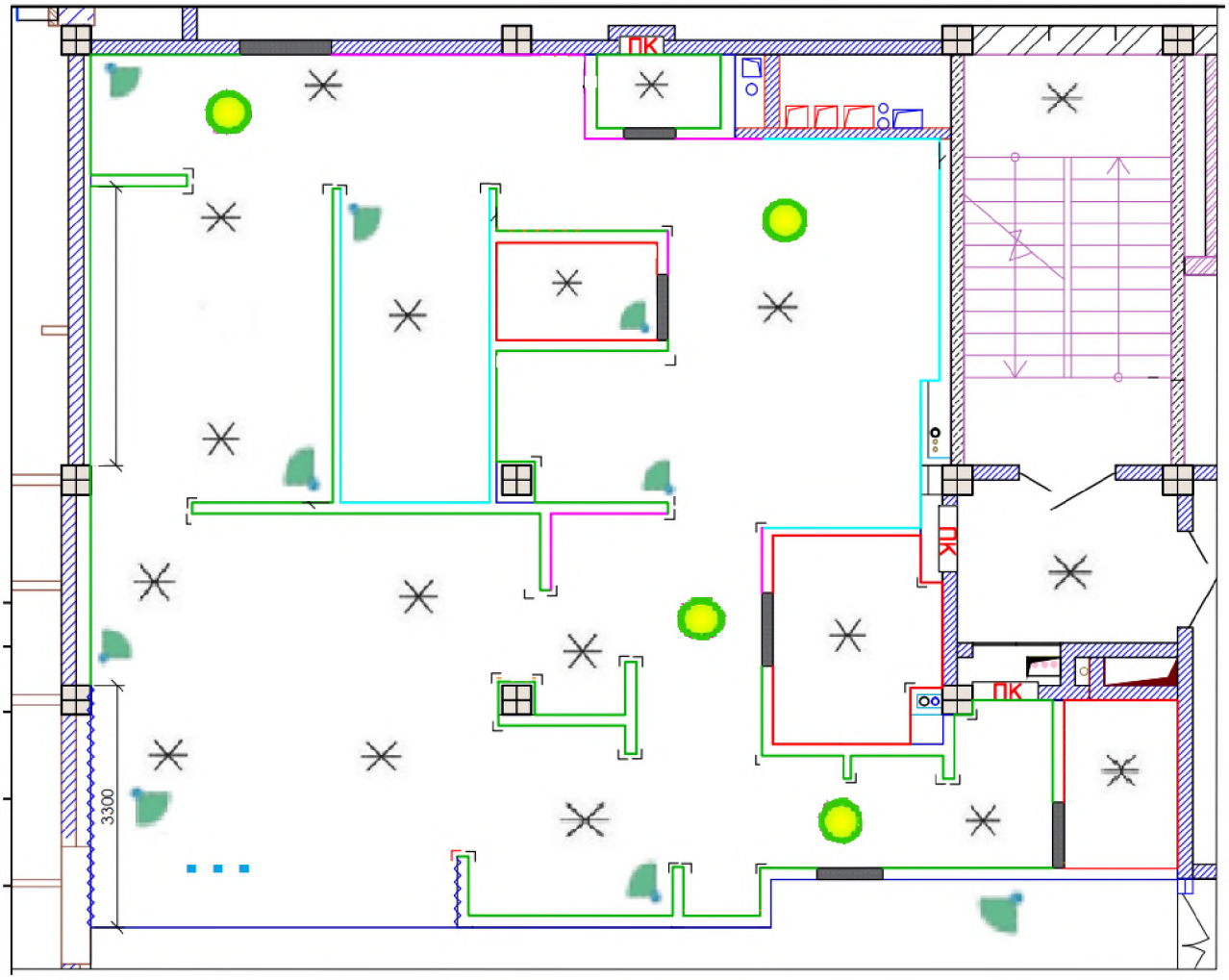


Рисунок 2.8 – Схема противопожежної та аварійної системи. Системи відеофіксаціїї.

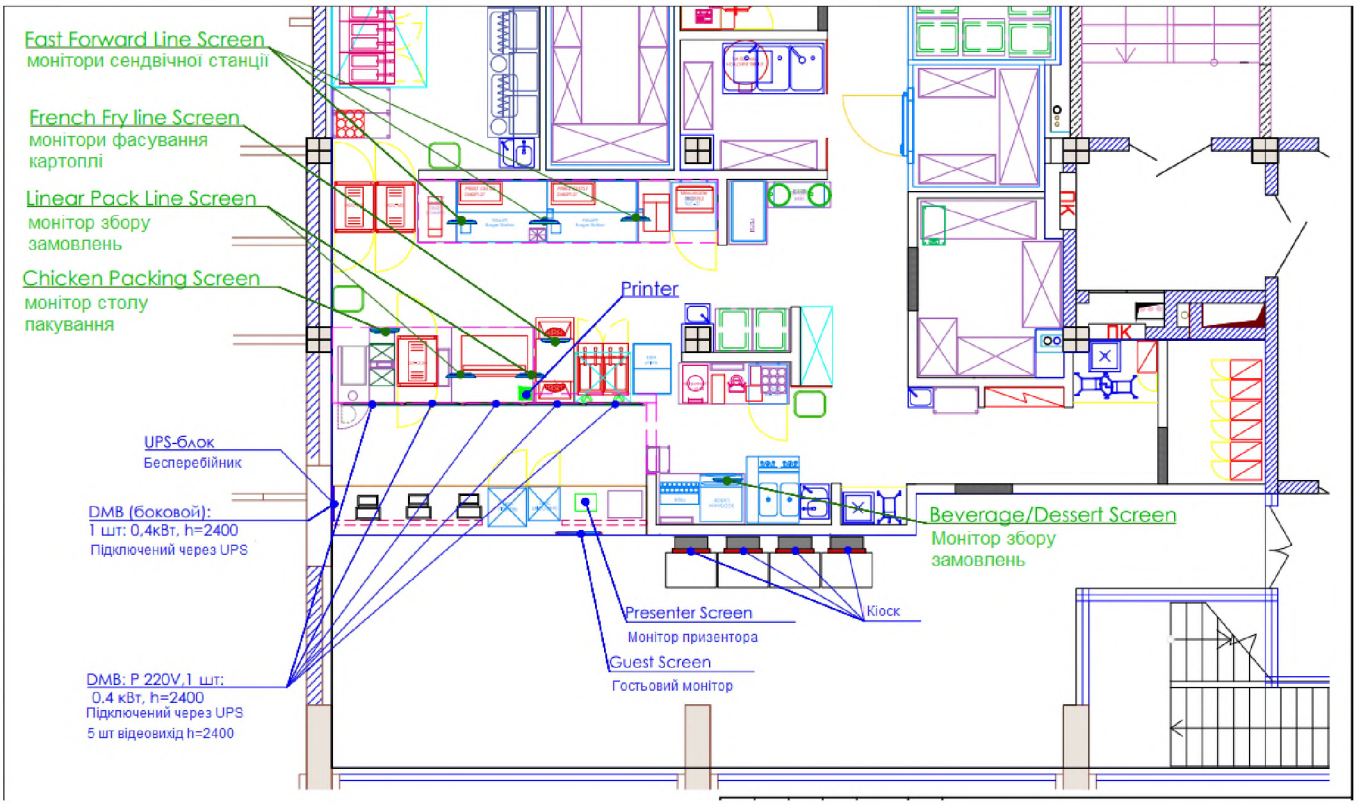


Рисунок 2.9 – IT – обладнення

Умовні позначення див. Рис. 2.6

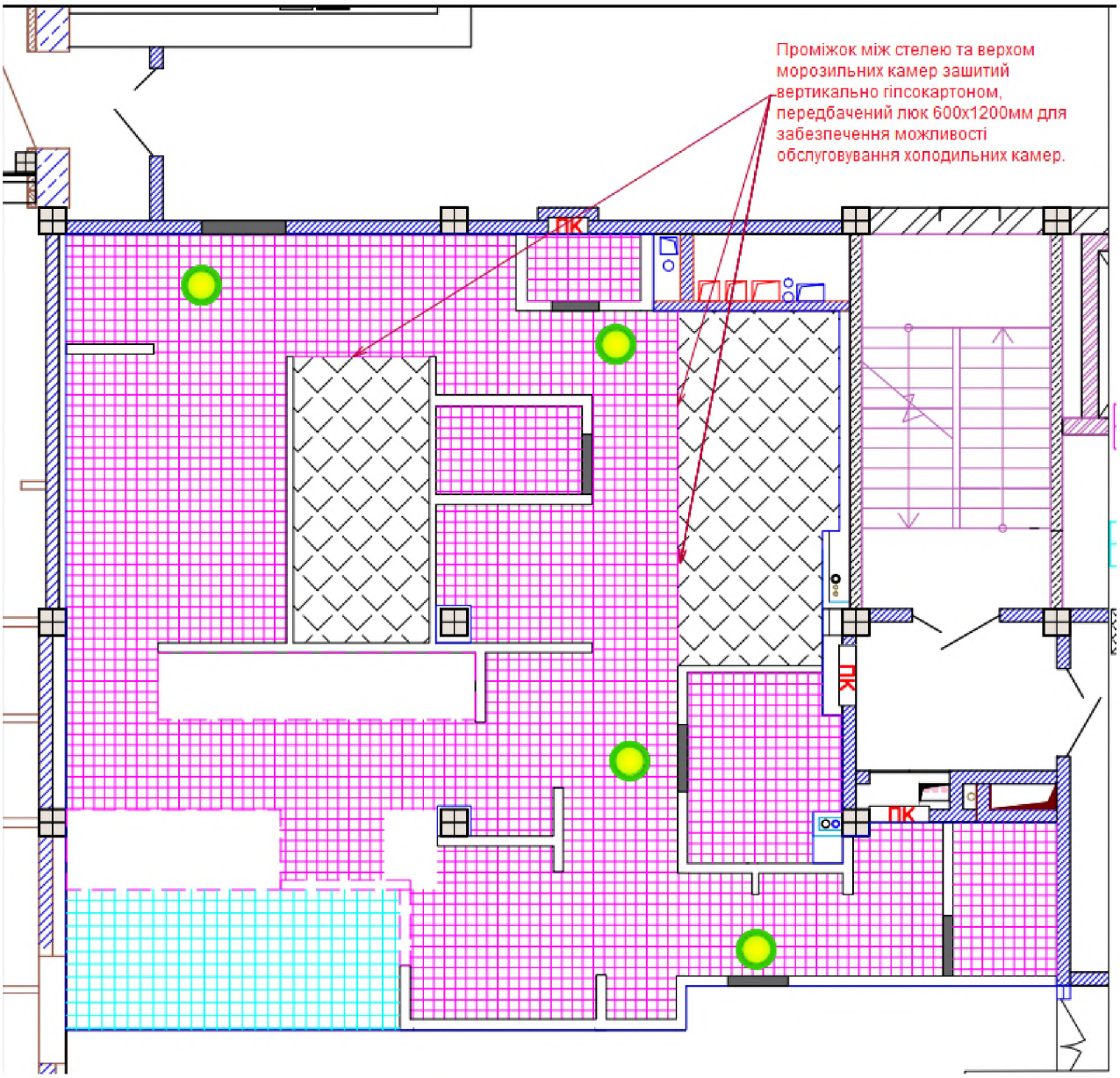


Рисунок 2.10 – Міжстельві простори.

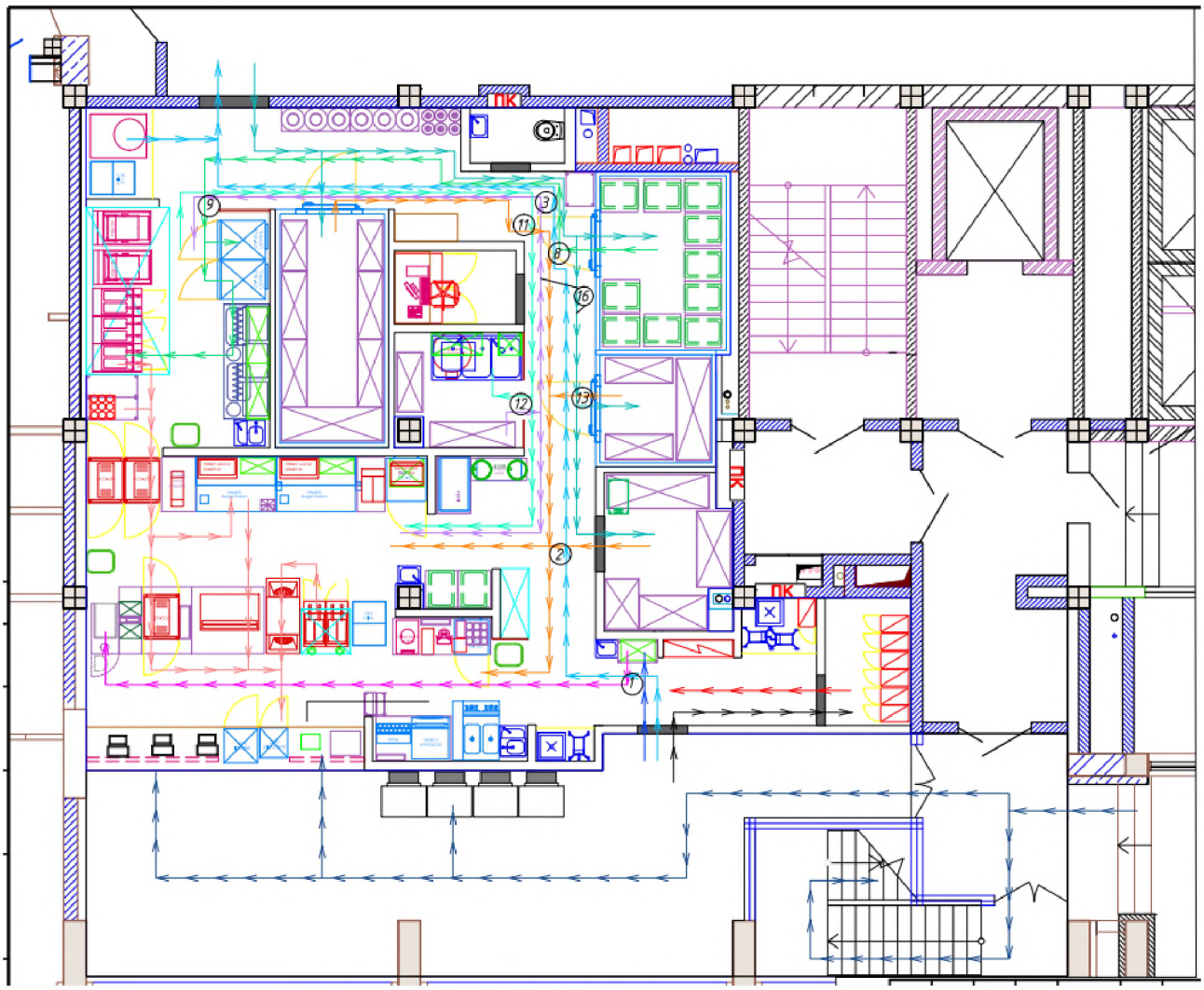


Рисунок 2.11 – рух людей на території ОІД

Гості

Винесення сміття

Брудні таці

Персонал у верхньому одязі

Сирі полуфабрикати

Персонал у спец одязі

Готові полуфабрикати

Готова продукція

Система інтернет під'єднана надземно, до 2х роутерів, перший роутер-приймач (основний) знаходится на даху будівлі (Starlink), другий роутер знаходится у серверній. Доступ до мережі можкть отримати усі охочі хто знаходится у межах будівлі, гості та працівники закладу під'єднуються до однієї звичайної мережі під назвою «KFC», але перед підключенням вони дивляться коротку рекламу, та мають інтернет зі швидкістю 60mb/s. Компьтери та усі технічні засоби кампанії під'днані до окремої мережі під назвою «Starlink» яка знаходится під паролем та має швидкість 100mb/s, якої цілком вистачає для запуску та роботи ПЗ.

Кампанія має особистого IT – інженера який займається перевіркою обладнення, обслуговуванням та налаштуванням інтернет з'єднаня.

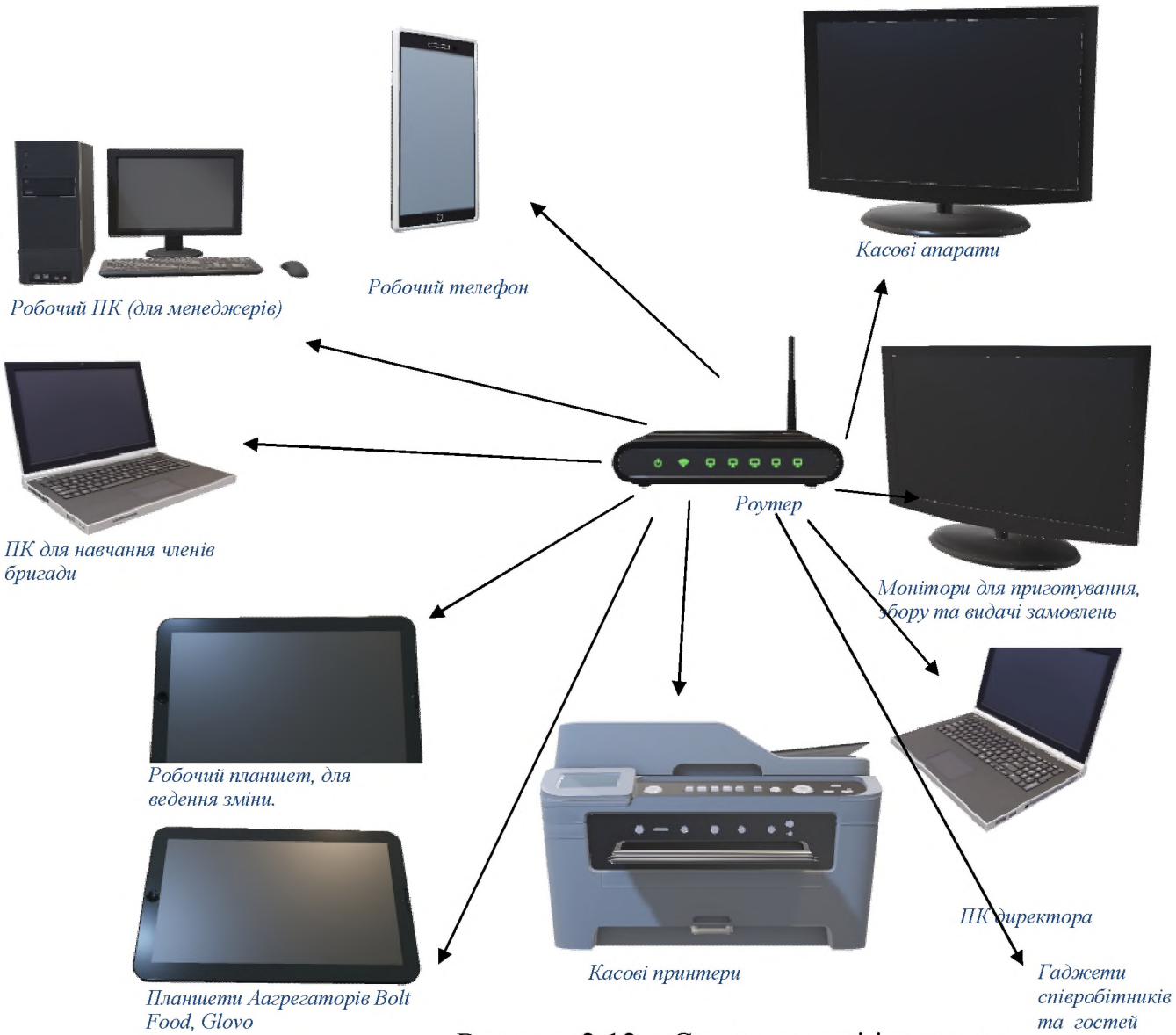


Рисунок 2.12 – Схема мережі інтеренет

Таблиця 2.2 - IT - Обладнення

| № | Назва | Виробник | Модель | Серійний номер | Розміщення |
|---|---|---|---|---|---|
| 1 | POS - моноблок 1 | Detaik | DTK – AIO191 | AIO191D-0082 | На стіні |
| 2 | POS - моноблок 2 | | | AIO191D-0242 | На стіні |
| 3 | POS - моноблок 3 | | | AIO191D-0082 | На стіні |
| 4 | POS - моноблок 4 | | | AIO191D-0087 | На стіні |
| 5 | POS - моноблок 5 | | | AIO191D-1582 | На стіні |
| 6 | POS - моноблок 6 | | | AIO191D-7882 | На стелі |
| 7 | POS - моноблок 7 | | | AIO191D-2682 | На стелі |
| 8 | POS - моноблок 8 | | | AIO191D-1482 | На стіні |
| 9 | POS - моноблок 9 | | | AIO191D-2782 | На столі |
| 10 | POS - моноблок 10 | | | AIO191D-1682 | Вмонтований у стіну |
| 11 | POS - моноблок 11 | | | AIO191D-2182 | На стіні |
| 12 | Телевізор 1 | LG | LQ | 32LQ250B6LA | На стіні |
| 13 | Телевізор 2 | | | 32LQ630B6LA | На стіні |
| 14 | Телевізор 3 | | | 32LQ680B6LA | На стіні |
| 15 | Телевізор 4 | | | 32LQ670B6LA | На стіні |
| 16 | Телевізор 5 | | | 32LQ730B6LA | На стіні |
| 17 | Телевізор 6 | | | 32LQ430B6LA | На колоні |
| 18 | Телевізор 7 | | | 32LQ636B6LA | На колоні |
| 19 | Телевізор 8 | | | 32LQ637B6LA | На колоні |

Продовження таблиці 2.2

| № | Назва | Виробник | Модель | Серійний номер | Розміщення |
|---|---|---|---|---|---|
| 20 | Телевізор 9 | LG | LQ | 32LQ638B6LA | На стіні |
| 21 | Телевізор 10 | | | 32LQ670B6LA | На стіні |
| 22 | Телевізор 11 | | | 32LQ690B6LA | На стіні |
| 23 | Телевізор 12 | | | 32LQ130B6LA | На стіні |
| 24 | POS – термінал 1 | Sam4s | Forza 115 Black | FORZA115FHDKRVLDMKL | На столі |
| 25 | POS – термінал 2 | | | FORZA115FFEFHHLDMKL | На столі |
| 26 | POS – термінал 3 | | | FORZA115FHDYERFDMKL | На столі |
| 27 | POS – термінал 4 | | | FORZA115EJSLRVLDMKL | На столі |
| 28 | POS – термінал 5 | | | FORZA115FHDKRVLVFRY | На столі |
| 29 | POS – прінтер 1 | Sam4s | Giant-100 | B6AYG00578 | На столі |
| 30 | POS – прінтер 2 | | | B6AYG87595 | На столі |
| 31 | POS – прінтер 3 | | | B6AYG02457 | На столі |
| 32 | POS – прінтер 4 | | | B6AYG02456 | На столі |
| 33 | POS – прінтер 5 | | | B6AYG24875 | На столі |
| 34 | POS – прінтер 6 | | | B6AYG00235 | На столі |
| 35 | POS – прінтер 7 | | | B6AYG02015 | На столі |
| 36 | Планшет 1 | Lenovo | Tab M10 | ZA5T0418UA | На столі |
| 37 | Планшет 2 | Samsung | Galaxu Tab | SM-T022FZKGSEK | На столі |
| 38 | Pos - термінал | SUNMI | SUNMI v2 | VB36523670025 | На столі |
| 39 | Pos - термінал | | | VB36522570885 | На столі |
| 40 | Телефон 1 | Samsung | Galaxu A04 | SM-A054FZKGSEK | На столі |

Продовження таблиці 2.2

| № | Назва | Виробник | Модель | Серійний номер | Розміщення |
|---|---|---|---|---|---|
| 41 | Монітор | Samsung | S24 | LS24R365FZIFSD | На столі |
| 42 | Pos – термінал самообслуговування 1 | AV-integrator | | | Закріплений між стелею та підлогою |
| 43 | Pos – термінал самообслуговування 2 | AV-integrator | | | Закріплений між стелею та підлогою |
| 44 | Pos – термінал самообслуговування 3 | AV-integrator | | | Закріплений між стелею та підлогою |
| 45 | Pos – термінал самообслуговування 4 | AV-integrator | | | Закріплений між стелею та підлогою |
| 46 | Системний блок | AMD | ATHLON | ZEVSPCS615 | Під столом |
| 47 | Ноутбук 1 | HP | 250G8 | 7D8Y4GF | На столі |
| 48 | Ноутбук 2 | Lenovo | IdeaPad 1 15ada7 | 82RG00T4RA | На столі |
| 49 | Лазерний принтер | Canon | SENSYS MF3010 | 5264R008 | На столі |

Продовження таблиці 2.2

| № | Назва | Виробник | Модель | Серійний номер | Розміщення |
|---|---|---|---|---|---|
| 50 | Миша дротова 1 | Logitech | M100 | 910-125894 | На столі |
| 51 | Миша дротова 2 | | | 910-845975 | На столі |
| 52 | Миша дротова 3 | | | 910-178956 | На столі |
| 53 | Миша дротова 4 | | | 910-789542 | На столі |
| 54 | Миша дротова 5 | | | 910-789564 | На столі |
| 55 | Миша дротова 6 | | | 910-965847 | На столі |
| 56 | Маршрутизатор 1 | TP-link | Archer | 879D155E8464 | На полиці |
| 57 | Маршрутизатор 2 | Starlink | Dish Kit v2 | 1562558-0345 | На даху |
| 58 | Акивна колонка 1 | Triangle Borea | BR03 | 8964558-2367 | Вмонтована у стіну |
| 59 | Активна колонка 2 | | | 8964558-2978 | Вмонтована у стіну |
| 60 | Активна колонка 3 | | | 8964558-3648 | Вмонтована у стіну |
| 61 | Активна колонка 4 | | | 8964558-3697 | Вмонтована у стіну |
| 62 | Активна колонка 5 | | | 8964558-2597 | Вмонтована у стіну |
| 63 | Активна колонка 6 | | | 8964558-9764 | Вмонтована у стіну |
| 64 | Трансляційний підсилювач потужності | FONESTAR | MA91U2R | CS84554R5695T9 | На полиці |
| 65 | Клавіатура дротова 1 | Maxxter | KBM-U01 | DV87945E894E94 | На столі |

Таблиця 2.3 – Обладнення ресторану.

| № | Обозначення | Виробник | Модель | Серійний номер | Розташування |
|---|---|---|---|---|---|
| 1 | Фритюрниця відкрита 1 | HENNY PENNY | OFE-322 | GT8759R845D54 | На підлозі |
| 2 | Фритюрниця відкрита 2 | | EEE-141 | TR845FE845115E | На підлозі |
| 3 | Фритюрниця закрита 1 | | PXE-100 | GGRD595FRF44F | На підлозі |
| 4 | Фритюрниця закрита 2 | | | GEE84F8EE022FR | На підлозі |
| 5 | Теплова шафа | | HHC-980 | EVDV8158ECC51 | На підлозі |
| 6 | Теплова вітрина | Fabristeel | HBC-48-2T | TD48D4VVS4V4V | На столі |
| 7 | Теплова вітрина для фрі | Robolabs | STP-080 | FVS4F5V55SSS11 | На столі |
| 8 | Холодильник 1 | Capre | MXM | EADDC4S8SC4S4 | На підлозі |
| 9 | Холодильник 2 | | | SC5S4C5S4CSC4S | На підлозі |
| 10 | Холодильник 3 | | | CSSC2SC5SC555S | На підлозі |
| 11 | Холодильник 4 | | | CS5855S5565S511 | На 12підлозі |
| 12 | Холодильник 5 | PEPSI | - | ES888S88SCCS55 | На підлозі |
| 13 | Холодильник 6 | PEPSI | - | 515C5S55S115S55 | На підлозі |
| 14 | Холодильник 7 | Pepsi | - | SS544C54S88S88F | На підлозі |
| 15 | Саладет | GGM Gastro | Premium | DVSFS262S62SS2 | На підлозі |
| 16 | Пост-мікс | Pepsi | Avibar classic 6 | SCSC4C4S4CSCS4 | На столі |
| 17 | Апарат для приготування морозива | Carpigiani | - | CS8C4S44S55555S | На підлозі |
| 18 | Кавова машина | Rheavendors | LarRhea V+ | CSC4S1CSC11S1S | На столі |
| 19 | Кондиціонер 1 | Gree | U-MATCH Inventore | SCSC1SC1S2C12S1 | На стелі |
| 20 | Кондиціонер 2 | | | CS21DEFFEFE55S1 | На стелі |
| 21 | Кондиціонер 3 | | | ESEEBTN44155E55 | На стелі |
| 22 | Кондиціонер 4 | | | FE1S15ESC2212EE | На стелі |

Продовження таблиці 2.3

| № | Обозначення | Виробник | Модель | Серійний номер | Розташування |
|---|---|---|---|---|---|
| 23 | Кондиціонер 5 | Cooper&hunter | CH-IC125 | ES12E12ESE555655 | На стелі |
| 24 | Кондиціонер 6 | | | VRBDB1DBD212D | На стелі |
| 25 | Кондиціонер 7 | | | VR1V2DR1V21DV | На стелі |
| 26 | Кондиціонер 8 | | | WERGRBDA2222A | На стелі |
| 27 | Датчик пожежний тепловий (41шт) | Артон | СПТ-2Б-НЗ | - | На стелі |
| 28 | Радіоконтроллер пожежної сигналізації | | 4-П | 88555655-5264 | На стіні |
| 29 | Аварійний світильник 1 | LUG MULTIWENUS | G-5 | 52122212-030 | На стелі |
| 30 | Аварійний світильник 2 | | | 12000305-652 | На стелі |
| 31 | Аварійний світильник 3 | | | 15251200-560 | На стелі |
| 32 | Камери відеоспостереження (17шт) | Hikvision | Turbo HD | 11120000-2626 | На стіні |
| 33 | Генератор електроенергії | Alimar | Alimar-300 | F5F4S555E55F1E | На підлозі |
| 34 | Радіоконтроллер тривоги | Elmes Electronic | U1-HS | EFEFW44D4WD4 | На стелі |
| 35 | Кнопка тривоги (2шт) | | | | У шафі |

Таблиця 2.4 Характеристики технічних засобів

| № | Назава | Конфігурація | Користувач |
|---|---|---|---|
| 1 | POS – термінал SAM4S Forza 115 | Екран: 15 дюймів PCAP, 1024x768/ Процесор: Intel Celerone J1900 Quad Core(2.0 ГГц)/ Відеоадаптер – вбудований/ Оперативна пам'ять - 4ГБ/ Накопичувач: SSD 120ГБ | Касири ресторану, менеджери, директор, системні адміністратори. |
| 2 | POS – термінал Sunmi V2 | Дисплей: 5.45 дюймів HD+1440x720/ Процесор: Cortex-A53 Quad Core 1.3GHz/ Оперативна пам'ять - 2ГБ/ Накопичувач: 8ГБ | Касири ресторану, менеджери, директор. |
| 3 | POS - Термінал самообслуговування Realtek | Міні-карта 802.11b/g/n RTL8188EE | |
| 4 | PC: AMD ATHLON | Процесор: AMD Athlon 200GE 2x3.2GHz/ Оперативна пам'ять - 4ГБ/ DDR 4/ Відеокарта: Radion Vega 3/ Об'єм відеопам'яті 2ГБ/ Накопичувач: SSD 240ГБ/ Блок живлення 400W | Менеджери, директор, системні адміністратори. |
| 5 | Ноутбук HP 250 G8 | Екран: 15,6 дюймів IPS 60Гц 1920x1080 Full HD/ Процесор: Intel Pentium N5030 – 4 ядра 1,1 Гц/ Оперативна пам'ять - 8ГБ/ DDR 4/ Накопичувач: SSD 128ГБ/ Відеокарта: Intel UHD Graphics | Працівники ресторану, менеджери, директор, системні адміністратори. |
| 6 | Ноутбук Lenovo IdeaPad 1 15ADA7 | Екран: 15,6 дюймів IPS 1920x1080 Full HD/ Процесор: AMD Ryzen 5 3500U – 4 ядра 2.1ГГц/ Оперативна пам'ять - 8ГБ/ DDR 4/ Накопичувач: SSD 256ГБ/ Відеокарта: AMD Radion Vega 8 | Директор. |

Таблиця 2.5 Програмне забезпечення ТЗ

| № | Пристрій | Ліцензія | Строк закінчення ліцензії |
|---|---|---|---|
| 1 | POS – термінал SAM4S Forza 115 | Microsoft Windows 10 Pro | безстрокова |
| 2 | POS - Термінал самообслуговування Realtek | Microsoft Windows 10 Pro | безстрокова |
| 3 | POS - моноблок | Microsoft Windows 10 Pro | безстрокова |
| 4 | POS – термінал Sunmi V2 | Android 13 | безстрокова |
| 5 | PC: AMD ATHLON | Microsoft Windows 10 Pro | безстрокова |
| 6 | Ноутбук HP 250 G8 | Microsoft Windows 10 Pro | безстрокова |
| 7 | Ноутбук Lenovo IdeaPad 1 15ADA7 | Microsoft Windows 10 Pro | безстрокова |
| 8 | POS – термінал SAM4S Forza 115/ Pos – термінал самообслуговування | R_keeper v10 | 18.09.2025 |
| 9 | PC: AMD ATHLON/ Ноутбук Lenovo IdeaPad 1 15ADA7 | 1С Бухгалтерія | 12.06.2024 |
| 10 | PC: AMD ATHLON/ Ноутбук Lenovo IdeaPad 1 15ADA7 | Telegram | Не потребує ліцензії |
| 11 | PC: AMD ATHLON/ Ноутбук Lenovo IdeaPad 1 15ADA7 | Viber | Не потребує ліцензії |
| 12 | PC: AMD ATHLON/ Ноутбук Lenovo IdeaPad 1 15ADA7 | Bitrix | 12.12.2023 |
| 13 | PC: AMD ATHLON/ Ноутбук Lenovo IdeaPad 1 15ADA7/ Ноутбук HP 250 G8 | Microsoft Office | безстрокова |
| 14 | PC: AMD ATHLON/ Ноутбук Lenovo IdeaPad 1 15ADA7/ Ноутбук HP 250 G8/ POS – термінал SAM4S Forza 115/ Pos – термінал самообслуговування | Google Chrome | безстрокова |
| 15 | PC: AMD ATHLON/ Ноутбук Lenovo IdeaPad 1 15ADA7 | R_keeper v10 office | 18.09.2025 |

2.4 – Внутрішне середовище підприємства та його інформаційний простір.

Кожне замовлення проходить через систему R-keeper, замовлення може бути здійсненно різними шляхами:

Перший та основний вид замовлення коли гість підходить до касової стійки де стоїть спеціально навчений касир, гість робить замовлення після чого проходить оплата або за допомогою кредитної карти гостя, або за готівку у першому випадку гість проводить картку через термінал, у другому випадку гість дає необхідну суму, касир розраховує гостя, видає решту, закриває замовленя через програму R-keeper, замовлення заносится до бази даних R-keeper, після чого друкується чек та видається гостю, в той момент коли проходить оплата замовлення, замовлення висвічується у пакерів та працівників кухні для збору та видачі замовлення. Після того як гість оплатив замовлення він може відстежувати його виконання через вмонтований у стіну монітор, після приготування замовленя, зібране замовлення переходить до призентора, той натискає кнопку що замовлення готове та видає замовлення гостю, стандартний час прийому та видачі замовленя складає 1хв 15секунд.

Другий вид замовлення – замовлення через POS – термінал самообслуговування, гість підходить до терміналу вибирає тип замовленя та замовляє після чого здійснює оплату банківською карткою через спеціальний термінал, після успішної оплати замовлення заносится до бази даних R-keeper, гість отримує чек з номером замовлення та відстежує приготування свого замовленя через вмонтований у стіну монітор, після приготування замовленя, зібране замовлення переходить до призентора, той натискає кнопку що замовлення готове та видає замовлення гост, стандартний час прийому та видачі замовленя складає 1хв 15секунд.

Третій вид замовлення – це замовлення на доставку, гість використовує спеціальні застосунки Glovo або Bolt Food через них робить необхідне

замовленя та сплачує банківською картою на рахунок компаній агрегаторів Glovo або Bolt Food, після оплати замовлення, воно надходить до найближче розташованого закладу, спеціально навчений касир приймає замовлення в обробку та пробиває його друкуючи чек по безготівковому розрахунку, після друку чеку замовлення заносится до бази даних R-keeper, працівнки кухні та пакери збирають замовлення та заклеюють його стрічками безпеки, та прикріпляють чек, після чого приходить кур'єр, фотаграфує чек та забирає замовлення, після чого доставляє його гостю, на початку наступного місяця агрегатори підраховують кількість успішно виповнених замовлень та виплачують кошти організації. Стандартний час прийому, видачі та доставки замовленя складає 22-25хв.

Також у організації є клубні карти для гостей та співробітників, гість або співробітник може використати карту на касі будь-якого закладу на будья-яку страву. Інформація про замовленя та персональні дані гостя заносяться до спеціальної бази даних та R-keeper. Кожен гість може залишити свій коментар на сайті компанії який вказан у чеку. Також якщо гостю не сподобалась якась із страв менеджер закладу може повернути кошти за цю страву зробивши відміну чеку через R-keeper, при відміні чеку гість отримує свої грощі, а менеджер чек на товар та чек повернення який відразу друкується, відміна чеку заносится до бази даних R-keeper.

Оптове замовлення робится через програму 1С, будь-який менеджер або директор може зробити отове замовленя, для цього потрібно відкрити у програмі окрему вкладку та вибрати період замовлення, після чого програма надасть залишки товарів на ресторані, та підрахує необхідну кількість для замовлення тих чи інших товарів, якщо менеджер не згоден з тією або іншою позицією він може самостійно її відредагувати, після чого замовленя формерується та надсилається поштовими засобами до логістичної кампанії.

Особисті справи працівників знаходяться у 2х укземплярах, один екземпляр знаходится у офісі ресторану у спецйальній шухляді, до якої має доступ весь менеджерський склад та директор, другий екземпляр знаходится

у головному офісі підприємсва, де доступ до них має тільки уповноважена особа. Після звільнення особиста справа парцівника зберігається протягом 3х місяців, за цей період працівник може влаштуватися знову на ту ж сааму посаду, після 3х місяців особиста спарва знащується средствами шредера.

Інформація про клієнтів зберігається на спеціальному сервері, до осбистих даних клієнтів відносится ПІП, номер телефону та дата народження. Доступ до цієї інформації має системні адміністратори та ІТ – спеціаліст.

У кампанії є своя окрема бухгалтерія, бухгілтерські звіти зберігаются і формуются у системі 1С, формує звіти по ресторану директор. Є адміністратори бухгалтерії які контролюють правельність звітів та формерують окремі звіти самостійно. Після чого усі звіти передаются до податкової інтернет засобами.

Уся юридична інформація зберігається на спеціальному сервері та у паперовому вигляді, знаходится у головному офісі кампанії у спеціальному відділені.

Облікова інформація зберігається у програмі 1С доступ до якої може отримати будь-який менеджер, директор та адміністратор по обліковій інформації кампанії.

Робочий графік для менеджерів зіставляється директором на особистому компьтері до 20-го числа кожного місяця, (на місяць), у графік враховують 80% побажань менеджерів. Робочий графік для основного персоналу зіставляє окремо відведений менеджер на робочому ПК до якогомає доступ удь-який менеджер ресторану та диретор, графік зіставляється на одну неділю, співробітники пишуть свої побажання у групі у Viber, а менеджер на основі цих побажань та вимог до праці виставляє графік працівників враховуючи 80% побажань.

Заробітна відомість формується 2 рази з 01 по 15 та з 16 по 31, окремо відведеним менеджером фоомується на робочому ПК до якого має доступ

будь-який менеджер ресторану та диретор. Менеджер вигружає дані з бази даних у якій кожен з співробітників відмічається кожного дня коли працює відбитком свого пальця, та відправляє для уточнення співробітникам, та при потребі редагує відомість, після чого відправляє відомість до бухгалтерії поштовими засобами, а бухгалтерія у свою чергу вже прощитує заробітну плату працівників та відправляє розрахунки до банку для начислення заробітної плати.

Таблиця 2.6 – доступ до інформації організації

| Потоки інформації ресторану | Автор | Редагування | Відстежування | Видалення | Доступ з іншого пристрою | Місце зберігання | Чи можливе копіювання |
|---|---|---|---|---|---|---|---|
| Особисті спарави співробітників | Директор/Працівник кадрового відділу | Директор/Працівник кадрового відділу | Директор/Працівник кадрового відділу/ Територіальний управляючий | Директор/Працівник кадрового відділу | Так | Головний офіс кампанії у паперовому вигляді та на спеціальному сервері | Так |
| Особиста інформація клієнтів | Клієнт/ системний адміністратор/ IT - спеціаліст | Клієнт | Клієнт/ системний адміністратор/ IT - спеціаліст | Клієнт/ системний адміністратор/ IT - спеціаліст | Так | На сервері | Так |
| Бухгалтерські звіти | Директор/Бухгалтер | Директор/Бухгалтер | Директор/Бухгалтер/ менеджери/ заступник директора | Директор/Бухгалтер | Так | На сервері | Так |
| Юридична інформація | Директор/ юрист | Директор/ юрист | Директор/юрист | Директор/ юрист | Так | Головний офіс кампанії у паперовому вигляді та на спеціальному сервері | Так |

Продовження таблиця 2.6

| Потоки інформації ресторану | Автор | Редагування | Відстежування | Видалення | Доступ з іншого пристрою | Місце зберігання | Чи можливе копіювання |
|---|---|---|---|---|---|---|---|
| Поточні замовлення | Касир/ менеджер /директор/ системний адміністратор | Касир/ менеджер/директор/ системний адміністратор | Касир/ менеджер/директор/ системний адміністратор | Менеджер/ директкор/системний адміністратор | Так | У базі данних R-keeper | Так |
| Відпрацьвані замовлення | Касир/ менеджер /директор/ системний адміністр | Касир/ менеджер /директор/ системний адміністратор | Касир/ менеджер /директор/ системний адміністратор | Менеджер/ директкор/системний адміністратор | Так | У базі данних R-keeper | Так |
| Видалені замовлення | Менеджер/ директкор/системний адміністратор | Менеджер/ директкор/системний адміністратор | Менеджер/ директкор/системний адміністратор | - | Так | У базі данних R-keeper | Так |
| Облікова інформація | Менеджери / директор/ адміністратор програми 1С/ працівники фінансового відділу/ працівники віділу продажів | Менеджери / директор/ адміністратор програми 1С/ працівники фінансового відділу/ працівники віділу продажів | Менеджери / директор/ адміністратор програми 1С/ працівники фінансового відділу/ працівники віділу продажів | Адміністратор програми 1С | Так | У програмі 1С | Так |
| Інформація про кількість грошей у сейфі | Менеджери /директор | Менеджери /директор | Менеджери /директор | - | - | У менеджерській кімнаті | - |

Продовження таблиця 2.6

| Потоки інформації ресторану | Автор | Редагування | Відстежування | Видалення | Доступ з іншого пристрою | Місце зберігання | Чи можливе копіювання |
|---|---|---|---|---|---|---|---|
| Інформація про кількість грошей у касовому ящику касира | Касир /Менеджери /директор | Касир /Менеджери /директор | Касир /Менеджери /директор | - | - | Під касовим апаратом | |
| Новини кампанії | Всі авторизовані користувачі кампанії | Всі авторизовані користувачі кампанії | Всі авторизовані користувачі кампанії | Системний адміністратор | Так | У програмі Bitrix та у соцмережах | Так |

Продовження таблиця 2.6

| Нововедення кампанії/ зміни стандартів | Всі авторизовані користувачі кампанії | Всі авторизовані користувачі кампанії | Всі авторизовані користувачі кампанії | - | Так | У програмі Bitrix та у соцмережах | Так |
|---|---|---|---|---|---|---|---|
| Справність технічних засобів | Директор/ менеджери /співробітники | Технік | Директор/ менеджери /співробітники | - | - | На території реторану | - |
| Робочий графік | Директор/ менеджери | Директор/ менеджери | Директор/ менеджери/ співробітники ресторану | Директор/ менеджери | Так | На робочому ПК/ На особистому ПК директора | Так |
| Зарпалатна відомість | Директор/ менеджери | Директор/ менеджери | Директор/ менеджери/ співробітники ресторану | Директор/ менеджери | Так | На робочому ПК | Так |

Таблиця 2.7 Визначення конфеденційності, цілістночті та доступності

| Інформація | Рівень конфеденційності | Рівень цілісності | Рівень доступності |
|---|---|---|---|
| Особисті спарави співробітників | C2 | I0 | A0 |
| Особиста інформація клієнтів | C2 | I1 | A3 |
| Бухгалтерські звіти | C3 | I2 | A3 |
| Юридична інформація | C3 | I2 | A3 |
| Поточні замовленя | C0 | I0 | A0 |
| Відпрацьвані замовлення | C1 | I1 | A2 |
| Видалені замовленя | C2 | I1 | A2 |
| Облікова інформація | C1 | I1 | A1 |
| Інформація про кількість грошей у сейфі | C2 | I2 | A3 |
| Інформація про кількість грошей у касовому ящику касира | C2 | I2 | A3 |
| Новини кампанії | C0 | I0 | A0 |
| Нововедення кампанії/ зміни стандартів | C1 | I0 | A1 |
| Справність технічних засобів | C2 | I0 | A0 |
| Робочий графік | C0 | I1 | A0 |
| Зарпалатна відомість | C2 | I1 | A2 |

Рівні конфіденційності:

C0 - інформація, яка не вимагає спеціального захисту та може бути доступна публічно. До неї належать загальнодоступні дані, такі як публічні новини, інформація на сайтах компанії та інші нечутливі дані.

C1 - інформація може бути доступна лише співробітникам та іншим уповноваженим особам. Може включати документи, звіти, процедури, внутрішні комунікації та інші матеріали, не призначені для громадського доступу.

C2 - інформація, яка вимагає особливого захисту через свою чутливість

і потенційні збитки, які можуть бути заподіяні, якщо вона потрапить у неправильні руки. Може включати персональні дані клієнтів, фінансову інформацію, комерційні секрети, патенти, стратегічні плани та інші конфіденційні матеріали.

С3 - найвищий рівень конфіденційності, який застосовується до найчутливішої інформації, що потребує особливого режиму зберігання та доступу. Може призвести до краху кампанії

Рівні цілісності:

I0 - Дані на низькому рівні цілісності можуть бути змінені без істотних наслідків чи шкоди організації. Це можуть бути, наприклад, загальнодоступні дані, які не потребують особливого захисту цілісності.

I1 - Дані на середньому рівні цілісності мають певний ступінь важливості та вимагають захисту від несанкціонованих змін. Це можуть бути, наприклад, фінансові дані, особисті дані клієнтів або внутрішні документи, які можуть вплинути на роботу організації.

I2 - Дані на високому рівні цілісності є критичними для роботи організації та потребують найвищого рівня захисту. Це можуть бути, наприклад, клієнтські секрети або інші конфіденційні дані, зміна яких може призвести до серйозних наслідків.

A0 – Дані з повною доступністю мають бути доступні у будь-який час для авторизованих користувачів без будь-яких обмежень. Цей рівень доступності зазвичай потрібний для критично важливих систем і даних, де просто недоступність може мати серйозні наслідки для бізнесу чи діяльності організації.

A1 – Дані на цьому рівні доступності мають бути доступні у значній частині часу, з мінімальними періодами недоступності. Це забезпечується через резервування систем та резервне копіювання даних, щоб мінімізувати втрати доступності у разі виникнення збоїв або відмов.

A2 – Дані цього рівня доступності можуть мати обмеження

доступності, наприклад, за розкладом обслуговування або плановим роботам. Цей рівень доступності може бути застосований для некритично важливих даних або систем, де деяка недоступність може бути прийнятною.

А3 – Дані мають значні обмеження доступності, наприклад, доступ до них може бути дозволений тільки в певні періоди часу або в певних умовах. Цей рівень доступності може бути застосований для дуже чутливої інформації, яка потребує високого ступеня контролю доступу.

2.5 – Складеня моделі порушника

Модель порушника дозволяє оцінити можливості та мотивацію різних типів порушників, щоб вжити відповідних заходів щодо забезпечення безпеки інформаційних систем. Це важливий інструмент для розробки стратегії безпеки та реагування на можливі загрози.  для ідентифікації та класифікації потенційних загроз та уразливостей в інформаційних системах. Вона допомагає визначити, які типи порушників можуть бути зацікавлені в атаці на систему та які методи вони можуть використовувати.

Модель порушника допомагає в оцінці ризиків безпеки та розробленні відповідних заходів щодо захисту інформаційних ресурсів. Загалом модель порушника може включати такі категорії:

— Внутрішні порушники: Це співробітники чи особи, які мають легальний доступ до інформаційної системи. Внутрішні порушники можуть містити зловмисних працівників, незадоволених працівників, а також випадки некоректного використання прав доступу.

— Зовнішні порушники Це особи або організації, які не мають авторизованого доступу до інформаційної системи. Зовнішні порушники можуть містити хакерів, кіберзлочинців, конкурентів, державні агенції та інших зловмисників.

— Неавторизовані порушники: Це особи чи організації, які намагаються отримати несанкціонований доступ до інформаційної системи чи її ресурсів. Неавторизовані порушники можуть використовувати такі

методи, як злом паролів, фішинг, атаки переповнення буфера та інші методи злому.

— Внутрішні загрози: Це загрози, які походять від внутрішніх співробітників, які ненавмисно можуть спричинити порушення безпеки. Наприклад, це може бути необережне поводження з конфіденційною інформацією або помилки у налаштуваннях системи.

— Фізичні загрози: Це загрози, пов'язані з фізичним доступом до інформаційної системи або її обладнання. Наприклад, це можуть бути крадіжки обладнання, знищення чи пошкодження фізичної інфраструктури, повені тощо.

Для складання моделі порушника визначаются такі пункти:

— Цілі та мотивація: Визначають можливі цілі та мотивацію порушника. Це може бути фінансове збагачення, руйнування, крадіжка даних, шпигунство, активізація противника і т.д.

— Рівень доступу: Визначає рівень доступу, який може порушник мати до інформаційної системи. Різні рівні доступу можуть визначити, які дані та ресурси доступні порушнику.

— Технічні навички: Оцінення технічного знання та навичок, якими володіє порушник. Це може включати знання різних видів атак, використання інструментів та програм, аналіз уразливостей та інші навички.

— Методи атаки: Визначає можливі методи атаки, якими може скористатися порушник. Це може бути фішинг, шкідливі програми, атаки на мережеві вразливості, соціальна інженерія, відмова в обслуговуванні та інші.

— Засоби та ресурси: Визначає доступні порушнику засоби та ресурси для здійснення атаки. Це може містити обчислювальні потужності, програмне забезпечення, мережеве обладнання, фінансові ресурси та інші.

— Внутрішні та зовнішні загрози: Враховуються можливі внутрішні та зовнішні загрози. Внутрішні загрози можуть містити зловмисних співробітників або помилки та недогляди всередині організації. Зовнішні

загрози можуть містити хакерів, кіберзлочинців, конкурентів та інших зовнішніх акторів.

— Сценарії атак: Розроблення різних сценаріїв атак на основі вищезгаданих факторів. Розгляд можливих наслідки атаки та способи проникнення порушника в інформаційну систему.

Цілями поршників можуть бути:

— Фінансове збагачення - багато порушників прагнуть отримати фінансову вигоду через свої дії. Це може включати крадіжку фінансових даних, шахрайство з пластиковими картками, та інші схеми, спрямовані на незаконне отримання коштів.

— Шпигунство та кіберрозвідка - деякі порушники працюють на державні або приватні структури, які цікавляться отриманням конфіденційної інформації, інтелектуальної власності, стратегічних планів та іншої чутливої інформації.

— Руйнування та заподіяння шкоди - деякі порушники можуть мати на меті завдати шкоди організації або інфраструктурі. Це може бути виявлено через цілеспрямовані атаки на інформаційні системи, деструктивне програмне забезпечення, відмову в обслуговуванні (DDoS-атаки) або фізичне руйнування обладнання.

— Репутаційна шкода - деякі порушники можуть мати на меті завдати шкоди репутації організації або окремих осіб. Це може бути досягнуто через витік конфіденційної інформації, поширення хибної інформації, маніпуляції з даними або атаки на онлайн-ресурси.

— Незаконний доступ до конфіденційної інформації - деякі порушники можуть прагнути отримати несанкціонований доступ до конфіденційних даних, таких як фінансова інформація, інтелектуальна власність, особисті дані клієнтів тощо. Метою може бути крадіжка цих даних для подальшого використання чи продажу на чорному ринку.

— Розповсюдження шкідливих програм - деякі порушники можуть

використовувати інформаційні системи для поширення шкідливих програм, таких як віруси, черв'яки, троянські програми та інші.

— Порушення конфіденційності - деякі порушники можуть прагнути порушити конфіденційність інформації або комунікацій. Вони можуть прослуховувати або перехоплювати передачу даних, зламувати шифрування або використовувати інші способи доступу до приватної інформації.

Таблиця 2.8 – Побудова моделі порушника

| Працівник | Різвень знань щодо ІТС | Рівень подалання систем захисту | Спонукання порушень | Можливості за часом дій | Можливості за місцем дій | Кількість загроз |
|---|---|---|---|---|---|---|
| Директор | L3 | O2 | I4/I5 | T1/T4/T5/T6 | P1/P4/P5 | 40 |
| Заступник директора | L3 | O2 | I4/I5 | T1/T4/T5/T6 | P1/P4/P5 | 40 |
| Менеджер | L3 | O2 | I5/I4/I6 | T1/T4/T5/T6 | P1/P5 | 42 |
| Молодший менеджер | L2 | O2 | I4/I6 | T1/T4 | P1 | 20 |
| Инструктор з виробничого навчання | L2 | O1 | I3 | T2 | P1 | 9 |
| Касир | L1 | O1 | I3 | T2 | P1 | 8 |
| Член бригади | L1 | O1 | I1/I3 | T2 | P1 | 9 |
| Комірник | L1 | O1 | I5 | T1/T2 | P1 | 11 |
| Системний адміністратор | L3 | O3 | I5 | T3/T4/T5/T6 | P2/P3/P4 | 38 |
| Спеціаліст ремонтної служби | L1 | O1 | I3 | T2 | P1 | 8 |
| ІТ – спеціаліст | L4 | O3 | I5 | T3/T4/T5/T6 | P3/P4 | 37 |

Продовження таблиці 2.8

| | | | | | | |
|---|---|---|---|---|---|---|
| Прибиральник | L1 | O1 | I5 | T1/T2 | P1 | 11 |
| Хакери | L4 | O3 | I1/I5 | T2/T4 | P3 | 22 |
| Колишні робітники | L2 | O1 | I1 | T2 | - | 6 |

Рівні знань щодо ІТС

— L1 - Низький рівень обізнаності: Користувачі з низьким рівнем обізнаності мають обмежені знання, не усвідомлюють ризики, пов'язані з неправильним використанням інформаційних ресурсів. Вони можуть бути незнайомими з базовими поняттями, такими як паролі, антивірусне програмне забезпечення, оновлення системи тощо.

— L2 - Користувачі із середнім рівнем обізнаності мають базові знання усвідомлюють деякі ризики. Вони знають, як створювати та використовувати складні паролі, перевірять справжність веб-сайтів, здійснювати регулярні резервні копії даних та бути обережнішими при відкритті вкладень електронної пошти.

— L3 - Користувачі з високим рівнем обізнаності мають глибокі знання про ІТС

— L4 - Експертний рівень обізнаності це найвищий рівень обізнаності, де користувач має глибокі знання. Ці користувачі можуть бути адміністраторами систем або професіоналами в галузі управління.ї

Рівень подаланя систем захисту:

— O1 – Низький рівень знань технічних засобів, вміє працювати з технічними приладами

— O2 – Середній рівень знань ТЗ, вміє працювати з технічними приладами та знається на роботі організації.

— O3 – Високий рівень знань ТЗ, вміє долати механізми засобів захисту, знає побудову та функції ІТС.

Мотиви порушень:

— I1 – Заради задоволення

— I2 – Ідеологічні мотиви

— I3 – Незнання

— I4 – Самоствердження

— I5 – Корисна вигода

— I6 – Безвідповідальність

Можливості за часом дій:

— T1 – Під час не робото - здатності ІТС.

— T2 – Під час повної бездіяльності та знехтуванням правил безпеки.

— T3 –Під час технічних робот на ІТС

— T4 – Під час передачі даних або передачі обладнення та продукції, порушники можуть перехоплювати або змінювати передані матеріали, особливо якщо вони передаються незахищеними або ненадійними каналами.

— T5 – При фізичному доступі, якщо зловмисник має фізичний доступ до обладнання або серверів ІТС, він може спробувати внести зміни до системи, вкрасти дані або обладнення, пошкодити обладнання.

— T6 – Під час експлуатації

Можливості за місцем дій:

— P1 – З робочих місць працівників у середені приміщень

— P2 – З робочих міст системних операторів

— P3 – Дистанційно

— P4 – З доступом до керування ІТС

— P5 – З доступом до керування систем безпеки

Роздивившись таблицю 2.8 (Побудова моделі порушника), я виявив що високу вирогідність порушень у внутрішньому середовищі кампанії має менеджер, директор, заступник директора, системний адміністратор, та ІТ – спеціаліст, вони мають самий високий рівень доступу до інформації, високу

обізнаность у ІТС, та доступ до систем захисту, також володіють доступом до всієї інформації кампанії. Можуть заволодіти даними або технічними засобами кампанії, як дистанційно так і на території кампанії.

На зовнішньому колі порушень я виявим загрозу у вигляді хакерів, через свої вміння та навички вони можуть вкрасти інформацію або змінити її дистанційно без будь-яких проблем.

2.6 – Вразливості які можуть бути на підприємстві

Техногенні врзливості:

— Аварії та збої в системах непередбачені збої та аварії в комп'ютерних системах, серверах, мережах або інших технічних пристроях, які можуть призвести до втрати доступу до даних та непродуктивності.

— Втрата даних або пошкодження даних внаслідок збоїв обладнання, помилок працівників, атак хакерів або інших факторів, що може призвести до втрати цінної інформації.

— Порушення інформаційної безпеки, уразливості в системах, несанкціонований доступ, зломи, віруси, шкідливе ПЗ та інші атаки, які можуть завдати шкоди інформаційним ресурсам і порушити конфіденційність даних.

— Порушення цілісності даних, небажана зміна даних, підробка або пошкодження інформації, що може призвести до недостовірних результатів або хибних рішень.

— Неправильне використання технічних средств, чи зловживання технічними засобами, включаючи неправильну конфігурацію систем, несанкціоновану установку програмного забезпечення, витік інформації та інші.

— Порушення інтелектуальної власності крадіжка або порушення прав інтелектуальної власності, включаючи програмне забезпечення, дизайн, патент, товарні знаки та інші елементи.

— Фізичні загрози порушення безпеки фізичних об'єктів та інфраструктури, включаючи крадіжки, вандалізм, пожежі, повені та інші події.

— Порушення конфіденційності витік конфіденційної інформації через несанкціонований доступ, виток даних або помилок у системах.

— Технологічні зміни швидкий розвиток технологій та зміни в середовищі можуть призвести до застаріння систем та обладнання

Антропогенні

— Внутрішні загрози що походять від співробітників або осіб, які мають доступ до інформації та ресурсів організації, такі як крадіжка даних, зловживання привілеями, саботаж або необережне поводження з інформацією.

— Несанкціонований доступ спроби несанкціонованого доступу до систем та даних організації з боку зловмисників або неавторизованих користувачів, наприклад, шляхом злому паролів або використання вразливостей у системі.

— Соціальна інженерія, маніпуляція та обман співробітників організації з метою отримання доступу до інформації або систем, наприклад шляхом фішингу, підроблених дзвінків або обману.

— Несумлінне використання ресурсів порушення правил та політик організації з метою незаконного одержання вигоди, у тому числі використання інформації чи ресурсів організації в особистих інтересах або для конкурентних цілей.

— Помилки та недбалість порушення безпеки, спричинені помилками, неправильним поводженням з інформацією або недбалою поведінкою співробітників, наприклад, втрата або неправильне видалення даних, некоректне налаштування систем або недотримання правил безпеки.

— Витік інформації порушення конфіденційності та витік інформації через незаконне розкриття або несанкціоноване поводження з даними,

наприклад, продаж або передача конфіденційних даних третім особам.

— Соціальні конфлікти та крадіжки, конфлікти між співробітниками, крадіжка майна організації чи крадіжки даних усередині організації.

— Помилки в управлінні, неправильне прийняття рішень у сфері безпеки, недостатнє фінансування або недостатня увага до питань безпеки з боку керівництва, що може створити вразливість у системах та процесах.

— Недостатнє навчання та поінформованість, недостатнє знання співробітників про основні заходи безпеки, неправильне використання систем та відсутність поінформованості про поточні загрози та способи запобігання їм.

2.7 Профіль захищеності

Профіль захищеності (або профіль безпеки) – це оцінка рівня захищеності інформаційної системи чи організації на основі різних аспектів безпеки. Він є комплексною оцінкою вразливостей, загроз і заходів безпеки, що застосовуються в системі. Профіль захищеності допомагає організаціям оцінити поточний рівень безпеки та вжити заходів для підвищення захищеності інформаційної системи. Він є важливим інструментом для забезпечення надійності та захисту інформації від різних загроз та атак.

Виходячи з нашого аналізу безпеки данного підприємства я обрав наступний профіль захищеності:

$КЦД.1 = \langle ДВ-1, ЦД-1, ЦВ-1, ЦО-1, НИ-2, НВ-1, НР-2, НО-1, НК-1, НТ-2, НЦ-2, КВ-1 \rangle$

ДВ – 1 Ручне відновлення - це процес відновлення роботи інформаційної системи або даних шляхом втручання адміністратора системи без використання автоматичних засобів чи процесів.

Ручне відновлення може бути необхідним у випадках, коли відбувається збій системи, порушення безпеки, втрата даних або інші проблеми, які потребують відновлення роботи системи. У процесі ручного відновлення адміністратор системи виконує ряд дій для відновлення

нормального функціонування системи або відновлення втрачених даних. Ручне відновлення може вимагати певних навичок і знань з боку адміністратора системи. Важливо мати розуміння роботи системи, процедур відновлення та відповідних інструментів та методів.

ЦВ – 1 Мінімальна цілісність при обміні інформацією відноситься до рівня збереження та недоторканності даних у процесі їх передачі між системами чи суб'єктами. Цей рівень цілісності забезпечує мінімальні вимоги, щоб інформація не була змінена або пошкоджена в процесі передачі. Інформація має бути передана у незмінному вигляді без будь-яких несанкціонованих змін, втрат чи пошкоджень. Для забезпечення цієї цілісності можуть використовуватись різні механізми, такі як хешування даних, цифрові підписи та перевірка контрольних сум. Інформація має бути передана лише між суб'єктами, які мають право на доступ до неї. Для цього можуть застосовуватися механізми автентифікації та авторизації, такі як використання облікових записів, паролів, сертифікатів та інших засобів ідентифікації. Якщо інформація є конфіденційною, мінімальна цілісність при обміні такою інформацією передбачає захист від несанкціонованого розкриття. Це можна досягти шляхом застосування шифрування даних або інших методів захисту конфіденційності.

Загалом мінімальна цілісність при обміні інформацією забезпечує збереження даних та захист від несанкціонованих змін або пошкоджень. Вона є основою забезпечення безпечного обміну інформацією між системами і суб'єктами.

ЦО – 1 Обмежений відкат також відомий як обмежений відкат транзакції або скасування операції - це процес скасування транзакції або операції з обмеженнями та контролем. Обмежений відкат дозволяє скасувати чи відкотити зміни, створені у системі, внаслідок виконання певної операції чи транзакции. Він може бути корисним. Якщо в систему були внесені некоректні або помилкові дані, обмежений відкат дозволяє скасувати операцію та відновити вихідний стан даних. Якщо виконання операції

суперечить певним бізнес-правилам або обмеженням, обмежений відкат може бути використаний для скасування операції та запобігання небажаним наслідкам.

У розрахованому на багато користувачів середовищі або при паралельному виконанні операцій можуть виникати конфлікти і проблеми з цілісністю даних. Обмежений відкат дозволяє усунути такі конфлікти та повернути систему у узгоджений стан.

У фінансових системах, таких як банківські системи, може виникнути необхідність скасування виконаних фінансових транзакцій. Обмежений відкіт дозволяє здійснити цю відміну з урахуванням фінансових та юридичних обмежень. Важливо відзначити, що обмежений відкат потребує відповідних механізмів і контролю, щоб гарантувати, що операції, що скасовуються, виконуються безпечно і без порушення цілісності даних. Це може включати перевірку доступу, журналування операцій та відновлення стану даних до попереднього стану. Обмежений відкат є важливим інструментом забезпечення надійності та цілісності систем обробки даних. Він дозволяє виправляти помилки, усувати проблеми та відновлювати систему у разі непередбачених ситуацій чи порушень.

НИ – 2 Поодинока ідентифікація та аутентифікація - це процеси, пов'язані із встановленням особистості користувача та перевіркою його справжності в інформаційній системі.

Одиночна ідентифікація (Single Sign-On, SSO) являє собою механізм, який дозволяє користувачу отримати доступ до багатьох пов'язаних систем або програм з використанням єдиного набору облікових даних. При одиночній ідентифікації користувач вводить свої облікові дані (логін і пароль) лише один раз, і ці дані використовуються для аутентифікації та авторизації користувача в різних системах, без необхідності повторного введення даних. Це підвищує зручність використання та спрощує керування обліковими записами користувачів.

Аутентифікація - це процес перевірки автентичності облікових даних користувача, щоб переконатися, що він є тим, за кого себе видає. Під час аутентифікації користувач надає облікові дані, наприклад, логін та пароль, і система перевіряє їх на відповідність збереженим даним у базі даних або інших джерелах аутентифікації. В результаті користувачеві надається доступ до системи або відмова у доступі у разі невідповідності або невірних даних.

Поодинока ідентифікація та аутентифікація працюють разом для забезпечення безпечного доступу користувачів до інформаційних систем. При використанні одиночної ідентифікації користувач проходить аутентифікацію лише один раз, і його ідентифікаційні дані зберігаються в захищеному сховищі. Потім ці дані використовуються для автоматичної автентифікації користувача інших пов'язаних системах. Це спрощує досвід користувача, оскільки користувачеві не потрібно запам'ятовувати і вводити різні облікові дані для кожної системи. Однак, для забезпечення безпеки, особливо при роботі з конфіденційними даними, необхідно використовувати надійні методи аутентифікації, такі як двофакторна аутентифікація або біометрична аутентифікація, щоб запобігти несанкціонованому доступу до інформації.

НВ – 1 Аутентифікація вузла, процес автентифікації вузла або пристрою в мережі. Під час аутентифікації вузла перевіряється, чи є вузол дійсним та авторизованим для доступу до мережі або для виконання певних операцій. Аутентифікація вузла зазвичай виконується з використанням унікальних ідентифікаторів або сертифікатів, які надаються вузлу та підтверджують його дійсність.

Вузол надає пароль або секретний ключ для перевірки автентичності. Пароль може бути попередньо встановлений або згенерований під час аутентифікації.

Вузол надає цифровий сертифікат, який містить інформацію про його ідентифікацію та підписаний сертифікаційним центром. Сторона, що

перевіряє, може використовувати цей сертифікат для перевірки автентичності вузла.

Також вузол може використовувати методи криптографії, такі як обмін ключами або підписи повідомлень, для підтвердження своєї автентичності перед іншими вузлами або серверами. Вузол може бути автентифікований за допомогою біологічних характеристик, таких як відбиток пальця, сканування сітківки або розпізнавання обличчя. Біометричні дані вузла порівнюються зі збереженими шаблонами для автентифікації.

Аутентифікація вузла відіграє важливу роль у забезпеченні безпеки мереж та запобіганні несанкціонованому доступу або заміні вузлів. Вона дозволяє мережевим адміністраторам перевіряти та контролювати доступ до ресурсів та даних, а також виявляти та запобігати спробам атак чи зловмисних дій з боку несанкціонованих вузлів.

HP – 2 Захищений журнал – це механізм, який використовується для запису та зберігання подій та дій, що відбуваються в інформаційній системі чи мережі, з метою забезпечення безпеки, відстеження та аудиту. Захищений журнал включає записи про різні події, такі як автентифікація користувачів, доступ до ресурсів, зміни конфігурації системи, виявлення аномальних подій та інші дії, які можуть бути важливими для безпеки та аналізу. Захищені журнали є важливим інструментом забезпечення безпеки інформаційних систем. Вони допомагають у виявленні та реагуванні на інциденти безпеки, надають докази та аудит інформаційних

HO – 1 Виділення адміністратора, процес отримання або розширення привілеїв користувача або процесу в інформаційній системі чи мережі. Зазвичай користувачі мають обмежені привілеї, щоб запобігти несанкціонованому доступу та зловживанню правами. Однак, у разі успішного виділення адміністратора, зловмисник отримує вищі привілеї, ніж у нього є спочатку. Виділення адміністратора є серйозною загрозою для безпеки інформаційних систем, оскільки зловмисник з розширеними

привілеями може мати доступ і контроль над цілою низкою функцій та ресурсів. Тому важливо вживати заходів для запобігання виділенню адміністратора, включаючи регулярне оновлення системи та додатків, обмеження доступу до привілейованих облікових записів, контроль та моніторинг активності користувачів, використання засобів виявлення вторгнень та антивірусних програм, а також навчання користувачів основ безпеки інформаційних систем.

НК – 1 Односпрямований достовірний канал: тип зв'язку або комунікаційного каналу, який забезпечує передачу даних тільки в одному напрямку та забезпечує достовірність інформації, що передається. Однонаправлений канал гарантує, що інформація може бути передана тільки від відправника до одержувача та не може бути зворотного потоку інформації від одержувача до відправника. Це забезпечує контроль над потоком даних та запобігає можливості внесення змін або підробки даних по ходу передачі. Достовірність означає, що інформація, що передається однонаправленим каналом, не може бути підроблена, змінена або скомпрометована. Він також забезпечує захист від несанкціонованого доступу та перехоплення інформації третіми особами. Прикладом односпрямованого достовірного каналу є система передачі даних через оптичний кабель або кабель з лазерною заслінкою. У цьому випадку дані передаються за допомогою світлових сигналів, і канал фізично забезпечує односпрямованість і неможливість внесення змін до інформації, що передається. Односпрямовані достовірні канали є важливим інструментом у сфері інформаційної безпеки, оскільки вони дозволяють забезпечити конфіденційність і цілісність інформації, що передається, мінімізуючи ризики витоку даних та несанкціонованого доступу.

НТ – 2 Самотестування при старті, також відоме як самоперевірка або самодіагностика, є процесом, при якому комп'ютерна система або пристрій виконує автоматичну перевірку своїх компонентів та функціональності при включенні або перезавантаженні. Мета самотестування при старті полягає в

тому, щоб виявити можливі проблеми або несправності в системі, а також переконатися у правильній роботі всіх компонентів перед запуском операційної системи чи додатків. Під час самотестування система проходить через низку тестових процедур та алгоритмів, які перевіряють працездатність процесора, пам'яті, жорсткого диска, периферійних пристроїв та інших компонентів.

Процес самотестування при старті може включати наступні кроки:

— Power-on self-test (POST): Це початкова перевірка, яку виконує система після включення живлення. POST перевіряє основні компоненти системи, такі як процесор, пам'ять, графічний адаптер та клавіатуру, і відображає повідомлення про помилку чи попередження, якщо виявлено проблеми.

— Перевірка BIOS/UEFI: Перевірка в системі наявність та правильність BIOS або UEFI, які є програмним забезпеченням, яке контролює основні функції системи.

— Перевірка роботи жорсткого диска та інших пристроїв зберігання даних перевірка доступність та працездатність жорсткого диска або інших пристроїв зберігання даних, щоб переконатися, що вони готові до використання.

— Перевірка пристроїв введення-виведення система може перевірити працездатність та правильне підключення пристроїв введення-виводу, таких як клавіатура, миша, монітор та принтер.

— Перевірка пам'яті: тестування оперативної пам'яті (RAM) для виявлення можливих помилок або несправностей.

— Перевірка периферійних пристроїв: Залежно від конфігурації системи можуть бути виконані додаткові перевірки периферійних пристроїв, таких як звукова карта, мережна картка або порти USB.

У разі виявлення проблем або помилок під час самотестування система може видати відповідні повідомлення, попередження або звукові сигнали, які

допоможуть користувачеві або адміністратору визначити причину та вжити заходів для усунення проблеми.

НЦ – 2 Комплекс засобів захисту з гарантованою цілісністю (КСЗГЦ) є сукупністю технічних та організаційних заходів, спрямованих на забезпечення безпеки та недопущення порушення цілісності інформації. Він призначений для захисту інформаційних систем та даних від несанкціонованого доступу, зміни чи знищення. КСЗГЦ включає різні компоненти і методи, що забезпечують гарантовану цілісність інформації. Це можуть бути криптографічні алгоритми та протоколи, цифрові підписи, системи контролю цілісності даних, фізичні заходи безпеки (наприклад, відеоспостереження, контроль доступу), політики та процедури управління інформаційною безпекою тощо. Основний принцип КСЗГЦ полягає в тому, що він повинен забезпечувати неприпустимість несанкціонованої зміни інформації та гарантувати її цілісність у всіх станах та на всіх етапах обробки, передачі та зберігання. Для цього застосовуються різні методи та механізми, включаючи перевірку цифрових підписів, алгоритми хешування, контрольні суми, системи реєстрації та аудиту тощо. Метою комплексу засобів захисту з гарантованою цілісністю є запобігання несанкціонованому доступу до інформації та її змін, а також виявлення та реагування на будь-які спроби порушення цілісності даних. Це дозволяє захистити критично важливу інформацію та забезпечити надійну роботу інформаційних систем та процесів.

КВ – 1 Політика конфіденційності при обміні інформацією є набором правил, принципів та заходів безпеки, які встановлюються для захисту конфіденційності інформації в процесі її обміну між сторонами. Мета політики конфіденційності – забезпечити контроль за доступом до інформації, запобігти несанкціонованому розкриттю або використанню даних та захистити конфіденційність клієнтів, партнерів та інших зацікавлених сторін.

## 2.8 Розробка політики безпеки інформації

Розробка політики безпеки інформації є важливим кроком для забезпечення безпеки інформаційних ресурсів та захисту конфіденційності, цілісності та доступності даних в організації. Проаналізувавши загрози на підприємстві я дійов висновку, що треба розробити елементи політики безпеки інформації, для запобігання та зниження рівня загроз.

Най вищій рівень небезпечності мають:

— Отримання конфіденційної інформації

— Порушення цілісності даних

— Заподіяння серйозної шкоди системам

— Несанкціонований доступ до даних

— Помилки працівників

— Нанесення серйозної шкоди технічним системам

— Ураження шкідливим ПЗ

— Читання інформації на паперових носіях через оптичний канал

— Крадіжка майна організації

Перелічивши небезпечні загрози для організації, розробимо політику безпеки інформації.

### 2.8.1 Розробка політики «чистого столу»

Політика безпеки «чистого столу» є одним із заходів щодо забезпечення фізичної безпеки інформації в організації. Вона призначена для запобігання несанкціонованому доступу, витоку або втрати конфіденційної інформації, залишеної без належного спостереження на робочих місцях.

Основні засади політики "чистого столу" включають:

Очищення робочого місця: Менеджери та директор повинні очищати свої робочі столи від усіх документів, паперів, записів або інших матеріалів, що містять конфіденційну інформацію, перед виходом з робочого місця або поза робочим годинником.

Закриття та блокування: Співробітники повинні закривати та блокувати свої комп'ютери, ноутбуки, виходити з облікових записів на POS – терміналах, додатків які відносяться до організації, наприклад: 1С, Bitrix, та інші додатки організації, мобільних пристроїв та інших електронних пристрої під час залишення робочого місця або поза робочим годинником.

У кінці робочого дня всі ЕОМ повинні бути вимкненні

Видалення конфіденційних документів: Менеджери та директор повинні правильно утилізувати конфіденційні документи, використовуючи спеціальні контейнери для знищення документів або системи керування відходами.

Закриті приміщення: Приміщення організації, такі як переговорні кімнати, дах, кімнати для збереження обладнення повинні бути закриті у повсякденний час, та відкриватися тільки під контролем менеджера або директора.

У кінці дня менеджер повинен заховати усі паперові носії з ІзОД у відповідні ящики які зачиняются на ключ.

Менеджер обов’зково повинен перевірити зачинення ресторану, всіх сейфів та ящиків з ІзОД.

Ключі від ресторану, та ключи від ящиків з ІзОД не повинні залишатися на території ресторану без нагляду.

Обмежений доступ: Зовнішні відвідувачі та сторонні особи не повинні мати доступу до робочих місць та документів з конфіденційною інформацією без дозволу чи супроводу відповідального менеджера або директора.

Неприйнятно занотовування та запис на папері, дошці або ЕОЗ логінів та паролів.

Навчання співробітників: Співробітники повинні бути ознайомлені з політикою "чистого столу" та проходити навчання зі збереження конфіденційності інформації та дотримання заходів безпеки. Співробітники повині чітко визначати свої права та обов’язки, відпрошуватись на 5хв, обід,

йдучи додому, у головного менеджера зміни, співробітники не мать права виходити на зміну раніше ніж вказано в у графіку. Менеджер повинен контролювати знаходження співробітників у не робочий час (5хв, обід, йдучи додому). Менеджер повинен контролювати поводження співробітників з обладненням та правилами безпеки.

Перевірка електроно обчислювальних засобів: Кожен менеджер та директор повинен перед початком роботи з електронообчислювальними засобами переконатися у правельній роботі ЕОЗ. Через засоби профілю захищеності у розділі 2.8 «НТ-2». Менеджер може перевіряти такі ЕОЗ – компьютери, ноутбуки, телефони, планшети. Для перевірки інших пристроїв таких як POS – термінали, POS – моноблоки, POS – термінали самообслуговування менеджер повинен давати завдання системним адміністраторам.

Впровадження політики "чистого столу" допоможе знизити ризик витоку конфіденційної інформації, допоможе запобігти несанкціонованому доступу та допоможе підтримувати безпеку робочого середовища. Вона є важливим складником політики інформаційної безпеки організації.

Працівники ресторану, що порушать данні правила безпеки повинні бути покарані шляхом дисциплінарного висловлювання та покарання шляхом виплати штрафу або звільнення, в залежності від наслідків для кампанії.

2.8.2 Розробка політики встановлення систем сигналізації

Встановлення систем сигналізації на підприємствах відіграє важливу роль у забезпеченні безпеки та захисту від різних загроз. Ці системи призначені для виявлення, сигналізації та реагування на можливі проблеми, такі як пожежі, проникнення, аварії та інші надзвичайні ситуації.

Для компанії ТОВ "Тесі Фуд" необхідна стема охоронної сигналізації, вона допоможе захистити підприємство від несанкціонованого проникнення та вторгнення на територію. Вона може включати датчики руху, магнітні контакти на дверях і вікнах, відеокамери та інші пристрої, які виявляють

підозрілу активність і миттєво активують сигнали тривоги.

Для підключення такої системи необхідно встановити

Датчики руху: Це пристрої, які виявляють рух у певних зонах чи приміщеннях. Вони можуть бути встановлені на стінах, стелі або підлозі і реагувати на зміни в інфрачервоному випромінюванні або інших фізичних параметрах, що вказують на присутність людини.

Магнітні контакти: Ці пристрої встановлюються на дверях та вікнах та реагують на їх відкриття або закриття. Коли контакт розмикається або замикається, сигналізація активується.

Відеокамери: Охоронна сигналізація може включати систему відеоспостереження з камерами, які записують те, що відбувається на підприємстві. Відеозаписи можуть використовуватися для ідентифікації порушників або як докази у разі інциденту.

Сенсори на вікна та двері: Це спеціальні пристрої, які можуть виявляти спроби зламування або форсування дверей та вікон. Вони можуть реагувати на зміну тиску, вібрації або інших параметрів та активувати сигнал тривоги.

Клавіатури та пульти керування: Система охоронної сигналізації зазвичай має клавіатуру або пульт керування, за допомогою яких персонал може активувати або деактивувати сигналізацію, а також керувати її параметрами.

Сигнальні пристрої: Коли система охоронної сигналізації виявляє підозрілу активність, вона активує сигнали тривоги. Це можуть бути звукові сирени, світлові сигнали або навіть автоматичні дзвінки на службу охорони.

Всі ці компоненти працюють разом, щоб забезпечити захист підприємства від різних загроз та виявити можливі інциденти. Охоронна сигналізація може бути підключена до системи моніторингу або охоронної служби, які можуть негайно реагувати на активацію сигналу тривоги та вживати відповідних заходів для запобігання загрозі або виклику правоохоронних органів.

Також додатково можна встановити моніторинг навколишнього середовища, деякі системи сигналізації можуть включати датчики навколишнього середовища, які моніторять параметри, такі як рівень газу, витоку води, температура і вологість. У разі виникнення аномалій ці системи можуть активувати сигнали тривоги, щоб оперативно реагувати на потенційні небезпеки.

2.8.3 Політика антивірусного захисту

Антивірусний захист є важливим компонентом загальної політики безпеки інформації та служить для виявлення, запобігання та видалення шкідливих програм, таких як віруси, черв'яки, троянські програми, шпигунське програмне забезпечення та інші загрози, які можуть завдати шкоди комп'ютерним системам та даним організації. Встановлення антивірусного ПЗ допомогає виявляти шкідливі програми забезпечення. Анивірусна програма сканує файли та систему щодо наявності вірусів та інших шкідливих програм. Воно виявляє та ідентифікує загрози, які можуть бути непомітними для звичайного користувача. Антивірусний захист блокує спроби впровадження шкідливих програм на комп'ютер або мережу. Вона може запобігти завантаженню, виконанню або розповсюдженню шкідливого коду, захищаючи систему від інфікування. Допомогає видаляти та знешкодувати загрози, якщо шкідлива програма виявлена, антивірусний захист надає можливість видалити або знешкодити загрозу, щоб запобігти її подальшому поширенню та пошкодженню системи. Забезпечує захист конфіденційності та цілісності даних. Віруси та інші шкідливі програми можуть призвести до витоку конфіденційної інформації, пошкодження файлів або порушення цілісності даних. Антивірусний захист допомагає запобігти таким інцидентам і забезпечує збереження та недоторканність даних. Антивірусне програмне забезпечення постійно моніторує нові загрози та оновлюється з метою розпізнавання та боротьби з останніми вірусами та шкідливим ПЗ. Це забезпечує актуальний захист від нових та еволюціонуючих загроз. Антивірусний захист є важливим складником

загальної стратегії інформаційної безпеки організації. Вона допомагає запобігти втраті даних, пошкодженню систем та перериванню бізнес-процесів, забезпечуючи надійний захист від шкідливих програм та знижуючи ризики для інформаційної інфраструктури.

Данна політика визначає вимоги до встановлення антивірусного програмного забезпечення на всіх комп'ютерах та серверах організації. Вона також пропонує регулярні оновлення та перевірки наявності останніх версій антивірусних баз даних. За допомогою політики АЗ ми зможемо сканувати файли та пошту. Політика може визначити розклад та параметри сканування файлів та пошти для виявлення шкідливого програмного забезпечення. Це може включати автоматичне сканування під час доступу до файлів або отримання пошти, а також регулярні заплановані сканування всієї системи. Політика визначає процедури обробки виявлених шкідливих файлів. Це може включати переміщення підозрілих файлів до карантину, блокування доступу до них та їх подальше видалення або додатковий аналіз, може наказувати регулярне оновлення операційних систем, програмного забезпечення та патчів безпеки для запобігання відомим уразливості, які можуть бути використані шкідливим програмним забезпеченням.

Для правильного функціонування політики АЗ потрібно включати вимоги щодо навчання користувачів у сфері безпеки та поінформованості про загрози, пов'язані зі шкідливим програмним забезпеченням. Це може включати інформування про правила використання електронної пошти, Інтернету, завантаження файлів тощо. Треба визначити вимоги до регулярного аналізу журналів антивірусного програмного забезпечення та створення звітів про виявлені загрози та вжиті заходи щодо їх усунення.

Політика вимагає встановіть відповідальних осіб, які відповідатимуть за розробку, впровадження та підтримку політики антивірусного захисту. Це можуть бути представники ІТ-відділу, інформаційної безпеки чи інших відділів, відповідальних за безпеку інформації. Потрібно регулярно оглядати та оновлювати політику антивірусного захисту відповідно до ризиків та

вимог, що змінюються. Це допоможе підтримувати актуальність та ефективність політики у довгостроковій перспективі.

Важливо відзначити, що розробка політики антивірусного захисту має бути індивідуальною, враховуючи її специфічні потреби і ризики.

2.8.4 Політика копіювання данних для їх збереження у разі втрати.

Копіювання важливих даних є важливою практикою в галузі інформаційної безпеки. Забезпечення резервного копіювання дозволяє створити та зберігати резервні копії, які можуть бути використані у разі втрати, пошкодження або видалення вихідних даних. Резервні копії служать для відновлення даних та мінімізації простою бізнес-процесів у разі збоїв або надзвичайних ситуацій. Копіювання даних допоможе запобігти втраті інформації у разі апаратних збоїв, програмних помилок, атак хакерів, стихійних лих та інших непередбачених подій. Відновлення даних із резервних копій дозволить мінімізувати втрати та відновити працездатність системи. Багато галузевих стандартів та регуляторних норм вимагають створення та зберігання резервних копій даних для забезпечення безпеки та збереження інформації. Копіювання даних дозволить організації відповідати таким вимогам та мінімізувати можливі штрафи чи наслідки невиконання нормативних вимог.

Існує кілька методів резервного копіювання, включаючи повне, інкрементне та диференційне копіювання. Повне копіювання включає копіювання всіх даних, інкрементне копіювання зберігає лише змінені дані з моменту останнього повного або інкрементного копіювання, а диференціальне копіювання зберігає лише змінені дані з моменту останнього повного копіювання. Вибір методу залежить від вимог щодо часу відновлення та використання сховища. Для ефективного резервного копіювання визначємо щоденну регулярність процедури.

Резервні копії даних повинні зберігатися у надійному та захищеному сховищі. Це може бути сховище хмар. Важливо забезпечити фізичну та

логічну безпеку сховища для запобігання несанкціонованому доступу та пошкодженню даних. Вводимо регулярне тестування та перевірку резервних копій. Це дозволить переконатися в цілісності та доступності резервних копій, а також у можливості успішного відновлення даних за потреби.

Створення хмарного резервного копіювання даних надасть організації зручний та надійний спосіб збереження та відновлення даних. Хмарне резервне копіювання ґрунтується на використанні віддалених серверів зберігання даних, що надаються хмарними провайдерами. Хмарне резервне копіювання даних забезпечує високу доступність та надійність зберігання інформації, а також спрощує процес резервного копіювання та відновлення даних для організацій.

Висновок:

У другому розділі кваліфікаційної роботи було обстежено середовище ресторaного господарства на базі ОІД, а саме:

— Був проведений аналіз політик та процедур інформаційної безпеки;

— Була проведнен оцінка технічних засобів захисту;

— Перевірка доступу та управління правами;

— Аудит системи безпеки;

— Було побудовану модель порушника та модель загроз;

Роздивившись модель порушника та модель загроз було прийнято рішення розробити наступні заходи захисту:

— Розробка політики «читого столу»

— Встановлення систем сигналзації

— Встановлення антивірусного програмного забезпечення

— Політика копіювання даних для іх збереження

# 3 ЕКОНОМІЧНА ЧАСТИНА

## 3.1 Підстави для витрат пов'язаних із впровадженням політики безпеки

Політика безпеки інформації дозволяє запобігти і знизити загрози інформаційній безпеці, такі як кібератаки, витоку даних, порушення конфіденційності. Інвестиції в політику безпеки допомагають попередити потенційні збитки та ризики, пов'язані з порушенням безпеки. Наша мета полягає у визначені економіної єфективності, що були отримані в ході виконання роботи.

Економічна доцільніть - це оцінка, наскільки раціональні та виправдані витрати ресурсів з погляду економічних показників та очікуваних вигод. При аналізі економічної доцільності оцінюються витрати, вигоди та ризики, пов'язані з реалізацією проекту чи прийняттям певного рішення.

Можемо визначити економічну доцільність за допомогою розрахунків:

— Розроблені елементи безпекової політики вимагають значних капітальних витрат.

— Експлуатаційні витрати.

— Економічний ефект від впровадження інформаційної безпекової політики, який буде досягнутий протягом року.

Капітальні витрати

Реалізація запропонованих елементів політики безпеки потребує фінансових вкладень. Можемо віднести сюди:

— Розробка політики «читого столу»

— Встановлення систем сигналзації

— Встановлення антивірусного програмного забезпечення

Політика копіювання даних для іх збереження

## 3.2 Розрахунок витрат на створення політики безпеки інформації.

Розрахунок тривалості створення політики безпеки будемо визначати за формолую:

$$t = t_{\text{ТЗ}} + t_{\text{В}} + t_{\text{А}} + t_{\text{ВЗ}} + t_{\text{ОЗБ}} + t_{\text{ОВР}} + t_{\text{д}}, \text{ годин} \quad (3.1)$$

Де $t_{\text{ТЗ}}$ – час складання технічного завдання на розробку політики безпеки, становить 16 годин;

$t_{\text{В}}$ – час розробки копетенції політики безпеки у організації становить 10 годин;

$t_{\text{А}}$ – затрачений час на аналіз ризиків, становить – 6 годин;

$t_{\text{ВЗ}}$ – час затрачений на визначення вимог до заходів, методів та засобів захисту, становить 5 годин;

$t_{\text{ОЗБ}}$ – час на вибір основних рішень з забезпечення безпеки інформації, становить 4 години;

$t_{\text{ОВР}}$ – час на виконання організацією відновлювальних робіт і забезпечення постійного функціонування організації, становить 8 годин;

$t_{\text{Д}}$ – час на оформлення документів політики безпеки, становить 6 годин;

$$t = 16\text{год} + 10\text{год} + 6\text{год} + 5\text{год} + 4\text{год} + 8\text{год} + 6\text{год} = 55\text{годин}$$

Фінансовий розрахунок витрат на створення ситеми політики безпеки інформації

Розрахувати витрати на створення системи політики безпеки можемо через затрати на розробку безпеки інформації $K_{\text{РП}}$ на якій витрачаємо кошти на заробітну плату для спеціаліста інформаційної безпеки $З_{\text{ЗП}}$ та затрати на розрахунок витрат машиного часу, $З_{\text{Мч}}$ для розрахування використаємо формулу 3.2:

$$K_{\text{РП}} = З_{\text{ЗП}} + З_{\text{Мч}}, \text{грн} \quad (3.2)$$

Заробітна плата для працівника складається з основної та додаткової заробітних плат, також входить різні соціальні потреби: пенсійний фонд, соціальне страхування, страхування на випадок безробіття, і таке інше. Визначити можемо завдяки формулі 3.3:

$$З_{ЗП} = t * З_{ІБ}, грн \quad (3.3)$$

Де t – тривалість розробки політики безпеки загалом, грн;

$З_{ІБ}$ – повна середня заробітна плата за годину спеціаліста з інформаційної безпеки з премією , грн\год.

$$З_{ЗП} = 55 * 170 = 9350$$

Щоб розрахувати вартість машиного часу для розробки політики безпеки інформації необхідно примінити формулу 3.4

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

Де t – витрати праці компьютером за годину на розробку політики безпеки.;

$С_{Мч}$ – становить витрати машиного часу компьтера на одну годину, грн/годину.

Для того щоб розрахувати витрати машиного часу компьтера на одну годину, нам потрібно примінити формулу 3.5:

$$С_{Мч} = P * t_{нал} * C_e + \left(F_{зал} * \frac{Н_А}{Ф_Р}\right) + \left(К_{лпз} * \frac{Н_А}{Ф_Р}\right), грн \quad (3.5)$$

Де Р – встановлена потужність компьютера, кВт; (0,6)

$T_{нал}$ – кількість використаних компьютерів під час написання політики безпеки; (2)

$C_e$ – тариф на використання електричної енергії, грн/кВт годин; (2,64грн)

$F_{ЗАЛ}$ – остаточна ціна компьютера на поточний рік/грн; 25700

$Н_А$ – річна норма амортезації компьютера, частки одиниці;

$Н_{АПЗ}$ – річні витрати на амортизацію ліцензованого програмного забезпечення, частки одиниці;

$К_{ЛПЗ}$ - ціна на ліцензійне програмне забезпечення, грн;

$\Phi_р$ – фонд робочого часу за рік (за 40-годинного робочого тижня $\Phi_Р = 1980$

Розрахуємо:

$$С_{МЧ} = 0,6 * 3 * 2,64 + \left(25700 * \frac{0,5}{1980}\right) + \left(6000 * \frac{0,5}{1980}\right) = 12,42грн$$

$$З_{МЧ} = t * C_{МЧ} = 55 * 12,42 = 688,6грн$$

3.3 Капітальні затрати

Для того щоб розрахувати капітальні затрати потрібна формула 3.6:

$$K = K_{ПР} + K_{ЗПЗ} + K_{РП} + K_{АЗ+}K_{НАВ} + K_{Н} \qquad (3.6)$$

Де $K_{ПР}$ – розробка вартості проєкту інформаційної безпеки та допомога з боку зовнішніх служб безпеки тис.грн. НЕ будемо враховувати данний показник так як стороню організацію по безпеці ми не найймали;

$K_{ЗПЗ}$ – розрахунок вартості покупки основного та за потреби додаткового ліцензійного програмного забезпечення, коштує 166 983грн

Таблиця 3.1 Розрахунок вартості програмного заюезпечення

| Назва програмного забезпечення | Кількість одиниць | Загальна вартість |
|---|---|---|
| Windows 10 Pro | 23 | 138 000 |
| ESET | 23 | 23 115 |
| DeviseLock | 3 | 5 868 |
| Всього | | 166 983грн |

$K_{РП}$ – послуги спеціаліста інформаційної безпеки для створення політики ІБ коштує 12 800грн;

$K_{АЗ}$ – затрати на основне та допоміжне апаратне забезпечення; Камери відеоспостереження Reolink RLK16-800B8 комплект з 8шт = 34209грн; Сейф УХЛ-Маш СН-65/1 = 6300грн; Мережеве сховище без HDD QNAP TS-873A-8G = 53119; Комплект охоронної сигналізації Ajax StarterKit Cam = 12700грн;

$K_{НАВ}$ – загальні витрати на навчання спеціалістів та системних адміністраторів, тис грн. Витрати на навчання системного адміністратора становлять 3100грн

$К_Н$ – витрати, пов'язані із встановленням обладнання та впровадженням системи інформаційної безпеки, 8000грн.

$$К_{ЗПЗ} = 6000 * 23 = 138\,000грн$$

$$К_{РП} = З_{ЗП} + З_{МЧ} = 9350 + 688{,}6 = 10038{,}6грн$$

$$К = 166983 + 12800 + 106328 + 3100 + 8000 = 297\,211грн$$

3.4 Розрахунок поточних витрат на ІБ

Для того щоб розрахувати витрати на функціонування системи ІБ за рік нам потрібна формула 3.7:

$$С = С_В + С_К + С_{АК}, тис.грн \qquad (3.7)$$

Де $С_В$ – витрати на оновлення систем інформаційної безпеки; в нашому випадку оновлення не потребується;

$С_{АК}$ – Витрати які викликані користувачами інформаційної безпеки; таких витрат немає;

$С_К$ – витрати напрвлені на керування інформаційною безпекою, для того щоб іх прорахувати нам потрібна формула 3.8:

$$С_К = С_Н + С_А + С_З + С_{ЄВ} + С_{ЕЛ} + С_О + С_{ТОС} \qquad (3.8)$$

Де $С_Н$ – Витрати на навчання адміністраторів та звичайних користувачів, становить 3000грн

$С_А$ - Річний обсяг амортизаційних відрахувань, виражених у відсотках від загальної суми капітальних інвестицій за різними видами основних фондів та нематеріальних активів програмного забезпечення. У ресторані експлуатується 11 POS – моноблоків загальною вартістю 330 000грн, 5 POS – терміналів загальною вартістю 200 000грн, 4 POS – терміналів самообслуговування загальною вартістю 400 000грн, 1 компьютер загальною вартістю 30 000грн, 2 ноутбуки загальною вартістю 52 000. Вартість програмного забезпечення всього обладнення коштує 166 983грн.

Загалом - 1 178 983грн. Мінімальний термін амортизації обладнення 2 роки.

Ліквідаційна вартість 11 POS – моноблоків загальною вартістю 55 000грн, 5 POS – терміналів загальною вартістю 25 000грн, 4 POS – терміналів самообслуговування загальною вартістю 120 000грн, 1 компьютер загальною вартістю 6 000грн, 2 ноутбуки загальною вартістю 20 000. Вартість програмного забезпечення всього обладнення коштує 13 000грн.

Загалом – 239 000грн

$$C_{\text{А}} = \frac{1\,178\,983 - 239\,000}{2} = 469\,991{,}5\text{грн}$$

$C_{\text{З}}$ – Заробітну плату інженерно-технічного персоналу, відповідального за обслуговування системи розрахуємо по наступній формулі 3.9:

$$C_{\text{З}} = \text{З}_{\text{ОСН}} + \text{З}_{\text{ДОД}}, \text{грн} \qquad (3.9)$$

Де, $\text{З}_{\text{ОСН}}$ – основна заробітна плата системного адміністратора 20000грн на місяць, 240 000грн на рік.

$\text{З}_{\text{ДОД}}$ – Премія системного адміністратора складає 5000грн на місяць, 60 000 на рік відповідно. У 2023 році основний податок ЄСВ складає 22%. Порахуємо:

$$\text{С}_{\text{ЄВ}} = 300000 * 22\% = 66000$$

$$C_{\text{З}} = 240000 + 60000 + 66000 = 366\,000\text{грн}$$

$\text{С}_{\text{ЕЛ}}$ – розрахунок вартості електроєнергії за рік яку споживає апартна складова інформаційної безпеки:

$$C_{\text{ЕЛ}} = P * F_P * \text{Ц}_{\text{Е}}, \text{грн} \qquad (3.10)$$

Де Р – Потужність апаратури інформаційної безпеки. 0,4 для одного технічного засобу, для всіх ТЗ маємо 9,2кВт;

$F_P$ – робочий час систем інформаційної безпеки на рік має 12 місяців*30 робочих діб/міс*15 робочих годин * 23 робочих технічних пристроїв = 124 200;

$\text{Ц}_{\text{Е}}$ – тариф на електроенергію, 2,64грн/кВт годину.

$$C_{ЕЛ} = 9{,}2 * 124\,200 * 2{,}64 = 3\,016\,569{,}6грн$$

$C_О$ – Це витрати на залучення зовнішніх організацій до виконання певних видів обслуговування та сертифікації персоналу, витрати на які несе підприємство.

Не будемо враховувати данний фактор так як залучення зовнішніх організацій нам не потрібно;

$C_{ТОС}$ - Витрати на технічне та організаційне адміністрування та обслуговування системи інформаційної безпеки визначаються на основі даних організації або у відсотковому співвідношенні від вартості капітальних витрат. Це становить 1% від загальної суми капітальних інвестицій, що становить 2972,11грн.

$$C_К = 3000 + 469\,991{,}5 + 366\,000 + 66\,000 + 3\,016\,569{,}6 + 2972{,}11 = 3\,924\,533{,}21грн$$

Тепер на основі всіх потрібних даних вирахуємо затрати на рік:

$$C = 3\,924\,533{,}21$$

3.5 Оцінка величини збиту

Таблиця 3.2 – Місячна заробітна плата працівників.

| Посада | Місяна заробітна плата |
|---|---|
| Директор | 39 060грн |
| Заступник директора | 2*25 752грн |
| Менеджер ресторану | 5*19 413грн |
| Молодший менеджер | 2*14 300грн |
| Інструктор з виробничого навчання | 5*13 235,2грн |
| Члене бригади | 15*12 900,8грн |
| Клінінг | 2*11 899,36грн |
| Всього | 499 714,12грн |

Втрати, пов'язані із зменшенням продуктивності співробітників атакованої системи мережі, є збитками, пов'язані з простоєм їх роботи під час атаки, що призводить до втраченя їх заробітної плати. ($П_П$)

Атакований вузол або сигмент становить упущену вигоду від простою, для того щоб розрахувати використаємо формулу (3.11)

$$U = \text{П}_\text{П} + \text{П}_\text{В} + \text{В} \qquad (3.11)$$

Де $\text{П}_\text{П}$ – оплата за робочий час, за період простою працівників, внаслідок націленої атаки на вузол або сигмент у корпоративній мережі, 13880,94 грн;

$\text{П}_\text{В}$ – ціна за відновлення вузла або сигмента мережі, грн;

В – Витрати на обсяг продажів за час простою при атаці на корпоративний вузол або сигмент, грн;

На місяць виділяється 180 годин робочого часу на одного працівника, час простою внаслідок атаки 5 годинє

$$\text{П}_\text{П} = (\frac{\text{З}_\text{С}}{\text{Ф}}) * t_A, \text{грн} \qquad (3.12)$$

Де $\text{З}_\text{С}$ – загальний обсяг витрат на заробітну плату співробітників за один місяць;

Ф – Місячний фонд робочого часу;

$t_A$ – час простою після атаки;

Враховуючи всі данні:

$$\text{П}_\text{П} = \left(\frac{499\,714{,}12}{180}\right) * 5 = 13880{,}94\text{грн}$$

Для того щоб розрахувати витрати на відновлення працездатності, ($\text{П}_\text{В}$) нам потрібно врахувати декілька показнтків:

$\text{П}_\text{ВИ}$ – витрати на заново ведені дані, грн;

$\text{П}_\text{ПВ}$ – витрати на повне відновлення системи, грн;

$\text{П}_\text{Зч}$ – ціна на заміну та встановлення нових частин замість зламаних, грн;

Розрахуємо витрати на заново ведені дані до системи:

$$\text{П}_\text{ВИ} = \left(\frac{\text{З}_\text{С}}{\text{Ф}}\right) * t_\text{ВИ}, \text{грн} \qquad (3{,}13)$$

Де $З_С$ – загальний обсяг витрат на заробітну плату співробітників за один місяць;

Ф – Місячний фонд робочого часу;

$t_{ВИ}$ – час затрачений на відновлення системи обслуговучим персоналом мережі;

$$П_{ВИ} = \left(\frac{499\ 714{,}12}{180}\right) * 8 = 22\ 209{,}51 грн$$

Розрахуємо витрати на відновлення ($П_{ПВ}$):

$$П_{ПВ} = \left(\frac{З_С}{Ф}\right) * t_В, грн$$

Де $З_С$ – місячна заробітна плата системного адміністратора;

Ф – Місячний фонд робочого часу;

$t_{ВИ}$ – час затрачений на відновлення системи обслуговучим персоналом мережі;

$$П_{ПВ} = \left(\frac{25000}{180}\right) * 8 = 1111{,}11, грн$$

$П_{Зч}$ – ціна на заміну та встановлення нових частин замість зламаних становить 2000грн;

$$П_В = П_{ВИ} + П_{ПВ} + П_{Зч,}, грн \qquad (3.15)$$

$$П_В = 22\ 209{,}51 + 1111{,}11 + 2000 = 25320{,}11$$

Прорахуємо витрати через зниження працездатності системи на яку була створена атака:

$$В = \left(\frac{О}{F_Р}\right)(t_П + t_В + t_{ВИ}) \qquad (3.16)$$

Де, О – сума продажів сегмента корпоративної системи після атаки на неї, рахуємо за рік 4 996 800грн;

$F_Р$ – Фонд робочого часу роботи організації за рік 5400 годин;

$t_{П}$ – простій внаслідок атаки 5 годин

$t_{В}$ – відновлення системи після атаки 8годин

$t_{ВИ}$ – встановлення інформації яка була втрачена 12 годин

$$В = \left(\frac{4\ 996\ 800}{5400}\right) * (5 + 8 + 12) = 23\ 133{,}25грн$$

Склавши усі необхідні данні можемо розрахувати втрачену можливість отримати прибуток через атаку на информаційно телекомунікаційну систему організації:

$$U = 13\ 880{,}94 + 25\ 320{,}11 + 23\ 133{,}25 = 62\ 334{,}3грн$$

Тепер можемо прорахувати загальний збиток завданний атакою на вузол або сегмент організації:

$$В = \sum i \sum n * U \qquad (3.17$$

Де $\sum i$ – атаковані вузли – 3

$\sum n$ – річний прогноз на кількість атак – 2

Таким чином:

$$В = 3 * 2 * 62\ 334{,}3 = 374\ 005{,}8грн$$

Прорахуємо загальний результат від впровадження системи інформаційної безпеки розраховується з урахуванням потенційних ризиків порушення інформаційної безпеки:

$$Е = В * Р - С \qquad (3.18)$$

Де В - загальний збиток завданний атакою на вузол або сегмент організації 374 005,8грн

Р – імовірність атаки на систему за рік становить 0,5 (так як річний прогноз на атки у нас складає 2, тобто 1 раз на 6 місяців);

С - витрати на функціонування системи ІБ за рік складає 3 924 533,21грн

$$Е = (374\ 005{,}8 * 05) - 3\ 924\ 533{,}21 = 3\ 737\ 530грн$$

3.6 показники економічної ефективності:

За коефіцієнтом повернення інвестицій ROSI можна оцінити, скільки додаткових витрат можна уникнути завдяки впровадженню системи інформаційної безпеки. При оцінці інформаційної безпеки зазвичай розглядають потенційні витрати, пов'язані з атакою на вузол чи корпоративну мережу, а чи не прибуток, яку принесе система інформаційної безпеки.

$$ROSI = \frac{E}{K} \qquad (3.19)$$

Де Е - загальний результат від впровадження системи інформаційної безпеки 3 737 530грн;

К - капітальні затрати 297 211грн;

$$ROSI = \frac{3\ 737\ 530}{297\ 211} = 12{,}57$$

Термін окупності капітальних інвестицій відображає період часу, за який інвестиції окуплятимуться за рахунок загального ефекту, досягнутого завдяки впровадженню системи інформаційної безпеки.

$$Т_О = \frac{К}{Е} = \frac{1}{ROSI}, \text{років} \qquad (3.20)$$

$$Т_О = \frac{1}{12{,}57} = 0{,}080 \text{ року (1місяць)}$$

Висновок:

Під час прорахунку третьої, економічної частини, виходячі з аналізу всіх вище прорахованих затрат на створення та побудування технік забезпечення політики безпеки інформації у організації в якій циркулює інформація з обмеженим доступом, я зміг визначити сумму капітальних затрат на впровадження та побудову систем інформаційної безпеки, для ресторану «KFC» за адресою вул. Князя Володимира 21Б ці витрати склали 297 211 гривень, за прорахунком стандартні експлуатаційні витрати склали 3 924 533,21грн на рік, при тому що збитків може бути завдано на 374 005,8грн, загальний результат від впровадження системи інформаційної безпеки виходить на сумму 3 737 530грн, для ресторану такого масштабу

приблизна окупність капітальних затрат на впровадження системи інформаційної безпеки складе 1 місяц. За результатами моїх підрахунків, можна зрозуміти, що впровадження системи ІБ, для данної кампанії на сьогоднішній час є доцільним.

# ВИСНОВКИ

Після виконання кваліфікаційної роботи мені вдалось розробити та впровадити політику інформаційної безпеки. За весь час роботи по кваліфікаційній роботі було розробленота виявлено:

Темпи росту кіберзлочинності, загальні відомості про кібератаки у світі. Було розглянуто перелік загроз для великих підприємств і закладів ресторанного господарства. Було проаналізовано нормативно – правову базу та основні закони України стосовно інформації. було обстежено середовище ресторного господарства на базі ОІД, а саме:

- Був проведений аналіз політик та процедур інформаційної безпеки;
- Була проведнен оцінка технічних засобів захисту;
- Перевірка доступу та управління правами;
- Аудит системи безпеки;
- Було побудовану модель порушника та модель загроз;

Роздивившись модель порушника та модель загроз було прийнято рішення розробити наступні заходи захисту:

- Розробка політики «читого столу»
- Встановлення систем сигналзації;
- Встановлення антивірусного програмного забезпечення;
- Політика копіювання даних для іх збереження;

Було прораховано загальні затрати на створення та побудування технік забезпечення політики безпеки інформації у організації в якій циркулює інформація з обмеженим доступом, також була проаналізована доцільність створення та впровадження політики безпеки, за результатами данних з економічної частини можна зрозуміти, що впровадження системи ІБ, для данної кампанії на сьогоднішній час є доцільним.

ПЕРЕЛІК ПОСИЛАНЬ


1. Parachute.clod – Електроний ресурс. – режим доступу: https://parachute.cloud/cyber-attack-statistics-data-and-trends/
2. Hackmageddon.com – Електроний ресурс. – https://www.hackmageddon.com/2023/04/21/q1-2023-cyber-attacks-statistics/
3. ESET.ua – Електроний ресурс – https://www.eset.com/ua/home/internet-security/?gclid=Cj0KCQjwnMWkBhDLARIsAHBOftpu8KyEWd_z-7IiCAkuSyloi84Dx9JiY1VrOq9s4BC0LZO4Nc4dn_waAmVoEALw_wcB
4. Microsoft.com – Електроний ресурс – https://www.microsoft.com/uk-ua/
5. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22» - Електроний ресурс – https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi
6. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)» – Електроний ресурс - https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi
7. НД ТЗІ 1.5-002-2012 «Класифікатор засобів технічного захисту інформації, наказ Адміністрації Держспецзв'язку від 29.08.2012 № 472» – Електроний ресурс – https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi
8. НД ТЗІ 1.6-002-2003 «Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації, наказ ДСТСЗІ СБУ від 24.04.2003 № 41 (Зміна № 1, наказ Адміністрації Держспецзв'язку від 03.11.2011 № 93 дск., зміна № 2, наказ Адміністрації Держспецзв'язку від 17.08.2013 № 451)» - Електроний ресурс – https://cip.gov.ua/ua/news/normativni-dokumenti-

sistemi-tzi

9. Закон України про захист інформації в інформаційно-комунікаційних системах – Електроний ресурс – https://zakon.rada.gov.ua/laws/show/2657-12#Text
10. Постанова кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» - Електроний ресурс – https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text

ДОДАТОК А Звіт матеріалів кваліфікаційної роботи

| № | Формат | Найменування | Кількість листів | Примітки |
|---|---|---|---|---|
| 1 | А4 | Реферат | 1 | |
| 2 | А4 | Список умовних скорочень | 1 | |
| 3 | А4 | Зміст | 1 | |
| 4 | А4 | Зміст питання. Встановлення задачі | 20 | |
| 5 | А4 | Спеціальний розділ | 60 | |
| 6 | А4 | Економічна частина | 10 | |
| 7 | А4 | Висновки | 1 | |
| 8 | А4 | Перелік посилань | 2 | |
| 9 | А4 | ДОДАТОК А. Звіт матеріалів кваліфікаційної роботи | 1 | |
| 10 | А4 | ДОДАТОК Б. Перелік документів на оптичному носії | 1 | |
| 11 | А4 | ДОДАТОК В. Відгук керівника кваліфікаційної роботи | 1 | |

ДОДАТОК Б Перелік документів на оптичному носії

Кваліфікаційна робота – Чумак Владислав Іванович 125-19-2.docx

Презинтація – Чумак Владислав Іванович 125-19-2.pptx

Рецензія – Чумак Владислав Іванович 125-19-2.docx

Диск з документами кваліфікаційної роботи – Чумак В.І. 125-19-2

## ДОДАТОК В. Відгук керівника кваліфікаційної роботи

**В І Д Г У К**

**на кваліфікаційну роботу студента групи 125-19-2**
**Чумака Владислава Івановича**

**на тему: «**Політика безпеки інформації інформаційно-комунікаційної системи закладу ресторанного господарства «KFC»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на_____сторінках.

Метою кваліфікаційної роботи є забезпечення деталізованої та актуалізованої ідентифікації інформаційних активів об`єктів захисту.

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; основні відомості про підприємство. Дослідженя інформаційної системи, обстеженя фізичного середовища аналіз організаційно-документаційного забезпечення.

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

За час виконання роботи Чумак 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**

**Керівник спец. розділу**