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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Чорного Дмитра Віталійовича*

академічної групи *125-19ск-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ "LIL GROUP"*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доцент Сафаров О. О.	90		
розділів:				
спеціальний	ст. викл. Войцех С. І.	87		
економічний	доцент Пілова Д. П.	90		

Рецензент		92		

Нормоконтролер	ст. викл. Тимофєєв Д. С.			

Дніпро
2022

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

«_____»_____2022 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Чорному Дмитру Віталійовичу* **академічної групи** *125-19ск-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації _____

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ "LIL GROUP"*

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

Розділ	Зміст	Термін виконання
Розділ 1	Загальний аналіз діяльності підприємства та нормативно правових документів, актуальність питання	07.05.2022
Розділ 2	Технічне обстеження, аналіз інформаційної системи підприємства, моделі порушника та моделі загроз	18.06.2022
Розділ 3	Економічна частина, розрахунки на реалізацію проекту	30.05.2022

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

Дата видачі завдання: 08.03.2022

Дата подання до екзаменаційної комісії: 15.06.2022

Прийнято до виконання _____ **Чорний Д.В.**
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 87 с., 15 рис., 28 табл., 4 додатка, 22 джерел.

Об'єкт дослідження: Інформаційно-телекомунікаційна система ТОВ «LIL GROUP»

Мета кваліфікаційної роботи: Підвищення рівня захисту інформації в інформаційно-телекомунікаційній системі ТОВ «LIL GROUP», розробка механізмів захисту в сфері інформаційної безпеки організації, розрахунок витрат на реалізацію проекту.

Методи розробки: спостереження, обстеження, аналіз, опис та розрахунки.

Робота містить 3 розділи і 18 підрозділів.

У першому розділі виконано обстеження підприємства, проаналізовано роботу співробітників їх обов'язків, вказано перелік програмного забезпечення та обладнання підприємства, було сформульовано висновки щодо результатів аналізу нормативно-правової бази.

У спеціальній частині проведено додатковий аналіз підприємства, розглянуто модель порушника, модель загроз, виявлено співробітників які становлять найбільшу загрозу підприємству визначено методи, засоби захисту інформації на об'єкті інформаційної діяльності та було проведено висновки щодо виконаної роботи.

У економічному розділі проведені розрахунки на доцільність впровадження КСЗІ, прорахунок поточних та капітальних витрат загального збитку від Ddos-атак на ІТС, рекомендації для зниження витрат від впровадження на ОІД.

Практичне значення роботи полягає у дослідженні та підвищенні рівня захищеності інформації в інформаційно-телекомунікаційній системі ТОВ «LIL GROUP».

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, РОЗРАХУНКИ

ABSTRACT

Explanatory note: 87 pp., 15 pic., 28 table, 4 app, 22 sources.

Object of the study: the information field of the commercial structure of LLC «LIL GROUP»

Purpose of qualification work: To increase the level of information protection in the information and telecommunications system of LIL GROUP LLC, development of protection mechanisms in the field of information security of the organization, calculation of costs for the implementation of the project.

Methods of development: observation, survey, analysis, description and calculation.

The work consists of 3 sections and 18 subsections.

In the first section a survey of the enterprise was conducted, the work of employees from the performance of their duties was analyzed, a list of software and equipment of the enterprise was specified, conclusions from the analysis of the regulatory framework were formulated.

In the special part additional analysis of the enterprise was conducted, the offender model, the threat model was considered, the employees posing the greatest threat to the enterprise were identified, the methods, means of protection of information at the object of information activity were determined and conclusions about the work done were drawn.

The economic section made calculations on the feasibility of implementing a CISS, calculation of current and capital costs of total losses from Ddos-attacks on ITS, recommendations for reducing the cost of implementation on the subject of IA.

The practical significance of the work lies in the study and improvement of the level of information security in the information and telecommunications system of LLC "LIL GROUP".

INTEGRATED INFORMATION SECURITY SYSTEM, THREAT MODEL, OFFENDER MODEL, INFORMATION SECURITY, CYBERSECURITY, INFORMATION AND TELECOMMUNICATIONS SYSTEM, CALCULATIONS

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

АТС – автоматична телефонна станція;

ДТЗС – допоміжні технічні засоби та системи;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

АС – автоматизована система;

ІТ – інформаційні технології;

ІС – інформаційна система;

ІТС – інформаційно-телекомунікаційна система;

ІЗоД – інформація з обмеженим доступом;

ІР – інформаційні ресурси;

КСЗІ – комплексна система захисту інформації;

КЗЗ – комплекс засобів захисту;

КС – комп’ютерна система;

НСД – несанкціонований доступ;

ОС – обчислювальна система;

ОІД – об’єкт інформаційної діяльності;

ПЗ – програмне забезпечення;

ПЗП – постійний запам’ятовуючий пристрій;

ПКП - приймально контрольний пункт;

ТОВ – товариство з обмеженою відповідальністю;

ЗМІСТ

с.

ВСТУП 8

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ 9
1.1 Актуальність питання 9
1.2 Аналіз об'єкту дослідження «LIL GROUP» 12
1.3 Аналіз нормативно правової бази підприємства 14
1.4 Об'єкт інформаційної діяльності підприємства 15
1.5 Інформаційні потоки підприємства 30
1.6 Висновки 36

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА 37
2.1 Аналіз основних методів захисту інформації в ІКС 37
2.2 Модель загроз і порушника 39
2.3 Класифікація АС. Аналіз профілю захищеності 51
2.4 Програмне забезпечення для захисту інформації 57
2.5 Аналіз недоліків системи захисту підприємства 60
2.6 Особливості реалізації та вдосконалення існуючих методів та систем захисту інформації 61
2.7 Політика безпеки підприємства 63
2.8 Висновок 65

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ 66
3.1 Розрахунок (фіксованих) капітальних витрат 66
3.2 Оцінка можливого збитку 73
3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки 77
3.4 Висновок 78

ВИСНОВКИ 79
ПЕРЕЛІК ПОСИЛАНЬ 80
ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи 83
ДОДАТОК Б. Перелік документів на оптичному носії 84
ДОДАТОК В. Відгук керівника економічного розділу 85
ДОДАТОК Г. Відгук керівника кваліфікаційної роботи 86

ВСТУП

Вже сьогодні однією з найважливіших завдань є підтримка достатнього рівня безпеки інформації на підприємстві. Через те, що ІТ галузь душе стрімко розвивається та абсолютна більшість підприємств використовують ІТС, у цій сфері з'являється все більше спеціалістів, а з ними і можливих зловмисників.

Для підприємства і для його клієнтів періодичне оновлення (вдосконалення) комплексної системи безпеки інформації необхідне і вигідне
через те, що викрадення, знищення, модифікація або оприлюднення приватної інформації може завдати великих фінансових та репутаційних збитків для компанії та її клієнтів.

Майже кожна держава має свої органи з питань забезпечення безпеки інформації. Вони розробляють стандарти, закони та правила, які покращують життєдіяльність підприємств, суспільства та інших галузей які можуть впливати на життєдіяльність держави та її ресурсів.

Кожного року кількість нових підприємств у цифровому просторі збільшується та розвиваються. Одне з цих підприємств це «LIL GROUP» яке постійно розвивається та створює нові гілки у своїй діяльності. Зі зростанням цих гілок та підвищенням впливів на ринку з'являються конкуренти, впроваджується нове програмне забезпечення, обладнання та технологічні рішення. З цим зростає ризик перехоплення конфіденційної інформації яка може вплинути на подальший розвиток та нанести суттєві збитки для компанії.

Для того щоб цього уникнути, використовують комплексні системи захисту інформації – сукупність організаційних і інженерних заходів програмно-апаратних засобів, які забезпечують захист інформації в ІТС.

В кваліфікаційній роботі розглянуто підприємство «LIL GROUP», його фізичну та інформаційну структуру.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Актуальність питання

На сьогоднішній день технології можуть дозволити створювати, зберігати, оброблювати та передавати інформацію без використання переносних носіїв інформації, таких як папери, флеш накопичувачі та тому подібні. Для цих маніпуляцій необхідно мати комп'ютер та підключення до глобальної мережі.

Майже кожна людина, тим паче підприємство, на сьогоднішній день використовує інформаційні системи та технології полегшення спілкування, умов праці, виробництва.

У користувачів інформація буває дуже різною, але у підприємстві може циркулювати конфіденційна та службова інформація, яку потрібно оберігати від копіювання, видалення, повторення, викрадення або передачі третім особам.

Для захисту інформації підприємства можливе використання програмних, технічних, організаційних та інженерних методів.

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

Інформація циркулює тільки в електромагнітному (електричному, магнітному), акустичному та матеріальному вигляді.

По фізичній природі носієм інформації можуть бути:

- світло - електромагнітні хвилі оптичного діапазону;
- акустичні (звукові) хвилі;
- електромагнітні хвилі;
- електричні сигнали у провідниках;
- матеріальний носій інформації.

Інших можливостей для переносу інформації не існує.

Класифікувати шляхи витоку інформації від джерела до зловмисника (канали витоку) можна по фізичній природі носія:

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

Відповідно до ДСТУ 3396.2-97 (Захист інформації. Технічний захист інформації. Терміни та визначення) - технічний захист інформації (ТЗІ) – це діяльність, спрямована на запобігання порушенню цілісності, блокуванню та (чи) витоку інформації технічними каналами.

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 відноситься 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).

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. Найбільша увага організаційним заходам приділяється при вирішенні питань побудови та організації функціонування комплексної системи захисту інформації.

До методів і засобів організаційного захисту інформації відносяться організаційно-технічні й організаційно-правові заходи, які проводяться в процесі створення й експлуатації системи для забезпечення захисту інформації. Ці заходи повинні проводитися при будівництві або ремонті приміщень, у яких буде розміщатися системи; проектуванні системи, монтажі й налагодженню її технічних і програмних засобів; випробуваннях і перевірці працездатності системи.

Основні призначення методів і засобів організаційного захисту:

– обмеження фізичного доступу до об'єктів захисту та реалізація режимних заходів;

– розмежування доступу до інформаційних ресурсів і процесів (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;

– проведення візуального огляду приміщення до наради та після на предмет виявлення закладних пристроїв;

– обмеження кількості осіб у конфіденційних переговорах;

– заборона на вхід сторонніх осіб під час проведення наради;

– обов'язковість присутності працівника служби безпеки при будь-яких роботах в кімнаті - прибирання , ремонт побутової техніки, невеликий косметичний ремонт тощо;

– між нарадами кімната для переговорів повинна бути закрита і опечатана відповідальною особою;

– обов’язкова профілактика щодо зараження комп'ютерними вірусами.

1.2. Аналіз об’єкту дослідження «LIL GROUP»

Підприємство «LIL GROUP» займається продажом цифрових товарів для користувачів, надання послуг з оренди серверів, аж-адрес та розробка програмного ПЗ під замовлення для невеликих за обсягом компаній. Організація почала вести власну діяльність з 2019 року. За 3 роки ведення діяльності було зроблено багато відгалужене для розширення спектру послуг, приблизно 20-30 проектів в сфері інформаційних технологій. Адреса головного офісу: м. Дніпро, вулиця Шевченка, 17.

Працівники являють собою невід’ємну частину для кожного підприємства, для реалізації певних проектів, продукції тощо. Нижче показано таблицю про загальний обсяг робітників даного підприємства.

Таблиця 1.1. – Штат працівників підприємства

Посада	Кількість працівників на посаді	Рівень кваліфікації
Директор	1	Високо-кваліфіковані робітники
Системний адміністратор	1	Кваліфіковані робітники
Програміст	3	Високо-кваліфіковані робітники
Бухгалтер	1	Високо-кваліфіковані робітники
Менеджер	1	Кваліфіковані робітники
Служба підтримки	2	Кваліфіковані робітники

Головним на підприємстві є директор. У його повноваження входить керування відділами підприємства, коригування робочих планів, надання відпусток працівникам, прийняття нового персоналу на роботу, внесення рішень до зміни елементів офісу або підприємства, розподіл фінансів на закупівлю розхідних матеріалів, контроль за виконанням планів та графіків, регулярне проведення співбесід із співробітниками (два рази на місяць).

Спеціаліст з питань кібербезпеки підприємства повинен стежити за інформаційною безпекою підприємства, аналізувати трафік співробітників протягом робочого часу.

Системний адміністратор повинен стежити за станом обладнання офісу, вчасним його обслуговуванням, оновленням систем та програмного забезпечення.

Бухгалтер повинен вчасно робити податкові відомості, створювати щомісячні звіти підприємства, визначати заробітну плату згідно процентної ставки співробітників, проводити аудити з керівництвом щодо зміни цін певних послуг підприємства.

Головний менеджер шукає нових клієнтів, проводить аудит з керівництвом щодо закупівлі реклами.

Співробітники в службі підтримки спілкуються з постійними клієнтами, дистанційно вирішують питання про можливі рішення щодо певних збоїв, передають інформацію до голови технічного відділу.

Програміст 1 – виконує замовлення керівництва та генерального менеджера для створення ПЗ. Слідкує за вже створеним ПЗ. Відповідає за технічну складову магазину.

Програміст 2 – слідкує за роботою відділу видачі віртуальних серверів та виконує замовлення по оновленню устаткування.

Програміст 3 – слідкує за роботою відділу видачі ір-адрес (проксі) та доменів та виконує замовлення по оновленню устаткування.

Більш детально структура підприємства представлена на рисунку 1.1.

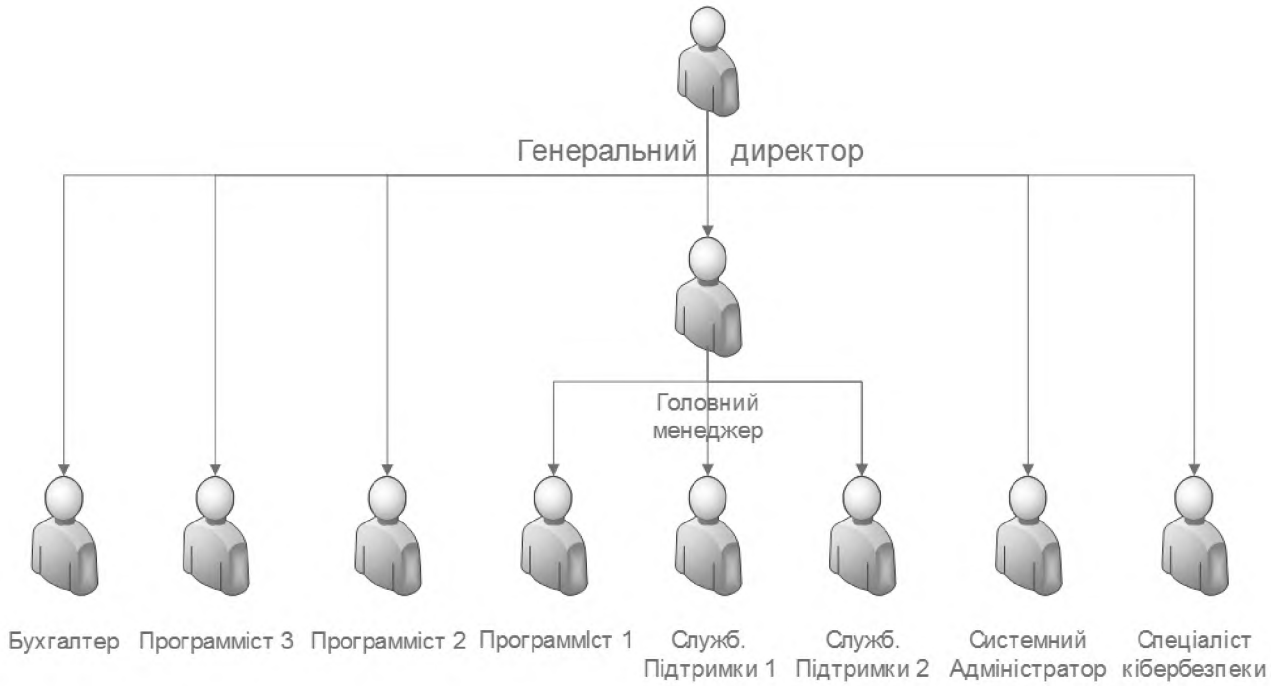


Рисунок 1.1. Структура підприємства

Будь-яка компанія потребує певного переліку документів, котрі будуть затвердженні державним законодавством, впливають на керування діяльністю організації.

Обстежено нормативно-правову базу підприємства, проведено аналіз нормативних документів, зроблено висновки стосовно необхідності КСЗІ для даної організації.

1.3 Аналіз нормативно правової бази підприємства

Згідно із ДСТУ 2732:2004 НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ «ДІЛОВОДСТВО Й АРХІВНА СПРАВА. ТЕРМІНИ ТА ВИЗНАЧЕННЯ»

«Нормативно-правова база – це обґрунтування на державному рівні діяльності будь-якого підприємства, незалежно від форми власності, сфери діяльності та масштабу. Діяльність всіх організацій / підприємств / установ завжди спирається на законодавство країни та на нормативні акти, які регулюють діяльність в певній сфері».

Можна сказати, що нормативно-правова база з точки зору діяльності підприємства передбачає наявність певного переліку нормативних документів.

Обсяг та перелік даних документів залежить від сфери діяльності організації, галузі розробки продукції компанії, нормативної поведінки в залежності від встановлених державних законів тощо.

Для ознайомлення з сферою діяльністю підприємства розглянуто та досліджено перелік документів, які складають нормативно-правову базу підприємства:

- Журнал обліку пожежної безпеки;
- Журнал обліку технічної безпеки;
- Трудовий договір;
- Договір медичного страхування;
- Документ, що свідчить про комерційну таємницю підприємства.

1.4 Об’єкт інформаційної діяльності підприємства

Акт обстеження представляє собою документ аналітичного характеру, де описана інформація про ІТС підприємства. Документ можна розподілити на декілька етапів:

1. Обстеження об’єктів фізичного характеру;
2. Аналіз програмно-апаратних ресурсів ІТС;
3. Дослідження профілю захищеності ІТС;

Обстеження об’єктів фізичного характеру – це аналіз роботи захисних механізмів До таких об’єктів відноситься: аналіз замків дверей та магнітного замку, якість встановлення обладнання, правильність під’єднання до систем безпеки.

Об’єктом інформаційної діяльності (ОІД) є приміщення товариства з обмеженою відповідальністю «LIL GROUP». Область діяльності – створення програмних продуктів.

ОІД знаходиться за адресою: м. Дніпро, Дніпропетровська область, вулиця Шевченка, 17. Будівля, в якій знаходиться ОІД, має чотири поверхи. Несучі стіни зроблені з білої цегли. Перекриття зроблені з використанням залізобетонних плит.

Дах будівлі виконаний з металочерепиці, який є стійким до вогню і має клас А по вогнестійкості. Не горить, не підтримує горіння. Матеріал також стійкий до сильних поривів вітру, не гниє, не покривається мохом і не псується грибком. Вікна металопластикові.

На першому поверсі є охоронець, який відповідає за доступ людей до приміщень та доступ авто на стоянку. З головного входу можна потрапити на будь який поверх через сходи, які розміщені зліва від охорони. Охорона у будинку цілодобова, оскільки вона відповідає 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 відвідуючих за допомогою відеоспостереження
- У неробочій час будівля є закритою, охорона слідкує за допуском до парковки та будівлі лише за перепустками. Будівля має нічне відеоспостереження, освітлення, сигналізацію, датчики руху

Режим КЗ забезпечується таким чином:

- У робочій час вхід у приміщення допускається усьому персоналу після відкриванням дверей директором або менеджером підприємства, які мають ключі від вхідних дверей офісу.
- У неробочий час офіс ставиться під охорону централізовано систем сигналізації з 19:00 вечора до 10:00 ранку зачиняються на 2 циліндричні замки під ключ.

Контрольована Зона (КЗ) – обмежена зовнішніми стінами будівлі, коридором та іншими офісними приміщеннями. Вхідні двері металічні з замками (циліндричними), датчиком відкриття дверей та замком з електронним доступом (через картку перепустку).

До будівлі проведено електро і водопостачання.

Лінії системи опалення проходять під землею до підвалу будівлі, де потім розмежуються 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.

Генеральний план ОІД та Ситуаційний план представлені на рис. 1.3 та рис. 1.4.

Навколо будівлі, де знаходиться ОІД, розміщені такі об'єкти: на півдні знаходиться 4-х поверховий Дніпровський ліцей інформаційних технологій, на півночі знаходиться 6-ти поверхова житлова споруда з 4-ма місцями для парковки та 20 поверховий житловий комплекс IQ House, на сході 3-х поверховий Дніпровський художній музей з хоз. корпусом та 3-х поверхова житлова споруда, на заході 3-х поверхова житлова споруда, 10-ти поверхова житлова споруда та 9-ти поверхова житлова споруда, на північно-східній стороні розташований 4-х поверховий фаховий коледж зварювання та електроніки ім. Є.О. Патона.

Рисунок 1.2. Місцезнаходження офісу «LIL GROUP» на мапі

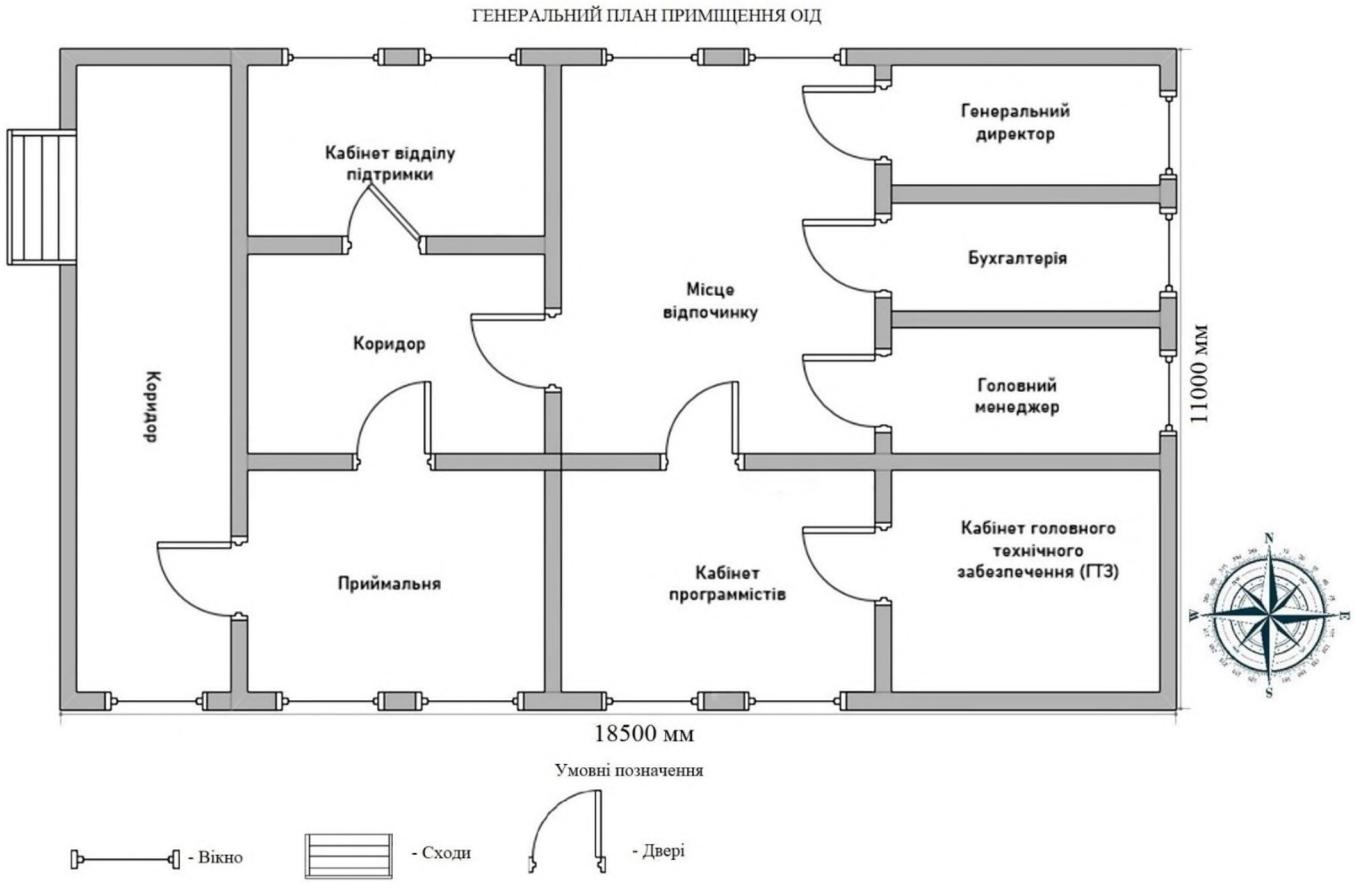


Рисунок 1.3. План приміщення ОІД

Вікна металопластикові, одностворчасті. На кожному вікні встановлені жалюзі.

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

Вимикачі системи освітлення, які підключені до щитової підприємства, далі підключені до поверхового щита.

Система охоронно-пожежної сигналізації – спроектована та встановлена під замовлення, вона підключена до системи охорони і може працювати дистанційно.

Система вентиляції, яка проведена до кожного приміщення – приточно-витяжна з кондиціонером, яка може як охолоджувати, так і підігрівати повітря в залежності від температури кімнати. Два режими роботи - замкнутого забору повітря та відкритого.

Система опалення у кожному приміщенні – біметалічні радіатори з металопластиковими трубами. Розводка вертикальна, яка надходить з підвального приміщення.

Локальна мережа - кручена пара та оптоволоконне покриття, які прокладені в КЗ від щитової провайдеру на першому поверсі і не виходять за його межі.

СИТУАЦІЙНИЙ ПЛАН
МАСШТАБ 1:500

Умовні позначення

— будівля

— паркан з каліткою

— територія ОІД

N — номер будівлі

Рисунок 1.4. Ситуаційний план

Рисунок 1.5. Генеральний план ОІД

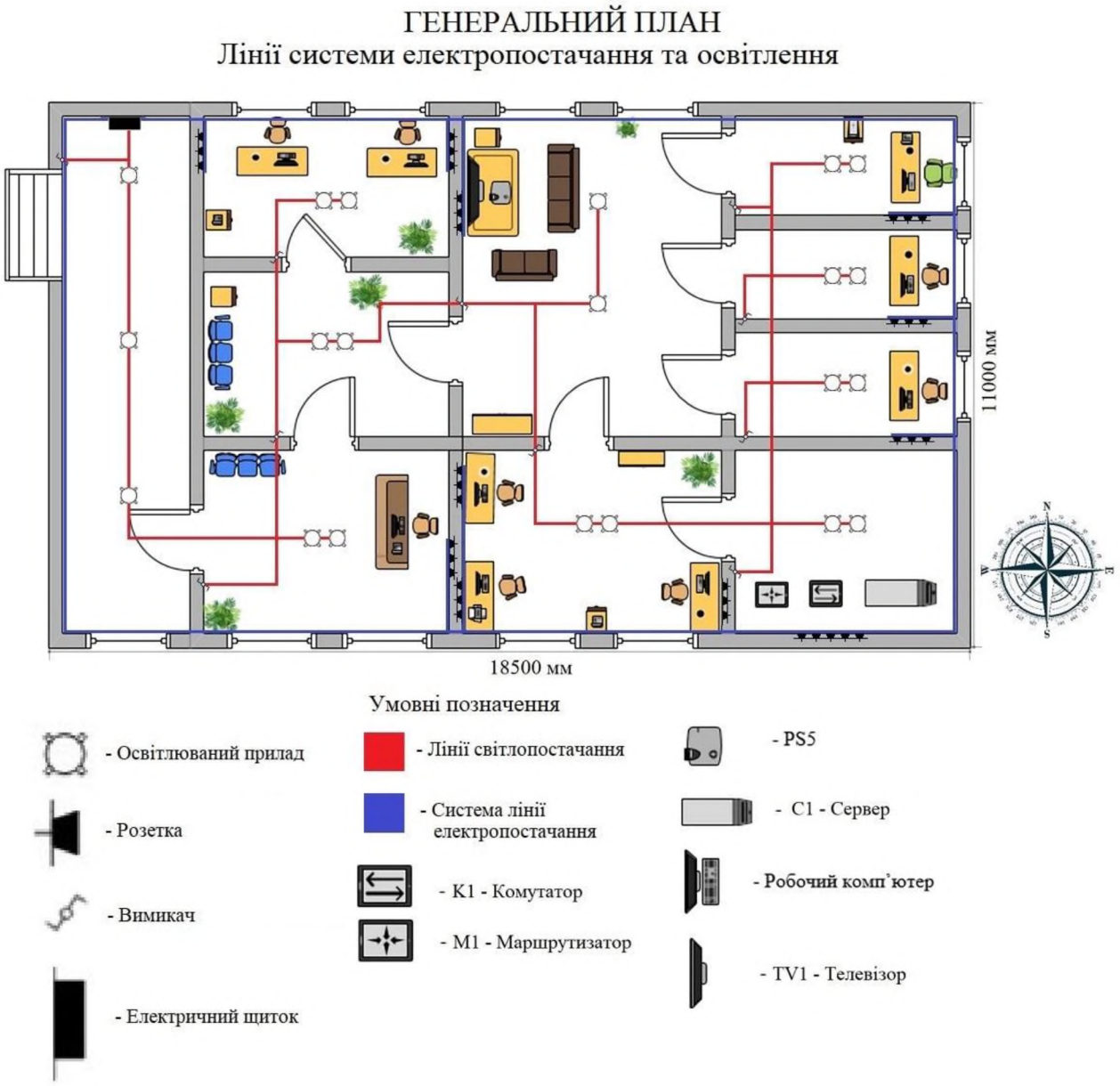


Рисунок 1.6. Генеральний план. Лінії системи електропостачання та освітлення

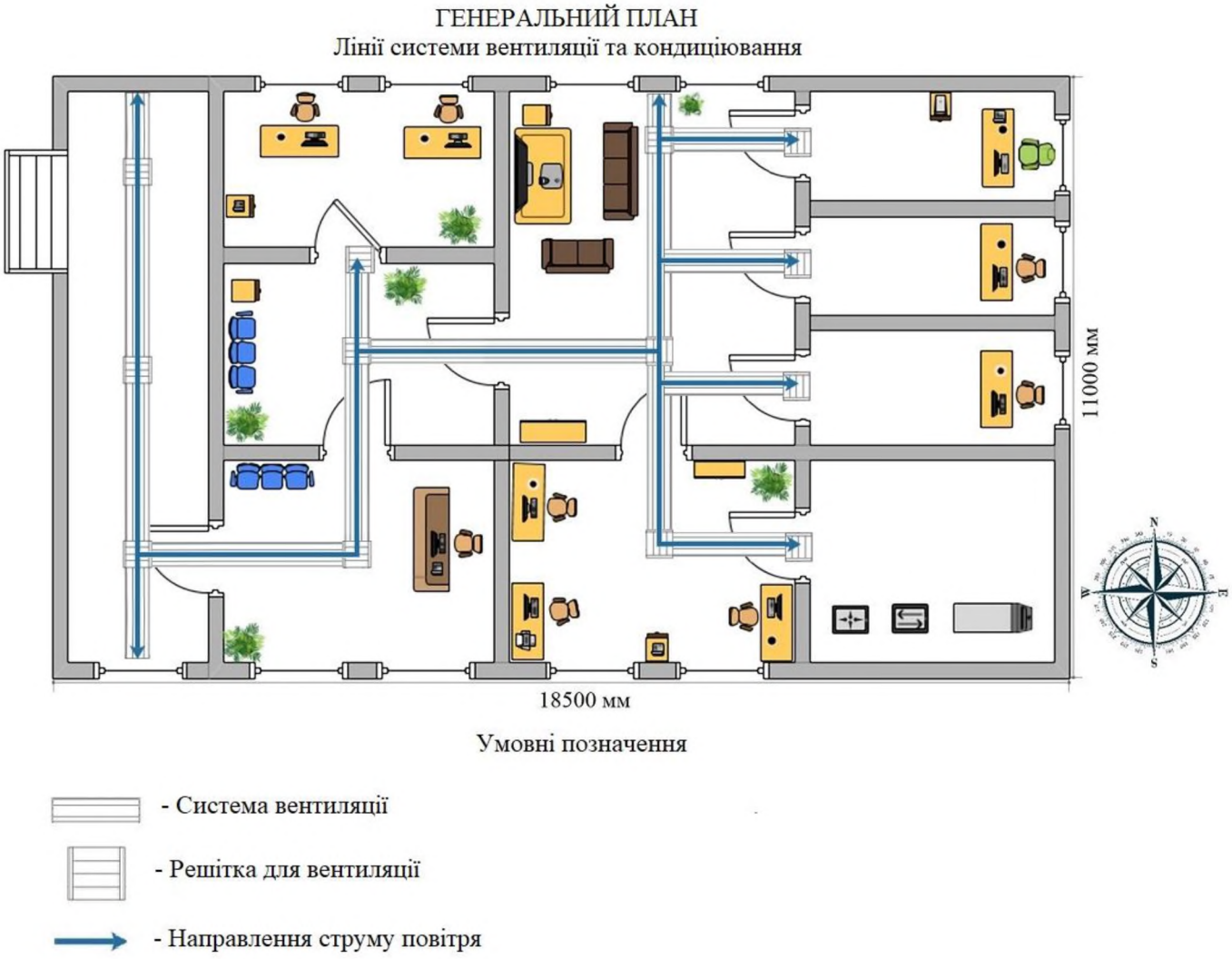


Рисунок 1.7. Генеральний план. Лінії системи вентиляції та кондиціювання

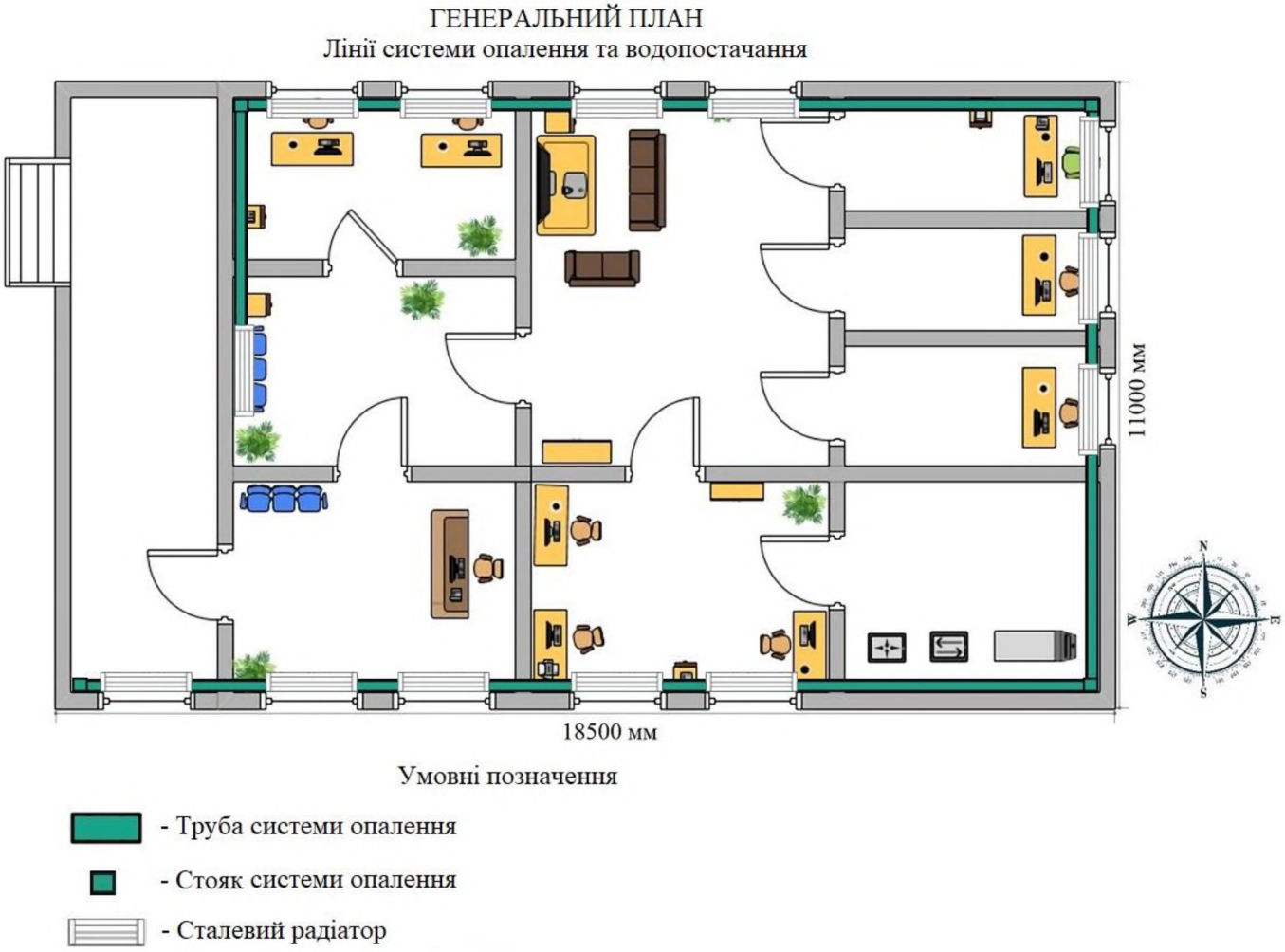


Рисунок 1.8. Генеральний план. Лінії системи опалення та водопостачання

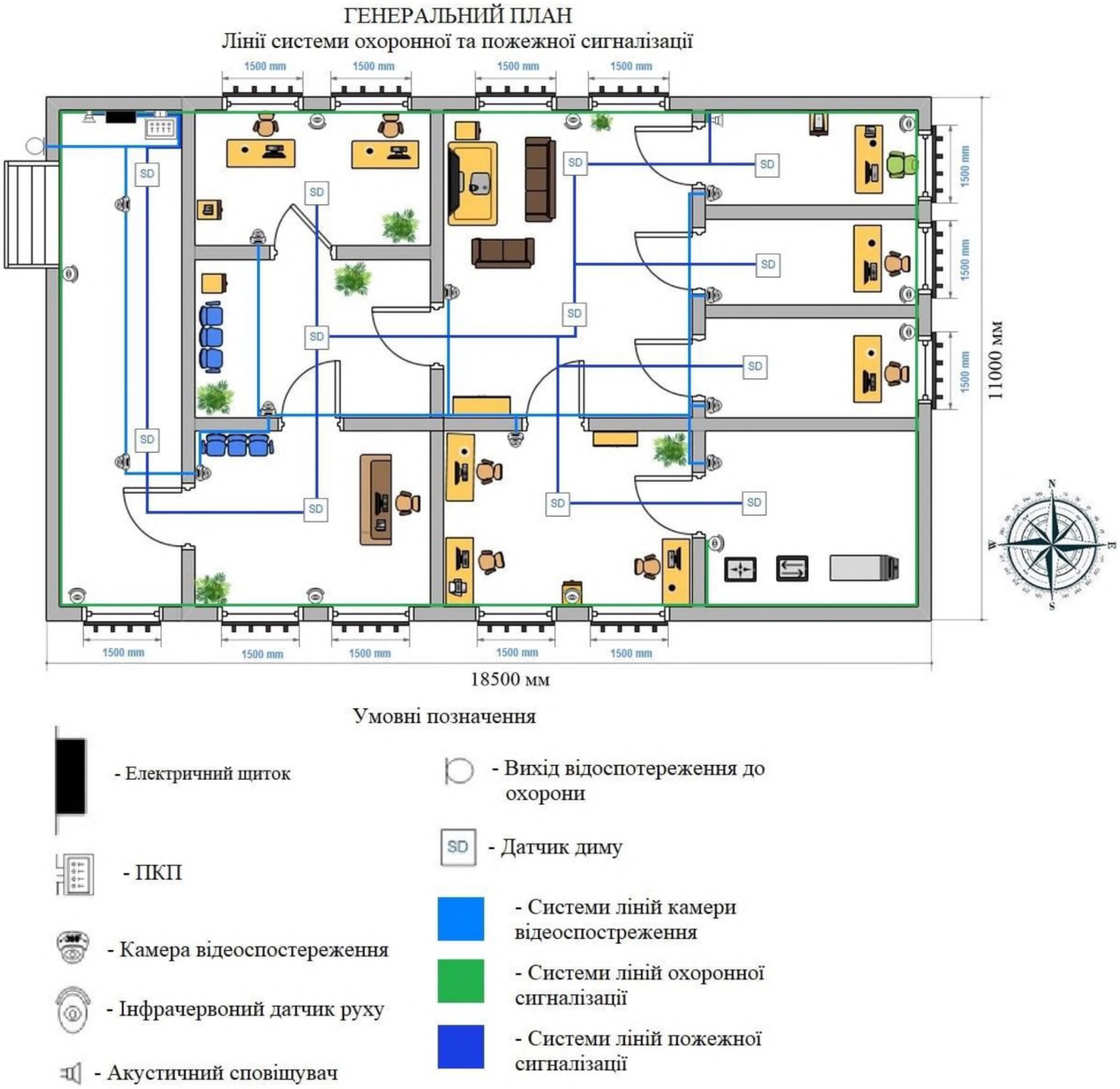


Рисунок 1.9. Генеральний план. Лінії системи охоронної та пожежної сигналізації

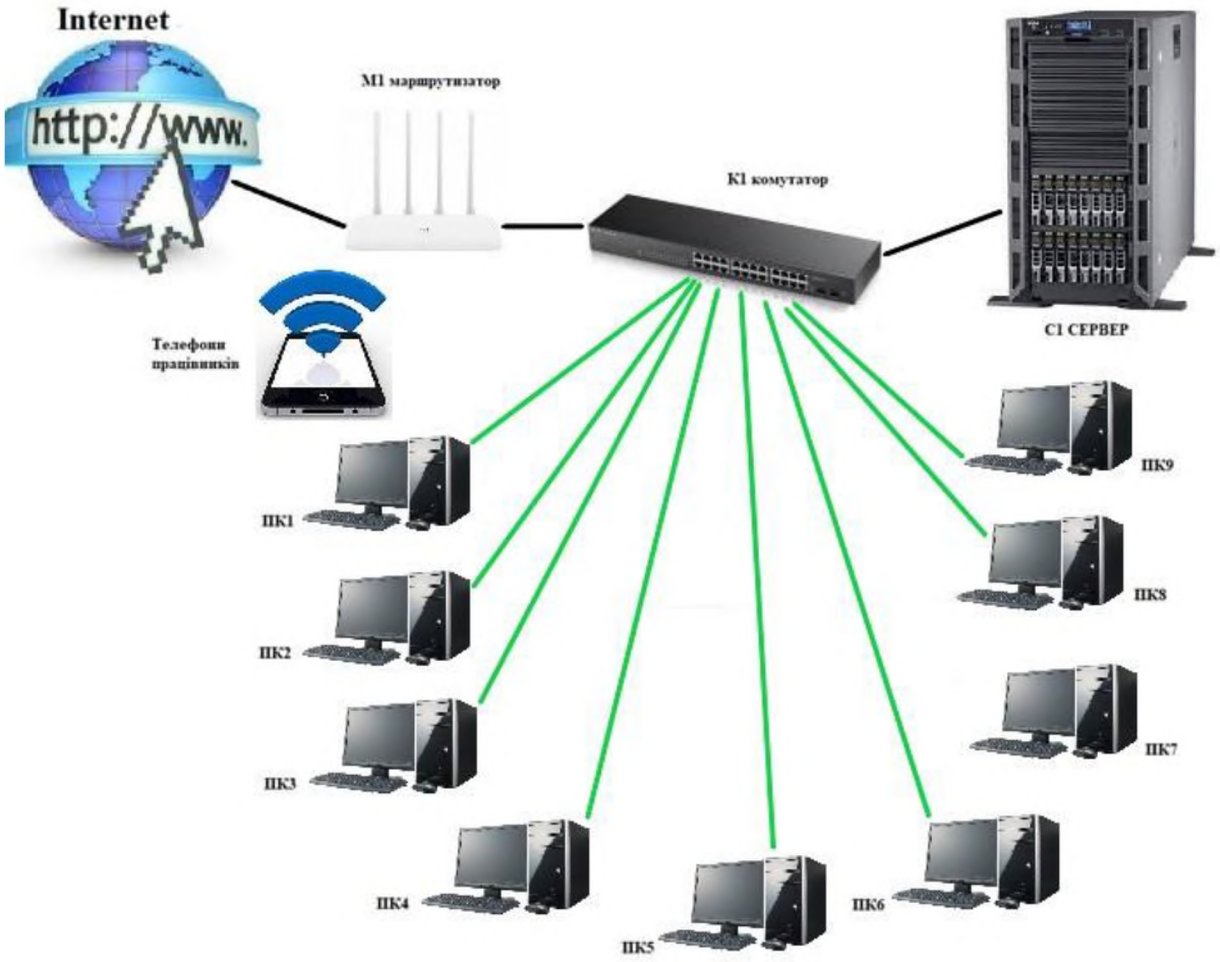


Рисунок 1.10. Схема ІТС підприємства

На рисунку 1.10. показана схема комп'ютерної мережі підприємства «LIL GROUP». Інтернет надходить з першого поверху окремим кабелем від постачальника послуг «Київстар». Маршрутизатор під'єднаний до інтернету. Комутатор має дротову мережу. Через дротову мережу він об'єднує всі робочі станції підприємства, які підключені за топологією «Зірка».

Таблиця 1.2. Перелік обладнання підприємства

№	Назва	Виробник	Модель	Серійний номер	Розміщення	Відстань до границі ОІД, м
1	Ноутбук	Hewlett Packard	HP Pavilion 15 Silver	420521	Генеральний директор	2,4
2	Миша	Acer	OMW020 USB Black	235678		

Продовження таблиці 1.2.

№	Назва	Виробник	Модель	Серійний номер	Розміщення	Відстань до границі ОІД, м
3	Сканер	EPSON	EPSON WorkForce DS-310	11153	Генеральний директор	2,7
4	Телефон	XIAOMI	XIAOMI POCO M3 Pro Black	78935		
5	Ноутбук	LENOVO	LENOVO V15 Iron Gray	75694	Програміст 1	3,1
6				75695	Програміст 2	3,2
7				75696	Програміст 3	2,8
8	Телефон	APPLE	APPLE iPhone 5	23455	Програміст 1	3,1
9		ZTE	ZTE Blade L210 1/32GB	41223	Програміст 2	3,2
10				41224	Програміст 3	2,8
11				41225	Відділ підтримки	7,5
12				41226		7,2
13		Samsung	Galaxy A03 Core 2/32GB Black	22865	Приймальня (Ресепшн)	8
14	Миша	Acer	OMW020 USB Black	235679	Програміст 1	3,1
15				235680	Програміст 2	3,2
16				235681	Програміст 3	2,8
17				235682	Відділ підтримки	7,5
18				235683		7,2
19				235684	Бухгалтерія	4,2
20				235684	Приймальня	8
21	Ноутбук	Acer	Nitro 5 AN515-55	12008	Відділ підтримки	7,5
22				12009		7,2
23		APPLE	MacBook Pro 15 Silver	55534	Бухгалтерія	4,2
24				55535	Гол. менеджер	3,5
25		Hewlett Packard	Laser135a	12032	Приймальня (Ресепшн)	8
26	Принтер	CANON	МФУ CANON Pixma TS3350	0534842	Кабінет програмістів	2,8

Продовження таблиці 1.2.

№	Назва	Виробник	Модель	Серійний номер	Розміщення	Відстань до границі ОІД, м
27	Комутатор	ZYXEL	GS1900-10HP	465073	Кабінет технічного забезпечення (ГТЗ)	1,1
28	Маршрутизатор	Xiaomi	Mi WiFi Router 4A DVB4218CN 1000 M Gigabit Edition	1034214		1,1
29	Сервер	Huawei	MateStation S	465053		1

Закупівля фарб до принтера, ремонту обладнання та ПК робиться під замовлення. Кожен співробітник працює з своїм ноутбуком для більшого комфорту. За проханням, підприємство може видавати свої ноутбуки для роботи, якщо у співробітника відсутній свій або за технічними причинами тимчасово не може використовуватися. Замовлення нових картриджів, перезаряджання принтерів, їх перелік та обслуговування обладнання проводить системний адміністратор.

Таблиця 1.3. Перелік елементів системи безпеки

№	Назва	Марка	Модель	Серійний номер	Розміщення
1	Датчик диму	Артон	СПД-3.4	89751	Кабінет технічного забезпечення (ГТЗ)
2				89752	Кабінет програмістів
3				89753	Місце відпочинку
4				89754	Місце відпочинку
5				89755	Генеральний директор

Продовження таблиці 1.3.

№	Назва	Марка	Модель	Серійний номер	Розміщення
6	Датчик диму	Артон	СПД-3.4	89756	Бухгалтерія
7				89757	Головний менеджер
8				89758	Коридор
9				89759	Кабінет відділу підтримки
10				89760	Приймальня
11				89761	Коридор
12				89762	Коридор
13	ПКП	Тирас	Тирас 4П.1 + модуль GSM	324548	Коридор
14	Електричний щиток				Коридор
15	Камера відеоспостереження	HDCVI	VSD-U714B1	235679	Коридор
16				235680	Коридор
17				235681	Приймальня
18				235682	Коридор
19				235683	Кабінет відділу підтримки
20				235684	Місце відпочинку
21				235684	Генеральний директор
22				235685	Бухгалтерія
23				235686	Головний менеджер
24				235687	Кабінет технічного забезпечення (ГТЗ)
25				235688	Кабінет программістів
26				235689	Відділ підтримки
27	Інфра-червоний датчик руху	Satel	Slim-PIR	10010	Коридор
28				10011	Коридор
29				10012	Приймальня
30				10013	Кабінет програмістів

Продовження таблиці 1.3.

№	Назва	Марка	Модель	Серійний номер	Розміщення
31	Інфра-червоний датчик руху	Satel	Slim-PIR	10014	Місце відпочинку
32				10015	Генеральний директор
33				10016	Бухгалтерія
34				10017	Головний менеджер
35				10018	Кабінет технічного забезпечення (ГТЗ)
36				10019	Відділ підтримки
37	Акустичний сповіщувач	LD	LD-95	20050	Коридор

Основна частина обладнання була придбана за рахунок власника приміщення та встановлена під замовлення.

1.5 Інформаційні потоки підприємства

Кожного дня на підприємстві «LIL GROUP» створюється, обробляється, зберігається інформація, яка в свою чергу необхідна для виконання замовлень підприємства, розуміння деяких аспектів проектування тощо. Ця інформація є складовою частиною роботи підприємства. Розголошення, крадіжка або спотворення інформації може призвести до великих фінансових та репутаційних втрат компанії.

Перелік інформації на підприємстві:

- Візуальна та звукова (За способом прийняття);
- Текстова, цифрова, графічна, звукова (За формою уявлення);
- Спеціальна, секретна, особиста (За призначенням);
- Актуальна, достовірна, повна, цінна (За значенням);
- Істинна (За істиною).

На підприємстві «LIL GROUP» збирається та оброблюється інформація про клієнтів, подробиці замовлень, контакти постачальників, звіти бухгалтерії, плани з розширення, документи ціноутворень.

Інформація про клієнтів містить ПІБ замовника, контактні дані, номер замовлення, реквізити оплати. Ця інформація є конфіденційною та не підлягає розголошенню або поширенню. Доступ до цієї інформації контрольований.

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

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.

Плани з розширення підприємства використовуються як інструкція для головного директора та головного менеджера.

Таблиця 1.4. 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	Обмежений	Конфіденційна	Графічна, текстова, звукова	К3	Ц2	Д2
2	Інформація про об’єкти та системи безпеки	Обмежений	Таємна	Графічна, текстова, звукова	К3	Ц3	Д3
3	Звіти бухгалтерії	Обмежений	Службова	Текстова, числова	К2	Ц3	Д2
4	Документи ціноутворень	Відкритий	-	Текстова, числова	К1	Ц1	Д1

Продовження таблиці 1.5.

№	Вид інформації	Режим доступу	Правовий режим	Вид представлення в ІТС	Вимоги до захисту		
					К	Ц	Д
5	Документи про постачання товарів	Обмежений	Службова	Графічна, текстова, звукова	К2	Ц2	Д1
6	Плани з розширення компанії	Обмежений	Таємна	Графічна, текстова, звукова	К3	Ц3	Д3

Таблиця 1.6. 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 1.7. 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 1.8. Рівень важливості доступності.

Оцінка рівня наслідків	Опис
Д1	Не впливає на доступність

Продовження таблиці 1.8.

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

Таблиця 1.9. Користувацьке середовище

Об'єкт Користувач	Кількість працівників	Рівень кваліфікації	Роль в ІС	Інформація					Повноваження керувати КСЗІ	Ресурси
				Про клієн.	Про об'єкти безп.	Звіти бухгалтерії	Пост. Товарів	Плани розширення		
Генеральний директор	1	Досвідчений	Користувач	RCSWP	RCDSP	RCDSP	RCDSP	RCDSP	+	PC PR SR
Системний адміністратор	1	Середній	Адміністратор	-	RWCMSP	-	-	-	+	PC PR
Програміст	3	Досвідчений	Адміністратор	-	RWCMSP	-	-	-	-	PC PR
Бухгалтер	1	Досвідчений	Користувач	-	-	RWCMSP	-	-	-	PC PR
Менеджер	1	Досвідчений	Користувач	RCSWP	-	-	RCP	-	-	PC PR
Служба підтримки	2	Середній	Користувач	RC	-	-	-	-	-	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

Таблиця 1.10. Інвентаризаційна відомість програмного забезпечення ІТС.

№	Назва	Тип	Опис	Ліцензія	Де встановлена
1	Windows 10 10.0.17763.1 (build 1809)	Системне	Операційна система для ПК і робочих станцій	Volume license	Всі ПК
2	Windows Server 2019	Системне	Операційна система для серверів	Volume license	Сервер
3	Norton 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 2020 Professional	Прикладне	ПЗ для роботи з різними видами документів, текстів, таблиць, тощо.	Volume license	Всі ПК
6	Adobe Photoshop CS6 (версія 13.01)	Прикладне	Засоби створення нерухомих і рухомих зображень	Volume license	Проектувальники, голова технічного забезпечення

Продовження таблиці 1.10.

7	Microsoft Edge (версія 44.18362.1.0)	Прикладне	Програми для роботи в комп'ютерній мережі	Freeware	Всі ПК
8	Google Chrome (версія 80.0.3987)	Прикладне	Програми для роботи в комп'ютерній мережі	Freeware	Всі ПК
9	Windows Media Player (версія 12.0.18362)	Прикладне	Програма для відтворення відео- та аудіофайлів	Freeware	Всі ПК
10	Visual Studio 2019 (версія 16.0)	Спеціальне	Об'єктно-орієнтовані мови програмування	Volume license	Проектувальники, голова технічного забезпечення, спеціаліст кібербезпеки, системний адміністратор
11	Adobe Acrobat (версія 2019.8.20071)	Спеціальне	Програма для роботи з pdf-файлами	Freeware	Всі ПК

Згідно з таблицею 1.10. ПЗ, яке встановлено на деяких ПК, не може самостійно шукати нові версії. Для вдосконалення роботи системи та полегшення роботи системного адміністратора можливе встановлення на всі ПК програм для повідомлення та автооновлення ПЗ. Оскільки в таблиці є ПЗ, яке не повідомляє про нові версії, необхідно робити пошук вручну, що займає певний робочій час.

1.6 Висновки

У першому розділі кваліфікаційної роботи проведено обстеження підприємства, що займається розробкою, встановленням та обслуговуванням систем захисту ТОВ «LIL GROUP». Проаналізовано роботу особового складу підприємства та його обов'язки також обстежено приміщення, у яких знаходиться та працює підприємство, визначено перелік ПЗ та обладнання, на якому проводиться обробка та зберігання інформації.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Аналіз основних методів захисту інформації в ІКС

У першому розділі розглянута інформація про підприємство, на основі якої можна провести більш детальне дослідження з питання захисту інформації.

Основні методи захисту інформації:

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

Програмні засоби захисту інформації – це системні та прикладні програми, призначені для захисту інформації, що передається по телекомунікаційним каналам, зберігається в базах даних і на інформаційних носіях. Найчастіше програмні засоби захисту інформації застосовують для виконання таких процесів, як ідентифікація й автентифікація користувачів, розмежування доступу користувачів до інформаційної мережі, парольний захист і перевірка повноважень, шифрування інформації, а також її захист від несанкціонованих змін, зчитування, копіювання.

Апаратні засоби захисту інформації та інформаційних систем реалізовані на апаратному рівні (різні електронні, електронно-механічні та інші пристрої, які вмонтовуються в серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки). Дані засоби є необхідною частиною безпеки інформаційної системи, хоча розробники апаратури зазвичай залишають вирішення проблеми інформаційної безпеки програмістам.

Фізичні засоби захисту інформації запобігають доступу сторонніх осіб на територію, що охороняється. Основним і найбільш розповсюдженим засобом фізичного перешкоди є установка міцних дверей, надійних замків, решіток на вікна. Для посилення захисту використовуються пропускні пункти, на яких

контроль доступу здійснюють люди (охоронці) або спеціальні системи. З метою запобігання втрат інформації також доцільна установка протипожежної системи. Фізичні засоби використовуються для охорони даних як на паперових, так і на електронних носіях.

Криптографічний захист інформації реалізується за допомогою перетворень інформації із використанням спеціальних даних (ключових даних), з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

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. Також це сукупність заходів щодо підбору, перевірки та навчання персоналу.

Апаратно-програмні засоби захисту інформації широко використовуються при аутентифікації користувачів автоматизованих банківських систем.

Аутентифікація - це перевірка ідентифікатора користувача перед допуском його до ресурсів системи.

Ідентифікація - це ідентифікація користувача в системі за 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.

Для виявлення слабких місць підприємства «LIL GROUP» розроблено модель порушника та модель загроз.

2.2 Модель загроз і порушника

Згідно з НД-ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації комп'ютерних систем від несанкціонованого доступу»:

Модель загроз (model of threats) – абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.

Порушник - користувач, який здійснює несанкціонований доступ до інформації.

Модель порушника (user violator model) – абстрактний формалізований або неформалізований опис порушника.

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). Проаналізувавши результати обстеження середовища функціонування ІТС підприємства ТОВ «LIL GROUP», можна зробити висновок, що потенційними порушниками можуть бути в першу чергу персонал та відвідувачі.

Далі проведено процедури, пов'язані з виявленням негативних факторів впливу на ІТС.

Модель порушника:

Таблиця 2.1. – Категорії порушників, визначених у моделі (Внутрішні за відношенням до ІТС)

Позначення	Визначення категорії	Рівень загроз
ПВ1	Технічний персонал який обслуговує будівлю та приміщення (прибиральники, електрики сантехніки, тощо)	2
ПВ2	Обслуговуючий персонал засобів ІТС (Системний адміністратор, Програміст)	2
ПВ3	Користувачі ІТС	2
ПВ4	Адміністратор ІТС (Системний адміністратор)	3
ПВ5	Керівники (директор)	1
ПВ6	Персонал без доступу до ІТС (Відділ підтримки)	1

Таблиця 2.2. – Категорії порушників, визначених у моделі (Зовнішні за відношенням до ІТС)

Позначення	Визначення категорії	Рівень загроз
ПЗ1	Відвідувачі (Запрошені гості)	1
ПЗ2	Представники організацій з питань технічного забезпечення (водопостачання, енергопостачання, теплопостачання тощо)	1
ПЗ3	Хакери (Особа що намагається отримати несанкціонований доступ до комп'ютерних систем)	3
ПЗ4	Конкуренти та їх представники (Агенти)	2

Таблиця 2.3. Специфікація моделі порушника за мотивами порушень

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

Таблиця 2.4. Специфікація моделі порушника за рівнем кваліфікації та обізнаності що до ІТС

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

Таблиця 2.5. 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 (флеш накопичувач), які можуть бути приховані та пронесені крізь охорону	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4

Таблиця 2.6. Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час функціонування ІТС	2
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 2.7. 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

Продовження таблиці 2.7.

Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

На підставі таблиць 2.1. – 2.7. створено модель порушника, підраховано суми загроз та визначено, хто з особистого складу підприємства є найбільш загрозою для підприємства.

Таблиця 2.8. 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	ПВ5	М1	К4	З3	Ч1	Д4	17
	1	1		4	3		
	ПЗ4	М4	4	З4	Ч4	4	23
	3	4		4	4		
Менеджер	ПВ3	М1	К2	З1	Ч1	Д2	11
	2	1		1			
	ПЗ4	М4	2	З3	3	2	18
	3	4		4			
Системний адміністратор	ПВ4	М1	К3	З3	Ч4	Д4	19
	3	1		4			
	ПЗ4	М4	3	З4	4	4	22
	3	4		4			
Програмісти	ПВ2	М1	К3	З3	Ч1	Д3	17
	3	1		4			
	ПЗ4	М4	3	З4	3	3	20
	3	4		4			
Бухгалтер	ПВ3	М3	К1	З1	Ч1	Д2	13
	2	4		1			

	ПЗ4	М4	1	З3	3	2	17
	3	4		4			

Продовження таблиці 2.8.

Служба підтримки24	ПВ6	М1	К2	З1	Ч1	Д1	9
	1	1		1			
	ПЗ4	М4	2	З2	3	1	15
	3	4		2			

Найбільшу загрозу несуть системний адміністратор та директор 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.

Таблиця 2.9. Модель внутрішнього порушника політики безпеки інформації

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	ПВ5	М1	К4	З3	Ч1	Д4	17
Менеджер	ПВ3	М1	К2	З1	Ч1	Д2	11
Системний адміністратор	ПВ4	М1	К3	З3	Ч4	Д4	19
Програмісти	ПВ2	М1	К3	З3	Ч1	Д3	17
Бухгалтер	ПВ3	М3	К1	З1	Ч1	Д2	13
Служба підтримки	ПВ6	М1	К2	З1	Ч1	Д1	9

Із таблиці 2.9. чітко видно, що найбільшу загрозу несе системний адміністратор, програмісти та директор. Всі працюють у одному офісі и підпорядковуються директору офісу. Тому організація роботи цих осіб повинна бути найбільш контрольованою, оскільки вони є основними потенційними порушниками безпеки інформації.

Згідно НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» модель загроз - це 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 безпеці 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 проектування 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 по 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);
- ненавмисне 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 отримання 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);

Таблиця 2.10. Перелік загроз з визначенням порушень властивостей

№	Потенційні загрози для інформації в ІТС	Ризики для			
		К	Ц	Д	С
Загрози об'єктивної природи					
1.1	Стихійні явища		+	+	
1.2	Відсутність електропостачання		+	+	
1.3	Відмова/збій обчислювальної техніки		+	+	
1.4	Відмова/збій програмного забезпечення	+	+	+	
1.5	Пошкодження паперової документації	+	+	+	
1.6	Відмова доступу до інтернету		+	+	
Загрози суб'єктивної природи					
2.1	Несанкціоноване підключення до технічних засобів	+	+		
2.2	Несанкціоноване підключення до мережевих вузлів	+	+	+	
2.3	Читання даних, залишених без нагляду та читання даних, що виводиться на екран	+			+
2.4	Перехоплення даних за допомогою акустичного каналу	+			+
2.5	Несанкціонований перегляд інформації за допомогою візуально-оптичного каналу	+			+
2.6	Зараження системи вірусами	+	+	+	
2.7	Втрата паролів	+	+	+	
2.8	Втрата резервних копій		+	+	+
2.9	Несанкціоноване внесення змін у технічні засоби	+	+	+	

2.10	Використання недозволеного програмного забезпечення або модифікація компонентів програмного та інформаційного забезпечення	+			+
2.11	Пошкодження носіїв інформації		+	+	
2.12	Вхід в систему недопущених осіб (подолання систем захисту)	+	+	+	
2.13	Недоступність до хмарного сховища			+	
2.14	Неправильне налаштування резервного копіювання		+	+	+
2.15	Неправильні налаштування прав доступу співробітників	+		+	
2.16	Недбале зберігання документів	+	+	+	+
2.17	Отримання сторонньою особою інформації у персоналу ІТС	+	+		+
2.18	Відсутність правильно налагодженої системи сигналізації	+	+		+
2.19	Відсутність шифрування даних	+			+
2.20	Передача важливих документів в незашифрованому вигляді	+			
2.21	Хакерська атака	+	+	+	
2.22	Використання заборонених ресурсів Інтернету в своїх цілях	+			
2.23	DDos-атака			+	

Модель загроз визначення рівня ризиків та збитків

3 бали – високий рівень загрози надає великих збитків

2 бали – середній рівень загрози надає помірних збитків;

1 бал – низький рівень загрози надає незначних збитків.

Таблиця 2.11. 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	1	2	3
К.3	Копіювання даних для ознайомлення сторонніми особами	1	3	4
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	2	3
К.8	Використання сторонньої інформації з посиланням на авторів	1	2	3

Таблиця 2.12. 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	2	3	5
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	2	3
Ц.6	Безпосередній доступ до інформації будь-яким способом сторонніми особами	1	3	4
Ц.7	Халатність співробітників щодо пропуску сторонніх осіб	1	3	4
Ц.8	Відсутність підтвердження відправника інформації що надходить на обробку	1	3	4

Таблиця 2.13. Загрози доступності інформації

№	Механізм реалізації	Рівень		Сума загроз
		ризики	збитки	
Д.1	Помилка користувача, яка призвела до знищення 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 2.14. 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

Продовження таблиці 2.14.

С.7	Безпосередній доступ до ІТС будь-яким способом сторонніх осіб	1	3	4
С.8	Можливе спостереження співробітниками охорони	1	2	3

Модель загроз з розрахунком сумарного рівня ризиків та збитків

Таблиця 2.15. Узагальнена таблиця загроз ІТС.

№	Види загроз	1	2	3	4	5	6	7	8	Сума загроз
1	Конфіденційності	4	3	4	5	2	4	3	3	28
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	5	3	3	4	4	4	31

На основі даних, отриманих з таблиці 2.15., найбільшими загрозами підприємству у разі розголошення, викрадення, модифікації інформації є цілісність та спостереженість. Зменшення рівня загроз треба починати саме з цілісності та конфіденційності. Для цього необхідно переглянути права користувачів, усунути можливість під'єднання сторонніх носіїв інформації, відстежувати дії співробітників та обмежити їх доступ до сторонніх об'єктів у інтернеті.

Конфіденційність – загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності.

Цілісність – загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності.

Доступність – загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності.

Спостереженість – ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості.

2.3 Класифікація АС. Аналіз профілю захищеності

Згідно НД ТЗІ 2.5-005-99 досліджене АС за ієрархією належить до класу «3» (розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності).

Мета введення класифікації АС і стандартних функціональних профілів захищеності – полегшення задачі співставлення вимог до КЗЗ обчислювальної системи АС з характеристиками АС.

Автоматизована система являє собою організаційно-технічну систему, що об'єднує ОС, фізичне середовище, персонал і оброблювану інформацію. Вимоги до функціонального складу КЗЗ залежать від характеристик оброблюваної інформації, самої ОС, фізичного середовища, персоналу і організаційної підсистеми. Вимоги до гарантій визначаються насамперед характером (важливістю) оброблюваної інформації і призначенням АС.

За сукупністю характеристик АС (Конфігурація апаратних засобів ОС і їх фізичне розміщення, кількість користувачів і повноважень користувачів) виділено три ієрархічні класи АС, вимоги до функціонального складу КЗЗ яких істотно відрізняються.

Клас «1» – одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох ступенів обмеження доступу.

Істотні особливості:

В кожний момент часу з комплексом може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька;

користувачі можуть мати різні повноваження (права) щодо доступу до інформації, яка обробляється.

Клас «2» – локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Істотна відміна від попереднього класу – наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку інформації різних ступенів обмеження доступу.

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

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

В межах кожного класу АС класифікуються на підставі вимог до забезпечення певних властивостей інформації. З точки зору безпеки інформація характеризується трьома властивостями: конфіденційністю, цілісністю і доступністю. В зв'язку з цим, в кожному класі АС виділяються такі підкласи:

автоматизована система, в якій підвищені вимоги до — забезпечення конфіденційності оброблюваної інформації (підкласи «х. К»);

автоматизована система, в якій підвищені вимоги до — забезпечення цілісності оброблюваної інформації (підкласи «х.Ц»);

автоматизована система, в якій підвищені вимоги до — забезпечення доступності оброблюваної інформації (підкласи «х.Д»);

автоматизована система, в якій підвищені вимоги до — забезпечення конфіденційності і цілісності оброблюваної інформації (підкласи» х.КЦ»);

автоматизована система, в якій підвищені вимоги до — забезпечення конфіденційності і доступності оброблюваної інформації (підкласи «х.КД»);

автоматизована система, в якій підвищені вимоги до — забезпечення цілісності і доступності оброблюваної інформації (підкласи «х.ЦД»).

автоматизована система, в якій підвищені вимоги до — забезпечення конфіденційності, цілісності і доступності оброблюваної інформації (підкласи «х.КЦД»).

Для кожного з підкласів кожного класу вводиться деяка кількість ієрархічних стандартних функціональних профілів, яка може бути різною для кожного класу і підкласу АС. Профілі є ієрархічними в тому розумінні, що їх реалізація забезпечує наростаючу захищеність від загроз відповідного типу (конфіденційності, цілісності і доступності). Наростання ступеня захищеності може досягатись як підсиленням певних послуг, тобто включенням до профілю більш високого рівня послуги, так і включенням до профілю нових послуг. Така класифікація корисна для полегшення вибору переліку функцій, які повинен реалізовувати КЗЗ ОС, проектованої або існуючої АС. Цей підхід дозволяє мінімізувати витрати на початкових етапах створення КСЗІ АС. Проте слід визнати, що для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.

Відповідно до методичного забезпечення для АС, яка має клас «3», було вибрано наступний профіль захищеності:

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

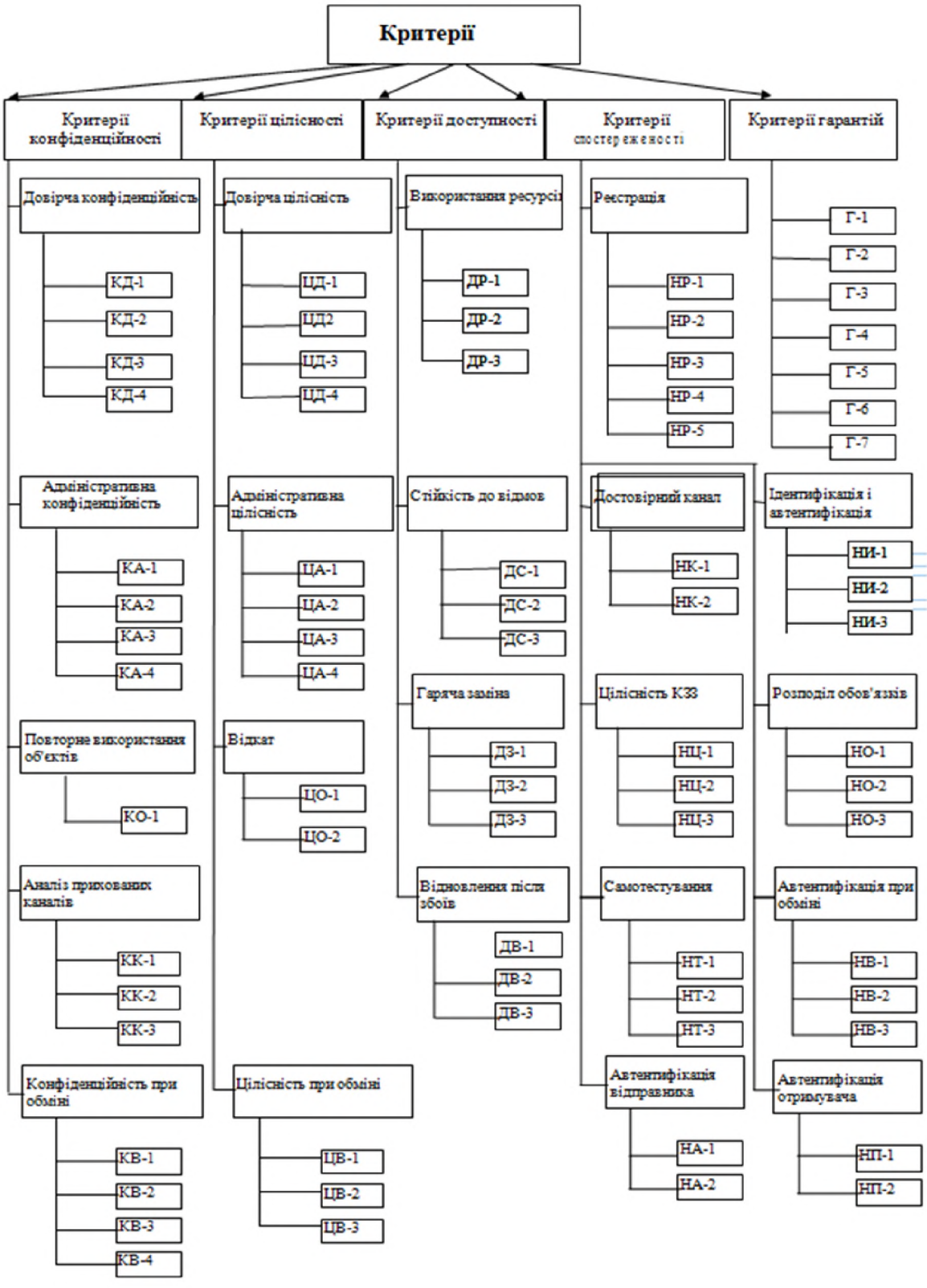


Рисунок 2.1. Структура критеріїв

Опис критеріїв конфіденційності:

КД-2 Базова довірча конфіденційність. 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.

КА-2 Базова адміністративна конфіденційність. КЗЗ здійснює розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта.

КО-1 Повторне використання об’єктів. Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта будуть скасовані Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, стане недосяжною.

КВ-2 Базова конфіденційність при обміні. КЗЗ забезпечує захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається. Запити на призначення або зміну рівня захищеності обробляються КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження.

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

ЦА-2. Базова адміністративна цілісність. КЗЗ здійснює розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

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

ЦВ-2: Базова цілісність при обміні. КЗЗ визначає множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується механізмами, які використовуються і спроможність користувачів і/або процесів керувати рівнем захищеності.

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

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

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

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

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

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

НЦ-2. КЗЗ з гарантованою цілісністю. 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. КЗЗ не описує властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ при старті.

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

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 : MSI Afterburner AIDA64. 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. Доступ до даної інформації можливий лише спеціалісту з кібербезпеки підприємства, системному адміністратору та директору.

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.

2.4 Програмне забезпечення з захисту інформації

ПЗ яке використовується для захисту підприємства:

- Norton Security – антивірусна програма яка є складовою ОС, проводить активну перевірку одержаних файлів, робить аналіз системи і не потребує втручання спеціалістів

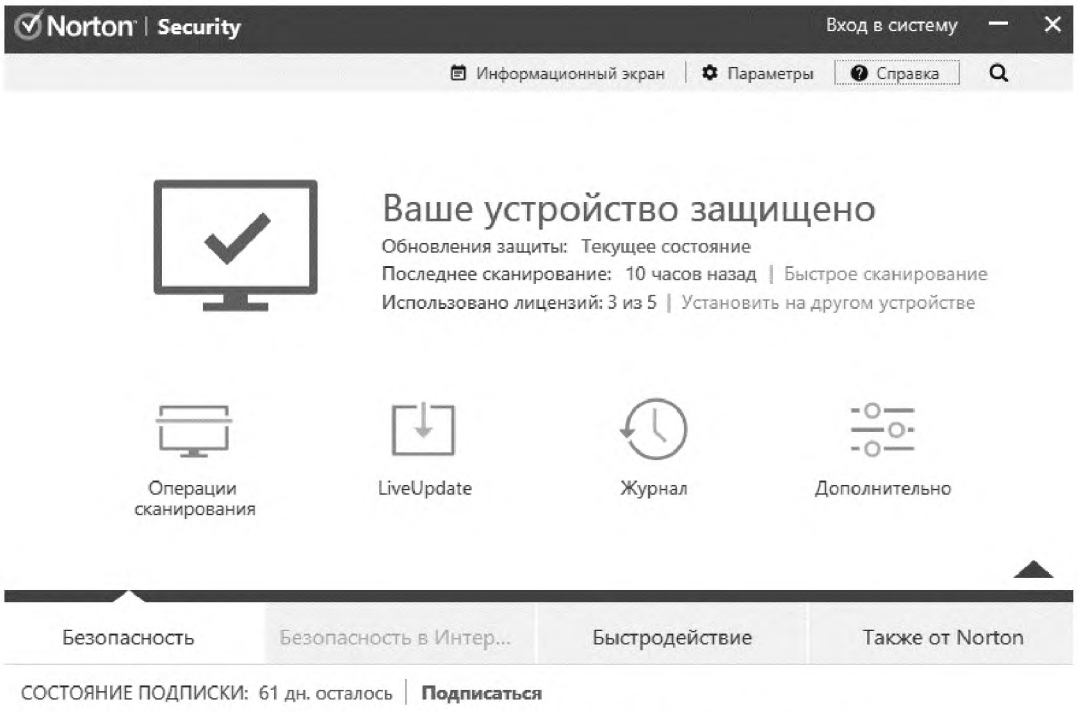
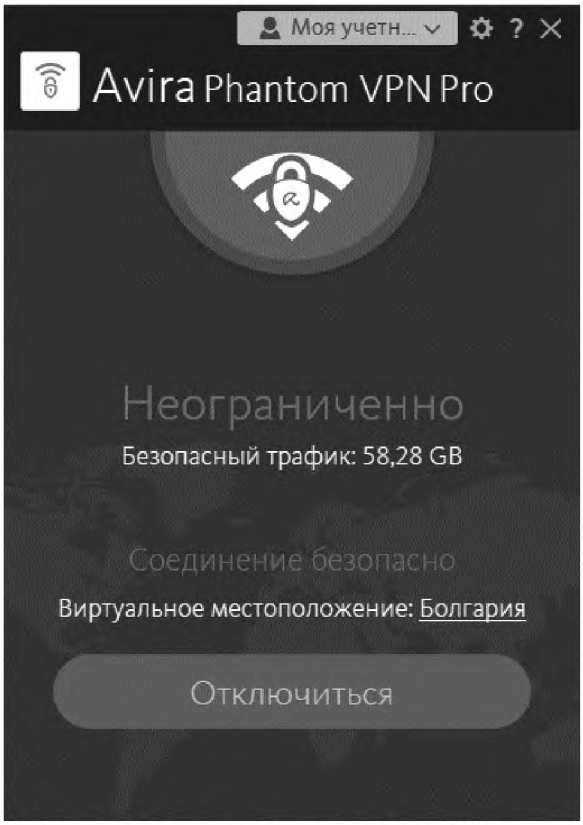


Рисунок 2.2 - Інтерфейс Norton Security

- Avira Phantom VPN – ПЗ VPN, яке створює захищене з'єднання між ПК та мережею інтернет, захищає від стеження за трафіком та стороннього втручання. Проста у використанні, має доступний інтерфейс та зручні пакети



налаштування, а саме підключення при запуску ПК та сервера

Рисунок 2.3. - Інтерфейс Avira Phantom VPN

- Unchecky – програма призначена для порятунку користувача від постійної напруги при установці безкоштовного софту. Ця програма сама зніматиме галочки з небажаних програм. Тим самим забороняє їхню установку. Утиліта невелика, але цілком здатна впоратися майже з усіма інсталяторами. Її легковажність і невибагливість до системних ресурсів дозволяє постійно знаходитись в панелі швидкого доступу. Швидкодія ПК при цьому не постраждає.

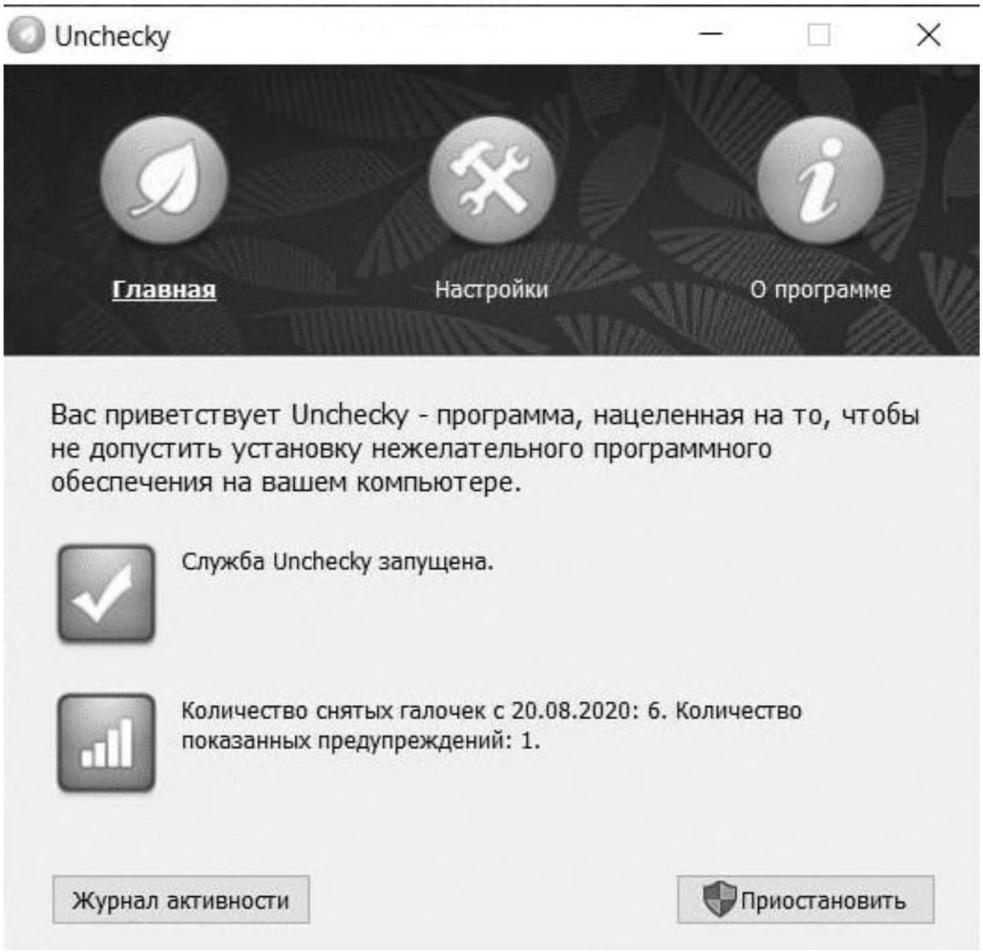


Рисунок 2.4. - Інтерфейс Unchecky

Антивірусна програма Norton 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.

Avira Phantom VPN - 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.

Unchecky – Встановлений на кожному ПК підприємства, працює фоном при старті системи.

Інструкція з користування ПЗ для користувача.

Після старту ПК перевірити антивірус - Norton Security на стан “ Ваш пристрій захищений ” та наявність останньої версії, при необхідності оновити. Перевірити стан Avira Phantom VPN на “ З'єднання безпечне”, при необхідності підключити. Перевірити у треї наявність програми Unchecky, за необхідністю запустити. Під час використання ПК слідкувати за спливаючими вікнами у нижньому правому куті екрана на повідомлення від програм Norton Security та Avira Phantom VPN. При невідомих помилках кликати системного адміністратора чи спеціаліста з питань кібербезпеки.

Інструкція з користування ПЗ для адміністратора.

Після старту ПК перевірити антивірус - Norton Security на стан “ Ваш пристрій захищений ” та наявність останньої версії, при необхідності оновити. Перевірити стан Avira Phantom VPN на “ З'єднання безпечне”, при необхідності підключити. Перевірити у треї наявність програми Unchecky, за необхідністю запустити. Під час використання ПК слідкувати за спливаючими вікнами у нижньому правому куті екрана на повідомлення від програм Norton Security та Avira Phantom VPN.

2.5 Аналіз системи захисту підприємства

При обстеженні офісного приміщення було виявлено наступний ряд недоліків:

- Відсутність перевірки приміщень на наявність закладних пристроїв;
- Відсутність тривожних кнопок в бухгалтерії.

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.

2.6 Особливості реалізації та вдосконалення існуючих методів та систем захисту інформації

Для реалізації нових та вдосконалення вже існуючих методів та систем захисту інформації будемо 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.

Виходячи з цих даних, а саме пункту 2.5., потрібно розробити необхідні акти перевірок на закладні пристрої та вдосконалити приміщення підприємства додавши тривожну кнопку.

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 слів виявляти якомога швидше. На підприємстві таких обстежень не проводять.

Для обстеження необхідно визначити відповідальну людину, а саме спеціаліста з питань кібербезпеки підприємства. Він повинен в встановлений час обстежити всі приміщення підприємства на можливу наявність закладних пристроїв.

Для вирішення питань з апаратного та програмного захисту інформації необхідно у більшій частині змінити права користувачів, більш детально налаштувати міжмережевий 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

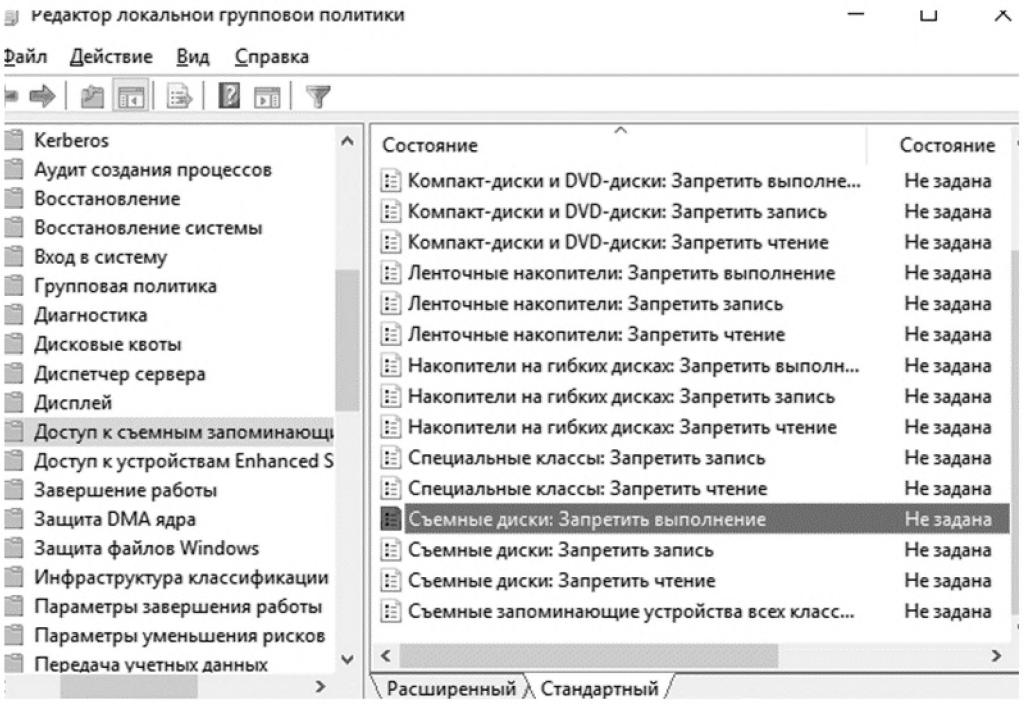


Рисунок 2.5. Заборона виконання програм зі з'ємних носіїв

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.

Для налаштування доповненого списку заборонених сайтів необхідно відкрити браунмауєр у режими підвищеного захисту, створити правило для вихідного підключення, з визначеним забороненим ір-адресом для всіх ір-адрес підприємства. При цьому співробітники не зможуть отримувати пакети даних з заборонених сайтів. Список буде постійно доповнюватись. За заборону відвідування сайтів копій або, як їх ще називають - «фішингових сайтів»,

відповідають Avira Phantom VPN та Norton Security, у яких блокування таких сайтів стоїть за замовчуванням.

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 дозволено необмежений доступ.

2.7. Політика безпеки підприємства

Політика інформаційної безпеки — набір вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в організації і спрямовані на досягнення і підтримку стану інформаційної безпеки організації.

Під політикою безпеки інформації розуміють набір законів, правил, обмежень, рекомендацій та інших заходів, які регламентують порядок обробки інформації на підприємстві і спрямовані на захист інформації від певних загроз

Політика резервного копіювання

Будь яка подія, яка може призвести до тривалої затримки обслуговування, має бути розглянуто. План аварійного відновлення часто є планом забезпечення безперервності роботи підприємства. Дана політика визначає вимоги до базового плану аварійного відновлення, який повинен бути розроблений і впроваджений.

Політика антивірусного захисту

Загальна частина – встановлює наступні загальні правила, які слід виконувати для вирішення проблемі вірусу:

- завжди підтримувати корпоративні вимоги, підтримка антивірусного ПЗ є необхідною для корпоративного вузла. Завантажувати і підтримувати поточну версію;
- НІКОЛИ не відкривати будь-які файли або макрокоманди, що торкаються електронної пошти від невідомого, підозрілого або ненадійного джерела. Видаліть ці повідомлення негайно, потім видаліть їх за допомогою спорожнення вашого сміття;

- видаляти Spam, ланцюг і іншу електронну пошту, які не мають атрибутів Вашої кампанії відповідно до політики безпеки;
- ніколи не завантажувати файли від невідомих або підозрілих джерел;
- уникати прямого дискового доступу (читання/запис), за винятком того, що відповідає необхідним діловим вимогам;
- перед використанням завжди сканувати зовнішній накопичувач від невідомого джерела на предмет вірусів;
- регулярно дублювати критичні дані і системні конфігурації зберігайте їх в безпечному місці;
- якщо лабораторна перевірка встановлює конфлікт з антивірусним ПЗ, запустити антивірусну утиліту, що гарантує не забрудненість машини, блокуйте ПЗ, потім двинути лабораторну перевірку. Тільки після лабораторної перевірки дозволяти використовувати антивірусне ПЗ. Під час блокування антивірусне ПЗ блоковано, ні в якому разі не завантажуйте будь-які додатки, які могли б перенести вірус.
- нові віруси відкриваються майже щодня. Періодично перевіряйте Антивірусну політику відділу і ці рекомендації для внесення змін.

Політика безпеки паролів користувачів

Планування й проведення політики паролів є ключовим моментом. Не настроївши політикові паролів для доменів, тим самим ви дозволите своїм користувачам уводити слабкі паролі, які не будуть вимагати зміни. У цьому випадку застосування атакуючого елементарного способу підбора пароля буде мати більші шанси на успіх. Можна вказати наступні параметри політики паролів.

- Вимагати неповторюваності паролів. Windows може забороняти користувачам повторно вводити ті самі паролі. Установите число паролів, які повинна пам'ятати Windows, за замовчуванням це значення дорівнює нулю.
- Максимальний термін дії пароля. Визначите кількість днів, протягом яких пароль дійсний (за замовчуванням - 42 дня). Після закінчення цього строку

користувач буде змушений перемінити пароль. Нульове значення цього параметра приводить до скасування контролю над витіканням терміну дії пароля.

- Мінімальний термін дії пароля. Для запобігання обходу користувачами контролю історії паролів служить установка значення мінімального терміну дії пароля в днях. Наприклад, ви визначили, що Windows повинна зберігати п'ять паролів в історії. Користувачі можуть п'ять разів протягом дня поміняти пароль і знову повернутися до свого улюбленого варіанта.
- Пароль повинен задовольняти вимогам складності. Установка цього параметра змушує користувачів вибирати складні паролі, задовольняючим наступним мінімальним вимогам:

а) не повинні містити в собі навіть частина імені користувача;

б) повинні мати довжину не менш шести символів;

в) повинні складатися із символів трьох із чотирьох наступних категорій:

A-Z, a-z, 0-9 і спец символів, таких як $, !, #, %.

- Зберігати паролі з використанням оборотного шифрування. Ніколи не включайте цей параметр через те, що, по суті, він означає зберігання паролів у текстовому виді замість хешованих значень.

2.8. Висновок

У другому розділі проведено додаткове обстеження підприємства, розглянуто модель порушника та внутрішнього порушника, виявлено співробітників, які становлять найбільшу загрозу підприємству, а саме системний адміністратор та програмісти. Розглянуто модель внутрішнього порушника, модель загроз. Результати виведено в таблицю 2.15. узагальнених загроз ІТС. Проаналізовано профіль захищеності, визначені програми захисту інформації та інструкції до них. Виявлено слабкі місця підприємства у інформаційному просторі та наведені рекомендації.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою розділу є визначення економічної доцільності розробки засобів захисту інформації в гетерогенних мережах 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.

Визначення витрат на розробку засобів захисту інформації в гетерогенних мережах для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації

Визначення трудомісткості розробки засобів захисту інформації в гетерогенних мережах для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації

Трудомісткість розробки визначається тривалістю кожної робочої операції:

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

де:

$t_{тз}$ – тривалість складання технічного завдання на розробку засобів захисту інформації в гетерогенних мережах, $t_{тз}=8$;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в=48$;

t_a – тривалість аналізу існуючих загроз безпеки інформації, $t_a=24$;

t_p – тривалість розробки засобів захисту інформації в гетерогенних мережах, $t_м=32$;

$t_д$ – тривалість підготовки технічної документації, $t_д=5$.

Отже,

$$t = 8+48+24+32+5 = 117 \text{ годин.}$$

Розрахунок витрат на розробку засобів захисту інформації в гетерогенних мережах

Витрати на розробку заходів безпеки $К_{пз}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки *Ззп* і вартості витрат машинного часу *Змч*:

$$К_{пз} = З_{зп} + З_{мч} = 15210 + 1634,95 = 16844,95 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 117*130 = 15210 \text{ грн.}$$

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:

$$З_{мч} = t*С_{мч} = 117*13,974 = 1634,95 \text{ грн.}$$

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:

$$С_{мч} = Р * t_{нал} * С_е + \frac{Ф_{зал} * Н_а}{F_р} + \frac{К_{лпз} * Н_{апз}}{F_р}, \quad грн,$$

де:

Р – встановлена потужність ПК, кВт;

$С_е$ – тариф на електричну енергію, грн/кВт*година

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

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

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

Клпз – вартість ліцензійного програмного забезпечення, грн.;

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

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.11,808+1,3541+0,8125

$$Смч = 0{,}8 * 5 * 1{,}64 + \frac{6500*0{,}4}{1920} + \frac{5200*0{,}3}{1920} = 13{,}974 \text{ грн.}$$

Відповідно до поставлених задач в контексті розробки засобів захисту інформації в гетерогенних мережах 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 в гетерогенних мережах

Матеріальний актив	Кількість	Ціна, грн.	Вартість, грн.
Активний медіа-конвертер	2	1600	3200
Оптоволоконний кабель, м	900	5	4500

ZYXEL GS1900-10HP	1	459	459

Продовження таблиці 3.1.

Xiaomi Mi WiFi Router 4A DVB4218CN 1000 M Gigabit Edition	1	510	510
Комплект безпровідна сигналізація GSM ATIS Kit-GSM100	1	2400	2400
Комплект Димовий пожежний датчик СПД-3.4	1	598	598
Разом:			11667

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

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

$$К = Кпр + Кзпз + Кпз + Каз + Кнавч + Кн$$

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.

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

$$К = 16844,95 + 11667 + 2500 = 31011,95 \text{ грн.}$$

Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

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

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).

$С_а$ – Річний фонд амортизаційних відрахувань, визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ).

При розробці засобів захисту інформації в гетерогенних мережах для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації витрати на відновлення й модернізації системи не матимуть місце.

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

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

Таблиця 3.2. Групи основних засобів та інших необоротних активів і мінімально допустимі строки їх амортизації

Групи	Мінімально допустимі строки корисного використання років

Продовження таблиці 3.2.

Група 4 – машини та обладнання З них: Електронно-обчислювальні машини, інші машини для автоматичного оброблення інформації, пов'язані з ними засоби зчитування або друку інформації, пов'язані з ними комп'ютерні програми (крім програм, витрати на придбання яких визнаються роялті, та/або програм, які визнаються нематеріальним активом), інші інформаційні системи, комутатори, маршрутизатори, модулі, модеми, джерела безперебійного живлення, та засоби їх підключення до телекомунікаційних мереж, телефони (в тому числі стільникові), мікрофони і рації, вартість яких перевищує 2500 гривень.	5 2

Таблиця 3.3. Строки амортизації нематеріальних активів

Групи	Строк дії права користування
Група 5 – авторське право та суміжні з ним права (право на комп'ютерні програми, програми для електронно-обчислювальних машин, компіляції даних (бази даних)), крім тих, витрати на придбання яких визнаються роялті;	Відповідно до правовстановлюючого документа, але не менш ніж 2 роки

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

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

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

$$С_а = (3200 + 459 + 510 + 2400 + 598) / 5 = 1433,4 \text{ грн.}$$

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

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 15210 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо реалізації засобів захисту інформації в гетерогенних мережах потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$$С_з = (15210*12 + 15210*12*0,1)*0,25= 50193 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2022 р. складає 22%. (мінімальний ЄСВ 1430,00 грн.)

$$С_{єв} = 50193 *0,22 = 11042,46 \text{ грн.}$$

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

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

де:

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

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

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

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

$$С_{ел} = 0,8*1920*1,64 = 2519,04 \text{ грн.}$$

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

$$С_{тос} = 31011,95 * 0,02 = 620,23 \text{ грн.}$$

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

$$С_к = 1433,4 + 50193 + 11042,46 + 2519,04 + 620,23 = 65807,9 \text{ грн.}$$

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

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

$$С = 65807,9 \text{ грн.}$$

3.2 Оцінка можливого збитку

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.), 20000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 10000 грн./міс.;

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

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 3 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 910 тис. грн. у рік;

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

I – число атакованих сегментів корпоративної мережі, 3;

N – середнє число атак на рік, 7.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де:

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

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

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

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

$$П_П = \frac{\sum З_с}{F} * t_п = \frac{10000*3}{176} * 4 = 681{,}81 \text{ грн},$$

де:

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

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

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де:

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

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

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

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

$$П_{ви} = \frac{\sum З_с}{F} * t_{ви} = \frac{10000*3}{176} * 3 = 511{,}36 \text{ грн.}$$

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

$$П_{пв} = \frac{\sum З_о}{F} * t_в = \frac{20000*2}{176} * 2 = 454{,}54 \text{ грн.}$$

Витрати на заміни встаткування або запасних частин можуть скласти 3400 грн.

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

$$П_в = 511{,}36 + 454{,}54 + 3400 = 4365{,}9 \text{ грн.}$$

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

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

$$V = \frac{910000}{2080} * (4 + 3 + 2) = 3937{,}5 \text{ грн.}$$

де:

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

$$U = 681{,}81 + 4365{,}9 + 3937{,}5 = 8985{,}21 \text{ грн.}$$

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

$$B = \Sigma_I \Sigma_N U = \Sigma_3 \Sigma_7\ 8985{,}21 = 188689.41 \text{ грн.}$$

Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \text{ грн.},$$

де:

B – загальний збиток від атаки у разі перехоплення інформації, 188689.41 грн.;

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

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

Загальний ефект від впровадження системи інформаційної безпеки за становитиме:

$$E = 188689.41 * 0,4 - 65807,9 = 9667,86 \text{ грн.}$$

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:

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

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:

$$ROSI = \frac{9667,86}{31011,95} = 0.31, \text{ частки одиниці,}$$

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

$$ROSI > (N_{деп} - N_{інф})/100),$$

де:

$N_{деп}$ – річна депозитна ставка, (10,75 %);

$N_{інф}$ – річний рівень інфляції, (10 %).

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,31 > (10–10,75)/100 = 0,31 > 0,0075.$$

Отже, запропоновані засоби захисту інформації в гетерогенних мережах 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:

$$T_o = \frac{К}{E} = \frac{1}{ROSI} = \frac{1}{0.31} = 3.22, \text{ років (38 місяців)}$$

3.4 Висновок

Запропоновані засоби захисту інформації в гетерогенних мережах для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації можна вважати економічно доцільними, оскільки значення коефіцієнту повернення інвестицій ROSI, що складає 0,31 при величині економічного ефекту 9667,86 грн. Отримане значення коефіцієнта ROSI перевищує дохідність альтернативного вкладення коштів. Термін окупності при цьому складатиме 3,22 років (приблизно 38 місяців). Капітальні витрати на засоби захисту інформації складуть в 31011,95 грн., а щорічні експлуатаційні витрати – 65807,9 грн.

ВИСНОВКИ

Головною метою кваліфікаційної роботи було підвищити рівень безпеки та захисту інформації у комплексній системі захисту інформації ТОВ «LIL GROUP»

У першому розділі проведено обстеження діяльності підприємства, Досліджена актуальність питання, особовий склад підприємства та його обов'язки, обстежені приміщення, у яких знаходиться та працює підприємство.

У спеціальному розділі наведено та обґрунтовано технічну частину даної роботи. Проведено аналіз інформаційного документообігу, можливих загроз інформаційній безпеці на підприємстві та розроблені модель порушника та внутрішнього порушника і модель загроз інформаційної безпеки. Виявлено співробітників, які становлять найбільшу загрозу підприємству. Наведено рекомендації щодо підвищення рівню інформаційної безпеки завдяки впровадженню політики антивірусного захисту, політики користування електронною поштою та політики безпеки паролів користувачів.

У економічному розділі проведено розрахунки збитку від реалізації загрози, визначено економічну доцільність та витрати на засоби забезпечення інформаційної безпеки підприємства. Термін окупності способів забезпечення безпеки інформації складатиме 3,22 років (приблизно 38 місяців).

ПЕРЕЛІК ПОСИЛАНЬ

1. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 кібербезпека / Упоряд.: О.В. Герасіна, Д.С. Тимофеєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП» 2020.
2. Методичні рекомендації до економічної частини дипломного проекту зі спеціальності 125 кібербезпека / Упоряд.: Д.П. Пілова – Дніпро: НТУ «ДП» 2019.
3. Рішення НКРЗ №512 від 11.11.2010 «Умови здійснення діяльності у сфері телекомунікацій з надання послуг доступу до Інтернет (Електрон. ресурс) Режим доступу до ресурсу: nkrz.gov.ua/uk/activities/ruling2/1289571519/
4. Закон Україні «Про інформацію» від 02.10.1992 No2657-XII // Відомості Верховної Ради України-1992-No48. (Електронний ресурс) Режим доступу до ресурсу: zakon.rada.gov.ua/laws/show/2657-12
5. Закон України № 1280-IV«Про телекомунікації»(Електрон. ресурс) / Режим доступу до ресурсу: *zakon.rada.gov.ua/go/1280-15*
6. Закон Україні «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 No80-VI // Відомості Верховної Ради України-1994-No80. (Електронний ресурс) Режим доступу до ресурсу: zakon.rada.gov.ua/laws/show/80/94-вр
7. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. (Чинний від

28.04.1999) – К.: ДСТСЗІ СБУ, 1999-No22 (Нормативний документ системи технічного захисту інформації)

8. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. (Чинний від 28.04.1999) – К.: ДСТСЗІ СБУ, 1999-No22 (Нормативний документ системи технічного захисту інформації)
9. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. (Чинний від 04.12.2000) – К.: ДСТСЗІ СБУ, 2000-No53 (Нормативний документ системи технічного захисту інформації)
10. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 28.04.1999] – К.: ДСТСЗІ СБУ, 1999-No22 (Нормативний документ системи технічного захисту інформації)
11. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. [Чинний від 28.04.1999] – К.: ДСТСЗІ СБУ, 1999-No22 (Нормативний документ системи технічного захисту інформації)
12. НД ТЗІ 3.6-001-2000 Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. [Чинний від 20.12.2000] – К.: ДСТСЗІ СБУ, 2000-No60 (Нормативний документ системи технічного захисту інформації)
13. ДСТУ 3396.1-96 Захист інформації. Технічний захист. інформації. Порядок проведення робіт
14. Гришачев В.В., Кабашкін В.Н., Фролов А.Д. Фізичні принципи формування каналів витоку інформації (Електронний ресурс):
    Режим доступу до ресурсу: https://it4business.ru/itsec/FizicheskiePrincipyFormirovanijaKanalovUtechkiInformaciiVVolokonnoOpticheskixLinijaxSvjazi
15. Домарьов В.В. Безпека інформаційних технологій. Методологія створення систем захисту. – вид. «ДіаСофт» 2011року

16. ОРГАНІЗАЦІЙНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ TZI.UA (Електронний ресурс) Режим доступу до ресурсу: https://www.tzi.ua/ua/organzacjn_metodi_zahistu_nformac.html
17. Політика облікових записів «STUDOPEDIA» (Електронний ресурс) Режим доступу до ресурсу: https://studopedia.su/5_47977_politika-paroliv.html
18. Політика антивірусного захисту «HELPIKS» (Електронний ресурс) Режим доступу до ресурсу: https://helpiks.org/6-26935.html
19. Загрози інформаційної безпеки коротко. Загроза інформаційної безпеки. Основні цілі та завдання інформаційної безпеки «sukachOFF» (Електронний ресурс) Режим доступу до ресурсу: https://sukachoff.ru/uk/noutbuki/ugrozy-informacionnoi-bezopasnosti-kratko-referat-ugroza/
20. Випробування комплексу засобів захисту «ІНФОПЕДІЯ» (Електронний ресурс) Режим доступу до ресурсу: https://infopedia.su/11xcbad.html
21. Програмні засоби захисту інформації «ВІКІПЕДІЯ» (Електронний ресурс) Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Програмні_засоби_захисту_інформації
22. Програмні засоби захисту інформації «ВІКІZERO» (Електронний ресурс) Режим доступу до ресурсу: https://www.wikizero.com/uk/Програмні_засоби_захисту_інформації

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	1	
5	А4	1 Розділ	28	
6	А4	2 Розділ	29	
7	А4	3 Розділ	13	
8	А4	Висновки	1	
9	А4	Перелік посилань	3	
10	А4	Додаток А. Відомість матеріалів кваліфікаційної роботи	1	
11	А4	Додаток Б. Перелік документів на оптичному носії	1	
12	А4	Додаток В. Відгук керівника економічного розділу	1	
13	А4	Додаток Г. Відгук керівника кваліфікаційної роботи	2	

ДОДАТОК Б. Перелік документів на оптичному носії

1. Презентація Диплом_Чорний_125-19ск-1.pptx
2. Текст до презентації.docx
3. Диплом_Чорний_125-19ск-1.pdf
4. Диплом_Чорний_125-19ск-1.docx
5. Рецензія Чорного Д.В..doc

ДОДАТОК В. Відгук керівника економічного розділу

Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку «відмінно» (90 балів).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-19ск-1

Чорного Дмитра Віталійовича

на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ "LIL GROUP"»

Кваліфікаційна робота виконана в повному обсязі у відповідності до завдання і представлена пояснювальною запискою та презентацією.

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 87 сторінках з додатками.

Об'єкт дослідження – Інформаційно-телекомунікаційна система ТОВ «LIL GROUP»

Мета кваліфікаційної роботи – підвищення рівня захисту інформації в інформаційно-телекомунікаційній системі ТОВ «LIL GROUP», розробка механізмів захисту в сфері інформаційної безпеки організації, розрахунок витрат на реалізацію проекту.

Тема безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека».

Актуальність обраної теми обумовлена необхідністю підвищення вимог до рівня інформаційної безпеки ІТС ТОВ «LIL GROUP» в сучасних умовах.

Для досягнення поставленої мети детально проаналізовано об'єкт дослідження та нормативно-правова база, інформаційні потоки, проведено

обстеження та визначені задачі, що потребують свого вирішення в кваліфікаційній роботі.

В спеціальній частині кваліфікаційної роботи проведено аналіз методів захисту інформації в ІТС, побудовано моделі загроз і порушника, розглянуто профіль захищеності, виявлено недоліки діючої ІТС та запропоновано методи та засоби щодо їх усунення.

Внесені додаткові елементи до діючої Політики безпеки на підприємстві.

В економічному розділі проаналізовано та визначено показники економічної ефективності запропонованих рекомендацій та загальний економічний ефект від їх впровадження.

Матеріали пояснювальної записки до кваліфікаційної роботи оформлено з дотриманням основних нормативних вимог.

Протягом дипломування проявив себе ініціативним, достатньо підготовленим та обізнаним фахівцем з питань кібербезпеки, здатним самостійно проводити дослідження та приймати ґрунтовні рішення, Має певний досвід практичної роботи по спеціальності.

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

В цілому кваліфікаційна робота заслуговує оцінки «д**обре**» (**87** балів), а її автор Чорний Д.В. присвоєння відповідної кваліфікації.

Керівник кваліфікаційної роботи,
к.т.н., доцент _____ О.О. Сафаров

Керівник спец. розділу,
старший викладач _____ С.І. Войцех