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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Хуторного Олександра Сергійовича*

академічної групи *125-19ск-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка підсистеми захисту інформації інформаційно-комунікаційної системи ТОВ "Авалон"*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц. Романюк Н.М.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Хуторному Олександру Сергійовичу* **академічної групи** *125-19ск-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка підсистеми захисту інформації інформаційно-комунікаційної системи ТОВ "Авалон"***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 18.05.2022 №268-с

Розділ	Зміст	Термін виконання
Розділ 1	Визначити актуальність питання та провести аналіз об'єкта дослідження, визначити структури підприємства, інформацію що циркулює та оброблюється.	29.03.2022
Розділ 2	Виконати аналіз основних методів захисту інформації, розробити модель порушника та загроз, визначити критерії захисту за профілем захищеності 3.КЦД.1, дослідити систему захисту на недоліки та визначити можливі варіанти їх вирішення.	24.05.2022
Розділ 3	Виконати розрахунок економічного ефекту від впровадження та налагодження комплексів засобів захисту інформації, підрахувати величину економічного ефекту, капітальні витрати, щорічні експлуатаційні витрати та термін окупності.	14.06.2022

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

Дата видачі: 08.01.2022р.

Дата подання до екзаменаційної комісії: 15.06.2022р.

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

РЕФЕРАТ

Пояснювальна записка: 95 с., 19 рис., 29 табл., 4 додатка, 8 джерел.

Об’єкт дослідження: система захисту інформації підприємства ТОВ “Авалон”.

Мета кваліфікаційної роботи: Підвищення рівня захисту інформації підприємства, шляхом модернізації програмного та апаратного захисту, організаційних процесів.

У першому розділі дослідили підприємство, а саме персонал та його обов’язки, робочі станції підприємства, приміщення у якому знаходиться контрольована зона, схема мережі підприємства, інформаційні потоки на підприємстві та огляд програмного забезпечення підприємства.

У другому розділі визначили модель порушника, можливі загрози та ризики для підприємства, опис профілю захищеності 3.КЦД.1, проаналізували основні методи захисту, обирали програмне забезпечення для захисту інформації, обстежили систему захисту на недоліки та реалізували нові методи захисту.

У економічному розділі визначили доцільність розробки нових та вдосконалення вже існуючих засобів захисту інформації, проводимо розрахунок капітальних витрат, річних експлуатаційних витрат на утримання і обслуговування об'єкта, річного економічного ефекту, показників економічної ефективності розробки та впровадження запропонованих рішень.

Практичне значення роботи полягає у дослідженні та покращенні функціонування комплексної системи захисту інформації, за рахунок її оновлення та визначення необхідних доповнень у вже існуючій системі.

ІНФОРМАЦІЙНА БЕЗПЕКА, КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ, МОДЕЛЬ ПОРУШНИКА, МОДЕЛЬ ЗАГРОЗ, ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ.

ABSTRACT

Explanatory note: 95 pp., 19 Fig., 29 Table., 4 Appendix, 8 sources.

Object of research: Comprehensive information protection system of Avalon LLC.

Purpose of qualification work: Improving the level of protection of enterprise information by modernizing software and hardware protection, organizational processes.

The first section examines the enterprise, namely the staff and their responsibilities, the workstations of the enterprise, the premises in which the controlled area is located, the scheme of the enterprise network, information flows in the enterprise and review of enterprise software.

The second section identified the violator's model, possible threats and risks to the enterprise, described the security profile 3.KCD.1, analyzed the main methods of protection, selected software to protect information, examined the protection system for shortcomings and implemented new protection methods.

In the economic section we determined the feasibility of developing new and improving existing means of information protection, we calculate capital costs, annual annual operating costs for maintenance and upkeep, annual economic effect, indicators of economic efficiency of development and implementation of proposed solutions.

The practical significance of the work is to study and improve the functioning of a comprehensive information security system, by updating it and identifying the necessary additions to the existing system.

INFORMATION SECURITY, COMPREHENSIVE INFORMATION PROTECTION SYSTEMS, INFRINGEMENT MODEL, THREAT MODEL, RESTRICTED INFORMATION.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДСТУ – державний стандарт України;

ЕОТ – електронно-обчислювальна техніка;

ІзОД – інформація з обмеженим доступом;

ІТС – інформаційно-телекомунікаційна система

КЗ – контрольована зона;

КЗЗ – комплекс засобів захисту;

КС – комп'ютерна система;

НД – нормативний документ;

НСД – не санкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ОС – операційна система;

ПЕМВН – побічне електро-магнітне випромінювання;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

ПКП – приймально-контролюючий пристрій;

ТЗІ – технічний захист інформації.

ЗМІСТ

ВСТУП

У часи активного розвитку кіберзлочинності, зростає потреба у спеціалістах з захисту інформації, потреба у обладнанні захисту підприємств, контролю доступу, тощо. Самостійно організувати захист підприємства, не маючи освіти у галузі кібербезпеки є складною задачею для охоронних підрозділів підприємств, особливо для малого бізнесу, який не має у складі працівників охорону, це майже неможливо.

Для вирішення цих питань існують люди з освітою у сфері кібербезпеки, які можуть забезпечити безпеку підприємства, установи, тощо. Якщо підприємство не має коштів на постійне працевлаштування спеціаліста з питань кібербезпеки, воно може звернутися до підприємств, які можуть розробити, встановити, обслуговувати вчасно технічні системи захисту інформації, тощо.

Умовою стабільної роботи підприємства є мінімізація ризиків та збитків.

Ризик – це невизначена подія або умова, яка у разі виникнення призводить до певної втрати. У підприємстві це може призвести до втрати грошових коштів, репутації, майна, тощо.

Щоб проаналізувати можливі ризики та збитки необхідно провести аналіз роботи підприємства, його функціонування у робочий та не робочій час, умови праці співробітників, наявність охоронної системи та її надійність.

Результати аналізу можуть сильно відрізнятися від досвідченості аналітика з питань безпеки підприємства. При цьому є різні види та методи досліджень, які можуть займати більше тижня, а інколи й місяця досліджень. Для найбільш оптимального оцінювання необхідно визначити необхідні сфери досліджень, щоб зменшити час дослідження, та переходити до етапу їх мінімізації.

Мінімізація ризиків – це процес модернізації або зміни певного робочого процесу, яка призводить до меншої вірогідності виникнення помилок.

Кожного дня створюються нові методи, принципи, схемі по заволодінню інформацією з обмеженим доступом і проблема кіберзахисту буде розвиватися з кожним роком.

Об’єкт розробки: Комплексна система захисту інформації підприємства ТОВ “Авалон”.

Предмет дослідження: Рівень захисту комплексної системи захисту інформації, її слабкі місця, модернізація системи.

Мета розробки: Підвищення рівня захисту інформації підприємства, шляхом модернізації програмного та апаратного захисту, організаційних процесів.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Актуальність питання

Технології сьогодення дозволяють створювати, зберігати, оброблювати та передавати інформацію без використання переносних носіїв інформації, таких як папер, флеш накопичувачі та тому подібні. Для цих маніпуляцій необхідно мати комп'ютер та підключення до глобальної мережі. На сьогодення важко знайти людину, а тим паче підприємство яке не використовую інформаційні системи для полегшення спілкування, умов праці, виробництва, тощо.

Інформація у будь-яких користувачів буває різною, але якщо ми говоримо про підприємства, державні установи, стратегічні об'єкти, то на них може циркулювати таємна, конфіденційна та службова інформація, яку необхідно берегти від передачі або викрадення третіми особами.

Для захисту інформації можна використовувати технічні, програмні, інженерні та організаційні методи.

Відомо, що будь-яка інформація взагалі може існувати та переноситися у вигляді фізичних полів або речовиною (матеріальним носієм інформації). Наприклад, це може бути акустична хвиля (звук), електромагнітні випромінювання, електричні сигнали, лист паперу з текстом, DVD-диск тощо.

Іншими словами, можна стверджувати, що інформація має циркулювати тільки в електромагнітному (електричному, магнітному), акустичному та матеріальному вигляді.

По фізичній природі носієм інформації можуть бути:

- світло - електромагнітні хвилі оптичного діапазону (у т.ч. інфрачервоного та ультрафіолетового;
- акустичні (звукові) хвилі;
- електромагнітні хвилі;
- електричні сигнали у провідниках;

- матеріальний носій інформації.

Іншої можливості для переносу інформації в природі не існує.

Звідси можна таким чином класифікувати шляхи витоку інформації від джерела до зловмисника (канали витоку) по фізичній природі носія.

Технічні канали витоку інформації:

- візуально-оптичний;
- акустичний;
- електромагнітний;
- електричний;
- матеріальний.

Всі, крім матеріального каналу витоку відносяться до технічних каналів витоку інформації. При цьому, технічні канали витоку інформації можуть бути як природними так й штучними (спеціально створеними зловмисниками).

Відповідно до ДСТУ 3396.2-97 (Захист інформації. Технічний захист інформації. Терміни та визначення):

«Технічний захист інформації (ТЗІ) - діяльність, спрямована на запобігання порушенню цілісності, блокуванню та (чи) витоку інформації технічними каналами».[1]

Закони й нормативні акти виконуються тільки в тому випадку, якщо вони підкріплюються організаторською діяльністю відповідних структур, створюваних у державі, у відомствах, установах і організаціях. При розгляді питання безпеки інформації така діяльність ставиться до організаційних методів захисту інформації.

Організаційні методи захисту інформації включають заходи та дії, які повинні здійснювати посадові особи в процесі створення й експлуатації системи для забезпечення заданого рівня безпеки інформації.

Відповідно до законів і нормативних актів у міністерствах, відомствах, на підприємствах (незалежно від форм власності) для захисту інформації

створюються спеціальні служби безпеки (на практиці вони можуть називатися й інакше). Ці служби підпорядковуються, як правило, керівництву установи.

Керівники служб організують створення й функціонування систем захисту інформації. Повну відповідальність за стан та функціонування інформаційної безпеки несуть керівники організації. На організаційному рівні вирішуються наступні завдання забезпечення безпеки інформації в системи:

- організація робіт з розробки системи захисту інформації;
- обмеження доступу на об'єкт і до ресурсів системи;
- розмежування доступу до ресурсів системи;
- планування заходів;
- розробка документації;
- виховання й навчання обслуговуючого персоналу й користувачів;
- сертифікація засобів захисту інформації;
- ліцензування діяльності по захисту інформації;
- атестація об'єктів захисту;
- удосконалювання системи захисту інформації;
- оцінка ефективності функціонування системи захисту інформації;
- контроль виконання встановлених правил роботи в системи.

Організаційні методи є базисом комплексної системи захисту інформації в системі. Тільки за допомогою цих методів можливе об'єднання на правовій основі технічних, програмних і криптографічних засобів захисту інформації в єдину злагоджену комплексну систему. Конкретні організаційні методи захисту інформації будуть приводитися при розгляді протидії загрозам безпеки інформації. Найбільша увага організаційним заходам приділяється при викладі питань побудови й організації функціонування комплексної системи захисту інформації.

До методів і засобів організаційного захисту інформації відносяться організаційно-технічні й організаційно-правові заходи, які проведені в процесі створення й експлуатації системи для забезпечення захисту інформації. Ці

заходи повинні проводитися при будівництві або ремонті приміщень, у яких буде розміщатися системи; проєктуванні системи, монтажі й налагодженню її технічних і програмних засобів; випробуваннях і перевірці працездатності системи.

Основні властивості методів і засобів організаційного захисту:

- обмеження фізичного доступу до об'єктів захисту та реалізація режимних заходів;
- обмеження можливості перехоплення ПЕМВН;
- розмежування доступу до інформаційних ресурсів і процесам (встановлення правил розмежування доступу, шифрування інформації при її зберіганні і передачі, виявлення та знищення апаратних і програмних закладок);
- резервне копіювання найбільш важливих з точки зору втрати масивів документів;
- перед проведенням наради необхідно проводити візуальний огляд приміщення на предмет виявлення закладних пристроїв;
- кількість осіб, що у конфіденційних переговорах має бути обмежена до мінімуму;
- вхід сторонніх осіб під час проведення наради має бути заборонений;
- повинна бути чітко розроблена охорона виділеного приміщення під час наради, а також спостереження за обстановкою на поверсі ;
- будь-які роботи в кімнаті, що проводяться поза часом проведення конфіденційних нарад, наприклад: прибирання, ремонт побутової техніки, невеликий косметичний ремонт, повинен проводитися в обов'язковій присутності працівника служби безпеки;
- після проведення наради кімната повинна ретельно оглядатися, закриватися і опечатуватися;
- між нарадами кімната повинна бути закрита і опечатана відповідальною особою;
- профілактику зараження комп'ютерними вірусами.[2]

1.2 Аналіз об’єкту дослідження

Об’єктом інформаційної діяльності (ОІД) є будівля в якій знаходиться товариство з обмеженою відповідальністю (ТОВ) «Авалон».

Область діяльності - надання послуг з підбору, встановлення, обслуговування, модернізації, охоронних систем для квартир, будинків, офісів, тощо.

ОІД розташована на четвертому поверсі чотирьох верхового бізнес центру “Хмельницький”, що знаходиться у місті Дніпро, вул. Богдана Хмельницького 4. Бізнес центр має один особистий та один загальний паркінг, свою особисту охорону.

На підприємстві працюють 13 співробітників, які постійно знаходяться у офісному приміщенні та 6 які виконують завдання на об’єктах.

1.2.1 Структура підприємства та особовий склад

Головним на підприємстві є керівник офісу. У його повноваження входить управління відділами підприємства, коригування робочих планів, надання відпусток працівникам, прийняття нового персоналу на роботу, винесення рішень до зміни елементів офісу або підприємства, контроль праці, планів та графіків.

Спеціаліст з питань кібербезпеки підприємства - повинен стежити за безпекою підприємства, встановлювати норми технічних та апаратних частин використовуваних апаратних засобів, які впливають на роботу підприємства, є одним із членів приймальної комісії для співробітників, аналізувати трафік співробітників під час роботи.

Системний адміністратор - повинен стежити за станом обладнання офісу, вчасно його обслуговування, оновлення систем та програмного забезпечення.

Головний бухгалтер - повинен вчасно робити податкові відомості, створювати щомісячні звіти підприємства, визначати заробітну плату відносно

від процентної ставки співробітників, проводить аудити з керівником, щодо зміни цін певних послуг підприємства.

Бухгалтер - приймає плату за замовлення клієнтів, видає кошти на закупівлю розхідних матеріалів, робить звіти за замовленням.

Головний менеджер - слідкує за роботою менеджерів, інформує за нові системи та обладнання, може спілкуватися з клієнтами, створювати план завдання за побажаннями клієнтів.

Менеджер 1 та 2 - шукають нових клієнтів, спілкуються з постійними клієнтами, дистанційно вирішують питання про можливі типи рішення певних збоїв, передають інформацію до голови технічного відділу.

Адвокат - проводить бесіди з клієнтами та особами, які можуть мати претензії, щодо встановлення систем охорони або стеження не певних об'єктах, захищає інтереси компанії та її співробітників, створює договори та угоди між сторонами згідно чинного законодавства.

Голова відділу технічного забезпечення - затверджує проєкти охоронних систем, плани їх модернізації, отримує звіти та плани від керівника офісу, головного бухгалтера та головного менеджера, приймає рішення та доводить його до бригадира, керує проєктувальниками.

Проєктувальник 1 та 2 - створюють проєкти для розміщення об'єктів, мереж охоронних систем, проводять обстеження вже існуючих систем, складають плани за модернізації та обслуговування.

Бригадир - отримує задачі від голови відділу технічного забезпечення, визначає необхідні матеріали та кількість груп для виконання завдання, доводить до відома голову відділу технічного забезпечення, та з його згоди передає інформацію про замовлення бригадам, особисто слідкує за виконанням робот та доповідає про їх стан.

Бригада 1 та 2 - встановлюють, налаштовують та обслуговують охоронні системи та мережі.

Більш детально ознайомитися зі структурою підприємства можна на рисунку 1.1, нижче.

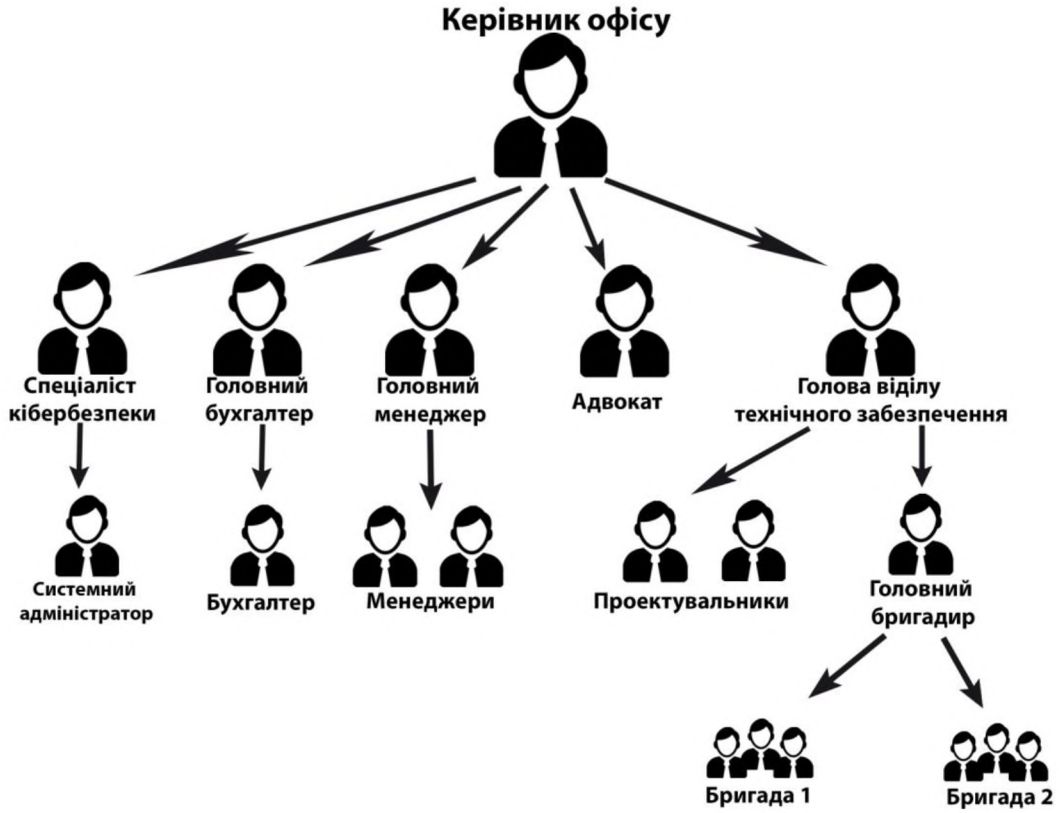

Рисунок 1.1 - Структура підприємства

Несучі стіни зроблені з білої цегли. Перекриття зроблені з використанням залізобетонних плит. Вікна металопластикові. Дах у формі трикутника. Фундамент виконаний з використанням залізобетонних забивних паль.

Будівля має 4 поверхи та 3 окремих входи, перший поверх виділений під магазини, сервісні центри, тощо. На першому поверсі є охоронець, який відповідає за доступ людей до приміщень, та за доступ авто на стоянці. Відокремлений вхід слугує для серверів “Triolan” та їх співробітників, він веде лише до приміщень “Triolan, до іншої частини будівлі неможливо потрапити. З головного входу можна потрапити на будь який поверх через сходи, які розміщені зліва від охорони. Охорона у будинку цілодобова, оскільки вони відповідають за будівлю та автомобілі.

Режим допуску до території будівлі забезпечується таким чином :

- У робочій час вхід до будівлі вільний, охорона спостерігає за безпекою та пересуванням відвідуючи за допомогою відеоспостереження, до паркінгу мають доступ лише автомобілі співробітників;
- У не робочій час будівля є закритою, охорона слідкую за допуском до паркінгу, до будівлі лише за перепустками. Будівля має нічне відеоспостереження, освітлення, сигналізацію, датчики руху.

Режим КЗ забезпечується таким чином:

- У робочий час вхід у приміщення допускається усьому персоналу після відкриванням дверей директором або менеджером підприємства, які мають ключі від вхідних дверей офісу. Клієнти можуть заходити у офіс після обговорення часу зустрічі;
- У не робочий час офіс ставиться під охорону централізованою системою сигналізації з 21:00 вечора до 9:00 ранку та двері зачиняють на 2 циліндричні замки під ключ.

Контрольована Зона (КЗ) - обмежена зовнішніми стінами будівлі, з інших боків внутрішніми стінами(коридором та іншими офісними приміщеннями). Під підлогою знаходяться інші офісні приміщення, зверху дах. Вхідні двері метал\мдф з 2-ома замками(циліндричними) під ключ та датчиком відкриття дверей.

Територія будівлі частково огороджена 2-ух метровим металевим парканом у вигляді грат з різними візерунками, навколо будівлі прокладена асфальтована дорога з місцями для паркування.

До будівлі підведені електро і водопостачання.

Лінії системи опалення проходять під землею до підвалу будівлі, яке потім розмежується вертикально до інших приміщень.

Лінія системи водопостачання (в будівлю заходить металева труба, і після лічильника йде пластикова) і каналізація (ПВХ труби).

Розподільний щит знаходиться у підвалі будинку, також на кожному поверсі встановлена своя окрема щитова, яка іде у щитову кожного офісного приміщення.

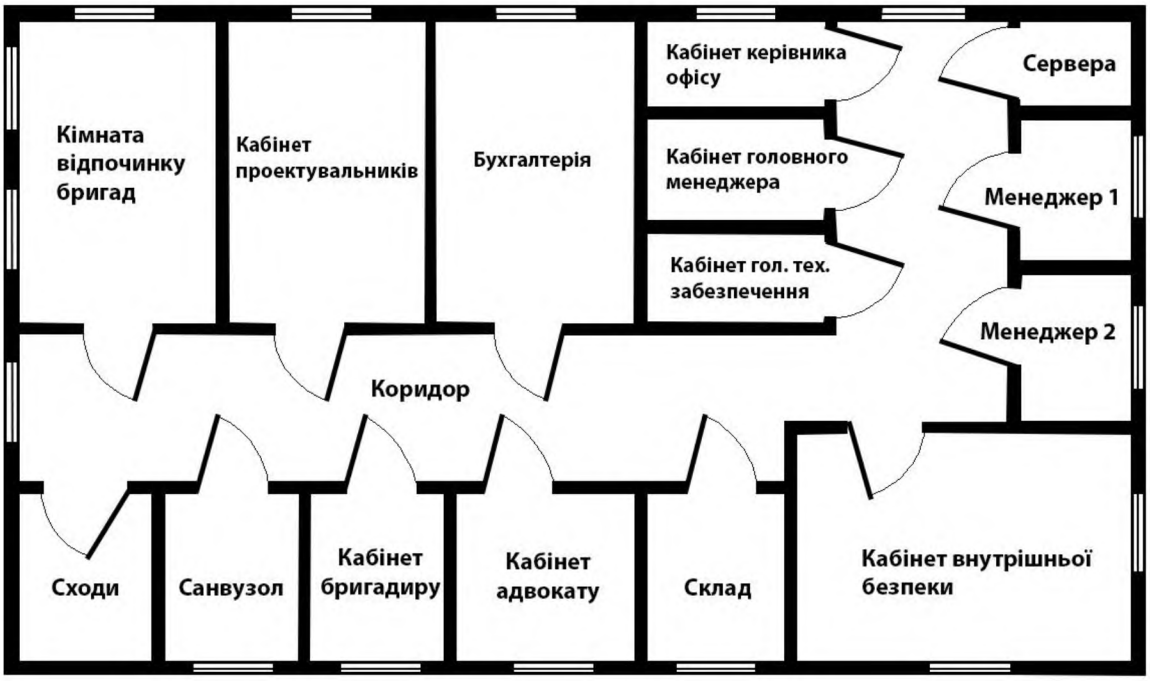

Рисунок 1.2 - План офісу

Лінія системи інтернет провайдера (оптоволоконний кабель) - прокладений в межах КЗ.

Вікна металопластикові, одностворчасті. На кожному вікні встановлені жалюзі.

Елементи системи електропостачання (Розетки) в приміщеннях з заземленням (3 дроту), які підключені до щитової підприємства, який далі підключений до поверхового щита.

Вимикачі системи освітлення одно клавішні, які підключені до щитової підприємства, який далі підключений до поверхового щити.

Лінії системи освітлення зроблене з силових кабелів ВВГ та з'єднуються з стельовими світлодіодними лампами.

Система охоронно-пожежної сигналізації - спроєктована та встановлена силами підприємства, вона підключена до системи охорони і може переглядатися дистанційно.

Система вентиляції, яка проведена до кожного приміщення - приточно-витяжна з кондиціонером, який може як охолоджувати, так і підігрівати повітря в залежності від пори року, він має два режими роботи, замкнутого забору повітря, та відкритого.

Система опалення, яка знаходиться у кожному приміщені - біметалічні радіатори з металопластиковими трубами. Розводка вертикальна яка надходить з підвального приміщення.

Локальна мережа - кручена пара та оптоволокно, яка прокладена в КЗ від щитової провайдеру на першому поверсі і не виходить за його межі.

Рисунок 1.3 - Схема розміщення меблів та обладнання

Рисунок 1.4 - Схема електроживлення та комп’ютерної мережі

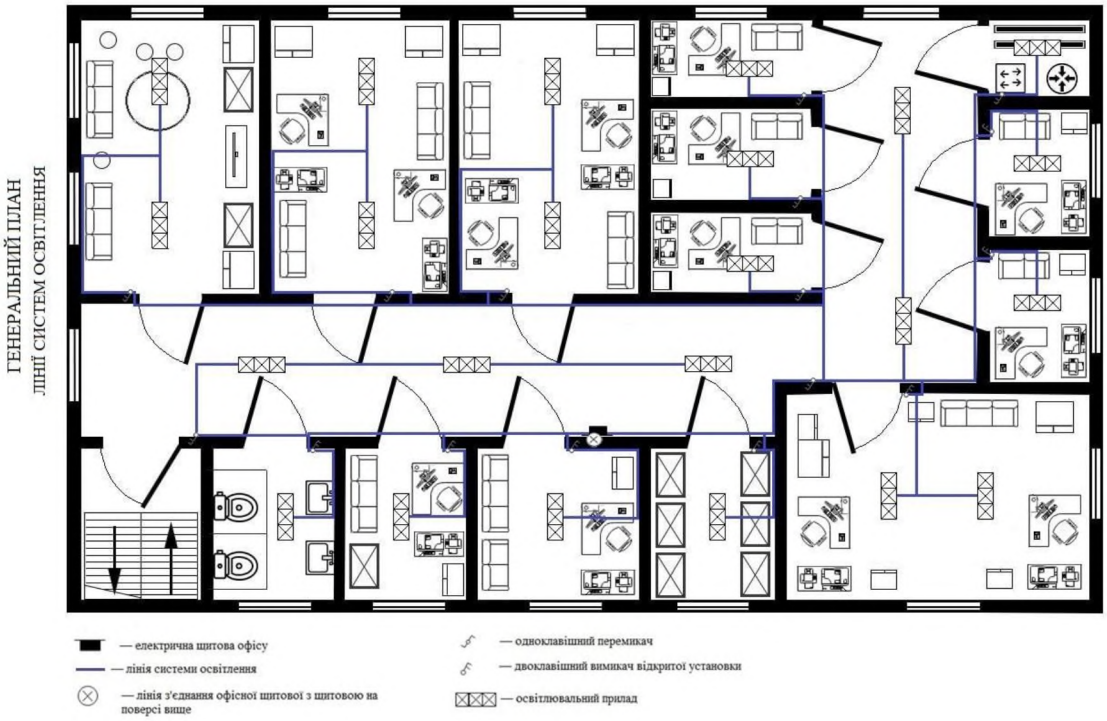

Рисунок 1.5 - Схема ліній системи освітлення

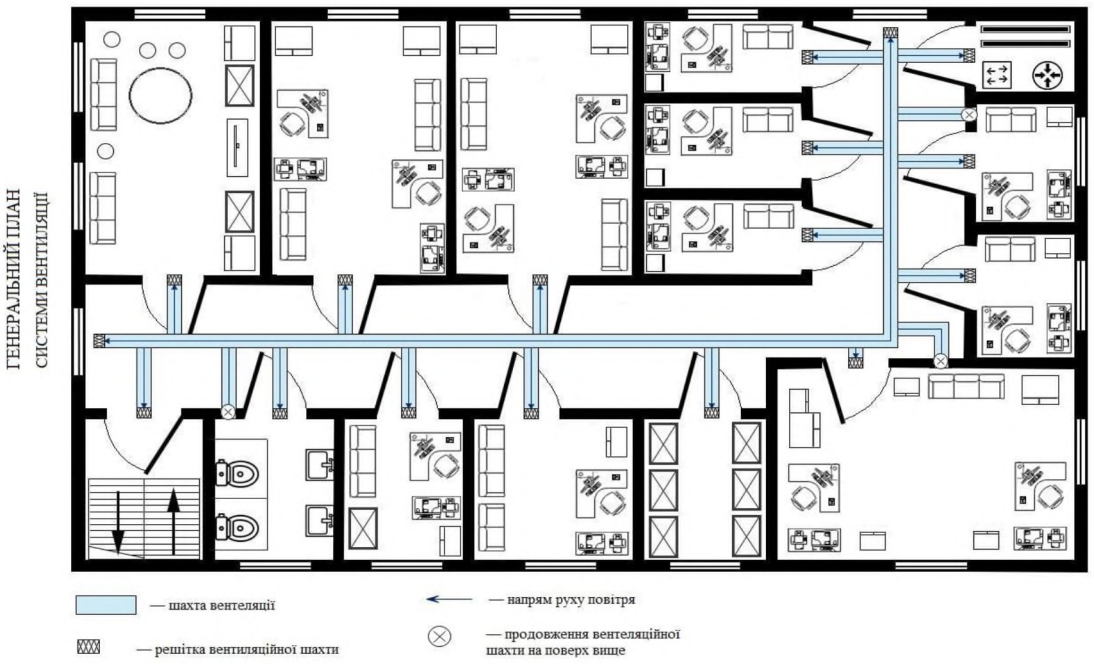

Рисунок 1.6 - Схема системи вентиляції

Рисунок 1.7 - Схема системи опалення та водопостачання

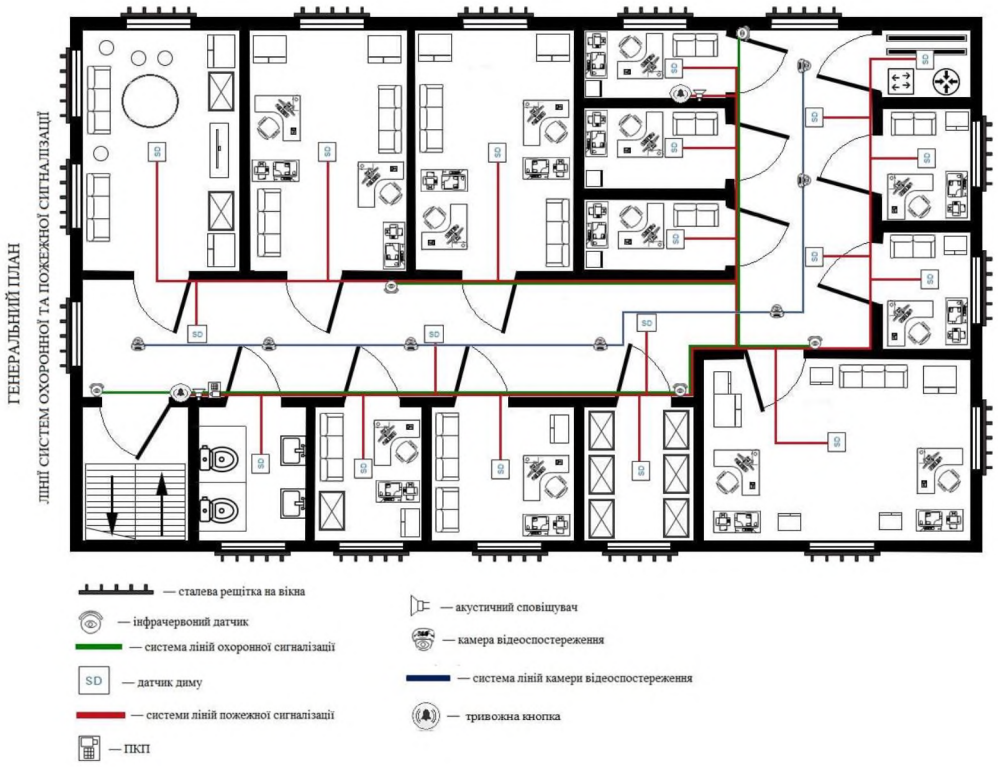

Рисунок 1.8 - Схема системи охорони та пожежної сигналізації

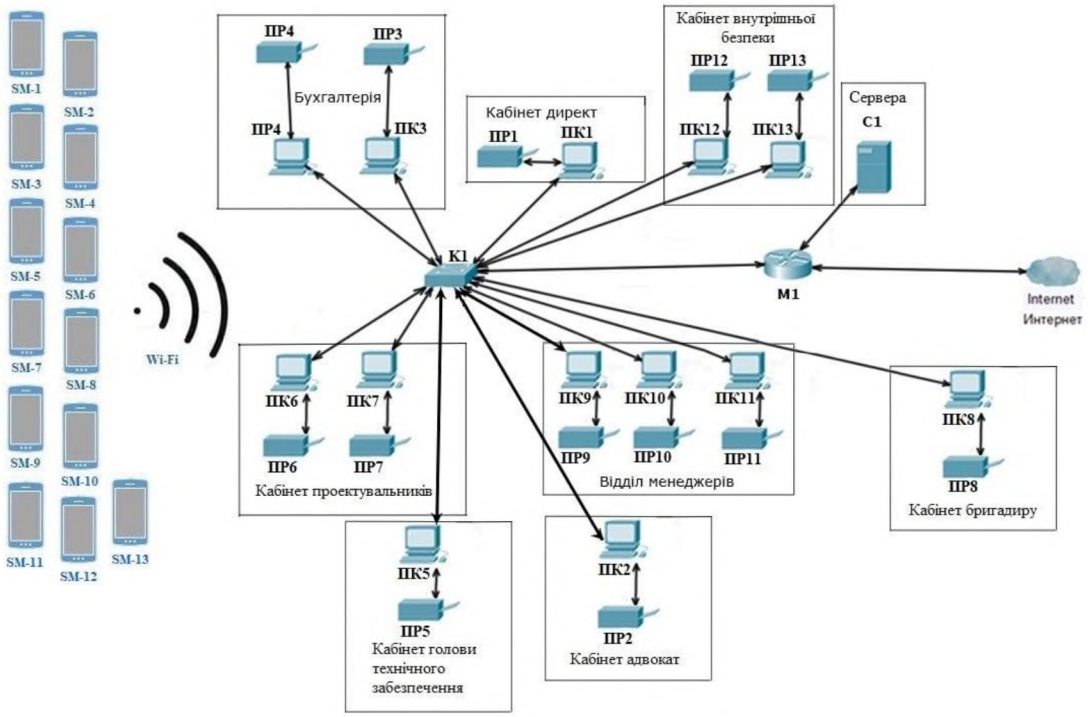

Рисунок 1.9 - Схема ІТС підприємства

На рисунку 1.9 зображено схему мережі підприємства. Інтернет, що надходить з першого поверху окремим кабелем від постачальника послуг “Triolan”, що розміщений у будівлі. Маршрутизатор під’єднаний до інтернету, сервера та комутатора. Комутатор має дротову та бездротову мережу. Через дротову мережу він об’єдную всі робочі станції підприємства, які в свою чергу підключені за топологією “Зірка”.

Таблиця 1.1 - Перелік обладнання підприємства

Назва	Марка	Модель	Серійний номер	Розміщення	Відстань до границі ОІД, м
Ноутбук	Acer	Nitro 5 AN515-55	12001	Кабінет керівника офісу	2м
			12002	Кабінет адвоката	3м
			12003	Кабінет бухгалтерії	7м
			12004	Кабінет бухгалтерії	10м
			12005	Кабінет голови технічного забезпечення	15м
			12006	Кабінет проєктувальників	7м
			12007	Кабінет проєктувальників	10м
			12008	Кабінет бригадиру	4м
			12009	Кабінет головного менеджеру	8м
			12010	Кабінет менеджера1	3м

Продовження таблиці 1.1

Ноутбук	Acer	Nitro 5 AN515-55	12011	Кабінет менеджера2	3м
			12012	Кабінет внутрішньої безпеки	2м
			12013	Кабінет внутрішньої безпеки	3м
Миша	Acer	OMW020 USB Black	12014	Кабінет керівника офісу	2м
			12015	Кабінет адвоката	3м
			12016	Кабінет бухгалтерії	7м
			12017	Кабінет бухгалтерії	10м
			12018	Кабінет голови технічного забезпечення	15м
			12019	Кабінет проєктувальників	7м
			12020	Кабінет проєктувальників	10м
			12021	Кабінет бригадиру	4м
			12022	Кабінет головного менеджеру	8м
			12023	Кабінет менеджера1	3м
			12024	Кабінет менеджера2	3м

Продовження таблиці 1.1

Миша	Acer	OMW020 USB Black	12025	Кабінет внутрішньої безпеки	2м
			12026	Кабінет внутрішньої безпеки	3м
МФУ	HP	Laser135a	12027	Кабінет керівника офісу	2м
			12028	Кабінет адвоката	1м
			12029	Кабінет бухгалтерії	8м
			12030	Кабінет бухгалтерії	8м
			12031	Кабінет голови технічного забезпечення	15м
			12032	Кабінет проєктувальників	8м
			12033	Кабінет проєктувальників	8м
			12034	Кабінет бригадиру	3м
			12035	Кабінет головного менеджеру	8м
			12036	Кабінет менеджера1	1м
			12037	Кабінет менеджера2	1м
			12038	Кабінет внутрішньої безпеки	1м

Продовження таблиці 1.1

МФУ	HP	Laser135a	12039	Кабінет внутрішньої безпеки	1м

На першому поверсі будівлі є сервісний центр з яким співпрацює підприємство. У сервісному центрі відбуваються закупівля фарб для принтерів, за необхідністю обладнання для ремонту ПК, тощо. Для співробітників був обраний варіант придбання однакових ноутбуків, принтерів та маніпуляторів, щоб не створювати відчуття нерівності між ними. Кожен співробітник стежить за станом свого принтера, кількості паперу для нього, при необхідності отримує папер та замінює картридж, після заміни повідомляє про це системного адміністратора. Системний адміністратор в свою чергу сам перезаряджає картриджі для принтерів, робить їх перелік, стежить за наявністю фарби, тощо.

Таблиця 1.2 - Перелік елементів системи безпеки

Назва	Марка	Модель	Серійний номер	Розміщення
ПКП	Satel	Integra 64 Plus	10001	Всередині КЗ біля вхідної двері
Датчик руху	Satel	Slim-PIR	10002	Коридор
			10003	Коридор
			10004	Коридор
			10005	Коридор
			10006	Коридор
			10007	Кабінет адвоката
			10008	Кабінет бригадира
			10009	Бухгалтерія
			10010	Кабінет проєктувальників
			10011	Кімната відпочинку
			10012	Склад
			10013	Кабінет внутрішньої безпеки
			10014	Кабінет менеджера 1
			10015	Кабінет менеджера 2
			10016	Серверна
			10017	Санвузол

Продовження таблиці 1.2

Датчик руху	Satel	Slim-PIR	10018	Кабінет головного менеджера
			10019	Кабінет голови офісу
			10020	Кабінет голови технічного забезпечення
Датчик відкриття дверний	Satel	K-1	10021	Вхідні двері до КЗ
			10022	Двері голови офісу
			10023	Двері головного менеджера
			10024	Двері голови технічного забезпечення
			10025	Двері серверної
			10026	Двері менеджера 1
			10027	Двері менеджера 2
			10028	Двері відділу внутрішньої безпеки
			10029	Двері до складу
			10030	Двері до кімнати відпочинку
			10031	Двері проєктувальників
			10032	Двері бухгалтерії
			10033	Двері кабінету бригадира
			10034	Двері адвоката
			10035	Двері до санвузла
Датчик відкриття віконний	Satel	K-1	10036	Вікно у коридорі
			10037	Вікно у коридорі
			10038	Вікно у кімнаті відпочинку
			10039	Вікно у кімнаті відпочинку
			10040	Вікно у кімнаті відпочинку
			10041	Вікно у санвузлі
			10042	Вікно у кабінеті бригадира
			10043	Вікно у бухгалтерії
			10044	Вікно у кабінеті проєктувальників
			10045	Вікно у кабінеті адвокату
			10046	Вікно на складі
			10047	Вікно в кабінеті внутрішньої безпеки
			10048	Вікно в кабінеті внутрішньої безпеки
			10049	Вікно у кабінеті голови офісу
			10050	Вікно менеджера 1
			10051	Вікно менеджера 2
Датчик диму	Артон	СПД-3	10052	Коридор

Продовження таблиці 1.2

Датчик диму	Артон	СПД-3	10053	Коридор
			10054	Коридор
			10055	Коридор
			10056	Кабінет адвоката
			10057	Кабінет бригадира
			10058	Бухгалтерія
			10059	Кабінет проєктувальників
			10060	Кімната відпочинку
			10061	Склад
			10062	Кабінет внутрішньої безпеки
			10063	Кабінет менеджера 1
			10064	Кабінет менеджера 2
			10065	Серверна
			10066	Кабінет голови технічного забезпечення
			10067	Кабінет головного менеджера
			10068	Кабінет голови офісу
			10069	Санвузол
Клавіатура ПКП	Satel	CA-10 KLCD	10070	Біля ПКП
Сповіщувач звуковий	Satel	SPW-150	10071	Біля ПКП
			10072	Кабінет голови офісу
Тривожна кнопка	Satel	PNK-1	10073	Біля ПКП
			10074	Кабінет голови офісу
Камера відеоспостереження	HDCVI	VSD-U714B1	10075	Коридор
			10076	Коридор
			10077	Коридор
			10078	Коридор
			10079	Коридор
			10080	Коридор
			10081	Коридор

Оскільки підприємство співпрацює з міжнародною компанію Satel та активно поширює її продукцію, в офісі встановлено саме цю систему безпеки, яка була придбана за приємною ціною. Система спроєктована та встановлена за рахунок підприємства та силами працівників.

1.2.2 Інформація підприємства та інформаційні потоки

На підприємстві постійно створюється, обробляється, зберігається інформація, яка в свою чергу необхідна для виконання замовлень підприємства,

розуміння певних аспектів проєктування, тощо. Ця інформація є складовою частиною роботи підприємства, її розголошення або крадіжка може призвести до великих фінансових та репутаційних втрат компанії.

Інформація, що циркулює на підприємстві буває

1. За способом сприйняття - візуальна та звукова.
2. За формою уявлення - текстова, цифрова, графічна, звукова.
3. За призначенням - спеціальна, секретна, особиста.
4. За значенням - актуальна, достовірна, повна, цінна.
5. За істиною - істинна.

На підприємстві циркулює та обробляється така інформація: інформація про клієнтів, плани будівель та рішень щодо встановлення систем безпеки(проєкти), звіти бухгалтерії, документи ціно утворень, звітність о наявності елементів систем безпеки, документи про постачання товарів, плани щодо встановлення обладнання.

Інформація про клієнтів містить ПІБ замовників, його контактні данні, особистий обліковий номер, тощо. Ця інформація є конфіденційною та не підлягає розголошенню або поширенню. Доступ до цієї інформації контрольований.

Плани будівель та рішення щодо встановлення систем безпеки розробляються співробітниками підприємства разом з замовником. У планах міститься інформація до адреси, точні виміри площі об’єкта, його стан, розміщення елементів системи, тощо.

Звіти бухгалтерії містять інформацію про пересування активів підприємства, нарахування заробітної платні співробітникам, вартість закупівель, розходи та прибутки за певні періоди часу та за певними договорами, звітність про оподаткування підприємства, тощо. Ця інформація обговорюється у тісному колі співробітників, які мають до неї доступ.

Документі ціно утворень містять в собі тарифні плани для обслуговування та встановлення систем та мереж, цей документ є ознайомчим для клієнтів компанії та у вільному доступі на сайті компанії.

Звітність о наявності елементів систем безпеки складається під час постачання нового обладнання, після списується під замовлення. Ця документація є у вільному доступі співробітників підприємства від технічного відділу.

Плани щодо встановлення обладнання використовуються як інструкція для бригад з встановлення, вони складаються за допомогою проєктів та видаються на руки під час виконання замовлень. У них розписані елементи, місця встановлення, необхідні матеріали, тощо. Після виконання завдань, здаються на підприємстві та підлягають знищенню.

Таблиця 1.3 - Інформація, яка циркулює на ОІД

№	Вид інформації	Режим доступу	Правовий режим	Вид представлення в ІТС	Вимоги до захисту		
					К	Ц	Д
1	Інформація про клієнтів компанії	Обмежений доступ	Конфіденційна	Графічна, текстова, звукова	К2	Ц2	Д2
2	Інформація про об’єкти та системи безпеки	Обмежений доступ	Таємна	Графічна, текстова, числова	К3	Ц3	Д3
3	Звіти бухгалтерії	Обмежений доступ	Службова	Текстова, числова	К2	Ц2	Д2
4	документи ціно утворень	Відкрита	—	Текстова, числова	К1	Ц1	Д1
5	звітність о наявності елементів систем безпеки	Обмежений доступ	Службова	Текстова, числова	К2	Ц2	Д1

Продовження таблиці 1.3

6	документи про постачання товарів	Обмежений доступ	Службова	Текстова, числова, графічна	К2	Ц2	Д1
7	плани щодо встановлення обладнання	Обмежений доступ	Таємна	Графічна, текстова, числова	К3	Ц3	Д3

Таблиця 1.4 - Рівень важливості конфіденційності

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

Таблиця 1.5 - Рівень важливості цілісності

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

Таблиця 1.6 - Рівень важливості доступності

Оцінка рівня наслідків	Опис
Д1	Не впливає на доступність
Д2	На деякий час впливає на доступність до ресурсу, що може принести незначні збитки або мати невеликий вплив на репутацію підприємства

Продовження таблиці 1.6

ДЗ	Унеможливлює користування ресурсом на тривалий час і має значний вплив на роботу підприємства

Таблиця 1.7 - Користувацьке середовище

Об'єкт / Користувач	Кіл працівників	Рівень кваліфікації	Роль в ІС	Інформація					Повноваження керувати КСЗІ	Ресурси
				Інф. про кл.	Проєкти	Бухгалт. звіти	Наявність	Планивст		
Керівник офісу	1	Досвідчений	Користувач	RCSP	RCDSP	RCDSP	RCDSP	RCDSP	+	PC PR SR SF
Головний менеджер	1	Досвідчений	Користувач	RWCMSP	RCP	-	RCP	RWCP	-	PC PR
Менеджер	2	Середній	Користувач	RWCMP	RP	-	RP	-	-	PC PR
Адвокат	1	Середній	Користувач	R	-	-	-	-	-	PC PR
Голова тех. забезпечення	1	Досвідчений	Користувач	-	RWCMSP	-	RWCMSP	RWCMSP	-	PC PR
Проєктувальник	2	Досвідчений	Користувач	-	RWCMSP	-	RP	RP	-	PC PR
Бригадир	1	Середній	Користувач	-	RCP	-	RP	RWCMSP	-	PC PR
Головний бухгалтер	1	Досвідчений	Користувач	-	-	RWCMSP	RWCMSP	-	-	PC PR
Бухгалтер	1	Досвідчений	Користувач	-	-	RWCMSP	-	-	-	PC PR
Спеціаліст кібербез.	1	Досвідчений	Адміністратор	-	RP	-	RP	RP	+	PC PR
Системний адмін..	1	Досвідчений	Адміністратор	-	-	-	RWCMSP	-	+	PC PR

Примітка:

R - читання;

W - запис (створення);

C - копіювання;

D - видалення;

M - модифікація;

S - зберігання;

P - друкування;

PC - персональний комп’ютер;

PR - принтер;

SR - сервер;

SF - сейф.

На кожному підприємстві необхідно визначити ПЗ яке необхідно для його функціонування, захисту, пошуку інформації, її обробки, тощо.

Таблиця 1.8 - Інвентаризаційна відомість програмного забезпечення ІТС

№	Назва	Тип	Опис	Ліцензія	Де встановлена
1	Windows 10 10.0.17763.1 (build 1809)	Системне	Операційна система для персональних комп'ютерів і робочих станцій	Volume license	Всі ПК
2	Windows Server 2019	Системне	Операційна система для серверів	Volume license	Сервер
3	ESET File Security (версія 7.1.12008)	Системне	Антивірусна програма	Commercial	Всі ПК
4	WinRar (версія 5.80)	Системне	Архіватор файлів для 32- і 64-розрядних операційних систем Windows	Shareware	Всі ПК
5	Базовий пакет Microsoft Office 2019 Professional	Прикладне	ПЗ для роботи з різними видами документів, текстів, таблиць, тощо.	Volume license	Всі ПК

Продовження таблиці 1.8

6	1С Підприємство 8.2. Базова версія	Прикладне	Програми, що дозволяють виконувати операції над даними, представленими в табличній формі	Volume license	ПК менеджерів, бухгалтерів, керівника офісу, головного менеджеру, голови технічного забезпечення
7	Adobe Photoshop CS6 (версія 13.01)	Прикладне	Засоби створення нерухомих і рухомих зображень	Volume license	Проєктувальники, голова технічного забезпечення
8	Microsoft Edge (версія 44.18362.1.0)	Прикладне	Програми для роботи в комп'ютерній мережі	Freeware	Всі ПК
9	Google Chrome (версія 80.0.3987)	Прикладне	Програми для роботи в комп'ютерній мережі	Freeware	Всі ПК
10	Windows Media Player (версія 12.0.18362.418)	Прикладне	Програма для відтворення відео- та аудіофайлів	Freeware	Всі ПК
11	Visual Studio 2019 (версія 16.0)	Спеціальне	Об'єктно-орієнтовані мови програмування	Volume license	Проєктувальники, голова технічного забезпечення, спеціаліст кібербезпеки, системний адміністратор
12	TeamViewer (версія 15.4.4445)	Спеціальне	Програми для роботи в комп'ютерній мережі через віддалений доступ	Freeware	Всі ПК
13	Adobe Acrobat (версія 2019.008.20071)	Спеціальне	Програма для роботи з pdf-файлами	Freeware	Всі ПК
14	Skype (версія 14.56.102.0)	Спеціальне	Забезпечує текстову, голосовий та відеозв'язок через Інтернет між комп'ютерами	Freeware	Всі ПК
15	Viber (версія 12.6.0.41)	Спеціальне	Забезпечує текстову, голосовий та відеозв'язок через Інтернет	Freeware	Всі ПК

Продовження таблиці 1.8

16	AutoCAD (версія 23.0)	Прикладне	Засоби створення об'ємних макетів та планів будівель	Volume license	Проєктувальники, голова технічного забезпечення
17	AIDA64 Business (Версія 6.70)	Спеціальне	Програма для стеження за показниками ПК та його тестування	Volume license	Всі ПК

Згідно з таблицею 1.8 ПЗ яке встановлено на певних ПК, не може самостійно шукати нові версії, для вдосконалення роботи системи та полегшення роботи системного адміністратора можливе встановлення на всі ПК програм, що відстежують нові версій ПЗ та повідомляють про їх знаходження. Оскільки в таблиці є ПЗ, яке не повідомляє про нові версії, необхідно робити пошук вручну, що займає певний робочій час.

1.3 Висновки

У першому розділі кваліфікаційної роботи провели обстеження підприємства, що займається розробкою, встановленням та обслуговуванням систем захисту, ТОВ "Авалон". Дослідили актуальність питання, особовий склад підприємства та його обов'язки, обстежили приміщення у якому знаходиться та працює підприємство, визначили перелік ПЗ та обладнання, на якому обробляється та зберігається інформація.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Аналіз основних методів захисту інформації в ІКС

На основі першого розділу та інформації, про підприємство можливе більш детальне дослідження питання захисту інформації, пошук слабких місць у системі захисту, можливі методи вдосконалення, оновлення або зміни методів та засобів захисту.

До основних методів захисту інформації можна віднести:

- Фізичні;
- Апаратні;
- Програмні;
- Апаратно-програмні;
- Криптографічні;
- Організаційні.

Фізичні засоби захисту - це засоби, необхідні для зовнішнього захисту засобів обчислювальної техніки, території та об'єктів на базі ПК, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів інформаційних систем та інформації, що захищаються.

Апаратні засоби захисту - це різні електронні, електронно-механічні та інші пристрої, які вмонтовуються в серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних, процесорів, ліній зв'язку, тощо.

Апаратно-програмні засоби захисту - ці засоби широко використовуються при аутентифікації користувачів автоматизованих банківських систем. Аутентифікація - це перевірка ідентифікатора користувача перед допуском його до ресурсів системи. Аутентифікація - це ідентифікація користувача в системі з допомогою його імені або псевдоніма, що приймає участь в реєстраційній

процедурі та пароля доступу, що відомий лише користувачу. Пароль - це код (набір символів), що забезпечує доступ до систем, файлів, апаратних засобів, тощо. Апаратно-програмні засоби захисту використовуються також при накладанні електронно-цифрових підписів відповідальних користувачів. Найпоширенішим в автоматизованих банківських системах є використання смарт-карт, які містять паролі та ключі користувачів.

Організаційні заходи захисту засобів комп'ютерної інформації складають сукупність заходів щодо підбору, перевірки та навчання персоналу.

Застосування криптографічного захисту, тобто кодування тексту з допомогою складних математичних алгоритмів, завойовує все більшу популярність. Звичайно, жоден з шифрувальних алгоритмів не дає цілковитої гарантії захисту від зловмисників, але деякі методи шифрування настільки складні, що ознайомитися зі змістом зашифрованих повідомлень практично неможливо. [3]

Для виявлення слабких місць підприємства необхідно розробити модель порушника та модель загроз.

2.2 Модель порушника та модель загроз

Модель порушника - абстрактний формалізований або неформалізований опис порушника.

Порушник - користувач, який здійснює несанкціонований доступ до інформації.

Проаналізувавши обстеження середовища функціонування інформаційно-телекомунікаційної системи (ІТС) компанії ТОВ «Avalon», можна зробити висновок, що потенційними порушниками можуть бути в першу чергу персонал та клієнти, відвідувачі.

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії. Відносно АС порушники можуть бути

внутрішніми (з числа персоналу або користувачів системи) або зовнішніми (сторонніми особами).

У кожного інформаційного активу є різні ризики, але найбільшим ризиком можна назвати людину, яка не розуміючи наслідки може поширювати інформацію за межі підприємства. Також можуть бути й зовнішні порушники, але це дуже рідкі випадки.

Таблиця 2.1 - Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загроз
Внутрішні за відношенням до ІТС		
ПВ1	Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІТС	2
ПВ2	Персонал, який обслуговує технічні засоби ІТС (системний адміністратор, ІТ спеціаліст)	3
ПВ3	Користувачі ІТС	2
ПВ4	Адміністратор ІТС(системний адміністратор)	3
ПВ5	Керівники різних рівнів(директор)	1
ПВ6	Персонал який не має доступу до ІТС	1
Зовнішні за відношенням до ІТС		
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання та інше)	2
ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів	3
ПЗ5	Випадковий відвідувач	1

Таблиця 2.2 - Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність	1
М2	Самоствердження	2

Продовження таблиці 2.2

М3	Корисливий інтерес	4
М4	Професійний обов'язок (ПЗ4)	4

Таблиця 2.3 - Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

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

Таблиця 2.4 - Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

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

Продовження таблиці 2.4

З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4

Таблиця 2.5 - Специфікація моделі порушника за часом дії

Позна-чення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час функціонування ІТС	3
Ч2	Під час бездіяльності компонентів системи (в неробочій час, під час планових перерв у роботі, перерв для обслуговування і ремонту і т.д.)	2
Ч3	Під час повної бездіяльності ІТС з метою відновлення та ремонту	2
Ч4	Як у процесі функціонування систем захисту інформації, так і під час зупинки компонентів системи	4

Таблиця 2.6 - Специфікація моделі порушника за місцем дії

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

На підставі таблиць 2.1 - 2.6 можна створити модель порушника, підрахувати суму загроз та визначити, хто з особистого складу підприємства є найбільш загрозою для підприємства. Оскільки окремі співробітники мають право перебувати та працювати у офісному приміщенні вночі за потреби, з

дозволю директора офісу, необхідно розглядати можливість порушення вдень та вночі окремо.

Таблиця 2.7 - Модель порушника

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Директор офісу	ПВ5	М2	К4	З3	Ч1	Д4	17
	1	2	4	3	3	4	
	ПЗ4	М4	К4	З4	Ч4	Д4	23
	3	4	4	4	4	4	
Голова технічного забезпечення	ПВ5	М1	К4	З3	Ч1	Д2	14
	1	1	4	3	3	2	
	ПЗ4	М4	К4	З4	Ч2	Д4	21
	3	4	4	4	2	4	
Головний менеджер	ПВ5	М1	К3	З3	Ч1	Д2	15
	1	1	3	4	3	2	
	ПЗ4	М4	К3	З3	Ч1	Д2	19
	3	4	3	4	3	2	
Менеджери	ПВ3	М1	К2	З1	Ч1	Д2	11
	2	1	2	1	3	2	
	ПЗ4	М4	К2	З3	Ч1	Д2	18
	3	4	2	4	3	2	
Проєктувальники	ПВ3	М3	К4	З1	Ч1	Д2	16
	2	4	4	1	3	2	
	ПЗ4	М4	К4	З3	Ч1	Д2	20
	3	4	4	4	3	2	
Системний адміністратор	ПВ4	М1	К3	З3	Ч4	Д4	19
	3	1	3	4	4	4	
	ПЗ4	М4	К3	З4	Ч4	Д4	22
	3	4	3	4	4	4	

Продовження таблиці 2.7

Спеціаліст кібербезпеки	ПВ4	М1	К4	З3	Ч4	Д4	20
	3	1	4	4	4	4	
	ПЗ4	М4	К4	З4	Ч4	Д4	23
	3	4	4	4	4	4	
Бригадир	ПВ3	М3	К2	З1	Ч1	Д2	14
	2	4	2	1	3	2	
	ПЗ4	М4	К2	З4	Ч1	Д2	18
	3	4	2	4	3	2	
Адвокат	ПВ3	М1	К1	З1	Ч1	Д2	10
	2	1	1	1	3	2	
	ПЗ4	М4	К1	З1	Ч1	Д2	14
	3	4	1	1	3	2	
Бухгалтерія	ПВ3	М3	К1	З1	Ч1	Д2	13
	2	4	1	1	3	2	
	ПЗ4	М4	К1	З3	Ч1	Д2	17
	3	4	1	4	3	2	
Бригади	ПВ6	М1	К2	З1	Ч2	Д1	8
	1	1	2	1	2	1	
	ПЗ4	М4	К2	З1	Ч2	Д1	13
	3	4	2	1	2	1	

Найбільшу загрозу несуть системний адміністратор та спеціаліст з питань кібербезпеки підприємства, через їх високу кваліфікацію та знання ПЗ підприємства, вони можуть становити загрозу для підприємства у разі підкупу конкурентами, з іншої сторони ці співробітники є основою безпеки підприємства. Під час роботи співробітників необхідно враховувати факти ненавмисного псування даних, через низку факторів.

При вдосконаленні комплексної системи захисту інформації необхідно знизити рівень загроз серед працівників.

Таблиця 2.8 - Модель внутрішнього порушника політики безпеки інформації

Категорія порушника «ПВ»	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Директор офісу	ПВ5	М2	К4	З3	Ч1	Д4	17
Голова технічного забезпечення	ПВ5	М1	К4	З3	Ч1	Д2	14
Головний менеджер	ПВ5	М1	К3	З3	Ч1	Д2	15
Менеджери	ПВ3	М1	К2	З1	Ч1	Д2	11
Проєктувальники	ПВ3	М3	К4	З1	Ч1	Д2	16
Системний адміністратор	ПВ4	М1	К3	З3	Ч4	Д4	19
Спеціаліст кібербезпеки	ПВ4	М1	К4	З3	Ч4	Д4	20
Бригадир	ПВ3	М3	К2	З1	Ч1	Д2	14
Адвокат	ПВ3	М1	К1	З1	Ч1	Д2	10
Бухгалтерія	ПВ3	М3	К1	З1	Ч1	Д2	13
Бригади	ПВ6	М1	К2	З1	Ч2	Д1	8

З останньої таблиці видно, що найбільшу загрозу підприємству становлять, системний адміністратор та спеціаліст кібербезпеки, оскільки вони працюють в одному відділі та підпорядковуються директору офісу. У випадку підкупу одного співробітника з двох можливе стеження іншого за роботою порушника. Тому організація роботи цих осіб повинна бути найбільш контрольованою, оскільки вони є основними потенційними порушниками безпеки інформації.

Модель загроз є важливою не тільки для підвищення захисту підприємства, вона може слугувати для страхування від збитків у різних випадках, наприклад якщо підприємство знаходиться у місцях де можливий

землетрус, його можна застрахувати та покрити частину збитків заподіяну землетрусом.

Згідно НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу:

Модель загроз - абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.

Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні.

Основні види загроз для безпеки інформації:

- зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);
- збої та відмови у роботі технічних або програмних засобів (далі - ПЗ) ІТС;
- наслідки помилок під час проєктування та розробки компонентів ІТС (технічних засобів, технології обробки інформації, ПЗ, засобів захисту, структур даних тощо);
- помилки персоналу (користувачів) ІТС під час експлуатації;
- навмисні дії (спроби) потенційних порушників.

Випадкові загрози суб'єктивної природи - це помилкові дії персоналу за неуважності, недбалості, незнанню тощо, але без навмисного наміру.

До них відносяться:

- дії, що призводять до відмови ІТС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм тощо);
- ненавмисне пошкодження носіїв інформації;
- неправомірна зміна режимів роботи ІТС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

- неумисне зараження ПЗ комп'ютерними вірусами;
- невиконання вимог до організаційних заходів захисту чинних в ІТС розпорядчих документів;
- помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;
- будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;
- неправомірне впровадження та використання заборонених політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення тощо);
- наслідки некомпетентного застосування засобів захисту тощо.

Навмисні загрози суб'єктивної природи - це дії порушника, спрямовані на проникнення в систему та одержання можливості НСД до її ресурсів або дезорганізацію роботи ІТС та виведення її з ладу.

До них відносяться:

- порушення фізичної цілісності ІТС (окремих компонентів, пристроїв, обладнання, носіїв інформації);
- порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІТС (електроживлення, заземлення, охоронної сигналізації, кондиціонування тощо.);
- порушення режимів функціонування ІТС (обладнання і ПЗ);
- впровадження та використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;
- використання (шантаж, підкуп тощо) з корисливою метою персоналу ІТС;
- крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);
- несанкціоноване копіювання носіїв інформації;

- читання залишкової інформації з оперативної пам’яті ЕОТ, зовнішніх накопичувачів;

- одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача;

- неправомірне підключення до каналів зв’язку, перехоплення даних, що передаються, аналіз трафіку тощо;

- впровадження та використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);[4]

Таблиця 2.9 - Перелік загроз з визначенням порушень властивостей

№	Потенційні загрози для інформації в ІТС	Ризики для			
		К	Ц	Д	С
Загрози об’єктивної природи					
1	Стихійні явища		+	+	
2	Відсутність електропостачання		+	+	
3	Відмова/збій обчислювальної техніки		+	+	
4	Відмова/збій програмного забезпечення	+	+	+	
5	Пошкодження паперової документації	+	+	+	
6	Відмова доступу до інтернету		+	+	
Загрози суб’єктивної природи					
1	Несанкціоноване підключення до технічних засобів	+	+		
2	Несанкціоноване підключення до мережевих вузлів	+	+	+	
3	Читання даних, залишених без нагляду та читання даних, що виводиться на екран	+			+
4	Перехоплення даних за допомогою акустичного каналу	+			+
5	Несанкціонований перегляд інформації за допомогою візуально-оптичного каналу	+			+
6	Зараження системи вірусами	+	+	+	
7	Втрата паролів	+	+	+	
8	Втрата резервних копій		+	+	+
9	Несанкціоноване внесення змін у технічні засоби	+	+	+	
10	Використання недозволеного програмного забезпечення або модифікація компонентів програмного та інформаційного забезпечення	+			+
11	Пошкодження носіїв інформації		+	+	
12	Вхід в систему недопущених осіб (подолання систем захисту)	+	+	+	

Продовження таблиці 2.9

13	Недоступність до хмарного сховища			+	
14	Неправильне налаштування резервного копіювання		+	+	+
15	Неправильні налаштування прав доступу співробітників	+		+	
16	Недбале зберігання документів	+	+	+	+
17	Отримання сторонньою особою інформації у персоналу ІТС	+	+		+
18	Відсутність правильно налагодженої системи сигналізації	+	+		+
19	Відсутність шифрування даних	+			+
20	Передача важливих документів в незашифрованому вигляді	+			
21	Хакерська атака	+	+	+	
22	Використання заборонених ресурсів Інтернету в своїх цілях	+			
23	DDos-атака			+	

Модель загроз з визначенням рівня ризиків та збитків

- високий - якщо реалізація загрози надає великих збитків (3 бали);
- середній - якщо реалізація загрози надає помірних збитків (2 бали);
- низький - якщо реалізація загрози надає незначних збитків (1 бал).

Таблиця 2.10 - Загрози конфіденційності інформації

№	Механізм реалізації	Рівень		Сума загроз
		ризики	збитки	
К.1	Халатність співробітників підприємства	2	2	4
К.2	Не дотримання чітких правил безпеки під час користування РС	2	3	5
К.3	Копіювання даних для ознайомлення сторонніми особами	2	3	5
К.4	Погана звукоізоляція приміщення	3	2	5
К.5	Не правильні умови зберігання паперових документів в архівах	1	1	2
К.6	Викрадення носіїв ІзОД з метою несанкціонованого ознайомлення сторонніх осіб	1	3	4
К.7	Відсутність опису використання зовнішніх носіїв	1	3	4
К.8	Використання сторонньої інформації з посиланням на авторів	1	2	3

Таблиця 2.11 - Загрози цілісності інформації

№	Механізм реалізації	Рівень		Сума загроз
		ризики	збитки	
Ц.1	Помилки (ненавмисні) користувачів ІТС, які призвели до модифікації або спотворення інформації на жорсткому диску або зовнішніх носіях	2	2	4
Ц.2	Несанкціонована (навмисне) модифікація або спотворення інформації персоналом ІТС на жорсткому диску або зовнішніх носіях	1	3	4
Ц.3	Відсутність вчасного резервного копіювання	3	3	6
Ц.4	Відсутність вчасного копіювання та зберігання важливих документів	1	3	4
Ц.5	Прояви помилок системного ПЗ, в наслідок яких стала можливою модифікація інформації або її спотворення користувачами	1	2	3
Ц.6	Безпосередній доступ до інформації будь-яким способом сторонніми особами	1	3	4
Ц.7	Халатність співробітників щодо пропуску сторонніх осіб	2	3	5
Ц.8	Відсутність підтвердження відправника інформації що надходить на обробку	1	3	4

Таблиця 2.12 - Загрози доступності інформації

№	Механізм реалізації	Рівень		Сума загроз
		ризики	збитки	
Д.1	Помилка користувача, яка призвела до знищенню даних	1	3	4
Д.2	Помилка адміністраторів, яка призвела до віддаленню даних	1	3	4
Д.3	Пошкодження парольних носіїв персоналом ІТС, що призвело до втрати доступу до інформації	2	3	5
Д.4	Прояви помилок системного ПЗ, яке призвело до втрати доступу до інформації або ІТС	1	2	3
Д.5	Прояви помилок системного ПЗ, в наслідок яких стала можливою модифікація інформації або її спотворення користувачами	1	1	2
Д.6	Безпосередній доступ до інформації будь-яким способом сторонніми особами	1	3	4
Д.7	Навмисне видалення або деформація інформації	1	3	4
Д.8	Можливість невчасного оновлення інформації	1	1	2

Таблиця 2.13 - Загрози спостереженості ІТС

№	Механізм реалізації	Рівень		Сума загроз
		ризики	збитки	
С.1	Помилки (ненавмисні) персоналу ІТС, які призвели до втрати спостереженості	2	3	5
С.2	Помилки (ненавмисні) адміністраторів ІТС, які призвели до втрати спостереженості	2	2	4
С.3	Некоректне налагодження засобів захисту адміністраторами ІТС, яке призвело до втрати спостереженості	1	3	4
С.4	Порушення спостережності користувачами ІТС внаслідок навмисних цілей	1	3	3
С.5	Порушення спостереженості внаслідок пошкодження, у тому числі навмисного, архівів та носіїв з архівами даних	2	3	5
С.6	Прояви помилок системного ПЗ, яке призвело до втрати спостереженості	1	1	2
С.7	Безпосередній доступ до ІТС будьяким способом сторонніх осіб	1	3	4
С.8	Можливе спостереження співробітниками охорони	1	2	3

Таблиця 2.14 - Узагальнена таблиця загроз ІТС

№	Види загроз	1	2	3	4	5	6	7	8	Сума загроз
1	Конфіденційності	4	5	5	5	2	4	4	3	32
2	Спостереженості	5	4	4	3	5	2	4	3	30
3	Доступності	4	4	5	3	2	4	4	2	28
4	Цілісності	4	4	6	4	3	4	5	4	34

На основі отриманих даних з таблиці 2.14, найбільшу загрозу підприємству, у разі розголошення, викрадення, модифікації інформації, є конфіденційність та цілісність. Це відбувається за рахунок того, що на підприємстві обробляється інформація, пов'язана з системами захисту приватних осіб та підприємств. У разі витоку такої інформації підприємство

буде нести відповідальність згідно чинного законодавства України. При цьому у разі поширювання інформації про клієнтів підприємство втратить свою репутацію та частину клієнтів, це може призвести до значного скорочення прибутків.

Для захисту інформації необхідно дослідити КС на критерії оцінки захищеності інформації від несанкціонованого доступу.

2.3 Критерії конфіденційності

Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

В контексті критеріїв комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного.

З таблиці 2.14, найбільшу загрозу від витоку інформації на підприємстві є конфіденційність та цілісність. Під час обстеження критеріїв необхідно звернути на них увагу, після досліджень необхідно розробити методи захисту для реалізації критеріїв, це значно підвищить захист інформації на підприємстві.

На рисунку 2.1 детальна структура критеріїв, та їх ієрархія.

Для підприємства даного типу можна визначити необхідний профіль захищеності, цим профілем є 3.КЦД.1.

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

Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги треба шукати в розділі “Критерії конфіденційності”.

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. Якщо існують вимоги щодо обмеження можливості модифікації інформації, то відповідні послуги треба шукати в розділі “Критерії цілісності”.

Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то відповідні послуги треба шукати в розділі “Критерії доступності”.

Спостереженість - ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні послуги треба шукати у розділі “Критерії спостереженості”.[5]

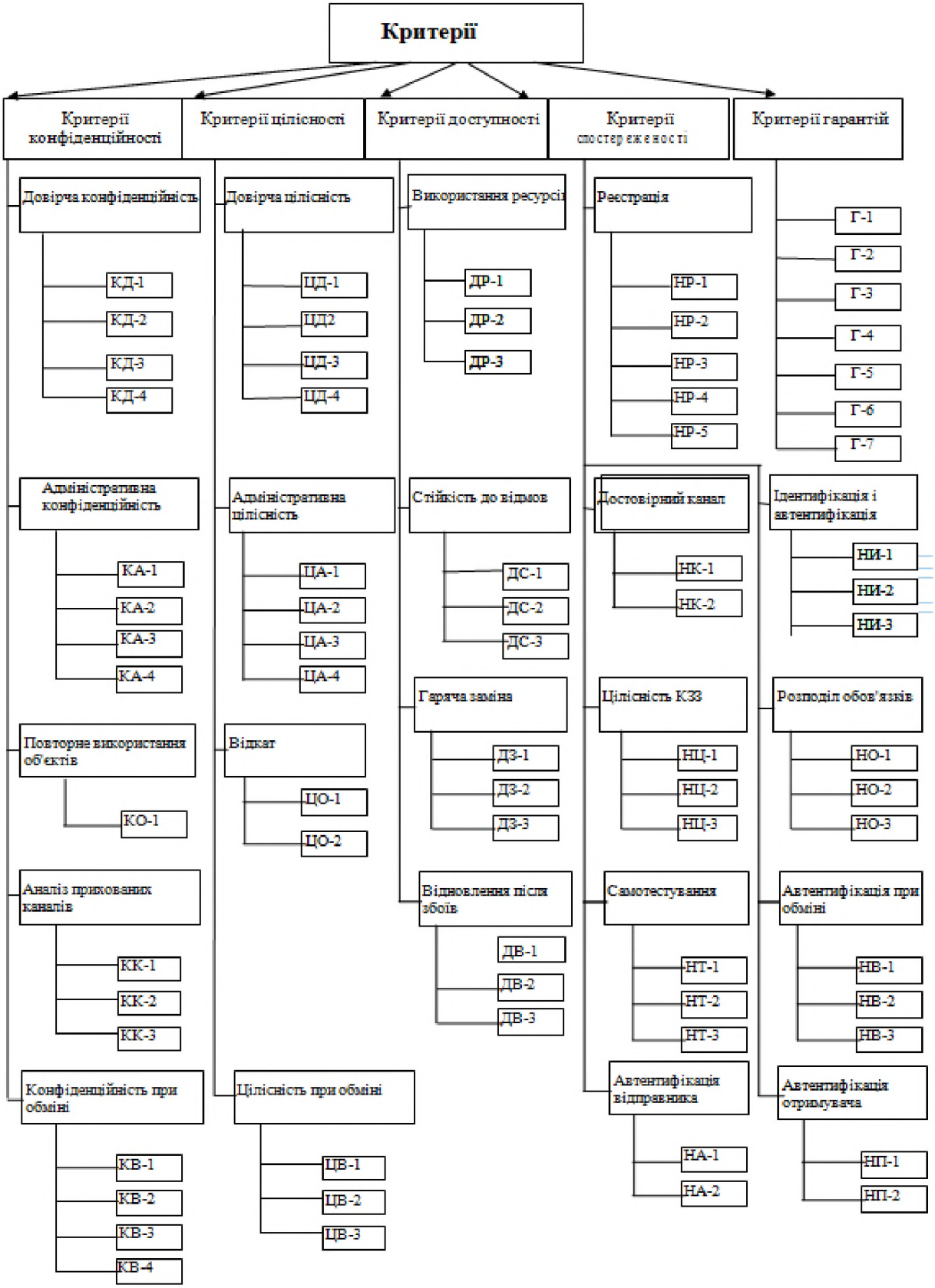

Рисунок 2.1 - Структура критеріїв

2.4 Профіль захищеності 3.КЦД.1

КД-2. Базова довірча конфіденційність. Реалізована. Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ надає користувачу можливість для кожного захищеного об’єкта, що належить його домену, визначати конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта.

Реалізація відбувається за рахунок налаштувань ОС, після запуску якої користувачі повинні ввести логін, який слугує маркером у системі, та підтвердити свій маркер паролем, який знає лише один користувач.

КО-1. Повторне використання об'єктів. Реалізована. Процесу необхідно декілька користувачів, в яких є розподілення облікових записів, інформація стане недосяжною, коли буде декілька користувачів системи.

Реалізована за допомогою особливостей розподільчої файлової системи сервера, а саме редагування або використання об’єкта можливе лише одним користувачем, після звільнення об’єкта інформації, ним зможе скористуватися інший користувач, при цьому об’єкт змінить на первинні свої властивості доступності.

КВ-1. Мінімальна конфіденційність при обміні. Реалізована. КЗЗ визначає множину об'єктів і інтерфейсних процесів, до яких вона відноситься.

Реалізована за рахунок використання топології “зірка”, яка дозволяє запитувати інформацію напряму з сервера, або маршрутизатора, не використовуючи сторонні ПК для отримання інформації шляхом транзиту.

ЦД-1. Мінімальна довірча цілісність. Реалізована. КЗЗ здійснює розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта.

Реалізована за рахунок чітко визначених користувачів, їх атрибутів доступності, цілісності. Розподільчий доступ до об’єктів і процесів системи виконаний за рахунок ОС.

ЦО-1. Обмежений відкат. Реалізована. Існують автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відновити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

Реалізована за рахунок ОС, яка записує у журнал подій дії користувачів, та робить можливим у проміжок певного часу не враховувати певні дії, також для реалізації можна віднести резервне копіювання даних.

ЦВ-1. Мінімальна цілісність при обміні. Реалізована. КЗЗ визначає множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності.

Реалізовано за рахунок унеможливлення зміни рівня захищеності процесами або користувачами, такі дії можливі лише з дозволу системного адміністратора, який повинен визначити процес та його повноваження до дій у системі.

ДР-1. Квоти. Реалізована. Політика використання ресурсів, що реалізується КЗЗ визначає множину об'єктів КС, до яких вона відноситься.

Можливе встановлення обмежень на використання певних ресурсів для користувачів є необхідною, для вчасного виявлення загроз. Реалізовано за рахунок обмежень користування, які надає ОС.

ДВ-1. Ручне відновлення. Реалізована. КЗЗ визначає множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки.

Чітко визначений рівень відмов ОС та ПЗ підприємства полягає в їх ідентифікації у системі. Якщо після відмов ОС або ПЗ порушує правила користування системою, які встановлені системним адміністратором, то

можливе ручне відновлення шляхом налаштування ОС або ПЗ під старими правилами.

НР-2. Захищений журнал. Реалізована. КЗЗ визначає перелік подій, що реєструються.

Журнал подій доступ до якого мають системні адміністратори та спеціаліст з питань кібербезпеки, у журналі є всі користувачі та всі їх дії.

НИ-2. Одиночна ідентифікація і автентифікація. Реалізована. КЗЗ автентифікує користувача з використанням захищеного механізму.

Реалізовано за допомогою входу до системи з використанням логіна та пароля.

НК-1. Однонаправлений достовірний канал. Реалізована. Достовірний канал повинен використовує для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

Реалізовано за рахунок використання налаштувань на передачу даних у системи, при підтримці ОС, де можна визначити яке саме ПЗ може передавати данні та коли. Обмеження використання трафіка ПЗ необхідне для зменшення потоку інформації підприємства та захищає від стороннього ПЗ.

НО-2. Розподіл обов'язків адміністраторів. Не реалізована. КЗЗ не визначає ролі адміністратора і звичайного користувача і притаманні їм функції.

НЦ-2. КЗЗ з гарантованою цілісністю. Не реалізована. КЗЗ не підтримує домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування.

НТ-2. Самотестування при старті. Не реалізована. КЗЗ не описує властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ при старті.

НВ-1. Автентифікація вузла. Реалізована. Підтвердження ідентичності виконується на підставі затвердженого протоколу автентифікації.

Реалізовано за допомогою процедури допуску до інформації по логіну, паролю, IP- адресою.

Для реалізації НО-2 необхідно розділити обов'язки системного адміністратора та спеціаліста з питань кібербезпеки підприємства. При однакових правах двох адміністраторів неможлива реалізація профілю захищеності.

Для реалізації НЦ-2 необхідно від імені адміністратора у ОС Windows встановити налаштування "Контроль цілісності". При цьому ОС буде контролювати цілісність системних та програмних файлів шляхом їх неможливого змінення, навіть від імені адміністратора. Цей механізм захисту не буде давати змогу оновлювати ПЗ за вимогою. При необхідності оновити ПЗ, а це означає змінити системні та програмні файли, необхідно буде вимкнути дану функцію у налаштування ОС Windows, після цього провести оновлення ПЗ та включити функцію знову для контролю цілісності.

Для реалізації НТ-2 необхідно у налаштуваннях BIOS ввімкнути само тестування при старті, але ця функція є не надійною через те, що вона тестує елементи до завантаження системи. Самотестування після старту ОС можна реалізувати наступними програмами : AIDA64, MSI Afterburner, Sandra 20/20. Для цього необхідно встановити їх на ПК та налаштувати на самоаналіз при старті, можливе доповнення тестування у встановлений час та збереження звітності з тестування систем для аналізу системним адміністратором.

На підприємстві кожен співробітник може увійти у свій обліковий запис з будь-якого ноутбука, який раніше був авторизованим у мережі підприємства. Вхід до системи дозволяється при спів падінні логіну та паролем. Логіни та паролі співробітників зберігаються на сервері у хешованному вигляді. Доступ до даної інформації можливий лише спеціалісту з кібербезпеки підприємства, системному адміністратору та керівнику підприємства.

Після входу в систему визначаються можливості користувача або адміністратора, його можливий доступ до сервера та певних файлів системи та

виробництва. Вся інформація підприємства розподілена на “гілки” у сховищі даних, кожному користувачеві надається можливість відкривати лише ті “гілки”, які йому необхідні при роботі.

Система робить резервне копіювання у стиснутому вигляді до сервера компанії кожний понеділок та п’ятницю.

Самотестування системи відбувається при запуску її за допомогою BIOS та за вимогою адміністратора спеціальним ПЗ.

Аналіз системи на захищеність відбувається у реальному часі за допомогою антивірусних програм та ПЗ що дозволяє слідкувати за інформаційними потоками підприємства. Також для цього у системі відбувається моніторинг журналу подій. За цим можуть слідкувати спеціаліст кібербезпеки та системний адміністратор.

За розподіл ресурсів відповідає ОС Windows, яка автоматично перенаправляє потужності на необхідні процеси при роботі з ПК.

За допомогою використання локальної та глобальної мережі з технологією VPN та обміном даними з сервером підприємства, реалізовується більшість норм з використання, зберігання, обробки і передачі інформації.

2.5 Програмне забезпечення з захисту інформації

ПЗ яке використовується для захисту підприємства:

- WireShark - програма для стеження пакетів даних, які відправляються та надходять до комп’ютерів та серверів. Зручна у вивчені та користуванні.
- 360 Total Security - антивірусна програма яка є складовою ОС, проводить активну перевірку одержаних файлів, робить аналіз системи і не потребує втручання спеціалістів.
- VPN CyberGhost - VPN створює захищене з’єднання між ПК та глобальною мережею, захищає від стеження за трафіком та стороннього втручання. Ця програма має зручні пакети налаштувань, а саме підключення

при запуску ПК та сервера, має зрозумілий інтерфейс та високу швидкість при навантаженнях, зручне ПЗ для використання у широких масштабах.

Програма WireShark використовує лише спеціаліст з питань кібербезпеки підприємства. За допомогою фільтру програми він може стежити як за всіма пакетами які надходять та виходять з підприємства, так і за певними пакетами або певними ПК. При перехопленні пакетів спеціаліст аналізує їх зміст, посилання на сторонні вебсторінки, вид інформації що надсилається, тощо.

У разі необхідності можливе відключення від мережі для запобігання перехоплення інформації з сторонніх каналів зв'язку.

Антивірусна програма 360 Total Security - встановлена на всіх ПК підприємства, вмикається зі стартом системи, забезпечує активний захист ПК у реальному часі, серед приємних бонусів безкоштовного антивірусного ПЗ є моніторинг завантажень файлів та системи, активне блокування шкідливих сайтів та реклами, безпосередній вплив шпигунського та шкідливого ПЗ шляхом видалення або переміщення у карантин, оголошення про стан системи користувачеві кожен раз коли необхідні дії з системою.

VPN CyberGhost - встановлений на кожному ПК підприємства, він починає працювати при старті системи, тому користувачам не потрібно вмикати його самостійно. Якщо програма не зможе встановити зв'язок з серверами, вона повідомить про це користувача, який зможе самостійно натиснути кнопку "з'єднання" та самостійно вирішить цю проблему.

Інструкція з користування ПЗ для користувача.

Після старту ПК перевірити антивірус 360 Total Security на стан "Під захистом" та наявність останньої версії, при необхідності оновити. Перевірити стан VPN CyberGhost на "Підключено", при необхідності підключити. Під час використання ПК слідкувати за спливаючими вікнами у нижньому правому куті екрана на повідомлення від програм 360 Total Security та VPN CyberGhost. При невідомих помилках кликати системного адміністратора чи спеціаліста з питань кібербезпеки.

Інструкція з користування ПЗ для адміністратора.

Після старту ПК перевірити антивірус 360 Total Security на стан “Під захистом” та наявність останньої версії, при необхідності оновити. Перевірити стан VPN CyberGhost на “Підключено”, при необхідності підключити. Під час використання ПК слідкувати за спливаючими вікнами у нижньому правому куті екрана на повідомлення від програм 360 Total Security та VPN CyberGhost.

Для використання WireShark необхідно запустити програму, оновити її за необхідністю. Після запуску виконати захват необхідної мережі та при необхідності встановити фільтр для сортування пакетів. За необхідності розпізнання пристроїв можна використати телефонію за дротовою або бездротовою мережею.

2.6 Обстеження системи захисту підприємства на недоліки

При обстеженні офісного приміщення було виявлено наступний ряд недоліків:

- Зберігання паперових документів бухгалтерії у звичайних шафах без можливості їх блокування або опечатування;
- Відсутність тривожних кнопок у бухгалтерії;
- Відсутність перевірки приміщень на наявність закладних пристроїв.

Збоку програмної та апаратної моделі загрози виникають через:

- Можливість підключення сторонніх носіїв інформації;
- Неповний перелік заборонених сайтів для відвідування співробітниками;
- Доступ до файлової системи сервера без аутентифікації користувача;
- Відсутність ліній резервного постачання ресурсів глобальної мережі;
- Відсутність тимчасових паролів користувачів.

Серед організаційних загроз:

- Відсутність політики безпеки серед співробітників про закладні пристрої;

- Відсутність актів документообігу серед співробітників.

Для криптографічного захисту підприємство використовує алгоритм шифрування даних, які зберігаються на сервері та ПК, на зберіганні або використанні, RSA. Завдяки такому алгоритму шифрування даних, зловмисникам необхідно буде викрасти закритий ключ з сервера підприємства.

Рисунок 2.2 - Схема шифрування RSA

Шифрування — у системах обробки інформації - алгоритмічне (криптографічне) перетворення даних, яке виконується у по символьній послідовності з метою одержання шифрованого тексту[6].

Алгоритм RSA складається з 4 етапів: генерації ключів, шифрування, розшифрування та розповсюдження ключів.

Безпека алгоритму RSA побудована на принципі складності факторизації цілих чисел. Алгоритм використовує два ключі — відкритий і секретний, разом відкритий і відповідний йому секретний ключі утворюють пари ключів. Відкритий ключ не потрібно зберігати в таємниці, він використовується для

шифрування даних. Якщо повідомлення було зашифровано відкритим ключем, то розшифрувати його можна тільки відповідним секретним ключем[7].

2.7 Реалізація нових та вдосконалення вже існуючих методів та систем захисту інформації

Для розробки нових та вдосконалення вже існуючих методів та систем захисту інформації необхідно спиратися на чинне законодавство України, а саме на Закон України о захисті інформації в інформаційно-телекомунікаційних мережах, Закон України про захист персональних даних, Закон України про інформацію, та акти обстеження підприємства, які були у першому та другому розділі.

Виходячи з цих даних, а саме пункту 2.6, необхідно вдосконалити приміщення підприємства, розробити необхідні акти перевірок на закладні пристрої, вирішити питання з програмною частиною захисту підприємства та розробити необхідні нормативні документи.

Для підвищення захисту паперових носіїв інформації необхідно зберігати їх у сейфі, це значно завадить фізично викрасти їх. Для цього необхідно придбати сейф, встановити його можливо силами підприємства та визначити перелік документі підприємства, які мають знаходитися в ньому, а саме документи звітності підприємства за певними об’єктом, фінансові звіти, тощо.

Перелік документів для зберігання може бути встановлений, доповнений співробітниками підприємства або його директором.

Ціна сейфів, які підходять для встановлення на підлогу, за розміром та рівнем захисту. При встановленні його на підлогу, необхідно зафіксувати його за допомогою спеціальних болтів з секретом. При спробі фізичного викрадення документів підприємства, зловмисникам необхідно потрапити до кабінету бухгалтерії через дві двері, одна з яких металева з двома циліндричними замками, та наступним кроком буде два методи, знищити болти з секретом щоб

винести сейф у безпечне місце, де продовжити його злам, або розпочати процес злому у приміщенні підприємства. Цього часу повинно вистачити до прибуття на місце співробітників поліції або охорони.

Можливе місце встановлення сейфу необхідно обирати біля стін, щоб зловмисникам було важче дістатися до них.

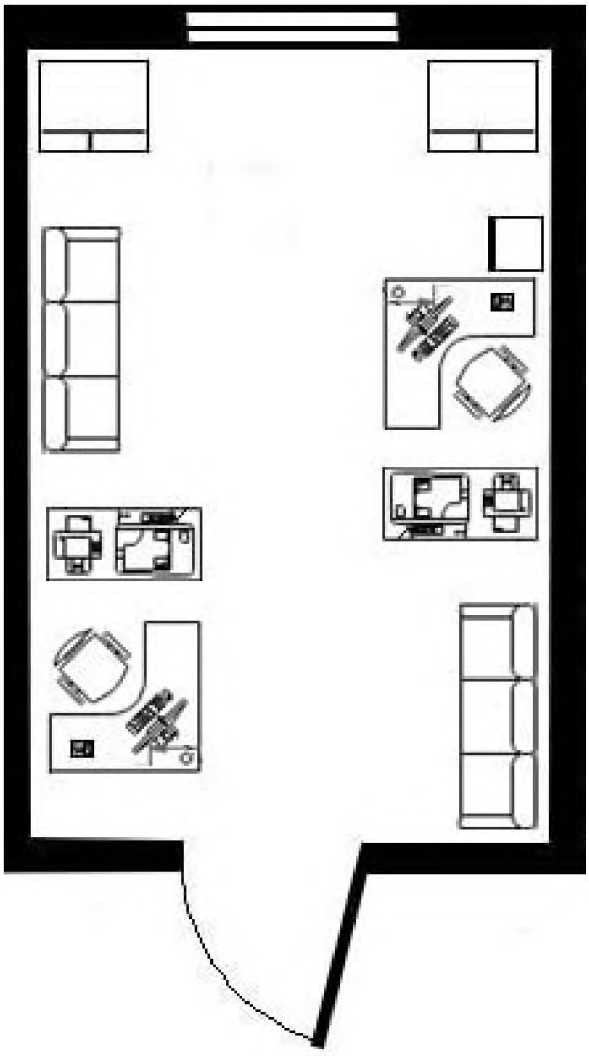

Рисунок 2.3 - Кабінет бухгалтерії з прикладом встановлення сейфу

Необхідність встановлення тривожної кнопки у кабінет бухгалтерії виникає через те, що у робочій час, зловмисник під виглядом клієнта може потрапити до кабінету, та нанести збитки підприємству, для сповіщення офісу необхідно зробити тривожну кнопку у кабінеті. Через те, що підприємство має

вид діяльності з встановленням систем захисту, це все можна зробити силами однієї бригади.

Зловмисники, під прикриттям відвідувачів, або співробітники, які є агентами компаній конкурентів, можуть принести та встановити закладні пристрої, такі як диктофон, міні камера, тощо. Такі пристрої слід виявляти якомога швидше. На підприємстві таких обстежень не проводять.

Для обстеження визначимо відповідальну людину, а саме спеціаліста з питань кібербезпеки підприємства. Він повинен в встановлений час обстежити всі приміщення підприємства на закладні пристрої.

Процес пошуку пристроїв зняття інформації спецслужби на наступні етапи:

1. Вивчення оперативної обстановки біля об'єкту:

- визначення найбільших імовірних місць розташування закладних пристроїв, ретрансляторів, пультів контролю;
- фіксація знайдених людей, машин.

2. Перевірка радіоефіру за межами приміщення:

- розташування пункту контролю радіоефіру;
- складання зайнятості радіоефіру;
- визначення та відокремлення частот радіостанцій;
- проведення статистичного аналізу виявлених частот.

3. Перевірка радіоефіру в місці:

- перенесення пункту контролю радіоефіру у приміщення;
- складання нової карти зайнятості радіоефіру. Карта зайнятості радіоефіру складається при ввімкненій та ввімкненій електриці, при ввімкнених та ввімкнених електроприладах, при опущеній та піднятій телефонній трубці;
- порівняння та аналіз усіх карток зайнятості радіоефіру.

4. Візуальне лікування всіх меблів та інших предметів. За потреби меблі розбираються.

5. Перевірка стіни приміщення радіолокатором.

6. Перевірка електротехніки:

- перевірка індикатором поля та частотоміром;
- приєднання паразитних випромінювання - вмикають джерело акустичного звуку і перевіряють ці випромінювання на наявність модуляції;
- при необхідності виконувати розбирання апаратури.

7. Перевірка лінії (телефонної, електричної):

- у розрив лінії вмикається резистор;
- за допомогою обладнання аналізується сигналу на резисторі;
- аналіз виконуватися на частотах до 30 МГц.

У сучасних реаліях бізнес центру буде важко виконувати фіксацію людей та автомобілів, відсутність ліній телефонного зв'язку полегшить обстеження, але при правильній перевірці приміщень значно знизиться ризик стеження за підприємством[8].

Для вирішення питань з апаратного та програмного захисту інформації необхідно у більшій частині змінити права користувачів, більш детально налаштувати між мережевий екран, налаштувати тимчасові паролі.

У правах користувачів необхідно виключити можливість підключення сторонніх носіїв інформації, а саме флешки, диски та інші. Для цього адміністратор повинен зайти до конфігурацій користувача, обрати необхідних користувачів, в пунктах з'ємні диски обрати критерії заборонити запис, заборонити читання, заборонити виконання. Після цих маніпуляцій, користувачі не зможуть копіювати, переглядати інформації на носіях, записувати туди нову інформацію та запускати програми з носіїв. Дане рішення є простим та необхідним для підвищення захисту інформації на підприємстві.

При необхідності заборонити інші носії інформації за таким самим принципом.

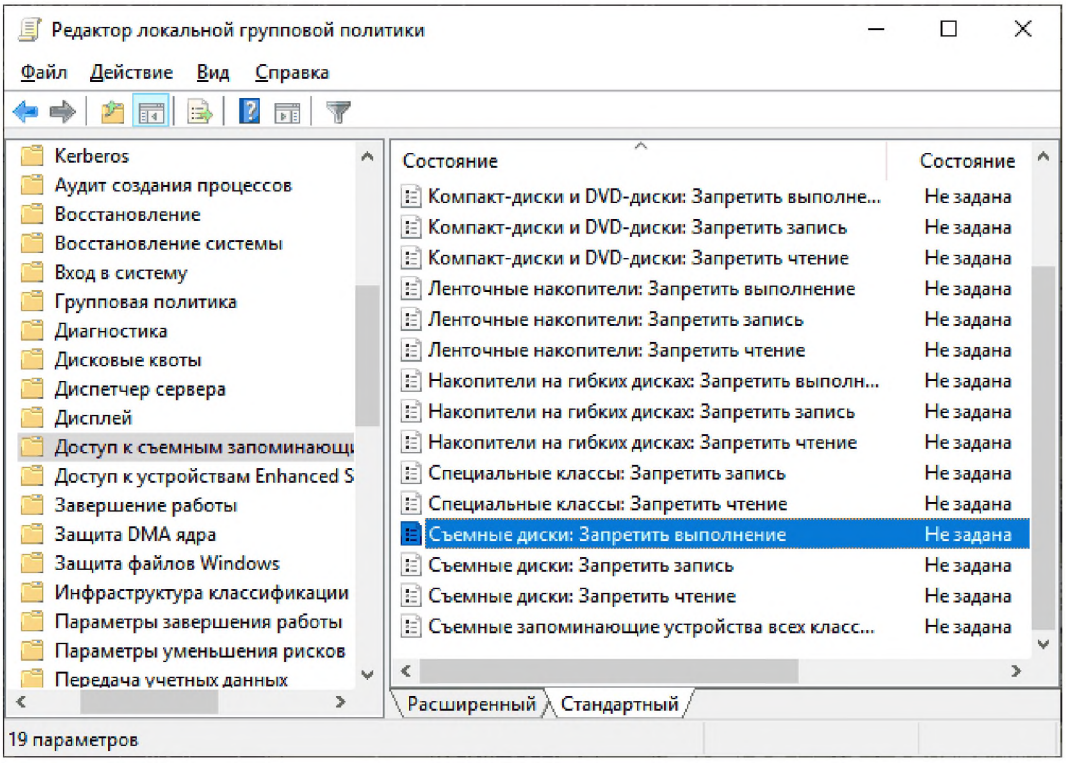

Рисунок 2.4 - Заборона виконання програм зі з‘ємних носіїв

Для налаштування доповненого списку заборонених сайтів необхідно відкрити браунмауєр у режими підвищеного захисту, створити правило для вихідного підключення, з визначеним забороненим ip-адресом для всіх ip-адрес підприємства. При цьому співробітники не зможуть отримувати пакети даних з заборонених сайтів. До цих сайтів можна віднести сайти з троянськими програмами, сайти з забороненим контентом, сайти інформаційної розсилки, сайти копії, тощо. Визначимо список сайтів які при відкритті можуть заразити ПК програмами шпигунами, майнерами, тощо.

Список сайтів, що несуть загрозу ПК:

- 17ebook.com.
- aladel.net.
- bpwhamburgorchardpark.org.
- clicnews.com.
- dfwdiesel.net.
- divineenterprises.net.

- fantasticfilms.ru.
- gardensrestaurantandcatering.com.
- ginedis.com.
- gncr.org.
- hdvideoforums.org.
- hihanin.com;

Список заборонених сайтів можна у глобальній мережі інтернет, також до заборони відвідування необхідно віднести сайти копії, які намагаються виманити данні у неуважних користувачів.

На підприємстві доступ до файлової мережі сервера відбувається наступним чином. Після авторизації користувача шляхом вводу логіну та пароля, йому надається можливість доступу до файлів на сервері, до яких йому необмежений доступ.

Змоделюємо ситуацію, наприклад проетувальник1 покинув місце праці, в цей час проєктувальник 2 заволодів його ПК, зайшов на сервер та змінив певні файли, система фіксує зміни від ПК проєктувальника 1, але в цей час він не володів своїм ПК, після викриття зміни файлів у протоколі дій підозра буде на проетувальника1, у навмисному псуванні файлів підприємства, хоча зловмисником буде проєктувальник 2.

Для запобігання такої моделі загроз необхідно встановити доступ до сервера за особистим паролем кожного користувача, його можна встановити іншим, ніж при авторизації у системі, а можна використовувати такий самий.

Після встановлення пароля на доступ до сервера, співробітники не матимуть доступ до сервера від ПК, які їх не належать.

Це можна зробити за допомогою файлу з розширенням .bat або спеціальним ПЗ, можливе налаштування у самій директиві ОС.

Для доступу за файлом .bat, створюємо текстовий документ з кодом.

```
cls
@ECHO OFF
title Folder Katalog
if EXIST "Privatno" goto DOSTUP
if NOT EXIST Katalog goto RASBLOK
ren Katalog "Privatno"
attrib +h +s "Privatno"
echo Folder locked
goto End
:DOSTUP
echo Vvedite parol, chtoby razblokirovat papku
set/p "pass=>"
if NOT %pass%== 111 goto PAROL
attrib -h -s "Privatno"
ren "Privatno" Katalog
echo Katalog uspeshno razblokirovana
goto End
:PAROL
echo Nevernyj parol
goto end
:RASBLOK
md Katalog
echo Katalog uspeshno sozdana
goto End
:End
```

Рисунок 2.5 - Зміст bat файлу

При першому запуску на сервері створюється папка, в яку необхідно перенести необхідні файли, після чого знову запустити файл. При цьому папка буде запускатися з паролем, який на рисунку 2.5 у червоному квадрату.

Для використання ПЗ необхідно встановити його на сервер, наприклад Lock-A-Folder, програма є безкоштовною та зрозумілою для користувачів, щоб скористатися нею вистачить базового знання ПК.

Рисунок 2.6 - Огляд ПЗ Lock-A-Folder

Відсутність тимчасових паролів підприємства може привести до їх розголошення. Це призведе до витоку інформації підприємства. Паролі співробітників можна змінювати раз на тиждень без оголошення їх наперед. Це можна робити вручну або за спеціальним ПЗ. Встановлювати нові паролі повинен системний адміністратор або спеціаліст з питань кібербезпеки підприємства.

При зміні вручну необхідно оголосити новий пароль користувачеві, це можна зробити на аркуші папера, або у месенджері особисто, без їх оголошення стороннім особам та іншим співробітникам підприємства.

При використанні ПЗ для слідкування паролів рекомендації будуть на ПЗ PassWork, CommonKey. Ці за стосунки є зручними у застосуванні для підприємств, з можливістю встановлення на сервері.

В них можна визначити множину користувачів, привласнити їх особисті паролі, назначити час їх зміни та варіанти їх оголошення.

Зручним методом буде друкування паролів на принтері співробітників безпеки, котрі потім їх доведуть до співробітників.

У разі аварійного відключення від глобальної мережі інтернет, підприємство не зможе у повному масштабі виконувати свою роботу, а це означає втрата доходів. Щоб запобігти таким ризикам слід подбати про

запасний варіант підключення до глобальної мережі. Оскільки найближчий сервер компанії з надання послуг глобальної мережі вже використовує підприємство, другий за віддаленості буде сервер компанії “Київстар”.

Для вирішення організаційних загроз слід донести до співробітників інформацію про закладні пристрої, як вони виглядають, що роблять та дії у разі їх виявлення, як завадити встановленню закладних пристроїв, тощо.

2.7.1 Встановлення та використання ПЗ Folder Lock 7

Програма аналогічна до Lock-A-Folder, або до інших блокувальників вільного доступу.

Необхідно завантажити програму з офіційного сайту за посиланням, https://www.newsoftwares.net/folderlock/, де можна придбати повну версію, або завантажити пробну.

Після завантаження встановити програму на ПК та запустити її.

Рисунок 2.7 - Головне меню програми Folder Lock

При першому запуску створити пароль, який згодом слугуватиме для доступу до захищених файлів.

Рисунок 2.8 - Простір роботи ПЗ Folder Lock

У вікні, що з'явилося, можна розпочинати роботу, а саме за допомогою миші перетягувати файли до за стосунку, створювати групи файлів, встановлювати на них пароль, видаляти пароль з файлів.

За допомогою кнопки "Add" можна обрати файл або папку для встановлення на неї пароля.

Кнопка "Remove" прибирає зі списку зайві файли.

Кнопка "Select All" обирає всі файли зі списку.

Кнопка "Lock" встановлює пароль на обраний файл або групу файлів.

Кнопка "Unlock" прибирає пароль з файлу або групи файлів.

2.7.2 Внутрішня політика безпеки підприємства щодо закладних пристроїв.

Для його розробки на підприємстві необхідно, щоб спеціаліст з питань кібербезпеки провів обстеження всіх приміщень, виявив можливі місця для закладних пристроїв, обстежив можливість стеження за працівниками підприємства з боку клієнтів, тощо.

Після обстеження, написати нормативний документ щодо закладних пристроїв, якими вони бувають, можливе наведення прикладів зображень їх видів, місця де вони можуть встановлюватися, у документі необхідно бути норми поводження з клієнтами, обстеження місця праці, дії у разі знаходження закладних пристроїв.

Оскільки закладні пристрої потрапляють на об'єкт зловмисниками з метою перехоплення інформації, у документі необхідно чітко прописати наступні пункти:

- Співробітник не має права залишати клієнта наодинці у кабінетах підприємства;
- Співробітник не має права оголошувати клієнту інформації, яка не стосується замовлення або технічного завдання клієнта;
- У разі виявлення клієнта у кабінеті в якому він знаходиться один, дочекатися співробітника і полишити їх;
- Не передавати клієнтові документи, або носії інформації які не стосуються інформації про замовлення клієнта;
- Не використовувати носії інформації клієнта;
- Стежити, щоб клієнт не забував особисті речі у кабінеті. У разі їх виявлення віднести на перший поверх до охорони на склад загублених речей.

Що слід робити у разі виявлення закладних пристроїв:

- Уразі виявлення закладних пристроїв негайно повідомити спеціаліста з питань кібербезпеки;

- При виявленні камери стеження, мікрофону або диктофону, не розголошувати інформацію в голос до усунення закладних пристроїв.

Для ознайомлення співробітників слід донести що, закладні пристрої не завжди є набором мікросхем, або не завжди стандартної форми. Наприклад невідома ручка на столі може бути диктофон, яку залишили навмисно для запису розмов, таку ручку можна забрати при наступному відвідуванні підприємства.

Рисунок 2.9 - Ручка диктофон

Для ознайомлення співробітників з можливими закладними пристроями можна використати рисунок 2.9 та рисунок 2.10, за для більшого ознайомлення навести більше прикладів, звичайних побутових речей, які можуть слугувати причиною витоку інформації.

Рисунок 2.10 - Камера відеоспостереження

2.8 Документообіг підприємства

Під час роботи підприємства, у співробітників виникає потреба ознайомитися з певними документами обмеженого доступу, які зберігаються у директора відділу в сейфі або у бухгалтерії. Ці документи є важливими для підприємства, але при цьому за їх пересуванням не стежать документально.

Для вирішення питання загрози витоку інформації необхідно створити документ прийому та передачі актів, документів, тощо. Для цього у місцях їх зберігання необхідно вести журнал, в якому буде вказано, хто, коли, що передає, кількість сторінок, на котрий час, коли повернули документ, кількість сторінок повернутого документу та дату повернення. Цей журнал повинні вести співробітники які відповідають за збереження документів у сейфі, ця процедура полегше пошук документів серед співробітників та у разі витоку інформації буде відомо особа, яка могла її розповсюдити.

2.9 Якісні зміни у моделі загроз

Після вирішення питання модернізації комплексної системи захисту інформації підприємства необхідно порівняти оновлену модель загроз з старою, щоб впевнитися у доцільності прийнятих рішень.

Таблиця 2.15 - Оновлені загрози конфіденційності інформації

№	Механізм реалізації	Рівень		Сума загроз
		ризики	збитки	
К.1	Халатність співробітників підприємства	1	1	2
К.2	Не дотримання чітких правил безпеки під час користування РС	1	1	2
К.3	Копіювання даних для ознайомлення сторонніми особами	1	2	3
К.4	Погана звукоізоляція приміщення	3	2	5
К.5	Не правильні умови зберігання паперових документів в архівах	1	1	2
К.6	Викрадення носіїв ІзОД з метою несанкціонованого ознайомлення сторонніх осіб	1	2	3
К.7	Відсутність опису використання зовнішніх носіїв	1	1	2
К.8	Використання сторонньої інформації з посиланням на авторів	1	1	2

Таблиця 2.16 - Оновлені загрози цілісності інформації

№	Механізм реалізації	Рівень		Сума загроз
		ризики	збитки	
Ц.1	Помилки (ненавмисні) користувачів ІТС, які призвели до модифікації або спотворення інформації на жорсткому диску або зовнішніх носіях	1	2	3
Ц.2	Несанкціонована (навмисне) модифікація або спотворення інформації персоналом ІТС на жорсткому диску або зовнішніх носіях	1	2	3
Ц.3	Відсутність вчасного резервного копіювання	1	1	2
Ц.4	Відсутність вчасного копіювання та зберігання важливих документів	1	2	3
Ц.5	Прояви помилок системного ПЗ, в наслідок яких стала можливою модифікація інформації або її спотворення користувачами	1	1	2
Ц.6	Безпосередній доступ до інформації будь-яким способом сторонніми особами	1	3	4

Продовження таблиці 2.16

Ц.7	Халатність співробітників щодо пропуску сторонніх осіб	1	2	3
Ц.8	Відсутність підтвердження відправника інформації що надходить на обробку	1	1	2

Таблиця 2.17 - Оновлені загрози доступності інформації

№	Механізм реалізації	Рівень		Сума загроз
		ризики	збитки	
Д.1	Помилка користувача, яка призвела до знищенню даних	1	1	2
Д.2	Помилка адміністраторів, яка призвела до віддаленню даних	1	3	4
Д.3	Пошкодження парольних носіїв персоналом ІТС, що призвело до втрати доступу до інформації	1	1	2
Д.4	Прояви помилок системного ПЗ, яке призвело до втрати доступу до інформації або ІТС	1	1	2
Д.5	Прояви помилок системного ПЗ, в наслідок яких стала можливою модифікація інформації або її спотворення користувачами	1	1	2
Д.6	Безпосередній доступ до інформації будь-яким способом сторонніми особами	1	2	3
Д.7	Навмисне видалення або деформація інформації	1	2	3
Д.8	Можливість невчасного оновлення інформації	1	1	2

Таблиця 2.18 - Оновлені загрози спостереженості ІТС

№	Механізм реалізації	Рівень		Сума загроз
		ризики	збитки	
С.1	Помилки (ненавмисні) персоналу ІТС, які призвели до втрати спостереженості	1	1	2
С.2	Помилки (ненавмисні) адміністраторів ІТС, які призвели до втрати спостереженості	1	2	3
С.3	Некоректне налагодження засобів захисту адміністраторами ІТС, яке призвело до втрати спостереженості	1	1	2
С.4	Порушення спостережності користувачами ІТС внаслідок навмисних цілей	1	1	2
С.5	Порушення спостереженості внаслідок пошкодження, у тому числі навмисного, архівів та носіїв з архівами даних	1	3	4
С.6	Прояви помилок системного ПЗ, яке призвело до втрати спостереженості	1	1	2

Продовження таблиці 2.18

С.7	Безпосередній доступ до ІТС будь-яким способом сторонніх осіб	1	2	3
С.8	Можливе спостереження співробітниками охорони	1	1	2

Таблиця 2.19 - Оновлена узагальнена таблиця загроз ІТС

№	Види загроз	1	2	3	4	5	6	7	8	Сума загроз
1	Конфіденційності	2	2	3	5	2	3	2	2	21
2	Спостереженості	2	3	2	2	4	2	3	2	20
3	Доступності	2	4	2	2	2	3	3	2	20
4	Цілісності	3	3	2	3	2	4	3	2	22

Для порівняння проведемо підсумки. З урахуванням змін, співробітники не можуть копіювати данні підприємства на особисті носії, а це означає, що значно ускладнився рівень розповсюдження інформації співробітниками підприємства. При більш частому оновленні резервних копій, ціна похибки копіювання або оновлення інформації з помилковим залишанням контактів постачальник знизилася. Знизився ризик ненавмисного псування інформації користувачами підприємства, та у разі псування можлива відміна дії у реєстрі подій, або завантаження старої копії файлу. Резервне копіювання системи стало значно частішим. Співробітники ознайомлені з поводженням зі сторонніми особами, та як завадити встановленню закладних пристроїв. При цьому спеціаліст з питань кібербезпеки підприємства тепер вчасно перевіряє кабінети на закладні пристрої. Пошкодження парольних носіїв персоналом ІТС, що призвело до втрати доступу до інформації не є високою загрозою, оскільки пароль можна змінити за зверненням до системного адміністратора.

При порівнянні суми загроз, слід враховувати наступні показники:

- Від 0 до 3 балів зміни несуттєві;
- Від 4 до 6 балів зміни задовільні для модернізації;
- Від 7 до 10 балів зміни задовільні для модернізації та оновлення;

- Від 10 та більше балів зміни задовільні для модернізації, оновлення та перетворень.

Таблиця 2.20 - Порівняння суми балів до внесення змін у КСЗІ та після

№	Види загроз	Сума загроз до оновлення	Сума загроз після оновлення
1	Конфіденційності	32	21
2	Спостереженості	30	20
3	Доступності	28	20
4	Цілісності	34	22

Виходячи з даних, отриманих з таблиці 2.20, бачимо зміни від 8 до 12 балів у кожному пункті, це задовільно для модернізації і часткового оновлення комплексної системи захисту інформації.

2.10 Висновки

У другому розділі проведено додаткове обстеження підприємства, створена модель порушника, модель загроз, проаналізовано профіль захищеності, визначені програми захисту інформації та інструкції до них, виявлено слабкі місця захисту підприємства та наведена інформація щодо їх можливого усунення, порівняні оновлені загрози зі старими.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою розділу є визначення економічної доцільності розробки нових та вдосконалення вже існуючих засобів захисту інформації на підприємстві для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації. Для досягнення цієї мети необхідно здійснити розрахунок капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення; річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування; річного економічного ефекту; показників економічної ефективності розробки та впровадження запропонованих рішень.

3.1 Розрахунок (фіксованих) капітальних витрат

До капітальних витрат належать витрати на розробку заходів із забезпечення інформаційної безпеки, а також витрати на придбання матеріальних та нематеріальних активів.

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

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

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів;

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

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів;

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

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

3.1.1. Визначення витрат на розробку засобів захисту інформації на підприємстві для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації

3.1.1.1 Визначення трудомісткості розробки засобів захисту інформації на підприємстві для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації

Трудомісткість розробки визначається тривалістю кожної робочої операції:

$$t = t_{тз} + t_в + t_а + t_р + t_д, \text{ годин,} \quad (3.2)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку засобів захисту інформації на підприємстві, $t_{тз}=12$;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в=24$;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а=20$;

$t_р$ – тривалість розробки засобів захисту інформації на підприємстві, $t_м=30$;

$t_д$ – тривалість підготовки технічної документації, $t_д=8$.

Отже,

$$t = 12+24+20+30+8 = 94 \text{ годин.} \quad (3.3)$$

3.1.1.2 Розрахунок витрат на розробку засобів захисту інформації на підприємстві

Витрати на розробку заходів безпеки Кпз складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки *Ззп* і вартості витрат машинного часу *Змч*:

$$К_{пз} = З_{зп} + З_{мч} = 22560 + 758,58 = 23318,58 \text{ грн.} \quad (3.4)$$

$$З_{зп} = t\, З_{пр} = 94*240 = 22560 \text{ грн.} \quad (3.5)$$

де t – загальна тривалість операцій, годин;

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

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t*С_{мч} = 94*12 = 758,58 \text{ грн.} \quad (3.6)$$

де t – трудомісткість операцій із побудови ефективної системи доступу персоналу, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = 0,5 \cdot 6 \cdot 2,1 + \frac{5900 \cdot 0,3}{1920} + \frac{5500 \cdot 0,3}{1920} = 8,07 \text{ грн.} \quad (3.7)$$

Відповідно до поставлених задач в контексті розробки засобів захисту інформації на підприємстві для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації необхідне придбання наступних матеріальних активів:

Таблиця 3.1 – Вартість матеріальних активів для розробки засобів захисту інформації на підприємстві

Матеріальний актив	Кількість	Ціна, грн.	Вартість, грн.
Сейф та встановлення	1	6800	6800
Тривожна кнопка	2	340	680
Wi-fi роутер	2	600	1200
Додатковий постачальник глобальної мережі	1	2400	2400
Разом:			11080

Заплановані витрати на налагодження системи інформаційної безпеки в розмірі 2500 грн. ($К_н$=2500 грн.)

Отже, капітальні (фіксовані) витрати на розробку засобів захисту інформації на підприємстві для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі складуть:

$$К = 2700+ 5500+23318,58 + 11080 + 2500 = 45098,58 \text{ грн.} \quad (3.8)$$

3.1.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad \text{грн.} \quad (3.9)$$

де $С_в$ - вартість відновлення й модернізації системи;

$С_к$ - витрати на керування системою в цілому;

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

Витрати на відновлення та модернізації системи прописані у статуті підприємства і складають 15% від вартості системи, з урахуванням зміни цін

та типів модернізації або ремонту підприємство має фонд у розмірі 12000 гривень($С_в$=12000 грн).

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

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.} \quad (3.10)$$

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

$$С_з = З_{осн} + З_{дод}, \text{ грн.} \quad (3.11)$$

Річні амортизаційні відрахування матеріальних активів, які відповідно до чинного законодавства України підлягають амортизації, визначатимуться, виходячи зі строку корисного використання 5 років. Сума амортизаційних відрахувань визначається за прямолінійним методом нарахування амортизації. Таким чином, річні амортизаційні відрахування складуть

$$С_а = (6800+680+1200) / 5 = 1736 \text{ грн.} \quad (3.12)$$

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

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 25000 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо реалізації засобів захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$$С_з = (25000*12 + 25000*12*0,1)*0,25= 82500 \text{ грн.} \quad (3.13)$$

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$$С_{єв} = 82500 * 0,22 = 18150 \text{ грн.} \quad (3.14)$$

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

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.}, \quad (3.15)$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,8 кВт);

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

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 2,1 грн./кВт за годину).

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

$$С_{ел} = 0,8*1920*2,1 = 3225,6 \text{ грн.} \quad (3.16)$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 2%:

$$С_{тос} = 45098,58 * 0,02 = 901,98 \text{ грн.} \quad (3.17)$$

Таким чином, витрати на керування системою інформаційної безпеки ($С_к$) становлять:

$$С_к = 1736 + 82500 + 18150 + 3225,6 + 901,98 = 103610,58 \text{ грн.} \quad (3.18)$$

Витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) не виникають.

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = 103610,58 \text{ грн.} \quad (3.19)$$

3.2 Оцінка можливого збитку

3.2.1 Оцінка величини збитку

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

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 3 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 25000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 15000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 2 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 11 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 890 тис. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 4000 грн;

І – число атакованих сегментів корпоративної мережі, 6;

N – середнє число атак на рік, 9.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V, \quad (3.20)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, 3900 грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), 1200 грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, 5000 грн.

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

$$П_П = \frac{\sum Зс}{F} \cdot t_n = \frac{15000 \cdot 11}{176} \cdot 4 = 3750 \text{ грн}, \quad (3.21)$$

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

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

$$П_в = П_{ви} + П_{пв} + П_{зч}, \quad (3.22)$$

де $П_{ви}$ – витрати на повторне уведення інформації, 300 грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, 900 грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин,1700 грн.

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

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{15000 \cdot 11}{176} \cdot 3 = 2812{,}5 \text{ грн.} \quad (3.23)$$

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

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в = \frac{25000 \cdot 2}{176} \cdot 2 = 568{,}18 \text{ грн.} \quad (3.24)$$

Витрати на заміни встаткування або запасних частин можуть скласти 4000 грн.

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

$$П_в = 2812{,}5 + 568{,}18 + 4000 = 7380{,}68 \text{ грн.} \quad (3.25)$$

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

$$V = \frac{О}{Fг} \cdot (t_П + t_В + t_{ВИ}) \quad (3.26)$$

$$V = \frac{890000}{2080} \cdot (4+2+3) = 3850{,}96 \text{ грн.} \quad (3.27)$$

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

$$U = 3750 + 7380{,}68 + 3850{,}96 = 14981{,}64 \text{ грн.} \quad (3.28)$$

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

$$B = \sum_i \sum_n U = \sum_6 \sum_9 14981{,}64 = 262178{,}7 \text{ грн.} \quad (3.29)$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \text{ грн.}, \quad (3.30)$$

де B – загальний збиток від атаки у разі перехоплення інформації, 262178,7 тис. грн.;

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

С – щорічні витрати на експлуатацію системи інформаційної безпеки, 103610,58 тис. грн.

Загальний ефект від впровадження системи інформаційної безпеки становитиме:

$$E = 262178{,}7 * 0{,}5 - 103610{,}58 = 27478{,}77 \text{ грн.} \quad (3.31)$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

За методикою сукупної вартості володіння (ТСО) визначають такі показники економічної ефективності системи інформаційної безпеки як Коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій (T_o).

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

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,} \tag{3.32}$$

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

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

Коефіцієнт повернення інвестицій ROSI складе:

$$ROSI = \frac{27478,77}{45098,58} = 0,6, \quad \text{частки одиниці,} \tag{3.33}$$

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

$$ROSI > (N_{деп} - N_{інф})/100), \tag{3.34}$$

де $N_{деп}$ – річна депозитна ставка, (6 %);

$N_{інф}$ – річний рівень інфляції, (5,5 %).

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,6 > (6–5,5)/100 = 0,6 > 0,005. \tag{3.35}$$

Отже, запропоновані засоби захисту інформації на підприємстві для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації можна вважати економічно доцільними.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки. Відповідно термін окупності розробки засобів підвищення ефективності системи захисту інформації провайдера доступу до мережі Інтернет складе:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{0,6} = 1,6, \quad \text{років (19 місяців).} \qquad (3.36)$$

3.4 Висновок

Запропоновані засоби захисту інформації на підприємстві для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації можна вважати економічно доцільними, оскільки значення коефіцієнту повернення інвестицій ROSI, що складає 0,6 при величині економічного ефекту 27478,77 грн. Отримане значення коефіцієнта ROSI перевищує дохідність альтернативного вкладення коштів. Термін окупності при цьому складатиме 1,6 років (біля 19 місяців). Капітальні витрати на засоби захисту інформації складуть в 45098,58 грн., а щорічні експлуатаційні витрати – 103610,58 грн.

ВИСНОВКИ

Метою кваліфікаційної роботи було підвищити рівень захисту інформації у комплексній системі захисту інформації підприємства ТОВ “Авалон” шляхом модернізації програмного та апаратного захисту, організаційних процесів.

Для вирішення питання захисту інформації, необхідно провести модернізацію комплексної системи захисту, для цього провели обстеження офісу підприємства, його особистого складу, програмного та апаратного комплекту підприємства.

Після проведення обстеження, створили модель загроз та порушника, яка визначає найбільш вразливі місця компанії. При цьому визначено суму загроз з кожного фактору захисту інформації.

Приведені можливі механізми захисту інформації на підприємстві, інструкції їх встановлення та користування для користувачів та співробітників відділу захисту, а саме, встановили окремий сейф для кабінету бухгалтерії, ознайомили співробітників з закладними пристроями та можливими місцями їх встановлення, навчили відповідально ставитися до безпеки у робочій час, запровадили тимчасові паролі, обстеження приміщень на закладні пристрої, налаштували мережевий екран, розмежували обов’язки адміністраторів системи, позбавили можливості самостійного запису інформації на носії, зробили доступ до архівів через унікальний пароль співробітника.

Після модернізації перевірили рівень загроз та встановили доцільність використання нових методів захисту.

Провели підрахунки трудомісткості розробки системи, її доцільність, амортизаційні якості, експлуатаційні витрати. Термін окупності даних засобів складе 19 місяців.

ПЕРЕЛІК ПОСИЛАНЬ

1 Стаття. Технічний захист інформації.. https://tzi.ua/ua/tehnchnij_zahist_nformac.html

2 Стаття. Організаційні методи захисту інформації. https://tzi.ua/ua/organzacjn_metodi_zahistu_nformac.html

3 Стаття. Засоби і методи захисту інформації. https://buklib.net/books/28625/

4 Нормативний документ. Технічний захист інформації, термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99. https://tzi.ua/assets/files/1.1_003_99.pdf

5 Нормативний документ. Технічний захист інформації. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf

6 Стаття. Шифрування. https://uk.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F

7 Стаття. Шифр RSA. https://uk.wikipedia.org/wiki/RSA

8 Стаття. Закладні пристрої. https://sirius.kiev.ua/zakladni-pristroyi

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	26	
6	А4	2 Розділ	42	
7	А4	3 Розділ	12	
8	А4	Висновки	1	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК
на кваліфікаційну роботу бакалавра на тему:
Розробка підсистеми захисту інформації інформаційно-комунікаційної системи ТОВ "Авалон"
ст. гр. 125-19ск-1 Хуторного Олександра Сергійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __ джерел та __ додатка.

Об'єкт дослідження: система захисту інформації підприємства ТОВ "Авалон".

Мета кваліфікаційної роботи: підвищення рівня захисту інформації підприємства, шляхом модернізації програмного та апаратного захисту, організаційних процесів.

У першому розділі дослідили підприємство, а саме персонал та його обов'язки, робочі станції підприємства, приміщення у якому знаходиться контрольована зона, схема мережі підприємства, інформаційні потоки на підприємстві та огляд програмного забезпечення підприємства.

У другому розділі визначили модель порушника, можливі загрози та ризики для підприємства, опис профілю захищеності 3.КЦД.1, проаналізували основні методи захисту, обирали програмне забезпечення для захисту інформації, обстежили систему захисту на недоліки та реалізували нові методи захисту.

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

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

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

Керівник