ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія забезпечення захищеного функціонування інформаційної системи підприємства»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

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

Виконав: здобувач вищої освіти групи БСДМ-63
БАРБУНОВ Ярослав
(ПРІЗВИЩЕ, Ім'я)

Керівник: Марченко Віталій
д.ф.,доцент. (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

ЗМІСТ

ПЕРЕЛІК ПОСИЛАНЬ

ASA – Adaptive Security Appliance

IPS – Intrusion Prevention System

IDS – Intrusion Detection System

IPSec – Internet Protocol Security

IKE – Policy Administration Node

ACL – Access Control List

VPN – Virtual Private Network

ВСТУП

Актуальність дослідження. В еру цифрового прогресу та високотехнологічних викликів, захищене функціонування інформаційних систем стає однією із найбільш критичних складових успішності будь-якого підприємства. З плином часу обсяги даних, їх важливість та швидкість обробки зросли настільки, що стали необхідністю в ефективній та надійній технології забезпечення захисту.

З ростом кількості кібератак та поширення загроз кібербезпеки, підприємства стикаються з надзвичайно складним завданням забезпечення цілісності своєї інформаційної інфраструктури. Надмірна важливість оснащення систем захистом від кіберзагроз стає сьогодні ключовою для уникнення фінансових втрат, втрати довіри клієнтів та втрати конкурентоспроможності на ринку.

Мета роботи – розробити варіант технології забезпечення захищеного функціонування інформаційної системи підприємства.

Об'єкт дослідження – процес забезпечення захищеності інформаційної системи підприємства.

Предмет дослідження – технології та методи, що спрямовані на захист інформаційної системи підприємства від потенційних загроз.

Наукові завдання:

- провести аналіз загроз та ризиків для інформаційної системи;
- проаналізувати основні загрози інформаційній системі підприємства;
- проаналізувати методи та засоби забезпечення захищеного функціонування інформаційної системи підприємства;
- розробити варіант технології забезпечення захищеного функціонування інформаційної системи підприємства.

Методи дослідження – опрацювання літератури за даною темою, аналіз загроз та ризиків ІС підприємства, методів та засобів забезпечення захисту простору,

моделювання технології забезпечення захищеного функціонування інформаційної системи підприємства.

Практичне значення одержаних результатів полягає в розробці технології забезпечення захищеного функціонування інформаційної системи підприємства та рекомендації щодо застосування технології, що дозволить забезпечувати необхідний рівень кібербезпеки організації.

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки».

1 АНАЛІЗ ЗАГРОЗ ТА РИЗИКІВ ДЛЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

В сучасному світі, де інформаційні технології визначають успіх підприємств, аналіз загроз та ризиків для інформаційної системи стає важливішим завданням ніж будь-коли. У цьому розділі проводитиметься глибокий аналіз потенційних небезпек, що ставлять під загрозу безпеку та стабільність інформаційної інфраструктури підприємства, з метою визначення ефективних заходів захисту.

1.1. Загрози інформаційній безпеці підприємства

Інформаційна безпека залежить від усього комплексу заходів та сучасних технологій, керування якими відбувається із застосуванням різноманітних інформаційних систем.

Захист інформації – комплекс заходів, спрямованих на забезпечення інформаційної безпеки. Аналізуючи підходи до проблем інформаційної безпеки, необхідно починати з виявлення суб’єктів інформаційних відносин та інтересів цих суб’єктів, пов’язаних з використанням інформаційних систем (ІС). Загрози інформаційної безпеки пов’язані з використанням інформаційних технологій[1].

Загрози інформаційній безпеці підприємства – це потенційні небезпеки, які можуть призвести до порушень конфіденційності, цілісності та доступності інформації та інших ресурсів підприємства. Ці загрози можуть виникати як з зовнішніх, так і з внутрішніх джерел, і їх можна класифікувати за різними параметрами.

Інформаційна безпека (InfoSec) – це багатопланова діяльність, і лише системний та комплексний підхід може досягти успіху. Безпека використання інформаційних систем полягає в забезпеченні доступності, цілісності, конфіденційності та підтримки інформаційних ресурсів її інфраструктури.

Це запорука ефективного захисту даних та безпеки інфраструктури організації, це основоположення інформаційній безпеці підприємства.

Конфіденційність – це основний компонент InfoSec, який полягає в тому, що доступ до інформації можуть отримувати лише авторизовані користувачі. Шифрування даних, багатофакторна автентифікація та захист від втрати даних – це приклади інструментів, які підприємства можуть використовувати для забезпечення конфіденційності інформації.

Цілісність — захист інформації від несанкціонованої модифікації. Підприємства мають підтримувати цілісність даних протягом усього їхнього життєвого циклу. Підприємства з розвинутим компонентом InfoSec визнають важливість використання точних і надійних даних та не дозволять неавторизованим користувачам отримувати доступ до них, змінювати їх або керувати ними. Такі інструменти, як дозволи для файлів, керування ідентичностями й елементи керування доступом користувачів, забезпечують цілісність даних.

Доступність — захист (забезпечення) доступу до інформації, а також можливості її використання. InfoSec включає безперервну підтримку фізичного обладнання й регулярне оновлення системи, щоб авторизовані користувачі мали надійний і узгоджений доступ до даних відповідно до своїх потреб.

До основних складових інформаційної безпеки відноситься конфіденційність, тобто запобігання несанкціонованому доступу до інформації.

Аналізуючи питання, пов’язані з інформаційною безпекою, необхідно враховувати конкретну ситуацію безпеки в цій сфері, тобто інформаційна безпека є невід’ємною частиною інформаційних технологій, а інформаційні технології розвиваються з небаченою швидкістю. Тут важливі не окремі рішення на сучасному рівні (закони, навчальні курси, програмні та технологічні продукти), а механізми, які генерують нові рішення, які дозволяють йти в ногу з технологічним прогресом[1].

Складність механізмів прийняття сучасних управлінських рішень щодо захисту інформації в новому інформаційному середовищі пов’язана з використанням стрімко

розвиваючих інформаційних систем, які розраховані на великі обсяги обробки, обміну та їх використання в сучасному житті кожної людини, підприємств, країн, світу та бурхливий розвиток технічних засобів.

Загрозою можна вважати напад і можливість порушення інформаційної безпеки та доступу до інформації, а особа, яка порушує інформацію, є зловмисником. Загрози проявляються через низький рівень захисту в системі захисту інформаційної системи або у виявленні вразливостей.

Основними завданнями системи інформаційної безпеки є:

– виявлення та усунення загроз безпеки нанесенню економічного, фінансового, матеріального та морального збитку;

– створення механізмів реагування на загрози розвитку і функціонуванню підприємства та національній безпеці;

– прийняття заходів щодо забезпечення безпеки персоналу підприємства та інше.

Поняття інформаційної безпеки включає:

1. надійність роботи комп’ютера;
2. збереження цілісності даних;
3. захист інформації від несанкціонованого доступу;
4. таємниця електронного листування.

Інформаційні загрози можуть бути обумовлені:

1. природними факторами;
2. зовнішніми факторами;
3. внутрішніми факторами.

Природні фактори для інформаційної безпеки підприємства виникають внаслідок природних катастроф або стихійних явищ. Ці загрози можуть призвести до фізичного руйнування інфраструктури, втрати даних та зупинки бізнес-процесів. Ось кілька природних загроз:

1. Повені та Затоплення можуть призвести до втрати обладнання та документації, а також може викликати електричні збої.

2. Землетруси можуть призвести до руйнування будівель, обладнання та інфраструктури.

3. Пожежі можуть виникнути внаслідок природних пожеж, технічних несправностей або інших причин. Вони загрожують фізичному обладнанню та даним.

4. Сильні вітри та опади, що супроводжують урагани та тайфуни, можуть призвести до руйнування будівель і виходу інфраструктури з ладу.

5. Екстремальні снігопади та льодовики можуть викликати обвалювання дерев, ламати лінії електропередачі та завдалиння.

6. Торнадо можуть призвести до виникнення значних руйнувань в області, що може вплинути на інфраструктуру підприємства.

7. Вулканічна діяльність може призвести до забруднення повітря та води, а також може викликати фізичні пошкодження обладнання.

Заходи для захисту від природних загроз включають в себе розробку та впровадження планів невідкладних ситуацій, резервне копіювання даних, фізичні заходи безпеки та забезпечення робочого місця відповідно до стандартів безпеки[2].

Зовнішні загрози інформаційній безпеці підприємства можуть бути різноманітними і включати в себе ризики з боку зовнішніх суб'єктів, які намагаються отримати несанкціонований доступ або завдати шкоду інформаційній системі підприємства. Ось кілька типових зовнішніх загроз:

1. Кібератаки:

Хакерські атаки: Зловмисники можуть використовувати техніки хакерства для отримання несанкціонованого доступу до систем та даних підприємства.

Фішинг: Зловмисники можуть використовувати маніпуляції та обман для отримання конфіденційної інформації від співробітників.

Віруси та шкідливе програмне забезпечення: Розповсюдження шкідливих програм для завдання шкоди системам та даним.

2. Кібершпигунство:

Шпигунське програмне забезпечення: Зловмисники можуть намагатися встановити програми для збору конфіденційної інформації.

Перехоплення комунікацій: Завдання шкоди чи витоку конфіденційної інформації шляхом перехоплення мережевого трафіку чи комунікацій.

3. Соціальний інженерінг:

Маніпуляції зі співробітниками: Зловмисники можуть використовувати соціальні інженерні методи для обману співробітників та отримання доступу до систем.

4. Конкурентні загрози:

Шпигунство від конкурентів: Конкуренти можуть намагатися отримати конфіденційну інформацію для отримання конкурентного переваги.

5. Фізичні загрози:

Фізичні атаки: Атаки на інфраструктуру підприємства, такі як крадіжки обладнання або фізичні пошкодження об'єктів.

6. Загрози від держав:

Кібератаки від держав: Деякі загрози можуть мати державний характер і бути спрямованими на економічні, політичні або військові цілі.

Забезпечення захисту від цих зовнішніх загроз включає в себе використання кіберзаходів, школування персоналу та постійне вдосконалення систем безпеки.

Внутрішні загрози інформаційній безпеці підприємства виникають здебільшого через дії або недії власних співробітників чи осіб, які мають легальний доступ до інформації та ресурсів підприємства. Вони можуть бути навмисними або ненавмисними. Ось кілька типових внутрішніх загроз[2]:

1. Неосвічений персонал:

Неправильне використання та нерозуміння політик безпеки можуть призвести до випадкового розголошення конфіденційної інформації.

2. Недостатня охорона паролів:

Слабкі паролі, використання одного пароля для багатьох облікових записів або неправильне зберігання паролів можуть викликати проблеми з безпекою.

3. Невірна реакція на загрози:

Неправильна реакція або ігнорування попереджень щодо безпеки інформації з боку співробітників.

4. Крадіжка або втрата пристроїв:

Втрата мобільних пристроїв чи ноутбуків, які містять конфіденційну інформацію.

5. Неправомірний доступ:

Співробітники, які використовують свій легальний доступ для отримання інформації, до якої вони не повинні мати доступ.

6. Внутрішні кіберзагрози:

Дії співробітників, які виходять за межі дозволених, такі як крадіжка ідентифікаторів, розголошення конфіденційної інформації чи введення шкідливого програмного забезпечення.

7. Несанкціоноване використання ресурсів:

Використання обладнання або ресурсів підприємства для особистих цілей, що може вплинути на продуктивність та безпеку.

8. Звільнені або виходячі працівники:

Звільнені або вийшовши з компанії працівники можуть використовувати свої знання для вчинення злочинних дій або розголошення конфіденційної інформації.

Забезпечення безпеки від внутрішніх загроз включає в себе не тільки технічні заходи, але й впровадження політик та процедур, що спрямовані на освіту та контроль дій персоналу.

1.2. Оцінка потенційних втрат та наслідків

1. Матеріальні втрати:

Оцінка матеріальних втрат включає в себе аналіз можливих фінансових збитків, які підприємство може зазнати внаслідок інцидентів в інформаційній системі. Це охоплює вартість відновлення систем, втрати прибутку внаслідок зупинки бізнес-процесів, а також можливі штрафи чи витрати на відшкодування клієнтам[3]:

Аналіз потенційних втрат даних включає в себе оцінку важливості та чутливості даних, які можуть бути втрачені. Це може бути втрата конфіденційної інформації, клієнтських даних або стратегічних планів, що може призвести до серйозних наслідків для діяльності підприємства.

Аналіз втрат репутації та довіри враховує можливі наслідки для іміджу підприємства в результаті інцидентів в інформаційній системі. Це охоплює вплив на споживачів, партнерів та інших зацікавлених сторін, а також можливі витрати на відновлення репутації та залучення додаткових маркетингових зусиль.

Оцінка юридичних наслідків включає в себе аналіз можливих правових наслідків для підприємства внаслідок інцидентів в інформаційній системі. Це може включати витрати на відшкодування, штрафи за порушення законодавства про захист даних, а також можливі судові позови від клієнтів чи партнерів.

1.3. Сучасні загрози та підходи до захисту інформаційних систем

Фішинг є одним із найбільш зареєстрованих кіберзлочинів у Сполучених Штатах, щороку спричиняє незліченні фінансові збитки. Мета полягає в тому, щоб викрасти конфіденційні дані та облікові дані, такі як облікові дані для входу або дані кредитної картки, і обманом змусити людей дозволити встановлення зловмисного програмного забезпечення. Методи фішингу можуть вимкнути елементи керування безпекою та дозволити зловмисникам переглядати корпоративні дані непоміченими.

Смішинг працює так само, як фішинг, але повідомлення-приманка надсилається за допомогою текстового повідомлення, а не електронною поштою. Зловмисники видають себе за довірені ролі та атакують мобільні пристрої, щоб отримати доступ до конфіденційної інформації. Коли ці мобільні пристрої підключаються до мережі компанії, зловмисники отримують доступ і викрадають дані клієнтів і співробітників, а також вихідний код організації[4].

Існує багато способів, якими організація може захистити себе та своїх співробітників від спроб фішингу, зокрема:

1. Навчання користувачів: співробітники повинні вміти розпізнавати спроби фішингу та розуміти, що вони не повинні відповідати на будь-які запити на спілкування. Організації повинні заохочувати працівників повідомляти про будь-яку підозрілу діяльність, щоб у разі потреби було вжито додаткових заходів безпеки.

2. Системи виявлення вторгнень і спам-фільтри: наявність цих систем у багатьох випадках допоможе виявити та заблокувати неавторизовані електронні листи, щоб вони не досягли цільового одержувача.

3. Надійні інструменти автентифікації: багатофакторна автентифікація та надійні, регулярно оновлювані паролі можуть уповільнити потенційних зловмисників.

Зрештою, не існує стандартного рішення для фішингу чи смішинга, оскільки кожен бізнес має свої слабкі місця. У результаті багато компаній обирають професійну оцінку загроз кібербезпеці, щоб надати індивідуальне рішення для окремих компаній залежно від їхніх потреб.

Зловмисне програмне забезпечення (засоби захисту від зловмисного програмного забезпечення) існує в багатьох формах. Зловмисники розробляють зловмисне програмне забезпечення, щоб отримати постійний бекдор-доступ до корпоративних пристроїв, який важко виявити. Потім вони можуть віддалено контролювати пристрій і використовувати його для викрадення даних, дослідження локальної мережі або надсилання спаму із зараженого пристрою. Приголомшливі 91%

кібератак починаються з фішингового електронного листа, тому фішинг і зловмисне програмне забезпечення часто йдуть рука об руку[4].

Інфекції є відносно поширеними і можуть серйозно вплинути на вашу мережу через крадіжку даних і паролів, уповільнення роботи системи та повне видалення файлів. Обладнання, заражене шкідливим програмним забезпеченням, часто стає непридатним для використання, що призводить до витрат на заміну обладнання, що може бути руйнівним для малого та середнього бізнесу.

Зловмисне програмне забезпечення не обмежується одним комп'ютером. Він швидко поширюється мережею організації, тобто вся організація може бути негайно скомпрометована.

Через проникаючий характер атак зловмисних програм для їх запобігання потрібно підходити з кількох сторін. Оцінка ризиків кібербезпеки є одним із багатьох профілактичних заходів, що ви можете вжити, які можуть включати в себе наступне:

1. Програмне забезпечення безпеки: розширене, оновлене програмне забезпечення для захисту від вірусів і шкідливого ПЗ є обов'язковим для пристроїв співробітників.

2. Оновлення системи: атаки шкідливого програмного забезпечення змінюються щодня, тому піклуйтеся про те, щоб ваша система була завжди оновлена, здатна справлятися з новими викликами і могла захистити вашу організацію від нових загроз.

3. Безпека мережі: необхідно регулярно перевіряти мережі, щоб виявити слабкі місця та перевірити наявність шкідливих програм. Для максимального пом'якшення загрози безпеку потрібно періодично оновлювати.

4. Навчання з безпеки для співробітників: порушення безпеки даних часто є результатом людської помилки. Навчання співробітників щодо зловмисного програмного забезпечення та того, як воно проникає у ваші комп'ютерні системи, допоможе їм зрозуміти ризики та розпізнати шкідливе ПЗ.

Програми-вимагачі, ця форма зловмисного програмного забезпечення може завдати катастрофічної шкоди бізнесу. Щойно зловмисне програмне забезпечення потрапляє у вашу систему, воно блокує її та позбавляє вас доступу до критично важливих даних, доки ви не заплатите викуп за отримання конфіденційної інформації та відновлення контролю над системою.

Програми-вимагачі ставлять компанії перед важким вибором: заплатити зловмисникам або втратити дані та доступ. Багато компаній вирішують платити викуп хакерам, але навіть якщо власники бізнесу платять викуп, вони не завжди можуть отримати доступ до своїх даних[4].

З розвитком програм-вимагачів методи атаки хакерів перейшли до більш складних операцій. Але малі підприємства не є винятком і вразливі для хакерів. Зловмисники знають, що малі підприємства не завжди мають ресурси для ефективного резервного копіювання своїх даних і можуть заплатити викуп, щоб забезпечити безперервність роботи.

Оскільки програмне забезпечення-вимагач є різновидом шкідливого ПЗ, воно потрапляє у ваші системи подібним чином, тому з самого початку потрібні ті самі профілактичні заходи. Крім них є деякі інші методи запобігання програмам-вимагачам:

1. Сучасні системи: хакери швидко знаходять діри в старих системах, але вдосконалення кібербезпеки впроваджуються часто, і вони допоможуть вам бути на крок попереду хакерів.

2. Окремі системи резервного копіювання: часто створюйте резервні копії ваших даних і не від’єднуйте їх від мережі. Зловмисники матимуть більше проблем із доступом до них, якщо вони зберігатимуться окремо.

3. Належна кібергігієна: проведіть інвентаризацію всіх пристроїв, підключених до вашої мережі, щоб визначити загрозу зловмисного програмного забезпечення.

4. Послуги віртуальних приватних мереж (VPN): віртуальні приватні мережі є важливими під час підключення до загальнодоступних мереж Wi-Fi, оскільки вони загрожують вашим даним.

5. Плани реагування на інциденти: плануйте заздалегідь, щоб спробувати забезпечити безперервність роботи в умовах атаки. Перевірте свою реакцію на інцидент і визначте слабкі місця, щоб мати змогу зробити корективи та підготуватися до справжньої атаки програм-вимагачів.

Також відомий як компрометація облікового запису електронної пошти, компрометація бізнес-електронної пошти або BEC (Business Email Compromise), це один із найдорожчих кіберзлочинів. Це проявляється в тому, що зловмисники компрометують електронну пошту компанії, щоб обдурити компанію. Процес починається зі злому злочинців бізнес-систем, щоб отримати інформацію про їхні платіжні системи. Потім вони обманювали працівників і спонукали їх платити на фальшиві банківські рахунки замість справжніх[5].

Фальшиві платіжні запити може бути важко ідентифікувати, оскільки вони виглядають майже ідентично справжнім запитам. Зловмисники можуть вносити незначні зміни в адреси електронної пошти, використовувати зловмисне програмне забезпечення або надсилати фішингові листи, щоб завоювати довіру жертви. BEC можуть завдати значної фінансової шкоди підприємствам, і можуть знадобитися місяці, щоб відстежити та повернути суми платежів, якщо такі є.

Шахрайство BEC може статися дуже швидко, тому співробітники повинні пройти навчання та бути пильними під час обробки платіжних запитів і дотримуватися найкращих практик кібербезпеки. Крім того, організації можуть застосувати деякі з наведених нижче найкращих практик кібербезпеки:

1. Надійні паролі: паролі слід регулярно змінювати, а співробітники повинні бути в курсі інформації, якою вони діляться в соціальних мережах. Прості паролі включають ім’я домашньої тварини та дату народження, тому їх легко зламати.

2. Ефективне програмне забезпечення: брандмауери, антивірусне програмне забезпечення та програмне забезпечення для захисту від зловмисного програмного забезпечення ускладнять кіберзлочинцям націлювання на своїх жертв.

3. Процес перевірки: під час подання запиту на платіж перевірка телефоном або особисто є критичною. Пропонуйте будь-які зміни в реквізитах рахунку або платіжних процесах безпосередньо одержувачу. Ретельно перевірте всі електронні адреси на наявність незначних відмінностей.

4. Багатофакторна автентифікація (MFA): запобігайте отримання доступу хакерами, якщо вони також не мають телефону або програми автентифікації для перевірки електронної адреси.

Багато людей у вашій компанії мають доступ до конфіденційної інформації. Незалежно від того, чи є вони нинішніми чи колишніми співробітниками, партнерами чи підрядниками, 25% порушень даних є результатом внутрішніх загроз. Погані хлопці діють через жадібність, а іноді незадоволені працівники діють через озлобленість. Незважаючи на це, поширення ними важливої інформації може призвести до значних фінансових втрат[5].

Внутрішні загрози є складними — вони вкорінені в людській природі й не слідують шаблонам, які можна ідентифікувати. Більшість інсайдерських загроз мотивуються фінансовою вигодою, хоча є й інші причини такої поведінки. Деякі можливі методи профілактики:

1. Зміна культури: міцна культура безпеки має вирішальне значення для пом’якшення потенційної шкоди, спричиненої внутрішніми загрозами. Співробітники будуть менш сприйнятливі до випадкових погроз і більше помічатимуть підозрілу поведінку інших колег.

2. Захист критично важливих активів: у багатьох випадках дані повинні бути доступні для кількох співробітників. Вживайте заходів цифрової безпеки, щоб захистити власні активи та дані клієнтів. Щоразу, коли співробітник залишає

компанію, вживайте відповідних заходів, щоб якомога швидше позбавити його доступу до конфіденційних даних.

3. Відстеження поведінки: підвищте організаційну прозорість того, що роблять співробітники. Поведінкова аналітика та машинне навчання можуть надати уявлення про загальний набір поведінки в даних в організації, полегшуючи відстеження аномальної активності.

Ненавмисне розголошення – співробітникам не обов'язково бути зловмисними чи жадібними, щоб ділитися конфіденційною інформацією – вони можуть зробити це випадково і все одно завдати фінансової шкоди вашій компанії. Помилка може бути такою ж простою, як випадкове надсилання електронного листа всім у компанії. Компанії з великою кількістю співробітників піддаються особливому ризику, якщо співробітники мають доступ до ваших основних баз даних[6].

Ця загроза виникає через помилку людини, що ускладнює планування та захист вашої компанії. Існують деякі методи, за допомогою яких можна обмежити ймовірність випадкового розголошення, в тому числі:

1. Обмежений доступ: врахуйте кількість співробітників, яким потрібен доступ до вашої бази даних, і обмежте доступ тим, хто цього не потребує.

2. Програмне забезпечення для запобігання витоку інформації та моніторингу активності: додавання цього програмного забезпечення надає кілька рішень для боротьби з ненавмисним розповсюдженням інформації і дозволяє організаціям контролювати свої дані та будь-які пов'язані з ними ризики.

Компанії зберігають великі обсяги даних у хмарі, і багато хто вважає, що ці дані автоматично захищені. Однак це не завжди так. Кіберзлочинці шукають незахищене хмарне сховище для доступу та використання даних. Хмарні інтерфейси не завжди підтримуються системами безпеки, що робить їх легкою здобиччю для кіберзлочинців.

Мабуть, найвідомішим прикладом був злам незахищеного хмарного сегмента S3, який містив велику кількість секретних даних Агентства національної безпеки. У

2017 році стався витік даних із серйозними наслідками. Компанії повинні знати, що зберігання конфіденційної інформації може бути під загрозою, якщо не вжити відповідних запобіжних заходів[6].

Якщо хмарне сховище не є безпечним, усі дані можуть бути втрачені та можуть легко потрапити в руки конкурентів. Компанії можуть надійно захистити своє хмарне сховище, якщо вживуть наступних заходів безпеки:

1. Шифрування: Хмарні служби безпеки шифрують інформацію в хмарі та на вашому комп'ютері, гарантуючи, що особиста інформація не буде доступною для неавторизованих сторін.

2. Інструменти надійної автентифікації: Багатофакторна автентифікація та регулярне оновлення надійних паролів можуть уповільнити зловмисників.

3. Відбір інформації: як організаціям, так і окремим особам слід уникати зберігання конфіденційної інформації (наприклад, приватних банківських даних) у хмарі.

4. Оновити зараз: якщо ваша хмарна система потребує оновлення, встановіть його зараз. Інтернет-провайдери часто розгортають оновлення для усунення вразливостей безпеки.

Атаки нульового дня використовують раніше невідомі вразливості в системах безпеки макромереж і використовують помилки до того, як розробники дізнаються про проблему. Це може негативно вплинути на компанії, які використовують несправні системи. Як тільки хакери виявляють вразливість, вони можуть написати вразливий код, щоб використовувати її.

Кіберзлочинність нульового дня особливо небезпечна, оскільки зловмисник часто єдиний, хто знає про вразливість. Він може вирішити використати цю перевагу негайно, але він також може зберегти її на більш сприятливий час.

Зведіть до мінімуму ймовірність інциденту нульового дня на вашому підприємстві, дотримуючись таких практик кібербезпеки:

1. Брандмауер: переконайтеся, що брандмауер налаштовано правильно та дозволяє лише необхідні транзакції.

2. Ефективне програмне забезпечення для запобігання вторгненням: брандмауери та антивірусні програми ускладнять кіберзлочинцям вибір потенційних жертв.

3. Миттєві оновлення: розробники часто виправляють слабкі місця в системах безпеки за допомогою оновлень, тому, якщо ви вирішите не встановлювати їх негайно, ваша конфіденційна інформація піддається ризику атак нульового дня.

Найефективніший спосіб запобігти атакам нульового дня — постійний моніторинг ваших систем. Компанії, які спеціалізуються на рішеннях з кібербезпеки, можуть надавати такі постійні послуги з кібербезпеки.

Кіберзлочинцям часто доводиться завойовувати довіру своїх жертв, щоб вони могли отримати інформацію, необхідну для завершення своїх операцій. Вони створюють фальшиві особи та профілі в соціальних мережах, щоб встановити фальшиві стосунки зі своїми цілями. Потім вони використовують ці відносини для досягнення своїх цілей фішингу та встановлення зловмисного програмного забезпечення, щоб порушити бізнес-діяльність або отримати фінансову вигоду[6].

Будь-яку форму соціальної взаємодії, розроблену з кінцевою метою обману бізнесу, можна класифікувати як соціальну інженерію. Цей процес може призвести до людської помилки співробітників і дозволити хакерам отримати доступ до корпоративних мереж і даних.

Заходи щодо попередження випадків соціально-інженерних загроз:

1. Навчання користувачів: соціальна інженерія зосереджена на шахрайських діях, націлених на членів організації. Переконайтеся, що члени команди знають про нещодавні випадки шахрайства та навчіть їх поводитися з підозрілими інцидентами та повідомляти про них.

2. Використання VPN: VPN запобігає блокуванню вашої мережі на мобільних або інших пристроях.

3. Процедури моніторингу: постійний моніторинг може допомогти виявити та пом’якшити наслідки соціальної інженерії.

Витік даних – це несанкціоноване переміщення даних з особистого чи робочого пристрою. Цей процес може бути випадковим або навмисним, але він завжди недоречний і несанкціонований. Це може включати переміщення, крадіжку або витік даних і призвести до серйозної репутаційної та фінансової шкоди[7].

Навмисне викрадання даних включає багато загроз, згаданих вище, зокрема фішинг і соціальну інженерію. Щоб виявити витоки даних у вашій організації, ви повинні мати інструменти, які постійно відстежують незвичний і потенційно зловмисний трафік.

Заходи проти витоку інформації[7]:

1. Управління загрозами: спеціальна платформа керування загрозами дозволяє компаніям контролювати доступ до даних і їх використання.

2. Відстежуйте дії користувачів, щоб запобігти витоку даних: моніторинг поведінки користувачів дозволяє відстежувати несанкціоноване переміщення даних і визначати потенційні джерела даних.

3. Брандмауер: встановлення брандмауера є важливою частиною запобігання несанкціонованому доступу до конфіденційної інформації.

1.4. Вимоги до захисту інформаційної системи

В сучасному бізнес-середовищі, де інформація визначає конкурентоспроможність та стійкість підприємства, вимоги до захисту інформаційної системи стають однією із ключових компонент безпеки. В цьому підрозділі розглядаємо основні аспекти, які визначають ефективність та надійність заходів захисту інформаційних активів підприємства[8].

1. Строгі вимоги до аутентифікації та авторизації:

Забезпечення безпеки інформаційної системи починається з чіткої ідентифікації та авторизації користувачів. Вимагається використання сучасних методів багаторівневої аутентифікації та точного контролю над правами доступу.

2. Шифрування та захист конфіденційної інформації:

Важливо впроваджувати механізми шифрування для захисту конфіденційної інформації під час передачі та зберігання. Використання сучасних алгоритмів шифрування є невід'ємною частиною стратегії захисту.

3. Захист від мережевих атак:

Створення ефективних мережевих бар'єрів та використання систем виявлення вторгнень є обов'язковими для запобігання атак зовнішніх загроз.

4. Заходи захисту від внутрішніх загроз:

Безпека також передбачає впровадження стратегій для виявлення та запобігання внутрішнім загрозам. Моніторинг дій персоналу та обмеження прав доступу грають ключову роль.

5. Регулярні аудити та тестування безпеки:

Аудит безпеки та пенетраційне тестування інформаційної системи регулярно проводяться для виявлення та усунення слабких місць у заходах захисту.

6. Ефективне управління інцидентами:

Важливо мати високоефективну систему управління інцидентами для оперативного реагування на потенційні загрози та відновлення нормального функціонування після атаки.

7. Забезпечення безпеки фізичної інфраструктури:

Окрім цифрових заходів, важливо не забувати про захист фізичних активів, таких як серверні приміщення та обладнання.

8. Антивірусні заходи:

Використання ефективних програм антивірусного та антималware захисту є обов'язковим для забезпечення інформаційної системи від загроз з боку шкідливих програм.

Цей аналіз вимог до захисту інформаційної системи підприємства визначає комплексний підхід до забезпечення безпеки, охоплюючи технічні, організаційні та процесуальні аспекти. Впровадження цих заходів спрямоване на мінімізацію ризиків та забезпечення надійності інформаційної системи підприємства в сучасному високотехнологічному середовищі[8].

Висновок до розділу 1

Проаналізовано та зроблено оцінку потенційних втрат та наслідків визначила, що інформаційна безпека підприємства безпосередньо пов'язана з його фінансовим станом, репутацією та законодавчими аспектами. Передбачення та мінімізація цих втрат вимагає комплексного підходу та управління ризиками на всіх рівнях.

Проаналізовано сучасні загрози інформаційним системам є динамічними та розвиваються, вимагаючи постійного удосконалення засобів захисту. Використання сучасних технологій та стратегій, таких як штучний інтелект та мережеві системи виявляється необхідним для ефективного протистояння загрозам.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОГО ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ

2.1. Технології захисту інформаційної системи

Інформаційно-комунікаційна безпека є комплексним підходом до захисту інформаційних ресурсів та забезпечення безпеки інформаційно-комунікаційних процесів. Захист інформаційних систем підприємства важливий аспект в умовах сучасного цифрового світу. Вона являється основним пріоритетом для сучасних підприємств в кіберпросторі.

Протік даних, що становлять під загрозу конфіденційну інформацію мільярдів клієнтів, не тільки завдають компаніям фінансових збитків, а й знижують цінність бренду та підірвають довіру клієнтів. У міру того, як хакери стають все більш витонченими, доведеться впроваджувати більш досконалі технології та методи, що допомагають підтримувати конфіденційність даних.

Безпека даних важлива з таких причин:

1. Забезпечує безпеку вашої інтелектуальної власності.
2. Зберігає цілісність даних.
3. Забезпечує дотримання нормативних та правових стандартів.

Конфіденційність даних: Підприємства часто обробляють та зберігають чутливу інформацію, таку як особисті дані клієнтів, фінансова інформація чи комерційні та ділові таємниці. Недостатній захист може призвести до витоку даних, порушення законодавства та пошкодження репутації підприємства.

Надійність інфраструктури: Забезпечення доступності та надійності інформаційних систем важливо для забезпечення безперебійної роботи підприємства. Атаки або вторгнення можуть призвести до втрати доступу до даних та послуг, що може негативно вплинути на продуктивність та ділові процеси[9].

Захист від фінансових втрат: Кіберзлочинці можуть використовувати атаки для вимагання викупу, викрадання фінансової інформації або здійснення фінансових маніпуляцій. Ефективний захист інформаційних систем може допомогти уникнути серйозних фінансових втрат.

Дотримання законодавства та стандартів: Багато країн мають законодавчі вимоги щодо захисту конфіденційності даних та інших аспектів інформаційної безпеки. Недотримання цих вимог може призвести до юридичних проблем та штрафів.

Захист від репутаційних ризиків: Втрати даних або вразливість до кібератак можуть значно пошкодити репутацію підприємства. Втрата довіри клієнтів та партнерів може вплинути на прибуток та довгостроковий успіх бізнесу[9].

Захист від шпигунства та крадіжок інтелектуальної власності: Підприємства інвестують в інновації та розробку нових продуктів. Захист інформаційної безпеки є важливим для збереження конкурентних переваг і запобігання крадіжці інтелектуальної власності.

Узагальнюючи, ефективний захист інформаційної безпеки є ключовим елементом для забезпечення стійкості та успіху підприємства в умовах зростаючих кіберзагроз.

2.2. Технічні засоби захисту інформаційної системи

Технічні засоби захисту інформаційної системи (ІС) - це апаратне та програмне забезпечення, призначене для забезпечення безпеки інформації та захисту ІС від несанкціонованого доступу, втручань, витоку чи втрати даних. ці технічні засоби використовуються для реалізації різних аспектів політики безпеки та включають в себе різноманітні технічні рішення.Основні категорії технічних засобів захисту інформаційних систем включають[10]:

1. Брандмауери (Firewalls) – це система захисту мережі, яка контролює та фільтрує мережевий трафік на основі передаваних правил безпеки. Брандмауери

використовуються для моніторингу та контролю мережевого трафіку між внутрішньою та зовнішньою мережами. Вони можуть блокувати або дозволяти певний трафік на основі заздалегідь визначених правил.

Основні функції брандмауера:

1. фільтрація пакетів: контроль та блокування певних типів мережевих пакетів в залежності від встановлених правил.

2. натуральна (Stateful) інспекція: спостереження за станом пакетів та рішення про допуск чи блокування на основі історії з'єднання.

3. VPN підтримка: дозвіл чи блокування VPN-з'єднань для забезпечення безпеки з'єднань на рівні мережі.

Типи Брандмауерів:

1. мережеві (Network) брандмауери: роблять фільтрацію на рівні мережевого рівня (OSI Model) та контролюють трафік між мережами.

2. прикладні (Application) брандмауери: фільтрують трафік на рівні застосунків та аналізують дані, що передаються через конкретні додатки.

Безпека Трафіку:

1. захист від вторгнень: виявлення та блокування несанкціонованих спроб доступу.

2. фільтрація доменних імен: блокування доступу до сайтів за певними доменними іменами.

Також Firewalls займає складову частину багатошарових систем захисту, та має інтеграцію з іншими системами безпеки для створення комплексних стратегій захисту. Запис подій та інцидентів для аналізу та виявлення аномалій. Постійний нагляд за мережевим трафіком для вчасного виявлення потенційних загроз. Інтеграція з іншими Засобами Захисту, а саме співпраця із Intrusion Detection System/Intrusion Prevention System (IDS/IPS): Обмін інформацією для виявлення та блокування загроз на рівні мережі. Блокування недозволених підключень та забезпечення безпеки беспровідного з'єднання[10].

2. Антивірусне та антимальварне ПЗ, ці програми призначені для виявлення, блокування та видалення шкідливого програмного забезпечення, такого як віруси, черв'яки, троянські коні та інші види малвари.

Основні функції антивірусного ПЗ:

1. сканування файлів, регулярне сканування файлів та системних ресурсів для виявлення потенційно шкідливого коду;

2. автоматичне оновлення, завантаження та встановлення оновлень баз даних для розпізнавання нових видів загроз;

3. резидентний (Background) режим, постійний моніторинг активності системи для виявлення загроз в реальному часі;

4. карантин та вилучення, поміщення підозрілих файлів в карантин та їх вилучення для забезпечення безпеки системи.

Типи загроз, які виявляються:

1. віруси – рограми, що приховуються в інших файлах і активуються при їх відкритті чи запуску;

2. черв'яки – саморозповсюджуючі програми, які розповсюджуються через мережі та інші засоби;

3. троянські коні – шкідливі програми, які виглядають як корисне ПЗ, але виконують небажані функції при активації;

4. шпигунське ПЗ – програми, що збирають та передають конфіденційну інформацію без належного повідомлення користувача.

Також у антивірусного та антимальварного прорамного забезпечення є можливість інтеграції з IDS/IPS, мультиплатформенність - виробники надають антивірусні рішення для різних операційних систем, включаючи Windows, macOS, Linux. Інформування користувачів про виявлення та блокування потенційних загроз. Моніторинг активності та генерація звітів щодо безпеки системи. Є і рішення для корпоративних мереж, а саме можливість встановлювати, конфігурувати та

оновлювати антивірусне ПЗ на великій кількості комп'ютерів з централізованої консолі[11].

3. Система виявлення атак та запобіганню вторгненням (IDS/IPS): IDS виявляє аномальну або потенційно шкідливу діяльність в мережі чи системі, а IPS може автоматично реагувати та блокувати несанкціоновані дії.

Система виявлення атак використовується для моніторингу та аналізу активності в мережі чи на окремій системі. Вона оперативно реагує на незвичайні чи підозрілі події, аналізуючи мережевий трафік та системні журнали. IDS використовує два основні методи виявлення атак: сигнатурний аналіз і аномалійний аналіз. Сигнатурний аналіз порівнює активність із відомими сигнатурами відомих атак, тоді як аномалійний аналіз виявляє невідомі атаки шляхом виявлення неприродних патернів чи аномалій у поведінці системи.

Основна мета IDS - це виявлення можливих загроз та сповіщення адміністраторів чи безпекового персоналу про тривожні ситуації. IDS не блокує трафік самостійно, але надає інформацію для подальшого аналізу та втручання.

У відміну від IDS, система запобігання вторгненням володіє активними функціями блокування та утримання атак. IPS автоматично реагує на виявлені загрози, блокуючи чи обмежуючи трафік, що викликає тривожні події. Це надає системі можливість запобігти потенційно шкідливим вторгненням, забезпечуючи реальний захист.

IPS використовує ті ж методи виявлення атак, що і IDS, але його головна функція - це забезпечення активного захисту. Відповідно до аналізу виявлених загроз, IPS може автоматично вживати заходів для блокування атак та захисту інформаційних ресурсів[12].

Ці дві системи часто інтегруються для створення комплексного захисного обрамлення для мережі чи інформаційної системи. Їх взаємодія надає організаціям засіб ефективного виявлення та захисту від широкого спектру кіберзагроз.

4. Шифрування даних є невід'ємною частиною сучасних систем безпеки та конфіденційності інформації. Цей процес використовується для захисту конфіденційності та цілісності даних, забезпечуючи їхню безпеку під час передачі чи зберігання.

Шифрування базується на математичних або алгоритмічних методах перетворення звичайного тексту (даних) у криптограму (зашифрований текст), що може бути розшифрована тільки за допомогою спеціального ключа. Основні принципи включають:

1. алгоритми шифрування, використовуються різноманітні математичні або логічні алгоритми для зміни структури даних так, щоб вони стали нерозпізнаваними без ключа;

2. ключі визначаються алгоритмом і використовуються для шифрування та розшифрування даних. Ключі можуть бути симетричними (один ключ використовується і для шифрування, і для розшифрування) або асиметричними (використовуються різні ключі для цих операцій).

Симетричне шифрування використовує один і той же ключ для шифрування та розшифрування даних. Наприклад, Advanced Encryption Standard (AES).

Асиметричне (публічний ключ) шифрування використовує два ключі: публічний і приватний. Публічний ключ використовується для шифрування, а приватний - для розшифрування. Наприклад, RSA (Rivest-Shamir-Adleman).

Хешування, метод шифрування, де створюється фіксований "хеш" (хеш-сума) для даних. Використовується для перевірки цілісності даних.

Шифрування даних є невід'ємною складовою для захисту інформації на підприємствах, забезпечуючи безпеку та конфіденційність важливих даних. Його ключові переваги: висока конфіденційність, захист від несанкціонованого доступу, довіреність даних.

5. Безпека Мережі (VPN, VLAN): Використовується для захисту мережевого трафіку та забезпечення конфіденційності під час передачі даних через мережу.

6. Системи резервного копіювання та відновлення даних:, забезпечують резервне копіювання і відновлення даних для запобігання втраті інформації в результаті непередбачених обставин.

Системи резервного копіювання та відновлення даних є ключовими елементами сучасної інформаційної безпеки та стратегій управління даними. Забезпечення безпеки та надійності даних, можливість відновлення інформації у разі втрати або пошкодження, забезпечення безперервності бізнес-процесів стають критичними завданнями для цієї системи.

Ключові аспекти включають розробку чіткого плану резервного копіювання, визначення стратегій резервного копіювання (повного, інкрементального, диференціального), використання надійних систем зберігання даних із можливостями стиснення та шифрування, тестування та перевірку процесів відновлення та планів аварійного відновлення.

Технологічна інфраструктура передбачає використання сучасних систем зберігання, а також автоматизацію щоденних завдань за допомогою управління та моніторингу. Надійна система резервного копіювання повинна враховувати такі заходи безпеки, як обмеження доступу, антивірусний захист тощо, щоб забезпечити захист копій від потенційних загроз.

Основна увага приділяється надійності процесу відновлення, включаючи регулярне тестування та врахування резервного відновлення в рамках загального плану аварійного відновлення організації. Розробка зосереджена на інтеграції хмарних рішень і використанні аналітичних інструментів для оптимізації стратегій резервного копіювання.

7. Ідентифікація та Аутентифікація: Включає в себе використання технологій, таких як паролі, біометричні дані, токени та інші методи для перевірки ідентичності користувачів.

Ідентифікація та автентифікація є ключовими поняттями у сфері інформаційної безпеки, призначеними для забезпечення безпечного та авторизованого доступу до

ресурсів. Ці аспекти стосуються як персональних систем, так і корпоративних середовищ, визначаючи, хто саме намагається отримати доступ (ідентифікація) і чи можна це насправді здійснити (автентифікація) [13].

Автентифікація використовує унікальний ідентифікатор, наприклад ім’я користувача, для ідентифікації особи чи системи. Ідентифікатор має бути унікальним і однозначно ідентифікувати конкретного користувача або систему.

Автентифікація визначає, чи може особа або система дійсно отримати доступ. Це включає перевірку особи користувача та надання факторів автентифікації, таких як паролі, біометричні дані, смарт-карти тощо.

Принципи ідентифікації та автентифікації включають забезпечення високого рівня безпеки без ускладнення процесу використання для законних користувачів. Двофакторна автентифікація стає стандартом для забезпечення додаткового рівня безпеки.

Сучасні технології включають біометричну аутентифікацію та синхронізацію з мобільними пристроями. Керування ідентифікацією та доступом використовує централізовані системи для керування користувачами та їхніми дозволами, тоді як аудит і журналювання допомагають виявляти аномалії та контролювати доступ.

Ідентифікація та автентифікація вимагають комплексного підходу для забезпечення безпеки та доступності в різних середовищах.

8. Засоби авторизації в інформаційних системах є ключовими елементами забезпечення безпеки та управління доступом до ресурсів. Цей процес визначає права та можливості конкретного користувача або системи після успішної автентифікації та включає різні технічні та організаційні аспекти.

Визначення прав доступу стає ключовим елементом інструментів авторизації, де автентифікованим користувачам призначаються певні дії та ресурси. Авторизація на основі ролей спрощує керування доступом, призначаючи користувачам ролі з відповідними дозволами.

Автоматизовані політики безпеки визначають правила авторизації на основі стандартів і вимог внутрішньої безпеки. Двофакторна аутентифікація використовує додатковий метод разом із звичайним паролем, що підвищує рівень безпеки.

Моніторинг і аудит дій користувачів є важливим аспектом інструментів авторизації, які виявляють несподівані або потенційно небезпечні взаємодії. Управління сеансами та моніторинг активних сеансів користувачів забезпечують додатковий рівень безпеки.

Усі ці аспекти засобів авторизації призначені для забезпечення ефективного та безпечного адміністративного контролю над доступом до ресурсів інформаційної системи.

9. Системи моніторингу та аудиту, які захищають інформаційні системи компанії, є комплексним підходом, призначеним для виявлення, ідентифікації та відстеження подій, які можуть вплинути на безпеку та надійність інформації.

Система відстежує можливі загрози та події в режимі реального часу, виявляючи аномалії та спроби несанкціонованого доступу в мережевому трафіку. Аудит активності користувачів включає детальну реєстрацію всіх дій в системі, починаючи від авторизації користувача і закінчуючи взаємодією з файлами та ресурсами[14].

Система також може виявляти аномалії та аномалії, використовуючи алгоритми та штучний інтелект для попередження про можливі загрози. Він зосереджений на захисті інфраструктури та даних, включаючи моніторинг серверів, мережевого обладнання та інших критичних компонентів.

Крім того, система забезпечує поглиблений аналіз журналів подій для виявлення вразливостей і слабких місць системи. Він також взаємодіє з програмами реагування на інциденти, щоб ефективно блокувати загрози та відновлювати стабільність системи.

Важливим аспектом є забезпечення відповідності та аудиту, коли система сприяє детальному обліку змін і доступу, забезпечуючи відповідність інформаційних систем нормативним вимогам і стандартам.

Усі ці зусилля спрямовані на захист критично важливих даних, забезпечення їх конфіденційності та недоступності від несанкціонованого доступу. Система моніторингу та аудиту стає невід'ємною частиною загальної стратегії безпеки інформаційної системи підприємства.

2.3. Заходи з фізичного захисту

Заходи фізичного захисту грають важливу роль у забезпеченні безпеки інформаційної системи на підприємстві. Нижче перераховано деякі ключові заходи, які можна впровадити для забезпечення фізичної безпеки[15]

Контроль доступу до приміщень:

1. встановлення системи контролю доступу, такої як електронні картки або біометричні системи;
2. обмеження доступу до приміщень, де знаходяться серверні кімнати та інші важливі ресурси;

Відеоспостереження:

1. встановлення системи відеоспостереження для моніторингу важливих зон та точок доступу;
2. розміщення камер в областях, де зберігається чи оброблюється важлива інформація.

Фізична охорона:

1. наявність фізичної охорони для моніторингу та контролю доступу;
2. здійснення регулярних перевірок та обходів для виявлення будь-яких незвичайних ситуацій.

Захист інфраструктури:

1. розташування серверних кімнат внутрішньої частини будівлі для ускладнення фізичного доступу;

2. захист інфраструктури від природних катастроф, таких як пожежі, повені, або землетруси.

Безпека обладнання:

1. фізичне закріплення серверів, комутаторів та іншого обладнання, щоб уникнути його крадіжки чи неправомірного доступу;

2. використання захисних корпусів та кабельних систем.

Забезпечення резервного живлення для систем інформаційної обробки та зберігання, щоб уникнути можливих втрат даних в разі відключення електроенергії.

Безпека пристроїв зберігання даних – захист фізичного доступу до пристроїв зберігання даних, таких як серверні багатоплатформенні системи чи файлові сервери.

Ідентифікація та маркування обладнання – застосування систем ідентифікації та маркування обладнання для визначення власності та виявлення неправомірного використання.

Ці заходи допомагають уникнути фізичних загроз, забезпечуючи безпеку об'єктів інформаційної системи на рівні їхнього розташування.

2.4. Управління доступом, ідентифікація та аудит

Управління доступом, ідентифікація та аудит є ключовими елементами системи захисту інформаційної системи на підприємстві, спрямованими на забезпечення безпеки та конфіденційності даних.

Управління доступом:

1. ролева модел, визначення ролей користувачів та присвоєння їм відповідних прав доступу. Це спрощує управління доступом та зменшує ризик надання непотрібних прав;

2. система контролю доступу, використання сучасних систем контролю доступу, таких як електронні картки або біометричні методи, для обмеження доступу до важливих приміщень та ресурсів;

3. централізоване управління, створення централізованої системи управління, що дозволяє ефективно керувати доступом та внесенням змін у права користувачів;

4. двофакторна аутентифікація, впровадження двофакторної аутентифікації для підвищення рівня безпеки шляхом використання додаткового методу, наприклад, коду з смарт-карти чи мобільного пристрою[16].

Ідентифікація:

1. ідентифікаційні системи, використання унікальних ідентифікаторів для кожного користувача чи системи, які включають логіни, паролі та/або біометричні дані;

2. централізоване керування ідентифікацією, створення централізованої системи управління ідентичністю, що дозволяє ефективно керувати реєстрацією та скасуванням доступу для користувачів;

3. активне відстеження, впровадження активної системи відстеження, яка дозволить вам негайно виявляти та реагувати на несанкціонований доступ або використання ідентифікаторів.

Аудит:

1. система журналювання подій, встановлення системи журналювання, яка реєструє всі події, пов'язані із змінами в системі та доступом користувачів;

2. глибокий аналіз, проведення глибокого аналізу журналів подій для виявлення аномалій, вторгнень чи інших потенційно небезпечних ситуацій;

3. регулярний аудит, проведення регулярних аудитів системи безпеки для виявлення і виправлення слабких місць та забезпечення відповідності стандартам безпеки.

Ці заходи сприяють створенню комплексної системи захисту, яка поєднує управління доступом, ідентифікацію та аудит для ефективного захисту інформаційної системи підприємства.

Висновок до розділу 2

Зроблено висновок, що дослідження технологій захисту інформаційних систем важливе для розуміння сучасних методів інформаційної безпеки. Виокремлено ключові аспекти, які допомагають у створенні комплексної системи захисту.

Зазначено, що використання технічних засобів, таких як антивірусне програмне забезпечення, брандмауери та системи IDS/IPS, має вирішальне значення для ефективного захисту інформаційної інфраструктури. Проаналізовано їхню взаємодію та роль у забезпеченні безпеки.

Підкреслено важливість заходів з фізичного захисту, таких як обмеження фізичного доступу та використання систем відеоспостереження. Досліджено їхню роль у створенні повноцінної системи захисту інформації в контексті фізичного середовища підприємства.

Проаналізовано, що ефективне управління доступом, ідентифікація та система аудиту є критичними компонентами системи захисту. Зазначено їхню роль у забезпеченні конфіденційності, цілісності та доступності даних. Зроблено висновок про необхідність їхнього поєднання для оптимальної захисту інформації.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОГО ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

3.1. Аналіз існуючої інформаційної системи підприємства

На всіх підприємствах, зберігаються великі обсяги інформації, конфіденційних даних, даних про працівників, потребує захисту і має важливе місце в кібербезпеці. І підприємство ТОВ «КЕРНЕЛ» також зацікавлене в покращенні своєї інформаційної системи. Інформаційна система підприємства володіє важливим значенням для забезпечення безпеки та ефективності діяльності. З урахуванням великої кількості конфіденційних даних, включаючи інформацію про працівників, підприємство приділяє велику увагу розвитку та захисту своєї інформаційної інфраструктури.

Найважливіша будівля в якій циркулює інформація з обмеженим доступом, розташована на території підприємства. Приміщення цілодобово охороняється черговою зміною охорони підприємства, здійснений контроль працівників за допомогою СКУД, також встановлена система відеоспостереження. На рис. 3.1 зображено відділи, робочі місця працівників, а також серверну.

Підрозділи, обробляють різні дані, забезпечуючи таким чином свою ефективність і чіткий розподіл даних, що обробляються в мережі. і дані, які повинні передаватися між блоками без порушення безпеки.

Бухгалтерія та юридична служба займаються найбільш важливими даними, оскільки підлягає захисту фінансова звітність, банківські дані та документообіг організації, договори на виконання замовлень, документи про право власності на певні об’єкти, тендерна інформація.

Якщо ці дані буде втрачено або змінено, бізнес може зазнати значних збитків або навіть повністю припинити своє існування.

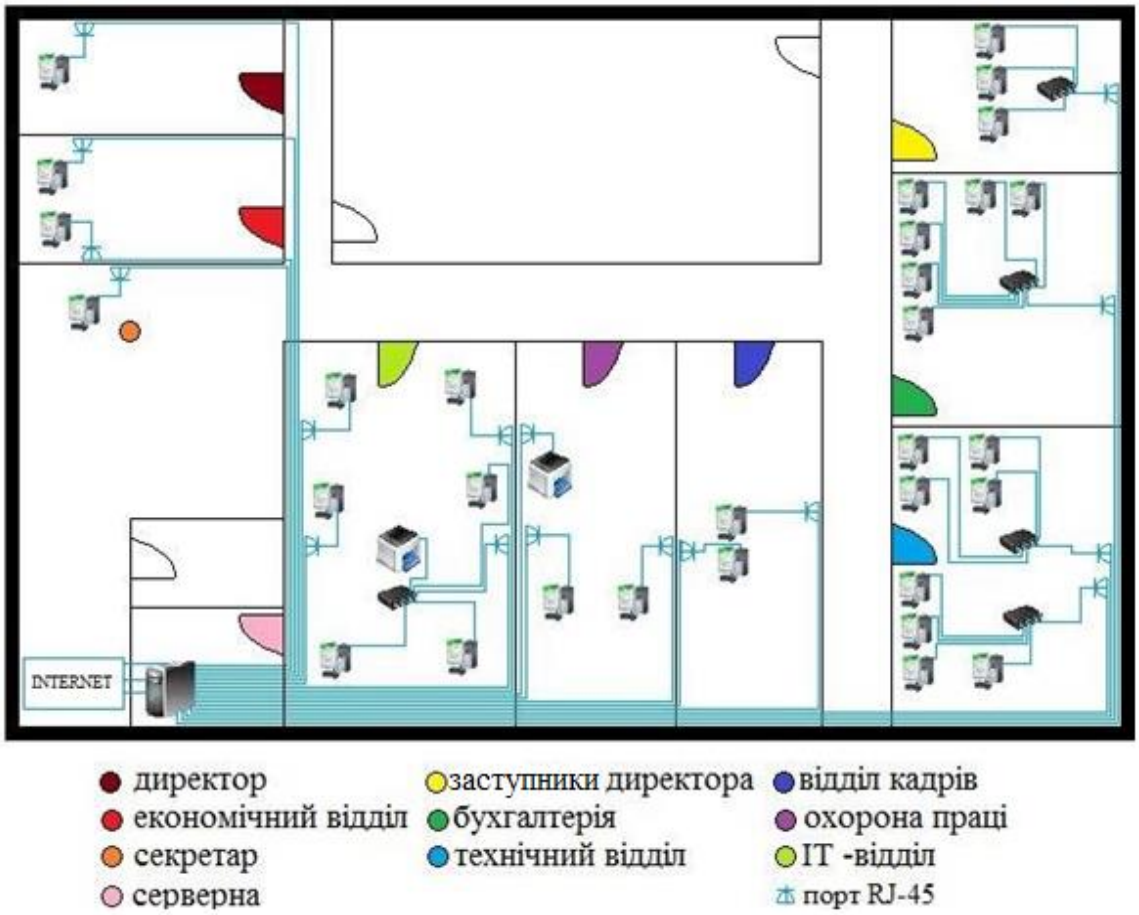

Рис. 3.1. Схематичне зображення будівлі

Інфраструктура ТОВ «КЕРНЕЛ» складається з наступних інформаційних ресурсів:

1. Відомості, що становлять комерційну таємницю:

– заробітна плата;
– контракти з постачальниками та покупцями;
– технологія виробництва.

Захищена інформація (інформація з обмеженим доступом):

– трудовий договір;
– особисті справи співробітників;
– документи відділу складу;
– особова картка працівника;

– зміст бухгалтерського та внутрішнього обліку;

– бухгалтерський та юридичний відділи;

– інші розробки та документи для внутрішнього користування.

2. Публічна інформація:

– статут та установчі документи;

прайс-лист товарів.

До складу підприємства входять наступні структурні елементи: комп'ютери, сервери, комутатори, маршрутизатори, мережеві принтери.

Сервер — це багатокористувацький комп’ютер, призначений для обробки запитів від усіх робочих станцій. Він надає робочим станціям доступ до системних ресурсів і розподіляє ці ресурси. Операційні системи серії Windows встановлені на серверах в магазинах і головних офісах.

Мережевий комутатор — пристрій, призначений для з’єднання кількох вузлів комп’ютерної мережі в межах одного сегмента мережі [18]. ТОВ «КЕРНЕЛ» використовує некеровані комутатори TP-Link і DLink у своїй комп’ютерній мережі. Некеровані комутатори не потребують конфігурації, тому їх встановлення не викликає проблем у користувачів. Некеровані комутатори мають меншу пропускну здатність, ніж керовані комутатори. Як правило, некеровані комутатори використовуються в домашніх мережах, тому це необхідно враховувати при розробці моделі захисту мережі для інформаційно-телекомунікаційних систем ТОВ «КЕРНЕЛ».

Маршрутизатор – це мережевий пристрій, який об’єднує різні комп’ютерні мережі та мережі, побудовані на різних технологіях, і керує обміном даними між ними [18]. У комп’ютерній мережі ТОВ «КЕРНЕЛ» використовуються маршрутизатори TP-Link.

Для підприємства рекомендується встановити брандмауер, наприклад Cisco ASA.

Якщо подивитись на функції та технології, які зазвичай використовуються підприємства, то вони присутні в брандмауерах і маршрутизаторах. Однак міжмережевий екран варто обрати в тому випадку, коли в головному офісі потрібно організувати безпечний доступ в Інтернет, захищений віддалений доступ користувачів і підключення віддалених філій [17].

Основною метою Cisco ASA є безпека. А з технічної точки зору такі функції безпеки, як брандмауер, IPS, VPN, підключення віддаленого користувача тощо, реалізовані краще, ніж звичайні маршрутизатори. Багато функцій безпеки ввімкнено за замовчуванням у брандмауерах, їх потрібно налаштовувати вручну на маршрутизаторах або взагалі недоступні [17].

В комп'ютерній мережі наукового закладу використовується кабель типу вита пара UTP5.

Захист інформаційних систем ТОВ «КЕРНЕЛ» забезпечується такими заходами:

1. Перевірка, чи дійсно користувач сервісу компонента розподіленої системи є користувачем, якому дозволено доступ до сервісів і даних системи (автентифікація).

2. Обмеження доступу до сервісів компонентів за результатами аутентифікації (авторизації). Щоб вирішити цю проблему, було реалізовано обмеження доступу на основі ролей.

3. Змініть стандартний порт маршрутизатора для підключень RDP.

Комплексний аналіз показує, що захист інформаційної системи ТОВ «КЕРНЕЛ» є недостатнім і потребує вдосконалення.

3.2. Розробка та впровадження заходів з підвищення захисту

При розробленні варіанта захищеного функціонування інформаційної мережі ТОВ «КЕРНЕЛ» необхідно враховувати, що вона має відповідати зростаючим вимогам підприємства, а саме підтримувати механізми забезпечення якості сервісу,

бути безпечною та продуктивною. Для формування інформаційної системи обрано обладнання Cisco Systems. При виборі обладнання керувалися його характеристиками.

Виходячи із фінансової і практичної точки зору, а також необхідністю кіберзахисту мережі підприємства, безпечного доступу в Інтернет обрано рішення встановити міжмережевий екран Cisco ASA 5506-X.

Cisco ASA 5506-X забезпечує безпрецедентний рівень захисту від мережевих загроз завдяки такии можливостям: глибока перевірка мережі, аналіз окремих потоків, безпека підключень за рахунок оцінки захищеності кінцевих пристроїв, підтримка передачі голосових і відеоданих через VPN (табл. 3.1). Міжмережевий екран Cisco ASA 5506-X: 8 портів 10/100/1000 BaseT Ethernet, 1 порт USB 2.0, серійні порти RJ-45 Console і Mini USB, блок живлення AC (рис. 3.2) [19].

Рис. 3.2 – Маршрутизатор Cisco ASA 5506-X

Таблиця 3.1

Технічні характеристики Cisco ASA 5506-X [28]

Тип пристрою	Міжмережевий екран
Порти доступу Ethernet	8 x GE RJ-45
Число IPSec VPN	10
Продуктивність FIREWALL	750 Мбіт/с
VLAN 802.1q стандарт/макс	5/30
Габаритні розміри (ВхШхГ)	4,45x20,04x17,45
Пам’ять FLASH	16 Гб
Об’єм ОЗУ	4 Гб
Тип живлення	AC 100-240В
IPSec VPN 3DES/AES	100 Мбіт/с
Нових сесій в секунду, макс	5000
Тип встановлення	Настільне
Продуктивність IPS	125 Мбіт/с
Висока доступність	Ні
Кількість захищених вузлів	Не обмежено

Також для підприємства обрано маршрутизатор Cisco 2811.

На маршрутизаторі Cisco 2811 встановлено програмне забезпечення Cisco IOS і підтримує ідею самозахисту мережі - Cisco Self-Defending Network, з розширеними функціями безпеки та підтримкою IPSec VPN система

Запобігання вторгненням (IPS), контроль доступу (NAC) і фільтрація URL (табл. 3.2).

Основні характеристики: висока продуктивність, модульна архітектура, апаратна підтримка, можливості використання засобів безпеки, технологія мережевої передачі живлення Power over Ethernet (PoE).

Маршрутизатор Cisco 2811: 2 порти Fast Ethernet (10/100BASE-T), 2 USB 1.1, 4 слоти HWIC/WIC/VIC/VWIC, 1 слот NM/NME, 2 слоти PVDM2, 2 слоти AIM (рис. 3.3) [19].

Рис. 3.3 – Маршрутизатор Cisco 2811

Таблиця 3.2

Технічні характеристики Cisco 2811

Тип пристрою	Маршрутизатор
Вбудовані порти LAN	2*10/100 TX
Пам’ять Flash, Мб (станд./макс)	64 / 128
Пам’ять DRAM, Мб (станд./макс)	256 / 768
Інтегровані PVDM (DSP) слоти	2
Підтримка інтерфейсних карт	4 слота (кожен слот підтримує любий HWIC, WIC, VIC и VWIC-модулі)
Наявність мережевих слотів	1
Порти USB 1.1	2
Консольний порт (до 115.2 Кбіт/с)	1
Додатковий порт (AUX) (до 115.2Кбит/с)	1
Апаратне прискорення VPN	DES, 3DES, AES 128, AES 192, та AES 256
AC-IP Maximum In-Line Power Distribution	160W

3.3. Оцінка ефективності технологій захисту Cisco ASA 5506-X

Забезпечення безпеки інформаційних систем є критичним завданням у сучасному цифровому середовищі. З урахуванням постійно зростаючих загроз та кількості кібератак, вивчення та оцінка ефективності технологій захисту, зокрема Cisco ASA 5506-X, стає необхідністю для забезпечення стійкості інформаційної інфраструктури підприємства[19].

Cisco ASA 5506-X вирізняється своєю міцністю та багатофункціональністю. Здатність виконувати функції фірменого фаєрволу, виявлення вторгнень та VPN-з'єднань робить його привабливим вибором для підприємства.

Аналізується ефективність систем виявлення вторгнень та системи запобігання вторгненням, зокрема, використання сигнатурних та аномалійних методів виявлення, активної реакції на атаки та використання систем аналізу поведінки.

Розгляд системи аутентифікації користувачів та пристроїв, зокрема, використання сильних паролів та механізмів багаторівневої аутентифікації.

Аналіз ефективності використання ACL для обмеження доступу до різних мережевих ресурсів та сервісів в залежності від користувацьких ролей.

Оцінка системи моніторингу для визначення, наскільки швидко та ефективно Cisco ASA 5506-X виявляє та реагує на спроби несанкціонованого доступу.

Дослідження заходів, які застосовуються для захисту від DoS-атак та інших атак, спрямованих на вичерпання ресурсів.

Визначення того, наскільки успішно система виявлення вторгнень визначає як відомі, так і невідомі загрози.

Оцінка здатності IPS реагувати на виявлені загрози, зокрема, блокування атак та виконання заходів для їх усунення.

Дослідження використання технологій, які виявляють незвичайні або аномальні патерни поведінки в мережі.

Глибокий аналіз рівня шифрування, використання тунельної архітектури та ефективності управління ключами для забезпечення безпеки VPN-з'єднань, а саме:

– оцінка надійності використовуваних алгоритмів шифрування для захисту передачі даних.

– дослідження та порівняння різних тунельних архітектур, що використовуються для створення VPN-з'єднань.

– аналіз ефективності системи управління ключами для забезпечення безпеки обміну ключами у VPN-з'єднаннях.

3.4. Розроблення рекомендацій щодо застосування технології забезпечення захищеного функціонування інформаційної системи підприємства на базі Cisco ASA 5506-X

Пристрій Cisco ASA 5506-X потрібно налаштувати для виконання функцій захисту мережі з використанням набору основних команд (interface, nameif, рівень безпеки, IP-адреса, маршрутизація). Розглянемо кожну докладніше:

– interface – використовується для визначення типу обладнання, яке використовується, встановлює параметри продуктивності та ініціалізує інтерфейси

– nameif – використовується для призначення імені інтерфейсу ASA.

– рівень безпеки – використовується для визначення рівня безпеки інтерфейсу. За замовчуванням рівень безпеки зовнішнього інтерфейсу Ethernet0 становить 0, а рівень безпеки внутрішнього інтерфейсу Ethernet1 становить 100. Синтаксис: рівень безпеки.

– ip-адреса - дозволяє призначити IP-адресу кожному інтерфейсу пристрою захисту.

– маршрутизація – використовується для встановлення статичних маршрутів для інтерфейсів[19].

Налаштовуємо два інтерфейси INET і LAN, перший для зовнішньої мережі, а другий – відповідно внутрішня мережа. Результати налаштування показано на рис. 3.4.

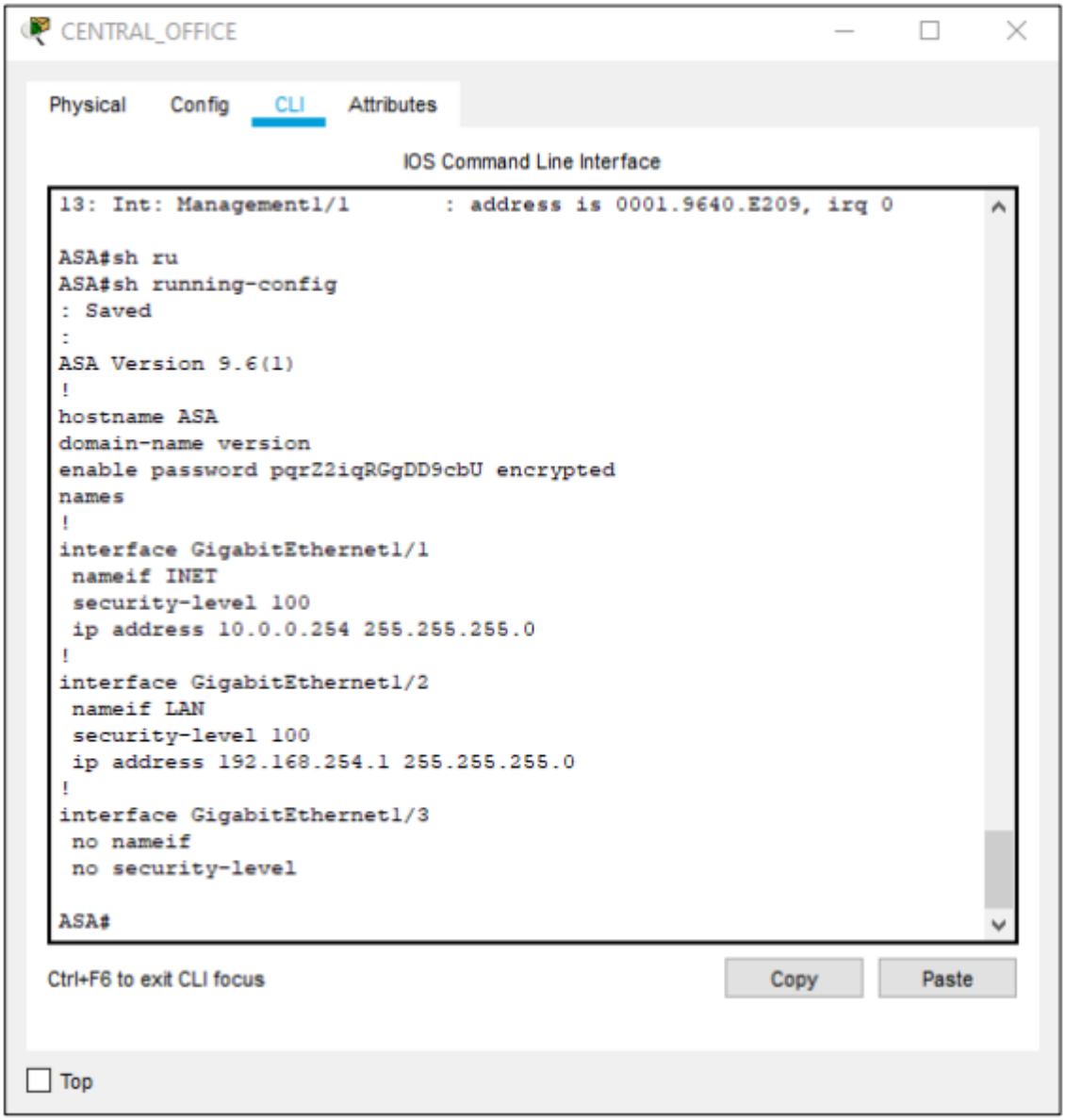

Рис. 3.4 – Налаштування інтерфейсів

Далі налаштуємо параметри шифрування за допомогою набору протоколів IPSec. IPSec забезпечує захист даних, що передаються через Інтернет-протокол IP. Результати коригування показані на рис. 3.5.

Збіг політики IKEv1 встановлюється, коли дві політики від двох однорангових вузлів містять ідентичні значення параметрів автентифікації, шифрування, хешування та Діффі-Хеллмана.

Для налаштування ми використовуємо команди, наведені в лістингу 3.1.

Лістинг 3.1 – Налаштування параметрів шифрування за допомогою набору протоколів IPSec

```
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-
hmac
crypto ikev1 policy 1
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
exit
```

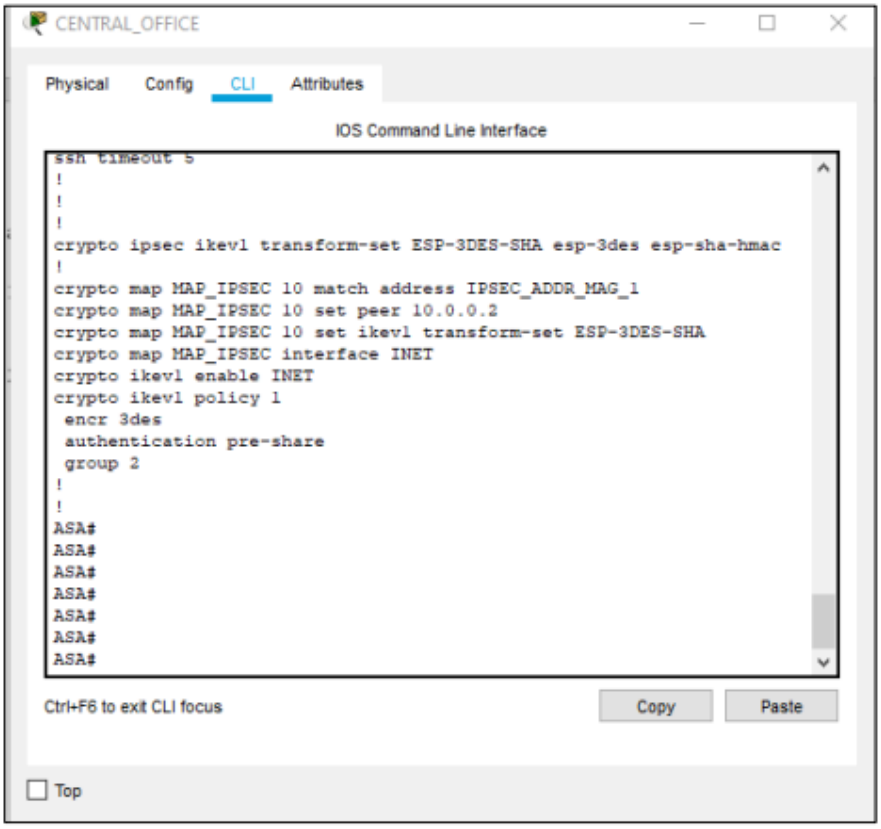

Рис. 3.5 – Налаштування параметрів шифрування за допомогою набору протоколів IPSec

Щоб налаштувати список контролю доступу для необхідного трафіку VPN, потрібно використовувати розширений або іменований список контролю доступу (лістинг 3.2) для зазначеного трафіку, який має бути захищений за допомогою шифрування. Результати налаштування показані на рис. 3.6.

Лістинг 3.2 – Налаштування списку контролю доступу

```
access-list IPSEC_ADDR_MAG_1 extended permit ip 192.168.254.0
255.255.255.0 192.168.1.0 255.255.255.0
```

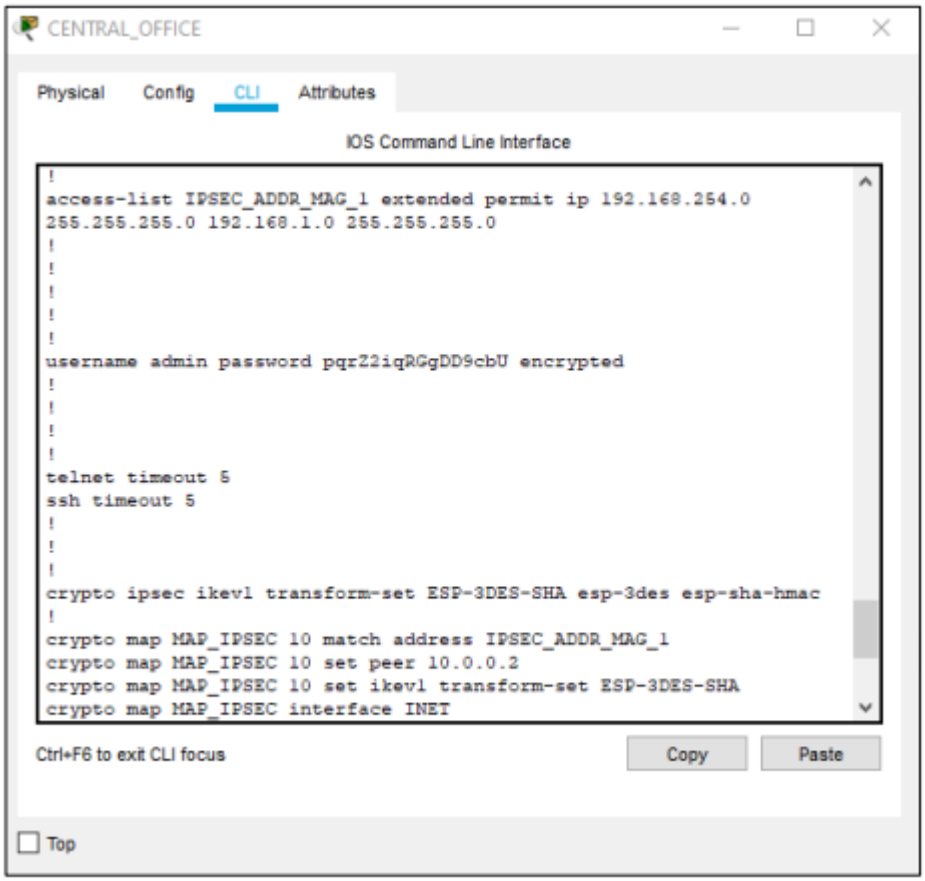

Рис. 3.6 – Налаштування списку контролю доступу

Налаштування шифрування та застосування до інтерфейсу INET (лістинг 3.3). Результати коригування показані на рис. 3.7.

Схема шифрування визначає політику IPsec, узгоджену в IPSEC SA, зокрема:

– Списки контролю доступу, які використовуються для визначення того, які пакети дозволені та захищені з’єднаннями IPSec.

– Ідентифікація тимчасових вузлів.

– Локальна адреса трафіку IPSec.

– Набір трансформацій IKEv1.

Лістинг 3.3 – Налаштування кріптосхеми

```
crypto map MAP_IPSEC 10 match address IPSEC_ADDR_MAG_1
crypto map MAP_IPSEC 10 set peer 10.0.0.2
crypto map MAP_IPSEC 10 set ikev1 transform-set ESP-3DES-SHA
crypto map MAP_IPSEC interface INET
```

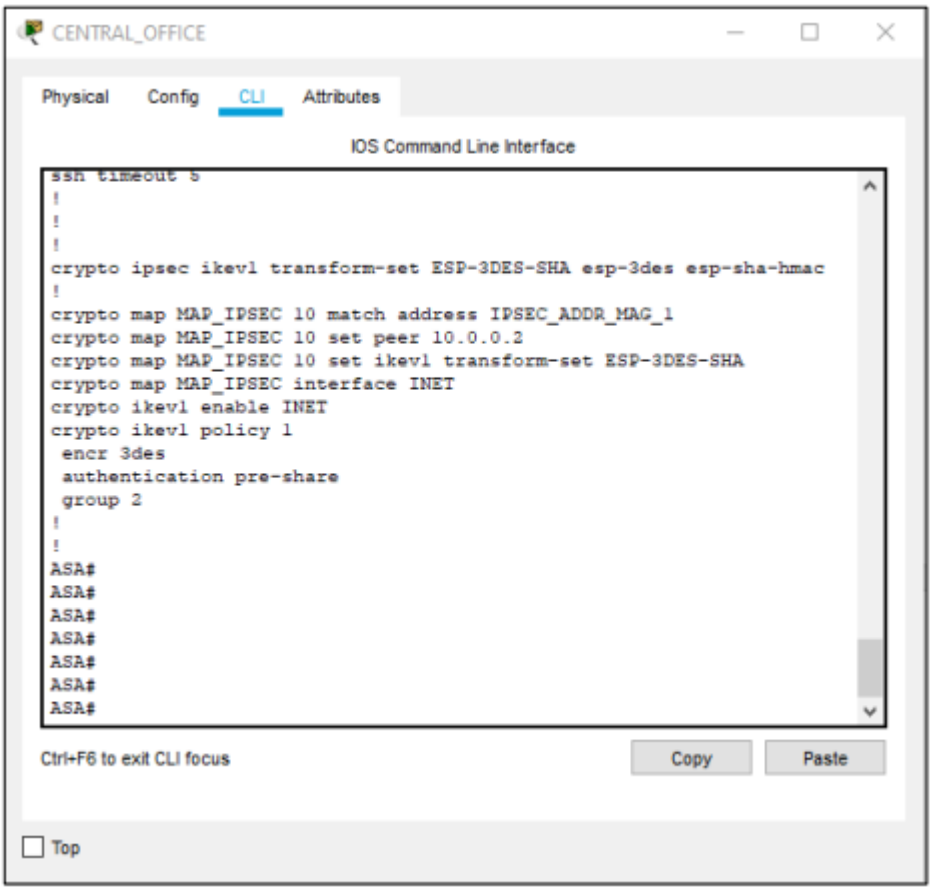

Рис. 3.7 – Налаштування кріптосхеми

Для підприємства ТОВ «КЕРНЕЛ» запропоновано використовувати маршрутизатор Cisco 2811. Спочатку, налаштуємо ISAKMP – обхід асоціації безпеки Інтернету та керування ключами. ISAKMP надає платформу обміну ключами для незалежного обміну ключами. Як правило, для обміну ключами використовується IKE – стандартний протокол для набору протоколів IPSec, який використовується для захисту зв’язку в VPN.

Створимо політику ISAKMP. Тип тунелю L2L (лістинг 3.4)

Лістинг 3.4 – Створення політики ISAKMP

```
crypto isakmp policy 10
hash sha
authentication pre-share
!
crypto isakmp key vpnuser address 10.0.0.254
```

Команда crypto isakmp policy використовується для створення політики IKE та визначення алгоритмів і параметрів, необхідних для створеного безпечного каналу. У наведеному списку створюється політика IKE з пріоритетом 10, результат виконання команди показано на рис. 3.8.

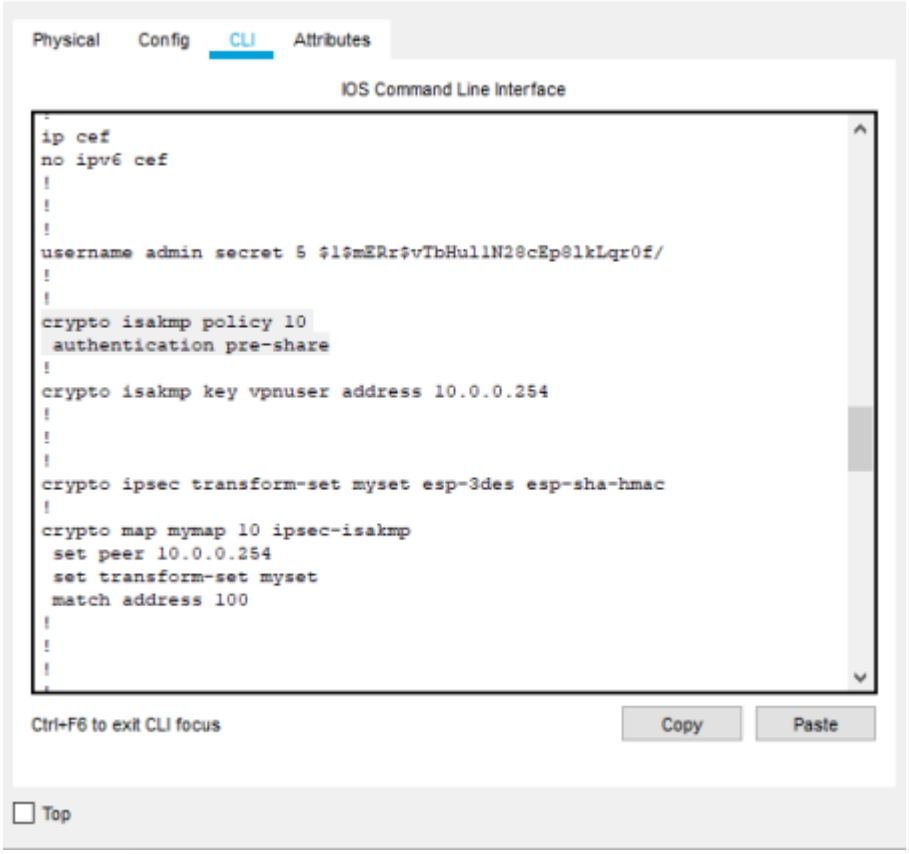

Рис. 3.8 – Створення політики ISAKMP

Створимо політику для забезпечення фактичного шифрування даних (лістинг 3.5)

Лістинг 3.5 – Створення політики

```
crypto ipsec transform-set myset esp-3des esp-sha-hmac
```

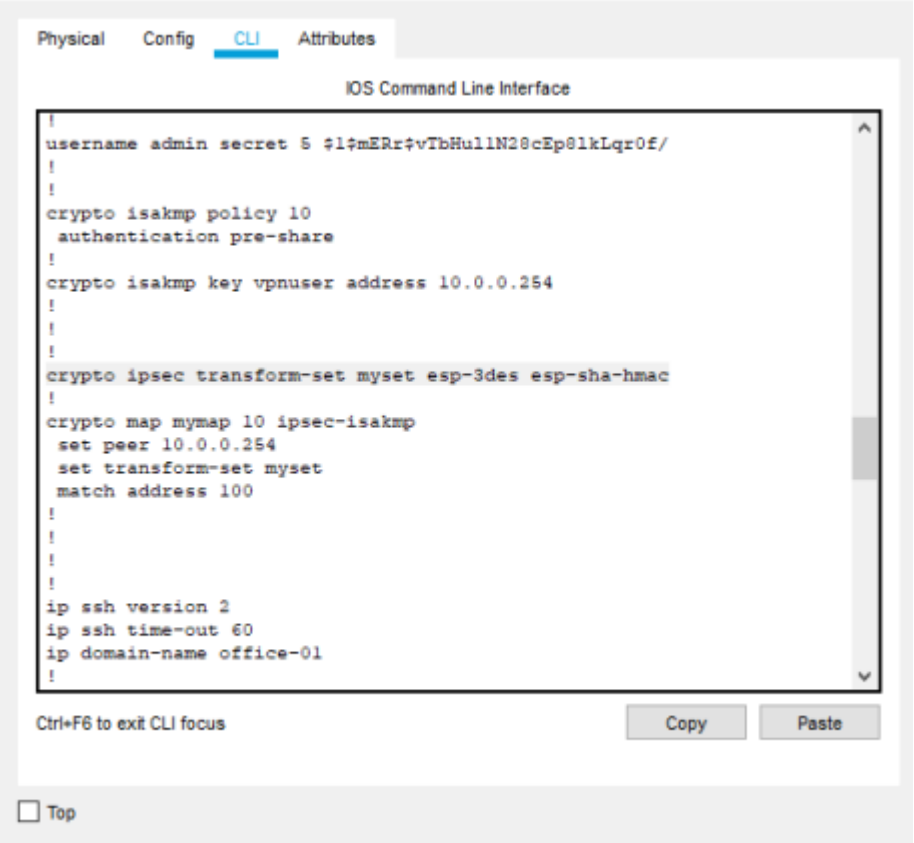

Рис. 3.9 – Створення політики

Створимо актуальну криптографічну карту (лістинг 3.6).

Лістинг 3.6 – Створення криптографічної карти

```
crypto map mymap 10 ipsec-isakmp
 set peer 10.0.0.254
 set transform-set myset
 match address 100
```

Результат виконання команди наведено на рис. 3.10

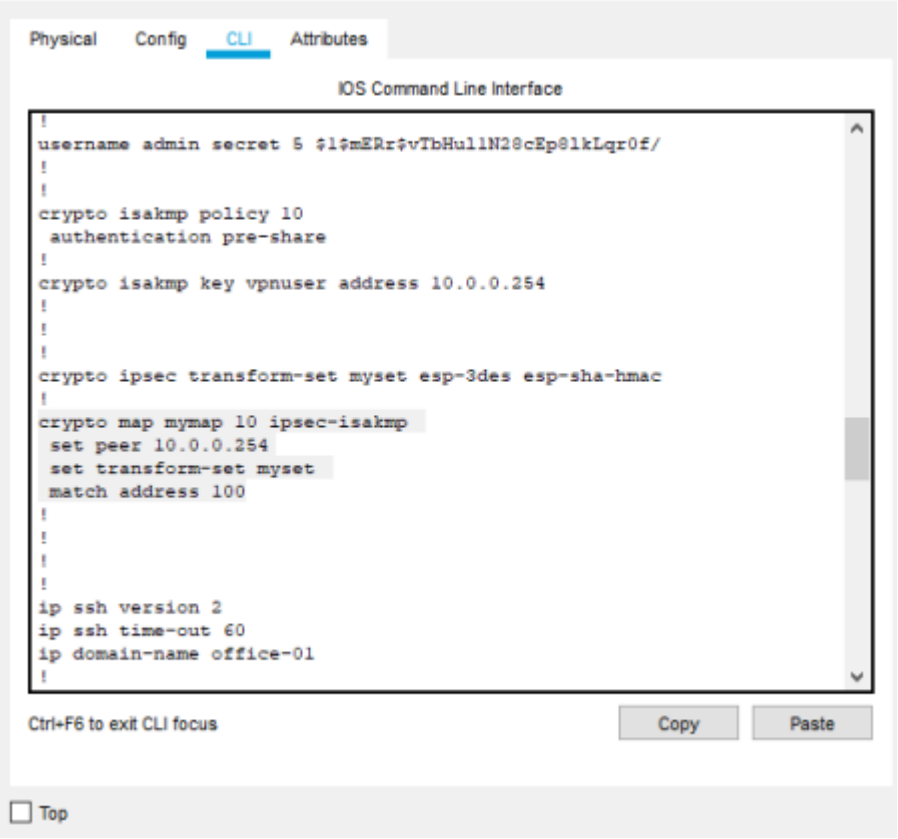

Рис. 3.10 – Створення криптографічної карти

Застосуємо криптографічну карту на зовнішній інтерфейс (лістинг 3.7).

Лістинг 3.7 – Застосування криптографічної карти на зовнішній інтерфейс

```
interface fastethernet0/0
 ip address 10.0.0.2 255.255.255.0
 crypto map mymap
```

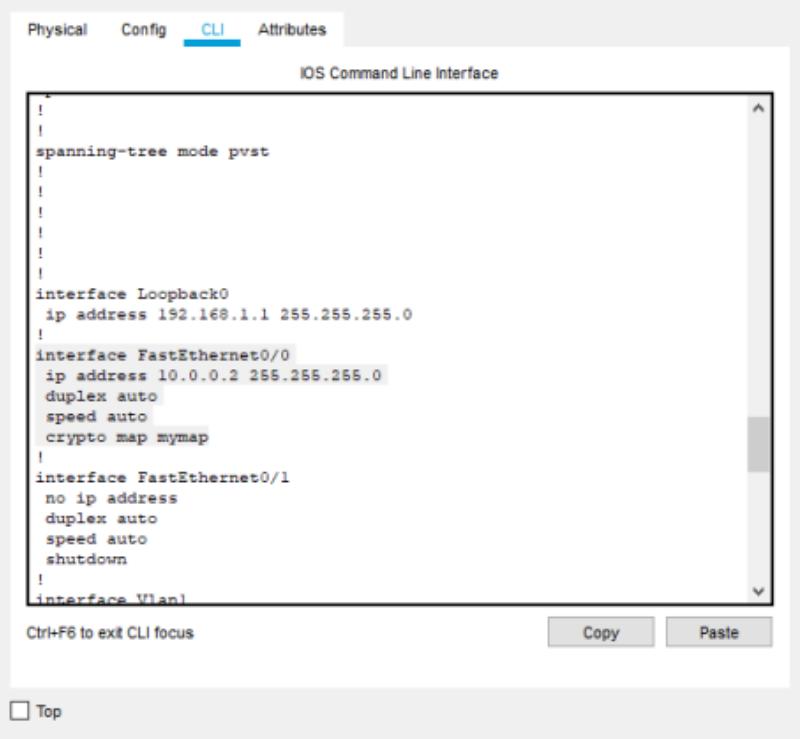

Рис. 3.11 – Застосування криптографічної карти на зовнішній інтерфейс

Створимо ACL (Access Control List) для зашифрованого трафіку (рис. 3.12).

Лістинг 3.8 – Створення ACL (Access Control List) для зашифрованого трафіку

```
    access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.254.0
0.0.0.255
    line con 0
    line aux 0
    line vty 0 4
```

Трафік з 192.168.1.0 до 192.168.254.0 зашифровано. Трафік, який не відповідає списку доступу, незашифрований для Інтернету.

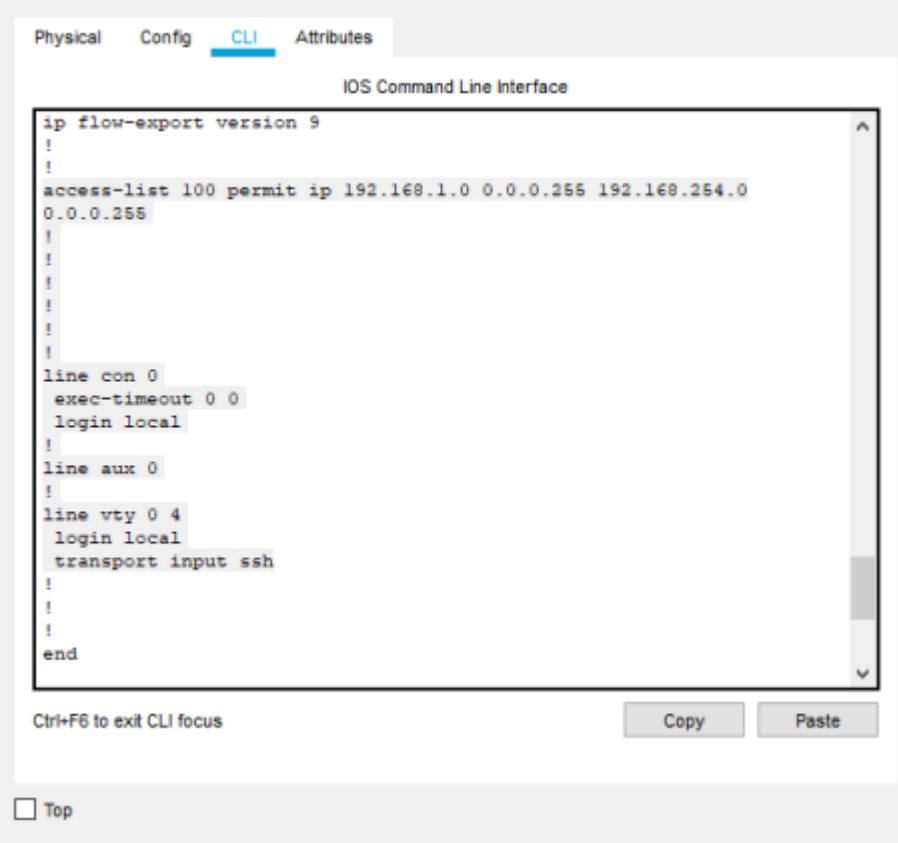

Рис. 3.12 – Створення ACL для зашифрованого трафіку

Висновки до розділу 3

В ході виконання дипломної роботи проаналізовано захищеність інформаційної системи підприємства ТОВ «КЕРНЕЛ» та зроблено висновок, що вона потребує захищеності, що підтверджує актуальність теми дипломної роботи.

При створенні технології забезпечення захищеного функціонування інформаційної системи підприємства було здійснено основні налаштування пристроїв забезпечення безпеки Cisco ASA, а саме налаштування інтерфейсів, параметрів шифрування, списків контролю доступу та криптосхем. Для забезпечення шифрування даних, які передаються по міжмережевому протоколу IP, налаштовано засіб IPsec.

Розроблено варіант технології забезпечення захищеного функціонування інформаційної системи підприємства.

ВИСНОВКИ

Проаналізовано та зроблено оцінку потенційних втрат та наслідків визначила, що інформаційна безпека підприємства безпосередньо пов'язана з його фінансовим станом, репутацією та законодавчими аспектами. Передбачення та мінімізація цих втрат вимагає комплексного підходу та управління ризиками на всіх рівнях.

Зроблено висновок, що дослідження технологій захисту інформаційних систем важливе для розуміння сучасних методів інформаційної безпеки. Виокремлено ключові аспекти, які допомагають у створенні комплексної системи захисту.

Зазначено, що використання технічних засобів, таких як антивірусне програмне забезпечення, брандмауери та системи IDS/IPS, має вирішальне значення для ефективного захисту інформаційної інфраструктури. Проаналізовано їхню взаємодію та роль у забезпеченні безпеки.

В ході виконання дипломної роботи проаналізовано захищеність інформаційної системи підприємства ТОВ «КЕРНЕЛ» та зроблено висновок, що вона потребує захищеності, що підтверджує актуальність теми дипломної роботи.

При створенні технології забезпечення захищеного функціонування інформаційної системи підприємства було здійснено основні налаштування пристроїв забезпечення безпеки Cisco ASA, а саме налаштування інтерфейсів, параметрів шифрування, списків контролю доступу та криптосхем. Для забезпечення шифрування даних, які передаються по міжмережевому протоколу IP, налаштовано засіб IPsec.

Розроблено варіант технології забезпечення захищеного функціонування інформаційної системи підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Center for Internet Security – Cybersecurity Threats [Електронний ресурс] / Center for Internet Security – Режим доступу: https://www.cisecurity.org/cybersecuritythreats/

2. Аксьончиков С.О., Ємельянова І.В., Маркова К.Д., Сватовський І.І. Регресійний аналіз тенденцій розвитку кібератак. Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління». 2017. Випуск 36. С. 5-13. URL: http://nbuv.gov.ua/j-pdf/VKhIMAM_2017_36_3.pdf.

3. Корпань Я.В. Класифікація загроз інформаційній безпеці в комп'ютерних системах при віддаленій обробці даних. Реєстрація, зберігання і обробка даних. 2015. Т.17. №2. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/131565/04-Korpan.pdf?sequence=1

4. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 19.04.2014 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 06.11.2023 р.).

5. Глоба Л.С. Розробка інформаційних ресурсів та систем: підручник. Київ: Політехніка, 2013. 380 с.

6. Романюк Б.В., Гавловський В.Д., Гуцалюк М.В., Бутузов В.М. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: наук.-практ. посіб. / за заг ред. проф. Я. Ю. Кондратьева. Київ, 2004. 144 с

7. Технології захисту інформації. Лекція 4. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186.

8. Бакін Д.С. Проблеми захисту інформації в комп'ютерних мережах: матеріали всеукр. наук.-практ. конф., м. Кропивницький, 23-25 листопада 2016 р.

Кропивницький, 2016. С. 79-80. URL: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/5101/1/AUConferenceCyberSecurity_November2016_p79.pdf

9. Jozef Janitor, Karol Kniewald. Visual Learning Tools for Teaching / Learning Computer Networks: Sixth International Conference on Networking and Services, 2010. P. 351-355.

10. Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network. URL: http://index-of.es/EBooks/German/Hacking/maximum_security.pdf.

11. Болехівський Н. Полотай О. Класифікація мережевих атак та методи протидії і ззахисту. URL: https://sci.ldubgd.edu.ua/bitstream/handle/123456789/6737/1.pdf?sequence=1&isAllowed=y (дата звернення: 16.08.2023 р.).

12. Cisco. URL: https://www.cisco.com/c/en/us/index.html (дата звернення: 22.08.2020 р.).

13. Beaver, K. Firewall Best Practices. [Електронний ресурс] - Режим доступу: http://www.principlelogic.com/docs/Firewall_Best_Practices.pdf

14. Cisco Systems, Inc. The Zone-Based Policy Firewall Design [Електронний ресурс] Режим доступу: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a0 0808bc994.shtml

15. Телекомунікаційні та інформаційні мережі.: Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.

16. Cisco Systems, Inc. Cisco Secure Access Control Server for Windows: ReleaseNotes. [Електронний ресурс] - Режим доступу: http://www.cisco.com/en/US/produ cts/sw/secursw/ps2086/prod_release_notes_list.html

17. Campus LAN and Vireless LAN Solution Design Design Good [Електронний ресурс], Режим доступу: URL: – https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan- design-guide.html

18. Cisco Systems, Inc. Cisco Router and Security Device Manager 2.4 User's Guide. [Електронний ресурс] – Режим доступу: http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_user_guide_list.html

19. Cisco Systems, Nz. The Zone-Based Shelves Firewall Design Signe Gude. [Електронний ресурс] – Режим доступу: http://vvv.cisco.chom/en/US/produtsss/sv/setsursv/ps1018/produtsss_tech_note09186a00808b994.shtml

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)