МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Сумський державний університет

Факультет електроніки та інформаційних технологій

Кафедра кібербезпеки

«До захисту допущено»

Завідувач кафедри

_____ Володимир ЛЮБЧАК

(підпис)

____ _____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавр

зі спеціальності 125 Кібербезпека та захист інформації, освітньо-професійної програми Кібербезпека

на тему: Розробка конфігурацій політик безпеки для елементів мережі відповідно до чинного законодавства України

Здобувачки групи КБ-01 Сазанова Анастасія Андріївна

(шифр групи) (прізвище, ім'я, по-батькові)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Анастасія САЗАНОВА

(підпис) (Ім'я та ПРІЗВИЩЕ здобувача)

Керівник старший викладач кафедри кібербезпеки, кандидат фізико-математичних наук, Віталій КОВАЛЬ _____

(посада, науковий ступінь, вчене звання, Ім'я та ПРІЗВИЩЕ) (підпис)

Суми – 2024

Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра кібербезпеки

«Затверджую»
Завідувач кафедри
_____ Володимир ЛЮБЧАК
(підпис)
«___»_____ 20___ р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ
на здобуття освітнього ступеня бакалавр
зі спеціальності 125 – Кібербезпека, освітньо-професійної програми «Кібербезпека»
здобувача групи КБ-01 Сазанової Анастасії Андріївни

1. Тема роботи: Розробка конфігурацій політик безпеки для елементів мережі відповідно до чинного законодавства України
затверджено наказом по СумДУ №0212-VI від «04» березня 20 24 р.
2. Термін подання студентом роботи: «04» червня 20 24 р.
3. Вихідні дані до роботи: _____
4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити):
1. Необхідність захисту інформації на науково-дослідних підприємствах;
2. Аналіз нормативних документів України щодо захисту інформації;
3. Визначення завдання; 4. Огляд організації; 5. Огляд об'єкта інформаційної діяльності; 6. Аналіз наявних ризиків для підприємства;
7. Розробка політик безпеки; 8. Впровадження політик безпеки;
9. Аналіз ризиків після впровадження політик безпеки.

5. Перелік графічного матеріалу (із зазначенням плакатів, презентацій тощо)
_____
6. Дата видачі завдання «____» _____ 20 ___ р.

Завдання прийняв до виконання _____ (підпис)
Керівник _____ (підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання	Примітка
1	Визначення завдання та об’єкта роботи		
2	Пошук та опрацювання теоретичного матеріалу з теми випускної роботи		
3	Огляд досліджуваного об’єкту та робота на місці		
4	Розробка та впровадження практичної частини кваліфікаційної роботи		
5	Оформлення кваліфікаційної роботи		

Здобувач вищої освіти _____ Керівник _____

(підпис) (підпис)

АНОТАЦІЯ

Кваліфікаційна робота виконана на 63 аркушах та містить 8 таблиць, 2 додатки та 32 джерела.

Об’єкт дослідження: захист оброблюваної інформації на підприємстві від зовнішніх та внутрішніх загроз .

Мета роботи: розробка та впровадження політик безпеки для забезпечення захисту інформації на основі чинного законодавства України, а також моделі загроз та моделі порушника.

Метод дослідження: комплексний метод, що поєднує в собі якісний та кількісний методи.

Результати роботи: визначено необхідність захисту інформації на досліджуваному підприємстві, проаналізовано закони, що регулюють захист інформації, проведено обстеження підприємства, а також розроблено модель загроз та модель порушника для ІС, розроблено та впроваджено політики безпеки, а також надано рекомендації керівництву щодо можливого покращення захисту інформації в системі.

Ключові слова: інформаційна система, модель загроз, модель порушника, політики безпеки, захист інформації, законодавство України.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ

АС – автоматизована система;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

КС – комп’ютерна система;

КСЗІ – комплексна система захисту інформації;

НСД – несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ПБ – політики безпеки;

ПЗ – програмне забезпечення;

СУІБ – система управління інформаційною безпекою.

ВСТУП

У час стрімкого розвитку світового інформаційного простору в Україні щодня впроваджуються нові та більш сучасні інформаційні та телекомунікаційні технології: розроблюються елементи смарт-інфраструктури у великих містах, впроваджується діджиталізація сфери охорони здоров'я, розробляються та впроваджуються системи електронного врядування, все частішим стає використання технологій інтернету речей, а також все більше розвивається автоматизація процесів, які донедавна ще виконувалися людьми. Телекомунікаційні системи активно впроваджуються чи не в усі сфери життя суспільства.

І одним із головних питань постає захист інформації, яка оброблюється в цих системах. У будь-якій інформаційній системі оброблювана інформація має бути захищеною, мають бути вжитими методи і засоби, які забезпечуватимуть конфіденційність, цілісність і доступність цієї інформації за умови впливу на неї загроз будь-якого походження.

Актуальність проблем захисту інформації в сучасних реаліях визначається наступними чинниками:

– зростанням кількості залучених користувачів у інформаційний процес, та відповідно їх інформаційних потреб;

– збільшенням рівня важливості та кількості важливої інформації;

– зростанням масштабів інформаційних систем, в яких циркулює інформація, яка підлягає захисту.

Відповідно, через наведені причини, зростає потреба в захисті інформаційних систем та оброблюваної ними інформації від компрометації, модифікації, викрадення та інших небажаних та протиправних дій.

Предметом дослідження є існуючі політики безпеки об'єкта інформаційної діяльності.

Об'єктом дослідження є інформаційна система підприємства, що займається дослідженнями та експериментальними розробками у сфері природничих і технічних наук.

Метою роботи є розробка та впровадження політики безпеки для підприємства, що займається дослідженнями та експериментальними розробками у сфері природничих і технічних наук згідно чинного законодавства України.

Практичне значення отриманих результатів полягає в удосконаленні існуючої системи захисту інформації на підприємстві шляхом впровадження розроблених політик безпеки.

Тезу про необхідність розробки та впровадження політик безпеки згідно чинного законодавства опубліковано у матеріалах Міжнародної наукової конференції молодих учених «IMA::2024», 22-26 квітня 2024 року [32].

1 ЗАХИСТ ІНФОРМАЦІЇ В НАУКОВО-ДОСЛІДНИЦЬКІЙ ДІЯЛЬНОСТІ: АНАЛІЗ НОРМАТИВНИХ ДОКУМЕНТІВ, ВИЗНАЧЕННЯ ЗАВДАННЯ

1.1 Захист інформації в інформаційних системах підприємств, що займаються дослідженнями та експериментальними розробками у сфері природничих і технічних наук

На підприємствах, що займаються дослідженнями та експериментальними розробками у сфері природничих і технічних наук ключовим фактором успішності та переваг над іншими аналогічними організаціями є використання інноваційних технологій, а також сучасні теоретично-практичні знання та навики спеціалістів. З цього слідує, що на таких підприємствах оброблюється така цінна інформація, як:

– результати розробок та досліджень;

– стратегії та плани розвитку;

– інтелектуальна власність;

– дані про партнерів та клієнтів.

Розголошення вищеописаної інформації третім особам може призвести до втрати довіри партнерів та/або клієнтів, а також до значних фінансових втрат, що в подальшому може призвести до банкрутства організації. Тому науково-дослідним підприємствам вкрай необхідно вживати заходів захисту оброблюваної інформації.

Захист цих даних від несанкціонованого доступу, модифікації, викрадення, розголошення або знищення є дуже важливим з ряду наступних причин:

1. Захист інтелектуальної власності: підприємства інвестують достатню кількість грошей в проведення досліджень та розробок, з очікуванням отримання прибутку. В подальшому, витік цієї інформації може призвести до того, що конкуренти можуть скопіювати ці технології, методи або продукти,

цим самим створивши конкуренцію на ринку послуг, або взагалі позбавивши організацію нових клієнтів, а відповідно і прибутку.

2. Захист конфіденційної інформації: підприємство володіє певною інформацією про своїх співробітників, партнерів та клієнтів. У разі її витоку, це може бути використано для нанесення шкоди репутації або інтересам підприємства. Як наслідок, буде втрачена довіра до організації, а також можуть бути фінансові втрати, а також судові позови до організації, що також не додає довіри.

3. Захист від кіберзлочинів: у випадку кібератак на підприємство організація може окрім фінансових втрат, зазнати перебоїв у роботі, викрадення цінної інформації з метою подальшого її викупу, або простої втрати всієї інформації, яка була напрацьована за роки існування, і яка приносила дохід підприємству.

4. Відповідність законодавству: існує ряд нормативних документів (в подальшому будуть проаналізовані в роботі), які регулюють захист інформації, недотримання яких може призвести до накладення штрафів на підприємство, судових позовів та інших заходів.

З вищенаведених факторів можна зробити висновок, що до захисту інформації у науково-дослідних організаціях слід підходити дуже уважно і з дотриманням вимог чинного законодавства, адже тоді підприємство буде успішно виконувати свою роботу, мати довіру серед клієнтів та потенційних клієнтів, а також отримувати з цього прибуток, що є головним у діяльності будь-якого підприємства.

1.1.1 Основні загрози інформаційній безпеці підприємства

Загрози захисту ІзОД в системі можуть бути як зовнішніми, так і внутрішніми. До зовнішніх загроз можна віднести:

– конкуренція;

– економічні зміни;

– зміни в державній політиці;

– геополітична нестабільність;

– кіберзлочинність.

Водночас до внутрішніх загроз можуть бути віднесені наступні фактори:

– великий плин кадрів;

– недостатня обізнаність працівників щодо поводження із пристроями, які є в системі;

– недостатнє усвідомлення робітниками цінності інформації;

– недостатній контроль за дотриманням культури інформаційної безпеки;

– особистий мотив працівників.

Для мінімізації наведених загроз необхідно вжити наступні заходи:

1. Розробити та впровадити стратегію інформаційної безпеки на підприємстві, з періодичним її переглядом та оновленням;

2. Використовувати технічні засоби захисту інформації;

3. Навчати персонал правилам інформаційної безпеки;

4. Забезпечувати регулярний контроль та аудит інформаційних систем підприємства.

1.1.2 Інциденти ІБ на підприємстві

Розглянемо поняття інциденту інформаційної безпеки, події інформаційної безпеки та управління інцидентами інформаційної безпеки відповідно до міжнародного стандарту ISO/IEC 27035-1:2023:

подія інформаційної безпеки – подія, яка вказує на можливе порушення інформаційної безпеки або збій засобів контролю [1];

інцидент інформаційної безпеки – пов’язана та ідентифікована подія (події) інформаційної безпеки, яка може завдати шкоди активам організації або поставити під загрозу її діяльність [1];

управління інцидентами інформаційної безпеки – це набір процесів для виявлення, звітування, оцінки, реагування на інциденти інформаційної безпеки, роботи з ними та навчання з них [1].

Основні цілі управління інцидентами ІБ:

1. Швидке відновлення систем та сервісів до нормальної роботи.

2. Мінімізація впливу інцидентів на організацію.

3. Ефективне використання ресурсів.

4. Єдина система обробки інцидентів.

5. Використання отриманої інформації для оптимізації процесів підтримки, запобігання повторенню інцидентів та планування майбутніх дій.

Для ефективного управління інцидентами система мати широкий спектр функцій, які охоплюють усі аспекти виявлення, реагування та аналізу інцидентів інформаційної безпеки. До ключових функцій належать:

1. Управління системою та обробка інцидентів:

– наявність власної консолі адміністрування для управління системою та налаштуванням її параметрів;

– розподіл ролей та повноважень користувачів;

– можливість налаштування правил обробки інцидентів, а також сповіщень;

– контроль цілісності системи та її компонентів.

2. Моніторинг та захист агентів:

– моніторинг статусу агентів, встановлених на комп’ютерах, в режимі реального часу;

– контроль роботи агентів;

– налаштування політик роботи агентів;

– захист агентів від видалення або виключення з комп’ютерів;

– контроль цілісності агентів та їх компонентів.

3. Система сповіщень та реагування:

– налаштування сповіщень про інциденти, які надсилаються відповідальним особам;

– автоматизована реакція на інциденти, що дасть змогу системі вжити певних заходів з мінімізації наслідків;

– аналіз подій для виявлення закономірностей та тенденцій;

– документація інцидентів для подальшого аналізу.

4. Звітність:

– формування звітів про роботу системи управління, включаючи інформацію про статистику, типи інцидентів, а також час їх вирішення, причини та наслідки;

– можливість генерувати звіти за різними періодами, категоріями інцидентів, підрозділами або користувачами;

– збереження звітів в локальному сховищі на випадок недоступності сервера;

– експорт звітів у різних форматах для подальшого аналізу та обробки;

– запис в журнал реєстрації дій адміністраторів системи.

Відповідно до ITIL визначено основні етапи управління інцидентами:

1. Ідентифікація інциденту.

2. Реєстрація інциденту.

3. Категоризація інциденту.

4. Визначення пріоритету інциденту.

5. Визначення впливу.

6. Вирішення інциденту.

7. Повідомлення користувачі.

8. Закриття інциденту.

Для ефективного розслідування та запобігання інцидентів інформаційної безпеки (ІБ) в організації рекомендується:

1. Створити чітку структуру відповідальності:

– розробити посадові інструкції, правила та регламенти, які чітко визначають права та обов'язки персоналу щодо ІБ, ці документи мають бути пов'язані з поточними бізнес-процесами, щоб допомогти персоналу прогнозувати й мінімізувати наслідки ІБ-інцидентів;

– розробити політики безпеки з детальними документами, чітко окреслюючи відповідальність працівників усіх рівнів у межах їхніх повноважень.

2. Впровадити дієвий дисциплінарний процес:

– створити чіткий процес розслідування порушень ІБ, який включає оцінку наслідків інцидентів;

– запровадити адекватні заходи впливу на порушників, ґрунтуючись на серйозності порушення.

3. Дотримуватися законодавства:

– при визначенні заходів запобігання ІБ-інцидентам фахівцю з ІБ необхідно керуватися чинним законодавством України.

Також необхідно:

– провести навчання персоналу з питань ІБ, щоб підвищити рівень обізнаності та розуміння ризиків;

– регулярно оновлювати політики та процедури ІБ, щоб вони відповідали мінливим загрозам;

– впровадити системи моніторингу та контролю для виявлення та реагування на ІБ-інциденти;

– проводити регулярні тести на проникнення та оцінки вразливості для виявлення потенційних проблем ІБ;

– створити культуру кібербезпеки в організації, яка заохочує персонал повідомляти про підозрілу активність та дотримуватися кращих практик ІБ.

Впровадження цих заходів допоможе організації ефективніше розслідувати ІБ-інциденти, запобігати їх повторенню та захищати свої інформаційні активи.

1.1.3 Політики безпеки

Відповідно до НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» під політикою безпеки інформації слід розуміти набір вимог, правил, обмежень, рекомендацій і т. ін.,

які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо АС, окремого її компонента, послуги захисту, що реалізується системою і т. ін. Політика безпеки інформації в АС є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи [2].

Політика безпеки повинна бути гнучкою та адаптивною, щоб не було потреби в частій модифікації. Занадто чітка деталізація, наприклад, вказівка конкретних назв або версій програмного забезпечення, може свідчити про надмірну конкретизацію, яка обмежує гнучкість.

Принципи, на яких має базуватися політика безпеки:

– неперервність захисту: забезпечення постійного та безперебійного захисту інформаційних ресурсів;

– відповідність загрозам: політика повинна враховувати та адаптуватися до актуальних загроз ІБ;

– системний підхід: комплексне та системне впровадження заходів захисту, що охоплюють всі аспекти ІБ;

– комплексність: використання різнобічних методів та засобів захисту для забезпечення багаторівневого захисту;

– достатність ресурсів: забезпечення достатнього рівня ресурсів та заходів захисту, адекватних ризикам та потребам організації;

– гнучкість: можливість адаптації системи захисту до мінливих умов та нових викликів;

– простота використання: проста та зрозуміла для користувачів система захисту, що мінімізує ризик помилок;

– відкритість алгоритмів: забезпечення відкритості алгоритмів та механізмів захисту, якщо це не суперечить іншим міркуванням.

Процедура розробки політики безпеки:

1. Формування концепції ІБ.

2. Аналіз ризиків ІБ.

3. Визначення вимог до засобів захисту ІБ.

4. Вибір основних рішень із забезпечення ІБ.

5. Організація відновлювальних робіт та безперервного функціонування інформаційної системи.

6. Документальне оформлення політики інформаційної безпеки.

1.2 Аналіз нормативних документів чинного законодавства України щодо захисту інформації

Система захисту інформації ґрунтується на комплексному підході, що включає нормативно-правове регулювання та практичні заходи.

Нормативно-правова база захисту інформації в Україні все ще перебуває на стадії розвитку, однак вже зараз визначено низку ключових напрямків роботи:

1. Розробка базового закону:

– цей закон має стати фундаментом для всієї системи захисту інформації;

– він повинен чітко окреслювати принципи та механізми інформаційної безпеки, а також розподіл повноважень між різними суб'єктами.

2. Регламентація рівнів безпеки:

– базовий закон має визначити різні рівні інформаційної безпеки, що відповідають різним категоріям інформації та її цінності;

– для кожного рівня безпеки мають бути встановлені відповідні методи та засоби захисту.

3. Стандартизація та сертифікація:

– ці два напрямки є важливими інструментами для забезпечення єдиного підходу до захисту інформації;

– стандартизація має визначити чіткі вимоги до систем та засобів захисту інформації;

– сертифікація має підтверджувати відповідність цих систем та засобів встановленим стандартам.

Важливими завданнями в цій сфері також є:

– розробка законодавчих актів та правових норм, що охоплюють всі аспекти захисту інформації;

– визначення специфічних підходів до захисту інформації в різних сферах діяльності;

– створення системи стандартизації та сертифікації, що відповідає міжнародним практикам;

– забезпечення нормативного та метрологічного підґрунтя для контролю за ефективністю систем та засобів захисту інформації.

1.2.1 Огляд законів України, що встановлюють правові норми в інформаційному середовищі

Інформаційна сфера України регулюється комплексом законів, які визначають права та обов’язки суб’єктів інформаційних відносин, встановлюють принципи доступу до інформації, її захисту та охорони.

Серед ключових законів, що визначають правові засади інформаційної сфери в Україні, можна виділити:

Закон України "Про інформацію": Цей базовий закон закріплює право громадян на вільний доступ до інформації, визначає систему інформації, її джерела, а також механізми захисту інформації від несанкціонованого доступу, поширення та використання [3].

Закон України "Про державну таємницю": Цей закон визначає порядок віднесення інформації до державної таємниці, її засекречування та розсекречування, а також заходи щодо її захисту [4].

Закон України "Про науково-технічну інформацію": Цей закон регулює діяльність у сфері науково-технічної інформації, встановлюючи правила збирання, обробки, зберігання та поширення науково-технічної інформації [5].

Закон України "Про захист інформації в автоматизованих системах": Цей закон встановлює порядок захисту інформації в автоматизованих системах, запобігаючи її несанкціонованому доступу, поширенню та використанню [6].

Законодавство України про інформаційну сферу постійно розвивається та вдосконалюється. Це зумовлено стрімким розвитком інформаційно-комунікаційних технологій та появою нових викликів та загроз.

1.2.2 Огляд нормативних документів в області технічного захисту інформації

В Україні діє ряд нормативних документів (НД ТЗІ), які регулюють технічний захист інформації:

– **ДСТУ 3396.1-96: Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт.** У цьому стандарті встановлено загальні вимоги до проведення робіт з технічного захисту інформації [7];

– **НД ТЗІ 1.1-002-99: Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.** Документ встановлює загальні положення щодо захисту інформації в КС від несанкціонованого доступу [8];

– **НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.** Цим документом встановлюються критерії оцінки захищеності інформації в КС від несанкціонованого доступу [9];

– **НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі несанкціонованого доступу.** Документ встановлює класифікацію АС та стандартні функціональні профілі несанкціонованого доступу [10];

– **НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі.** Цей документ визначає основні завдання, функції та структуру служби захисту інформації в АС [2];

– **НД ТЗІ 3.7-003-05: Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.** Цим документом визначається порядок розробки та впровадження комплексної системи захисту інформації в ІТС [11].

1.2.3 Огляд міжнародних стандартів забезпечення інформаційної безпеки на підприємствах

ISO/IEC 27001:2022: стандарт є основоположним для систем управління інформаційною безпекою (СУІБ) на підприємствах. Він описує вимоги до СУІБ, спрямовані на захист інформаційних активів від конфіденційності, цілісності та доступності [12].

ISO/IEC 27002:2022: стандарт містить практичні рекомендації щодо впровадження СУІБ, описуючи 149 елементів управління, які можуть бути використані для захисту інформаційних активів [13].

ISO/IEC 27017:2015: стандарт фокусується на захисті інформаційних активів в хмарних середовищах. Він містить рекомендації щодо встановлення вимог до постачальників хмарних послуг та управління ризиками, пов'язаними з використанням хмарних технологій [14].

ISO/IEC 27018:2019: стандарт описує вимоги до захисту персональних даних в інформаційних системах. Він базується на принципах GDPR (General Data Protection Regulation) та допомагає підприємствам дотримуватися вимог цього регламенту [15].

ISO/IEC 27032:2023: стандарт містить рекомендації щодо кібербезпеки. Він описує методи та практики, які можуть бути використані для захисту інформаційних систем від кібератак [16].

ISO/IEC 27007: стандарт описує керівні принципи для визначення та вимірювання рівня інформаційної безпеки в організаціях. Він допомагає

підприємствам оцінити ефективність своїх систем інформаційної безпеки та приймати обґрунтовані рішення щодо їх покращення [17].

ISO/IEC 27036: стандарт містить рекомендації щодо управління кіберстійкістю. Він описує методи та практики, які можуть бути використані для захисту інформаційних систем від кіберзагроз та мінімізації наслідків кіберінцидентів [18].

ISO/IEC 27701: стандарт описує систему управління захистом інформації на основі принципів ISO/IEC 27001. Він допомагає підприємствам впровадити систему захисту інформації, яка відповідає вимогам міжнародних стандартів та кращих практик [19].

ISO/IEC 27040: стандарт описує керівні принципи для розробки та впровадження систем управління інцидентами інформаційної безпеки. Він допомагає підприємствам ефективно реагувати на кіберінциденти та мінімізувати їхні наслідки [20].

1.3 Визначення завдання

Аналіз нормативно-правової бази чітко підкреслює необхідність захисту інформації на комерційних підприємствах. Це питання не лише безпеки, але й конкурентоспроможності та стійкості бізнесу. З метою ефективного захисту інформації на ФОП Сема О. Г. необхідно виконати ряд завдань:

1. Зібрати дані про підприємство, провести обстеження ОІД, інформаційного середовища та обчислювальної системи.

2. На основі зібраних даних розробити модель загроз, які можуть виникнути для інформації підприємства.

3. Сформувати політику безпеки та створити інструкції та рекомендації.

4. Провести аналіз ризиків та вибрати профіль захищеності.

5. Впровадити політику безпеки, провести аналіз ризиків після впровадження та забезпечити постійний контроль та вдосконалення.

Виконання цих завдань допоможе ФОП Сема О. Г. створити надійну систему захисту інформації, яка гарантує конфіденційність, цілісність та доступність інформаційних активів.

2 АНАЛІЗ РИЗИКІВ ТА ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

2.1 Огляд організації

В роботі аналізується діяльність приватного підприємства ФОП Сема О. Г., яке займається дослідженням й експериментальними розробками у сфері інших природничих і технічних наук.

2.1.1 Організаційна структура

Підприємство працює щодня, з понеділка по п’ятницю з 9:00 до 18:00, субота та неділя – вихідні.

Графік роботи співробітників:

Директор з 9:00 до 18:00 в робочі дні, перерва з 13:00 до 14:00 (1 година).

Дослідники (наукові співробітники, лабораторні працівники) з 9:00 до 17:45 в робочі дні, перерва з 12:45 до 13:45 (1 година).

Персонал з підтримки чистоти позмінно 2/2 з 10:00 до 17:00 у робочі дні, перерва з 13:30 до 14:15 (45 хвилин).

Чисельність штату співробітників:

– директор – 1 особа;

– наукові співробітники – 2 особи;

– лабораторні працівники – 2 особи;

– персонал з підтримки чистоти – 2 особи;

Загалом: 7 осіб.

2.2 Огляд об’єкта інформаційної діяльності

Об’єкт розташований у двоповерховій будівлі, що знаходиться у спальному районі із майже відсутнім рухом транспортних засобів.

Підприємство розміщується у 3 кімнатах кутового розташування на 1 поверсі. На рисунку 2.1 наведено генеральний план приміщень із зображенням розташування основних виробничих та додаткових об’єктів підприємства. Умовні позначення до плану наведені в таблиці 2.1.

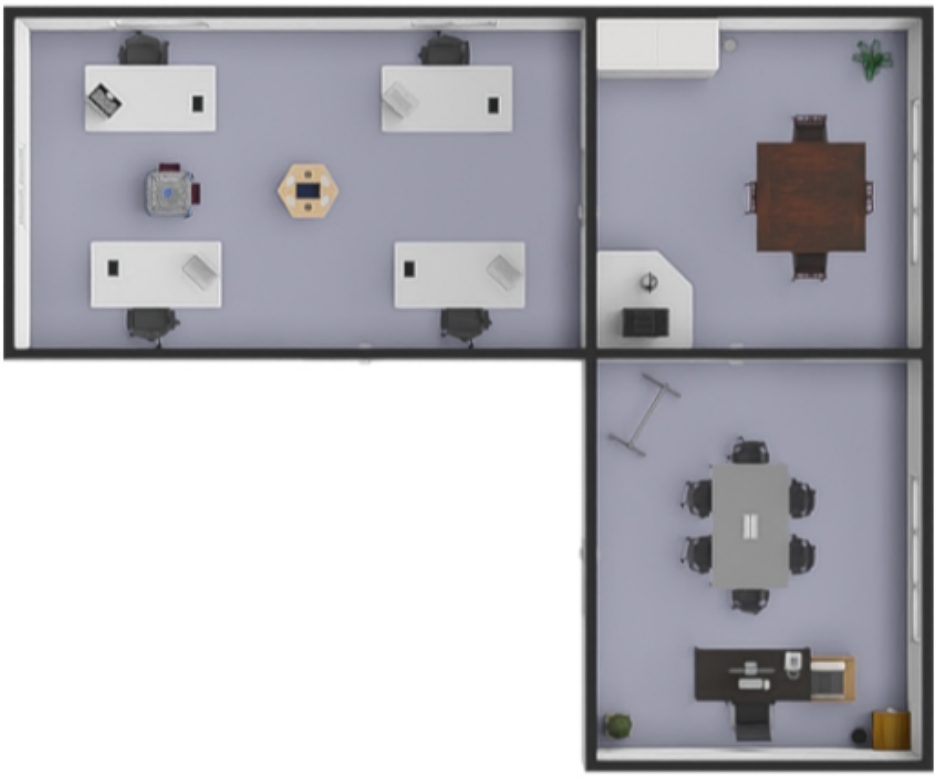
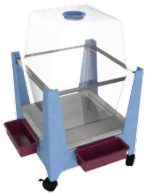


Рисунок 2.1 – Генеральний план приміщень підприємства ФОП Сема О. Г.

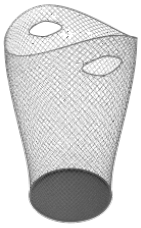
Таблиця 2.1 – Умовні позначення

№	Позначка	Найменування
1	**2**	**3**
1		Ноутбук співробітника
2		Записи співробітника

Продовження таблиці 2.1

1	2	3
3		Стіл співробітника
4		Стілець співробітника
5		Наукове обладнання
6		Наукове обладнання
7		Кухонне обладнання
8		Кухонний стіл

Продовження таблиці 2.1

1	2	3
9		Кавомашина
10		Електрочайник
11		Обідній стіл для робітників
12		Сміттєвий кошик
13		Фліпчарт

Продовження таблиці 2.1

1	2	3
14		Конференц-стіл зі стільцями
15		Шафа для документів
16		Робоче місце директора
17		Комп’ютер директора
18		Стаціонарний телефон

Продовження таблиці 2.1

1	2	3
19		Принтер
20		Тумба під принтер
21	 	Живі рослини

Доступ до об’єкта не контролюється системою контролю доступу. Охорона у організації відсутня, лише загальна охорона будівлі. Також у компанії відсутній спеціаліст з ІБ, який числиться у штаті співробітників, усі попередні налаштування мережі робили майстри тієї будівлі, в якій розташоване приміщення, доступ до приміщення було надано для подальшого проведення робіт, але документування розміщення пристроїв було заборонене.

2.2.1 Огляд обчислювальної системи підприємства

На об’єкті розташовано 1 комп’ютер у директора. Співробітники працюють на ноутбуках, що під’єднані до мережі через Wi-Fi. Також в кабінеті директора є принтер, а також стаціонарний телефон. Підприємство використовує лише ліцензійне ПЗ.

Мережу підприємства поділено на дві групи – директор має доступ до усієї інформації мережі, а інші співробітники лише до тієї, яка необхідна їм для виконання їх роботи. У кожного працівника є свій обліковий запис, який вони використовують для доступу до мережі.

Зовнішні носії інформації можуть використовувати усі співробітники. Доступ до мережі Інтернет є необмеженим для всіх працівників.

У середовищі Cisco Packet Tracer відтворено схему мережі інформаційної системи ФОП Сема О. Г. (рис. 2.2).

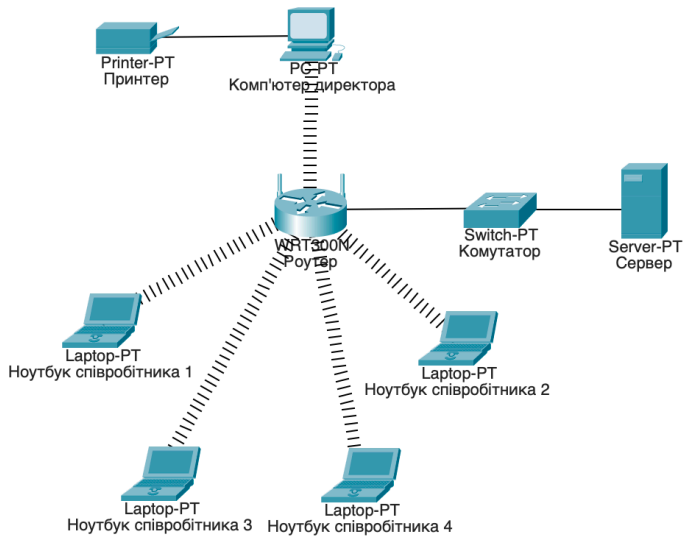


Рисунок 2.2 – Схема мережі інформаційної системи ФОП Сема О. Г.

Відповідно до НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» ФОП Сема А. Г. використовує автоматизовану систему третього класу, бо система складається з декількох комп'ютерів, що взаємодіють між собою, одночасно пристроями можуть користуватися декілька користувачів, у користувачів різні права доступу до інформації, а також у системі обробляється інформація різних категорій конфіденційності [10].

Таблиці 2.2 та 2.3 містять опис апаратного та програмного забезпечення мережі ФОП Сема О. Г.

Таблиця 2.2 – Перелік апаратного забезпечення

№	Назва	Модель	Кількість, шт.
1	Ноутбук	ASUS VivoBook 15 OLED M1505YA-L1037	4
2	Монітор	27" Samsung Curved LS27C366	1
3	Системний блок	Artline Business B27 v36	1
4	Wi-Fi роутер	TP-LINK Archer A8	1
5	Мишка	A4Tech Fstyler FM12ST	5
6	Клавіатура	OfficePro SK1550 Wireless	1
7	Принтер	Epson EcoTank L1250 with Wi-Fi	1
8	Сервер	ARTLINE Business T15 v16	1
9	Мережева карта	TP-LINK TG-3468	5
10	Комутатор	TP-LINK LS1008G	1

Таблиця 2.3 – Перелік програмного забезпечення

№	Тип ПЗ	Назва
1	**2**	**3**
1	Операційна система	Windows 8

Продовження таблиці 2.3

1	2	3
2	Прикладне ПЗ	Microsoft Office 2013
3		Google Chrome
4		Kaspersky Endpoint Security
5		WinRAR
6	ПЗ для роботи	Asana
7		Plotly
8		LabVIEW
9		SPSS
10		Zoom
11		Google Drive
12	Операційна система сервера	Microsoft Windows Server 2016

2.2.2 Огляд інформаційного середовища підприємства

Відповідно до НД ТЗІ 1.6-005-2013: об’єкт інформаційної діяльності – інженерно-технічна споруда (приміщення), транспортний засіб, де здійснюється озвучення та/або обробка технічними засобами інформації з обмеженим доступом [21].

ФОП Сема О. Г. працює з інформацією двох рівнів доступу – відкритою та з обмеженим доступом, а саме конфіденційною. Відповідно до ЗУ «Про інформацію»: конфіденційною є інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень, а також інформація, визнана такою на підставі закону. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом.

Відповідно до НД ТЗІ 1.1-003-99: конфіденційність інформації – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом [22].

На підприємстві не обробляється інформація, що належить до державної таємниці. Це підтверджується переліком інформації, що наведений у таблиці 2.4.

Таблиця 2.4 – Інформаційні активи ОІД

№	Інформація	Доступ	Обмеження
1	**2**	**3**	**4**
1	Наукові дослідження	Обмежений	Конфіденційна інформація
2	Експериментальні розробки	Обмежений	Конфіденційна інформація
3	Фінансова інформація	Обмежений	Конфіденційна інформація
4	Персональні дані	Обмежений	Конфіденційна інформація
5	Інформація про інтелектуальну власність	Обмежений	Конфіденційна інформація
6	Організаційно-правові документи підприємства	Обмежений	Конфіденційна інформація

Відповідно до НД ТЗІ 1.1-003-99: матриця доступу (access matrix) – n-мірна таблиця, вздовж кожного виміру якої відкладені ідентифікатори об’єктів КС одного типу (об’єктів-користувачів, об’єктів-процесів чи пасивних об’єктів), і містить як елементи права доступу за кожним із типів доступу [22].

У таблиці 2.5 наведено матрицю доступу до ІзОД співробітників підприємства.

Таблиця 2.5 – Матриця доступу співробітників до ІзОД

№	Директор	Співробітник
1	**2**	**3**
1	Ч, З, В	Ч, З

Продовження таблиці 2.5

1	2	3
2	Ч, З, В	Ч, З
3	Ч, З, В	–
4	Ч, З, В	–
5	Ч, З, В	Ч
6	Ч, З, В	Ч

Ч – право на читання інформації, З – право на запис інформації, В – право на видалення інформації, «–» – відсутнє право доступу до цієї інформації.

2.2.3 Аналіз загроз інформації

Відповідно до НД ТЗІ 1.1-003-99: модель загроз – абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз [22].

Загалом загрози можна поділити на три категорії:

– антропогенні (зумовлені діями суб’єкта);

– техногенні (зумовлені технічними засобами);

– стихійні (зумовлені стихійними джерелами).

Антропогенні загрози можна поділити на зовнішні та внутрішні. До зовнішніх загроз відносяться випадкові (недбалість або незнання осіб, що може завдати шкоди системі) та навмисні (спеціально націлені дії на завдання шкоди інформаційній системі, з метою власної вигоди). Внутрішні загрози також поділяються на випадкові та навмисні, обґрунтування дій таке саме, але дії виконуються саме співробітниками підприємства.

Техногенні загрози це загрози, що виникають через непередбачувані або неминучі збої в роботі обладнання, що призводить до ризику втрати або пошкодження інформації. Такі загрози важко спрогнозувати заздалегідь. Вони можуть бути як зовнішнього походження, так і внутрішнього.

Стихійними загрозами є події, що виникають внаслідок природних явищ, і можуть завдати шкоди персоналу, майну та інформації.

У таблиці 2.6 наведено перелік потенційних загроз із зазначенням того, яку властивість інформації буде порушено.

Таблиця 2.6 – Потенційні загрози інформації

№	Потенційна загроза	Властивість інформації, що буде порушена			
		К	Ц	Д	С
1	2	3	4	5	6
1	Несанкціоноване підключення до пристроїв	+	+	+	
2	Читання даних, що виводяться на екран, залишених відкритих файлів	+			+
3	Перехоплення акустичної інформації	+			+
4	Воєнні дії	+	+	+	+
5	Стихійні явища		+	+	
6	Відсутність електропостачання		+	+	
7	Відмова/збій програмного забезпечення	+	+	+	
8	Відсутність інтернету		+	+	
9	Несанкціонований перегляд візуальної інформації	+			+
10	Зараження системи вірусами	+	+	+	
11	Втрата паролів	+	+	+	
12	Втрата резервних копій		+	+	+
13	Пошкодження носіїв інформації		+	+	
14	Некоректне налаштування прав доступу працівників до інформації	+		+	

Продовження таблиці 2.6

1	2	3	4	5	6
15	Допуск до системи неавторизованих осіб	+	+	+	
16	Відсутність шифрування даних	+			+
17	Недбале зберігання документації	+	+	+	
18	Атаки на інформаційну систему	+	+	+	+

2.2.4 Модель порушника

Відповідно до НД ТЗІ 1.1-003-99: Модель порушника – формалізований або неформалізований опис порушника [22].

Порушники можуть бути внутрішніми (ті, що працюють на підприємстві) та зовнішніми. Відповідно до НД ТЗІ 1.4-001-2000 порушника можна класифікувати за:

1. Рівнем можливостей:

– 1 рівень визначає найнижчий рівень можливостей ведення діалогу з АС – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

– 2 рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

– 3 рівень визначається можливістю управління функціонуванням АС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

– 4 рівень визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

2. Рівнем знань про АС:

– 1 рівень визначає порушників, що володіють інформацією про функціональні особливості АС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;

– 2 рівень визначає порушників, що володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

– 3 рівень визначає порушників, що володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації АС;

– 4 рівень визначає порушників, що володіють інформацією про функції та механізм дії засобів захисту.

3. Використовуваними методами і способами:

– використовують виключно агентурні методи одержання відомостей; - використовують пасивні технічні засоби перехоплення інформаційних сигналів;

– використовують виключно штатні засоби АС або недоліки проектування КСЗІ для реалізації спроб НСД;

– використовують способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

4. Місцем здійснення дії:

– без одержання доступу на контрольовану територію організації (АС);

– з одержанням доступу на контрольовану територію, але без доступу до технічних засобів АС;

– з одержанням доступу до робочих місць кінцевих (у тому числі віддалених) користувачів АС;

– з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів тощо);

– з одержанням доступу до засобів адміністрування АС і засобів керування КСЗІ [2].

Після аналізу нормативного документу для підприємства можна розробити наступну модель порушника (табл. 2.7):

Таблиця 2.7 – Модель порушника

№	Порушник	Рівнем можливостей	Рівнем знань про АС	Використовуваними методами і способами	Місцем здійснення дії
Внутрішні					
1	Директор	3	3	3	4
2	Наукові співробіт-ники	2	2	2	3
3	Лаборатор-ні праців-ники	2	2	2	2
4	Персонал з підтримки чистоти	1	1	1	2
Зовнішні					
1	Конкуренти	2	2	2	2
2	Обслугову-ючий персонал	1	2	2	1
3	Хакери	4	4	3	1
4	Шантажисти	2	2	1	1

2.3 Аналіз ризиків для підприємства

На основі аналізу загроз та моделі порушника проведено аналіз ризиків. А саме визначено ймовірні наслідки, ймовірність їх виникнення, величина збитків та потенційні втрати.

Згідно з ISO/IEC 27000, аналіз ризику – це процес розуміння та визначення рівня ризику.

Під час проведення аналізу ризику необхідно:

1. Визначити види інформації, які можуть бути пошкоджені.

2. Оцінити ймовірність реалізації загрози.

3. Оцінити величину збитків.

4. Визначити ймовірні наслідки:

– Фінансові втрати:

– Прямі збитки (втрата доходів, витрати на відновлення даних, штрафи);

– Непрямі збитки (втрата клієнтів, шкода для репутації).

– Зниження продуктивності праці:

– Перебої в роботі, простої, втрата робочого часу;

– Зниження якості роботи, помилки.

– Неприємності для підприємства (які впливають на рівень суспільної довіри):

– Зниження довіри до підприємства з боку клієнтів, партнерів, інвесторів;

– Пошкодження іміджу та репутації;

– Можливі судові позови.

Аналіз ризику дозволяє прийняти обґрунтовані рішення щодо захисту інформації, оптимізувати витрати на інформаційну безпеку та знизити ймовірність виникнення негативних наслідків.

У додатку А наведено попередній аналіз ризиків для підприємства.

3 СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НАУКОВО-ДОСЛІДНОГО ПІДПРИЄМСТВА

3.1 Розробка політики безпеки

Метою розробки політики безпеки є забезпечення захисту інформації на підприємстві ФОП Сема О. Г. від загроз на основі системи поглядів, основних принципів, практичних вимог та рекомендацій.

Ця політика безпеки є обов'язковими для виконання всіма співробітниками ФОП Сема О. Г., а також особами, які працюють з інформацією, що належить ФОП Сема О. Г., в рамках укладеного контракту.

При розробці політики безпеки було враховано наступні фактори:

– види інформації, що обробляється в системі, а також технології обробки цієї інформації;

– особливості використовуваного апаратного та програмного забезпечення;

– фізичне розташування об'єктів інформаційної діяльності;

– модель порушника;

– попередній аналіз ризиків для підприємства.

Предметом політики безпеки є:

1. Політика налаштувань маршрутизатора.
2. Політика налаштувань брандмауерів.
3. Політика налаштувань IDS/IPS систем.
4. Політика використання антивірусного забезпечення.
5. Політика використання ноутбуків співробітниками.
6. Політика щодо систем резервного копіювання та відновлення.
7. Політика фізичного захисту мережі.
8. Політика регулярного оновлення ПЗ.

Політика налаштувань маршрутизатора

1. Паролі:

– Має бути встановлений надійний пароль для доступу до адміністративного інтерфейсу маршрутизатора. Пароль повинен бути складним, містити не менше 12 символів, включати в себе комбінацію букв, цифр та спеціальних символів.

– Змінити стандартний пароль маршрутизатора одразу після його налаштування.

– Не використовувати один і той самий пароль для різних пристроїв.

– Зберігати паролі в безпечному місці.

2. Шифрування:

– Включити шифрування для доступу до адміністративного інтерфейсу маршрутизатора. Використовувати протокол HTTPS або SSH.

– Включити шифрування для бездротової мережі. Використовувати стійкий до злому протокол шифрування, такий як WPA3-Enterprise.

3. Оновлення програмного забезпечення:

– Регулярно оновлювати прошивку маршрутизатора. Оновлення програмного забезпечення часто містять виправлення вразливостей безпеки.

– Встановлювати оновлення програмного забезпечення лише з офіційного сайту виробника маршрутизатора.

4. Контроль доступу:

– Обмежити доступ до адміністративного інтерфейсу маршрутизатора авторизованими користувачами.

– Створити окремі облікові записи для різних користувачів з різними рівнями доступу.

– Використовувати списки контролю доступу (ACL) для блокування доступу до маршрутизатора з несанкціонованих IP-адрес.

5. Брандмауер:

– Включити брандмауер на маршрутизаторі. Брандмауер допоможе заблокувати несанкціонований доступ до мережі.

– Налаштувати брандмауер таким чином, щоб він дозволяв лише авторизований трафік.

– Регулярно переглядати правила брандмауера та оновлювати їх за необхідності.

6. Фільтрування контенту:

– Використовувати функцію фільтрування контенту на маршрутизаторі, щоб блокувати доступ до шкідливих веб-сайтів.

– Налаштувати фільтрування контенту таким чином, щоб воно відповідало потребам підприємства.

7. Резервне копіювання:

– Регулярно створювати резервні копії налаштування маршрутизатора. Це допоможе відновити налаштування маршрутизатора у разі збою системи.

8. Моніторинг:

– Моніторинг активності у мережі допоможе виявити підозрілу активність та вжити відповідних заходів.

– Використовувати журнал реєстрації маршрутизатора, щоб відстежувати доступ до маршрутизатора та активність у мережі.

9. Фізична безпека:

– Розмістити маршрутизатор у безпечному місці, де до нього не матимуть доступу несанкціоновані особи.

– Захистити маршрутизатор від фізичного пошкодження.

Політика налаштувань брандмауерів

1. Брандмауери повинні бути налаштовані таким чином, щоб вони блокували несанкціонований доступ до мережі.

2. Брандмауери повинні дозволяти лише авторизований трафік.

3. Правила брандмауера повинні бути чітко документовані.

4. Брандмауери повинні регулярно оновлюватися для усунення вразливостей.

5. Використовувати брандмауер з функцією stateful inspection.

6. Створити правила брандмауера для дозволу та блокування трафіку на основі IP-адрес, портів та протоколів.

7. Використовувати списки контролю доступу (ACL) для блокування доступу до мережі з несанкціонованих IP-адрес.

8. Увімкнути функцію журналювання брандмауера, щоб відстежувати активність у мережі.

9. Шифрувати дані, які передаються через мережу.

Політика налаштувань IDS/IPS систем

1. Системи IDS/IPS повинні бути налаштовані таким чином, щоб вони виявляли підозрілу активність у мережі.

2. Системи IDS/IPS повинні бути налаштовані таким чином, щоб вони блокували шкідливий трафік.

3. Системи IDS/IPS повинні бути налаштовані таким чином, щоб вони мінімізували кількість помилкових спрацьовувань.

4. Правила IDS/IPS повинні бути чітко документовані.

5. Системи IDS/IPS повинні регулярно оновлюватися для усунення вразливостей.

6. Використовувати IDS/IPS з функцією signature-based detection та anomaly-based detection.

7. Мають бути створені правила IDS/IPS для виявлення та блокування відомих кіберзагроз.

8. Використовувати правила IDS/IPS для виявлення підозрілої активності, яка не відповідає нормальній поведінці мережі.

9. Налаштувати IDS/IPS таким чином, щоб вони надсилали попередження про підозрілу активність до авторизованих користувачів.

Політика використання антивірусного забезпечення

1. На всіх комп'ютерах повинне бути встановлено антивірусне програмне забезпечення.

2. Антивірусне програмне забезпечення повинне бути ліцензованим.

3. Антивірусне програмне забезпечення має регулярно оновлюватися.

4. Комп'ютери повинні регулярно скануватися на наявність вірусів та шкідливого програмного забезпечення.

5. У разі виявлення вірусу або шкідливого програмного забезпечення повинні бути вжиті заходи для його усунення.

6. Має бути увімкненим автоматичне оновлення антивірусних баз даних.

Політика використання ноутбуків співробітниками

1. Користувачі повинні використовувати ноутбуки лише у службових цілях.

2. Користувачі повинні зберігати в таємниці паролі для доступу до ноутбуків.

3. Користувачі повинні використовувати надійні паролі, які містять не менше 12 символів, включаючи в себе комбінацію букв, цифр та спеціальних символів.

4. Користувачі повинні не повідомляти свої паролі іншим особам.

5. Користувачі повинні не залишати ноутбуки без нагляду.

6. Користувачі повинні не підключати до ноутбуків сторонні пристрої без дозволу директора.

7. Користувачі повинні не встановлювати на ноутбуки програмне забезпечення з неперевірених джерел.

8. Користувачі повинні оновлювати операційну систему та програмне забезпечення на ноутбуках за вказівки директора або відповідальної особи.

9. Користувачі повинні використовувати антивірусне програмне забезпечення на ноутбуках.

10. Користувачі повинні створювати резервні копії важливої інформації з ноутбуків.

Політика щодо резервного копіювання та відновлення

1. Резервне копіювання інформації повинне проводитися регулярно.

2. Резервні копії інформації повинні зберігатися в безпечному місці, окремо від основного місця зберігання інформації.

3. Резервні копії інформації повинні бути доступними для швидкого відновлення в разі потреби.

4. Процеси резервного копіювання та відновлення інформації повинні бути документовані.

5. Користувачі повинні бути проінформовані про політику резервного копіювання та відновлення.

6. Має бути план резервного копіювання, який визначає частоту резервного копіювання, тип інформації, яка буде резервуватися, та місце зберігання резервних копій.

7. Регулярно проводити тестування резервних копій, щоб переконатися, що вони доступні для відновлення.

Політика фізичного захисту мережі

1. Доступ до інформаційних систем та даних повинен бути дозволений лише авторизованим користувачам.

2. Всі входи та виходи з приміщень, де розміщені інформаційні системи, повинні бути захищені.

3. Системи контролю доступу повинні бути встановлені на входах до приміщень, де розміщені інформаційні системи.

4. Регулярно повинні проводитися перевірки фізичної безпеки інформаційних систем.

Політика оновлення ПЗ

1. ПЗ повинне оновлюватися регулярно.

2. Оновлення ПЗ повинні встановлюватися після їх офіційного випуску.

3. Використання неактуального ПЗ заборонено.

4. Оновлення ПЗ повинні тестуватися перед їх встановленням.

5. Має бути план оновлення ПЗ, який визначає частоту оновлення ПЗ, тип ПЗ, яке буде оновлюватися, та відповідальних за оновлення осіб.

6. Використовувати автоматичні інструменти для оновлення ПЗ.

3.2 Впровадження політик безпеки

Виходячи з аналізу наведеного в пункті 2.2.1 було вирішено впровадити створені політики безпеки на підприємстві ФОП Сема О. Г.. Перше що було зроблено – це створено окрему LAN для цього підприємства. Згідно політики налаштувань маршрутизатора та брандмауера було придбано маршрутизатор TP-LINK Archer AX72 та встановлено у приміщенні підприємства маршрутизатор і налаштовано його за вимогами, що наведені.

У таблиці 2.3 наведено перелік ПЗ, що використовувалося на підприємстві. Перше що впадає в очі – використання Windows 8, підтримка якої виробником завершилася ще у січні 2016 року. Було вирішено оновити Windows до версії Windows 11 Pro for Workstations. Те саме стосується Microsoft Office 2013, термін дії підтримки якого завершився 11 квітня 2023 року, його було оновлено до Microsoft Office 2021. Ну і звичайно, використання Kaspersky Endpoint Security є неприпустимим, адже ПЗ країни-агресора не може бути безпечним. Замість нього було встановлено ESET PROTECT Elite. Також було рекомендовано оновити ПЗ сервера до версії Microsoft Windows Server 2022. І разом з керівництвом було вирішено встановити термін перегляду регулярного оновлення для ПЗ усіх елементів мережі – 60 діб, не зважаючи на те, що на тих пристроях де це можливо було – було встановлено автоматичне оновлення ПЗ.

Також до керівництва було доведено важливість та необхідність IDS/IPS систем на підприємстві і залишено рекомендацію встановити ліцензовану версію або Suricata або Snort.

Так як на підприємстві було оновлено версію ПЗ пристроїв до Windows 11 разом з керівництвом було вирішено резервне копіювання здійснювати за допомогою OneDrive.

Для забезпечення фізичного захисту підприємства в цілому було вирішено встановити термінали контролю доступу за RFID-картами ZKTeco SC700. Їх було встановлено на входах у приміщення зовні – окремо до кабінету директора, і окремо до робочого приміщення інших працівників. Після встановлення кожному працівникові було видано особисту картку для доступу. Для персоналу з підтримки чистоти було створено одну загальну картку на всіх, але вона працює лише тоді, коли в системі є запис про те, що в приміщенні присутній хоча б один працівник підприємства.

Також виходячи з розташування робочих місць у приміщенні було прийнято рішення на вікнах наклеїти тонувальну плівку аби запобігти зчитуванню інформації через візуальний канал.

По завершенню впровадження створених політик безпеки усім працівникам було проведено тренінг з кібергігієни, а також доведено до відома під розпис політики безпеки що було впроваджено, які стосуються їх діяльності.

3.3 Аналіз ризиків після впровадження політик безпеки

Після введених політик безпеки та проведених супутніх заходів було проведено повторний аналіз ризиків. Результати якого наведено в додатку Б.

Якщо коротко систематизувати це в порівняльну таблицю це матиме вигляд таблиці 3.1. З неї можна побачити що приблизно 60% загроз стали менш ймовірними, що свідчить про те, що інформаційна безпека на підприємстві підвищилася.

Таблиця 3.1 – Порівняльна таблиця аналізу ризиків до та після впровадження політик безпеки

№	Загроза	Ймовірність виникнення до впровадження ПБ	Ймовірність виникнення після впровадження ПБ
1	**2**	**3**	**4**
1	Несанкціоноване підключення до пристроїв	Висока	Низька
2	Читання даних, що виводяться на екран, залишених відкритих файлів	Висока	Низька
3	Воєнні дії	Висока	Висока
4	Стихійні явища	Низька	Низька
5	Перехоплення акустичної інформації	Висока	Висока
6	Несанкціонований перегляд візуальної інформації	Висока	Низька
7	Пошкодження носіїв інформації	Середня	Низька
8	Відмова/збій програмного забезпечення	Середня	Низька
9	Відсутність інтернету	Висока	Висока
10	Відсутність електропостачання	Висока	Висока
11	Зараження системи вірусами	Середня	Низька
12	Втрата паролів	Середня	Низька
13	Втрата резервних копій	Середня	Низька

Продовження таблиці 3.1

1	2	3	4
14	Некоректне налаштування прав доступу працівників до інформації	Висока	Висока
15	Допуск до системи неавторизованих осіб	Висока	Низька
16	Відсутність шифрування даних	Висока	Середня
17	Недбале зберігання документації	Середня	Середня
18	Атаки на інформаційну систему	Висока	Середня

ВИСНОВКИ

У рамках кваліфікаційної роботи було обґрунтовано необхідність розробки та застосування політик безпеки на підприємстві, що займається науковою діяльністю, способи забезпечення інформаційної безпеки.

Проаналізовано чинну нормативно-правову базу України, щодо забезпечення захисту інформації та визначено необхідні заходи, що необхідно виконати на підприємстві ФОП Сема О. Г. для покращення захисту оброблюваної інформації в інформаційній системі підприємства.

Зібрано дані про підприємство: обстежено об’єкт інформаційної діяльності, інформаційне середовище та обчислювальну систему.

На основі зібраних даних розроблено моделі порушника та моделі потенційних загроз.

Визначено загрози, які мають найбільшу ймовірність виникнення і на основі цього було розроблено політики безпеки.

Політики безпеки було впроваджено на підприємстві та проаналізовано ймовірність виникнення загроз знову – ймовірнісний показник виникнення загроз зменшився на 60%.

В подальшому можна спираючись на ці дані розробити КСЗІ для підприємства, а також на цьому прикладі розробити політики безпеки для інших комерційних підприємств, але вони не можуть бути універсальними для всіх, бо на кожному підприємстві обробляється різна інформація, на що слід звернути увагу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27035-1:2023(en) Information technology – Information security incident management – Part 1: Principles and process. *ISO - International Organization for Standardization*. URL: https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:27035:-1:ed-2:v1:en (дата звернення: 18.03.2024).

2. Типове положення про службу захисту інформації в автоматизованій системі : НД ТЗІ від 15.12.2000 р. № 1.4-001-2000.

3. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 01.04.2024).

4. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 05.04.2024).

5. Про науково-технічну інформацію : Закон України від 25.06.1993 р. № 3322-XII : станом на 19 квіт. 2014 р. URL: https://zakon.rada.gov.ua/laws/show/3322-12#Text (дата звернення: 07.04.2024).

6. Про внесення змін до Закону України "Про захист інформації в автоматизованих системах" : Закон України від 31.05.2005 р. № 2594-IV. URL: https://zakon.rada.gov.ua/laws/show/2594-15#Text (дата звернення: 08.04.2024).

7. Захист інформації. Технічний захист інформації. Порядок проведення робіт : ДСТУ від 01.07.1997 р. № 3396.1-96.

8. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ від 01.07.1999 р. № 1.1-002-99.

9. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ від 01.07.1999 р. № 2.5-004-99.

10. Класифікація автоматизованих систем і стандартні функціональні профілі несанкціонованого доступу: НД ТЗІ від 01.07.1999 р. № 2.5-005-99.

11. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: НД ТЗІ від 08.11.2005 р. № 3.7-003-05.

12. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. *ISO - International Organization for Standardization*. URL: https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:27001:ed-3:v1:en (дата звернення: 15.04.2024).

13. Information security, cybersecurity and privacy protection – Information security controls. *ISO - International Organization for Standardization*. URL: https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:27002:ed-3:v2:en (дата звернення: 21.04.2024).

14. Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services. ISO - International Organization for Standardization. URL: https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:27017:ed-1:v1:en (дата звернення: 16.04.2024).

15. Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. *ISO - International Organization for Standardization*. URL: https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:27018:ed-2:v1:en (дата звернення: 29.04.2024).

16. Cybersecurity – Guidelines for Internet security. *ISO - International Organization for Standardization*. URL: https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:27032:ed-2:v1:en (дата звернення: 15.04.2024).

17. Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing. *ISO - International Organization for Standardization*. URL: https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:27007:ed-3:v1:en (дата звернення: 20.05.2024).

18. Cybersecurity – Supplier relationships – Part 3: Guidelines for hardware, software, and services supply chain security. *ISO - International Organization for Standardization*. URL: https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:27036:-3:ed-2:v1:en (дата звернення: 14.04.2024).

19. Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines. *ISO - International Organization for Standardization*. URL: https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:27701:dis:ed-2:v1:en (дата звернення: 22.04.2024).

20. Information technology – Security techniques – Storage security. *ISO - International Organization for Standardization*. URL: https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:27040:ed-2:v1:en (дата звернення: 27.04.2024).

21. Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці: НД ТЗІ від 15.04.2013 р. № 1.6-005-2013:

22. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ від 01.07.1999 р. № 1.1-003-99.

23. Розробка моделі загроз інформації та вибір методів і засобів технічного захисту інформації для об’єкта інформаційної діяльності. *ElAr :: Головна*. URL: https://openarchive.nure.ua/entities/publication/1e74fc91-85f0-4cca-b641-931fc2ee7ed7 (дата звернення: 03.05.2024).

24. Основні правила використання та зміни паролів. *Державна служба спеціального зв’язку та захисту інформації України*. URL: https://cip.gov.ua/ua/faqs/osnovni-pravila-vikoristannya-ta-zmini-paroliv (дата звернення: 13.05.2024).

25. Що робити, якщо завантажили підозрілий файл у смартфон або на комп’ютер. *Державна служба спеціального зв’язку та захисту інформації*

України. URL: https://cip.gov.ua/ua/faqs/sho-robiti-yaksho-zavantazhili-pidozrilii-fail-u-smartfon-abo-na-komp-yuter (дата звернення: 07.05.2024).

26. Що таке резервне копіювання даних, як його здійснювати, і де краще зберігати інформацію?. *Державна служба спеціального зв'язку та захисту інформації України*. URL: https://cip.gov.ua/ua/faqs/sho-take-rezervne-kopiyuvannya-danikh-yak-iogo-zdiisnyuvati-i-de-krashe-zberigati-informaciyu (дата звернення: 11.05.2024).

27. Як діяти, щоб запобігти витоку службової інформації. *Служба Безпеки України*. URL: https://ssu.gov.ua/yak-diiaty-shchob-zapobihty-vytoku-sluzhbovoi-informatsii (дата звернення: 11.05.2024).

28. is113. Snort і Suricata - простий шлях до використання IDPS: від установки на сервер до грамотного налаштування. *Хабр*. URL: https://habr.com/ru/companies/selectel/articles/744478/ (дата звернення: 05.05.2024).

29. Оформлення цитувань та посилань. *library_sumdu*. URL: https://library.sumdu.edu.ua/uk/doslidnyku/akademichne-pismo/tsytuvannia-ta-posylannia/tsytuvannia?highlight=WyJcdTA0M2VcdTA0NDRcdTA0M2VcdTA0NDBcdTA0M2NcdTA0M2JcdTA0MzVcdTA0M2RcdTA0M2RcdTA0NGYiXQ== (дата звернення: 23.05.2024).

30. Приклади бібліографічних описів. *library_sumdu*. URL: https://library.sumdu.edu.ua/uk/doslidnyku/akademichne-pismo/pryklady-bibliohrafichnykh-opysiv?highlight=WyJcdTA0M2VcdTA0NDRcdTA0M2VcdTA0NDBcdTA0M2NcdTA0M2JcdTA0MzVcdTA0M2RcdTA0M2RcdTA0NGYiXQ== (дата звернення: 23.05.2024).

31. Методичні вказівки до виконання оформлення кваліфікаційних робіт освітньо-професійної програми «Кібербезпека» для здобувачів бакалаврського рівня спеціальності 125 «Кібербезпека та захист інформації» (125 «Кібербезпека») всіх форм здобуття вищої освіти / укладачі Т. В. Лаврик,

В. О. Любчак, І. О. Пугач – Суми : Сумський державний університет, 2024. – 38 с.

32. Сазанова А. А., Кальченко В. В., Коваль В. В. Ефективний захист інформаційних ресурсів відповідно до законодавства України: розробка та впровадження конфігурацій політик безпеки. *Інформатика, Математика, Автоматика IMA :: 2024* : Матеріали та програма Міжнар. наук. конф. молодих уч., м. Суми – Астана, 22–26 квіт. 2024 р. Суми, 2024. С. 53.

Додаток А

Таблиця А.1 – Попередній аналіз ризиків для підприємства

№	Загроза	Інформація, що може бути пошкоджена	Ймовірність виникнення	Величина збитків	Ймовірні наслідки
1	2	3	4	5	7
1	Несанкціоноване підключення до пристроїв	Наукові дослідження, експериментальні розробки, фінансова інформація, персональні дані, інформація про інтелектуальну власність, організаційно-правові документи підприємства	Висока	Великі	Неприємності для підприємства (які впливають на рівень суспільної довіри), фінансові втрати, зниження продуктивності праці
2	Читання даних, що виводяться на екран, залишених відкритих файлів		Висока	Середні	Неприємності для підприємства (які впливають на рівень суспільної довіри)

1	2	3	4	5	7
3	Перехоплення акустичної інформації	Наукові дослідження, експериментальні розробки, фінансова інформація, персональні дані, інформація про інтелектуальну власність	Висока	Великі	Неприємності для підприємства (які впливають на рівень суспільної довіри), фінансові втрати
4	Несанкціонований перегляд візуальної інформації		Висока	Великі	
5	Пошкодження носіїв інформації		Середня	Великі	Фінансові втрати, зниження продуктивності праці

1	2	3	4	5	7
6	Воєнні дії	Наукові дослідження, експериментальні розробки, фінансова інформація, персональні дані, інформація про інтелектуальну власність, організаційно-правові документи підприємства	Висока	Великі	Зниження продуктивності праці, фінансові втрати
7	Стихійні явища		Низька	Великі	
8	Відмова/збій програмного забезпечення		Середня	Середні	
9	Відсутність інтернету		Висока	Середні	Зниження продуктивності праці
10	Відсутність електропостачання		Висока	Середні	
11	Зараження системи вірусами		Середня	Великі	Неприємності для підприємства (які впливають на рівень суспільної довіри), фінансові втрати, зниження продуктивності праці
12	Втрата паролів		Середня	Великі	
13	Втрата резервних копій		Середня	Великі	

1	2	3	4	5	7
14	Некоректне налаштування прав доступу працівників до інформації	Наукові дослідження, експериментальні розробки, фінансова інформація, персональні дані, інформація про інтелектуальну власність, організаційно-правові документи підприємства	Висока	Великі	Зниження продуктивності праці
15	Допуск до системи неавторизованих осіб		Висока	Великі	Неприємності для підприємства (які впливають на рівень суспільної довіри), фінансові втрати, зниження продуктивності праці
16	Відсутність шифрування даних		Висока	Великі	Неприємності для підприємства (які впливають на рівень суспільної довіри), фінансові втрати
17	Недбале зберігання документації		Середня	Середні	

1	2	3	4	5	7
18	Атаки на інформаційну систему	Наукові дослідження, експериментальні розробки, фінансова інформація, персональні дані, інформація про інтелектуальну власність, організаційно-правові документи підприємства	Висока	Великі	Неприємності для підприємства (які впливають на рівень суспільної довіри), фінансові втрати, зниження продуктивності праці

Додаток Б

Таблиця Б.1 – Повторний аналіз ризиків для підприємства після введення політик безпеки

№	Загроза	Інформація, що може бути пошкоджена	Ймовірність виникнення	Величина збитків	Ймовірні наслідки
1	2	3	4	5	7
1	Несанкціоноване підключення до пристроїв	Наукові дослідження, експериментальні розробки, фінансова інформація, персональні дані, інформація про інтелектуальну власність, організаційно-правові документи підприємства	Низька	Великі	Неприємності для підприємства (які впливають на рівень суспільної довіри), фінансові втрати, зниження продуктивності праці
2	Читання даних, що виводяться на екран, залишених відкритих файлів		Низька	Середні	Неприємності для підприємства (які впливають на рівень суспільної довіри)

1	2	3	4	5	7
3	Перехоплення акустичної інформації	Наукові дослідження, експериментальні розробки, фінансова інформація, персональні дані, інформація про інтелектуальну власність	Висока	Великі	Неприємності для підприємства (які впливають на рівень суспільної довіри), фінансові втрати
4	Несанкціонований перегляд візуальної інформації		Низька	Великі	
5	Пошкодження носіїв інформації		Низька	Великі	Фінансові втрати, зниження продуктивності праці

1	2	3	4	5	7
6	Воєнні дії	Наукові дослідження, експериментальні розробки, фінансова інформація, персональні дані, інформація про інтелектуальну власність, організаційно-правові документи підприємства	Висока	Великі	Зниження продуктивності праці, фінансові втрати
7	Стихійні явища		Низька	Великі	
8	Відмова/збій програмного забезпечення		Низька	Середні	
9	Відсутність інтернету		Висока	Середні	Зниження продуктивності праці
10	Відсутність електропостачання		Висока	Середні	
11	Зараження системи вірусами		Низька	Великі	Неприємності для підприємства (які впливають на рівень суспільної довіри), фінансові втрати, зниження продуктивності праці
12	Втрата паролів		Низька	Великі	
13	Втрата резервних копій		Низька	Великі	

1	2	3	4	5	7
14	Некоректне налаштування прав доступу працівників до інформації	Наукові дослідження, експериментальні розробки, фінансова інформація, персональні дані, інформація про інтелектуальну власність, організаційно-правові документи підприємства	Висока	Великі	Зниження продуктивності праці
15	Допуск до системи неавторизованих осіб		Низька	Великі	Неприємності для підприємства (які впливають на рівень суспільної довіри), фінансові втрати, зниження продуктивності праці
16	Відсутність шифрування даних		Висока	Великі	Неприємності для підприємства (які впливають на рівень суспільної довіри), фінансові втрати
17	Недбале зберігання документації		Середня	Середні	

1	2	3	4	5	7
18	Атаки на інформаційну систему	Наукові дослідження, експериментальні розробки, фінансова інформація, персональні дані, інформація про інтелектуальну власність, організаційно-правові документи підприємства	Середня	Великі	Неприємності для підприємства (які впливають на рівень суспільної довіри), фінансові втрати, зниження продуктивності праці