Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*
(повна назва)
Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

Планування інженерно-технічного захисту мережі офісу

(тема)

Виконав:
здобувач *4* року навчання,
групи *ТРІМІ-21-1*
Світлана КОЗАК
(власне ім'я, прізвище)

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)
Тип програми *освітньо-професійна*
(освітньо-професійна або освітньо-наукова)
Освітня програма
Інформаційно-мережна інженерія
(повна назва освітньої програми)
Керівник *доц. Наталія ХАРЧЕНКО*
(посада, власне ім'я, прізвище)

Допускається до захисту
Завідувач кафедри _____ *Валерій БЕЗРУК*
(підпис) (власне ім'я, прізвище)

2025 р.

Не містить відомостей заборонених до відкритого публікування.

Студент / Світлана Козак /

Керівник / Наталія Харченко /

Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*
Кафедра *Інформаційно-мережної інженерії*
Рівень вищої освіти *перший (бакалаврський)*
Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва)
Тип програми *освітньо-професійна*
Освітня програма *«Інформаційно-мережна інженерія»*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«____»_____ 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві *Козак Світлані Олексіївні*
(прізвище, ім'я, по батькові)

1. Тема роботи *Планування інженерно-технічного захисту мережі офісу*

затверджена наказом університету від 23 травня 2025 р. № 410 Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії 17 червня 2025 р.

3. Вихідні дані до роботи *Провести аналіз методів та засобів захисту інформації в офісних приміщеннях, особливу увагу приділити захисту інженерно-технічним питанням. Розробити систему управління об'єктом захисту, визначити критичні місця витоку інформації (акустичної, візуальної, електронної) та розробити комплекс мір для забезпечення інженерно-технічного захисту об'єкта. Провести модернізацію системи передачі даних за допомогою встановлення та настроювання мережного обладнання. Обрати необхідне ПЗ для інтеграції у систему захисту інформації.*

4. Перелік питань, що потрібно опрацювати в роботі
Вступ
1. Огляд методів та засобів захисту інформації
2. Розробка системи управління об'єктом захисту та безпеки
3. Реалізація моделі мережі засобами програми Packet Tracer
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) *назва, мета і актуальність кваліфікаційної роботи; класифікація інформації, що підлягає захисту; класифікація загроз інформаційній безпеці; рекомендований порядок визначення вимог до захисту інформації в системі; інженерно-технічні заходи захисту інформації; модель побудови системи інформаційної безпеки; критерії, яким має відповідати система захисту інформації; структурна схема системи безпеки; система передачі комп'ютерних даних; заходи для підвищення рівня інформаційної безпеки системи передачі; модернізована структура мережі передачі даних; налаштування спеціального програмного забезпечення захисту даних; висновки*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*23.05.25*	*виконано*
2	*Підбір літератури за темою роботи.*	*24.05-05.06.25*	*виконано*
3	*Огляд методів та засобів захисту інформації*	*06.06-07.06.25*	*виконано*
4	*Розробка системи управління об'єктом захисту та безпеки*	*08.06-10.06.25*	*виконано*
5	*Реалізація моделі мережі засобами програми Packet Tracer*	*11.06-15.06.25*	*виконано*
8	*Оформлення презентаційного матеріалу, підготовка до захисту в ЕК*	*16.06.25*	*виконано*

Дата видачі завдання 23 травня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ доц. Наталія ХАРЧЕНКО
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка 99 с., 29 рис., 3 табл., 11 джерел, 1 додаток.

Об'єкт дослідження – локальна мережа офісу.

Мета роботи – планування інженерно-технічного захисту локальної мережі.

Захист інформації можливий за допомогою різноманітних методів і засобів, як організаційних, так і технічних. Сукупність організаційних заходів, програмного забезпечення, технічних рішень та інших інструментів створює систему захисту інформації. Виклик, з яким стикається сучасний бізнес, полягає у виборі оптимального набору рішень з широкого спектру доступних технологій та засобів захисту. Головна складність захисту мережі не в недостатності технологій, а у виборі серед множини пропозицій такого рішення, яке ідеально підходить для специфіки конкретної мережі.

У роботі проведено аналіз методів та засобів захисту інформації, на основі якої проведено розробку системи управління об’єктом захисту з точки зору інженерно-технологічних засобів.

ЛОКАЛЬНА МЕРЕЖА, ЗАХИСТ ІНФОРМАЦІЇ, ІНЖЕНЕРНО-ТЕХНІЧНІ ЗАХОДИ ЗАХИСТУ, СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, OUTPOST FIREWALL PRO.

THE ABSTRACT

Explanatory slip 99 p., 29 fig., 3 tab., 11 sources, 1 attach.

Object of research - local office network.

The purpose of the work - planning of engineering and technical protection of the local network.

Information protection is possible using a variety of methods and tools, both organisational and technical. A combination of organisational measures, software, technical solutions and other tools creates an information security system. The challenge faced by modern businesses is to choose the optimal set of solutions from a wide range of available technologies and security tools. The main difficulty in protecting a network is not the lack of technology, but the choice of a solution that is ideally suited to the specifics of a particular network among a variety of offers.

This paper analyses the methods and means of information protection, on the basis of which the author develops a system for managing the object of protection in terms of engineering and technological means.

LOCAL NETWORK, INFORMATION PROTECTION, ENGINEERING AND TECHNICAL PROTECTION MEASURES, INFORMATION SECURITY SYSTEM, UNAUTHORISED ACCESS, OUTPOST FIREWALL PRO.

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

ASA – Adaptive Security Algorithm – алгоритм адаптивної безпеки;

NAT – Network Address Translation – протокол трансляції IP-адрес;

PIX – Private Internet Exchange – міжмережевий брандмауер Cisco;

SSH – Secure Shell Protocol – протокол безпеки на транспортному рівні;

ВТСС – високочастотний канал витоку в побутовій техніці;

ЕОМ – електронна обчислювальна машина;

НСД – несанкціонований доступ;

ОТСС – витік через непряме випромінювання терміналу;

ТЗПІ – технічні засоби передачі інформації.

ВСТУП

На сучасному етапі розвитку суспільства ми спостерігаємо збільшення значення інформаційного простору, який охоплює всю інформацію, інфраструктуру для її обробки, суб'єкти, що займаються збором, створенням, розповсюдженням та використанням інформації, а також системи, що регулюють соціальні відносини, які виникають у цьому процесі. Інформаційний простір, будучи ключовим елементом життєдіяльності суспільства, суттєво впливає на стан політичної, економічної, оборонної та інших аспектів безпеки. Національна безпека тісно пов'язана з інформаційною безпекою, і ця залежність буде лише зростати з розвитком технологій. Тому забезпечення інформаційної безпеки є важливим завданням.

Інформаційна безпека (або безпека даних) визначається як захищеність самої інформації та її носіїв (людей, організацій, систем і засобів, що дозволяють отримувати, обробляти, зберігати, передавати та використовувати інформацію) від різних загроз. Ці загрози можуть бути як умисними (з метою нелегального доступу до інформації), так і неумисними (без наміру завдати шкоди). Захист інформації можливий за допомогою різноманітних методів і засобів, як організаційних, так і технічних. Сукупність організаційних заходів, програмного забезпечення, технічних рішень та інших інструментів створює систему захисту інформації. Виклик, з яким стикається сучасний бізнес, полягає у виборі оптимального набору рішень з широкого спектру доступних технологій та засобів захисту. Головна складність захисту мережі не в недостатності технологій, а у виборі серед множини пропозицій такого рішення, яке ідеально підходить для специфіки вашої мережі та бізнес-вимог, при цьому витрати на підтримку та обслуговування обраного засобу захисту, запропонованого постачальником, будуть мінімальними.

1 ОГЛЯД МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Інформація як об'єкт захисту

Інформація - позначає дані про людей, об'єкти, події, феномени та процеси, незалежно від способу їх представлення.

Інформація стає доступною для людини, коли вона зберігається на фізичному носії. Є такі види носіїв інформації:

- джерело інформації;
- одержувач інформації.

Види інформації, що захищається, наведено на рис. 1.1.

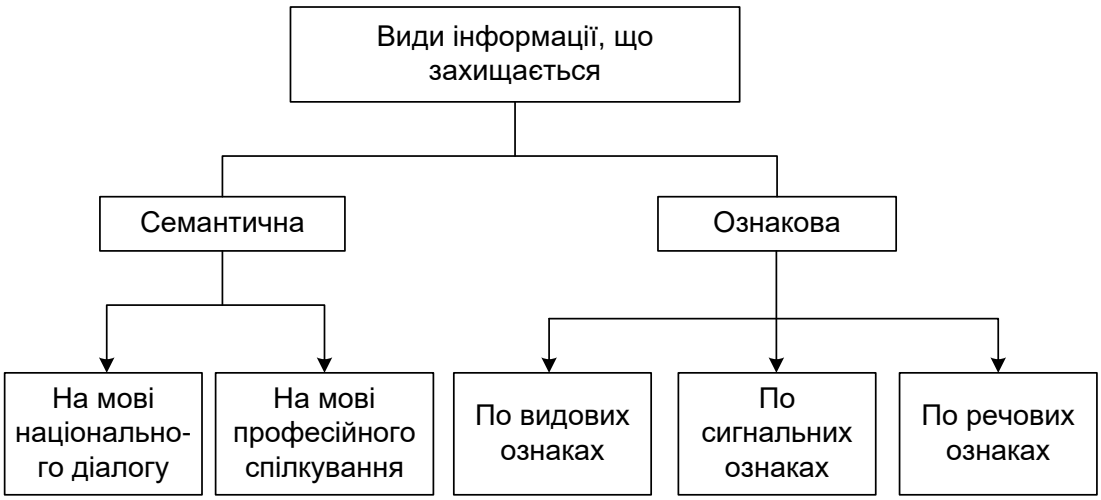

Рисунок 1.1 - Види інформації, що захищається

Семантична інформація у мові національного діалогу являє собою організовану низку символів, символів. Семантична інформація в мові фахівця відображає мови різноманітних наук, незрозумілих для тих, хто не має відповідної освіти. Характеристики інформації визначають певний матеріальний об'єкт за допомогою мови характеристик. Елемент інформації представляє собою інформаційний носій з чітко визначеними межами.

Захисту підлягає внутрішня, конфіденційна та секретна інформація.

Внутрішня інформація - це дані про компанію, які ще не були оприлюднені (використання такої інформації для біржових операцій вважається нелегальним) [1].

Конфіденційна інформація - це службова, професійна, промислова, комерційна або інша інформація, правовий статус якої визначається її власником на підставі законодавства про комерційну, професійну таємницю, державну службу тощо [1].

Під комерційною таємницею підприємства розуміють інформацію, яка не є державним секретом, але стосується виробництва, технологій, управління, фінансів та іншої діяльності підприємства, розкриття (передача, витік інформації) якої може нашкодити його інтересам [1].

До секретної інформації відноситься інформація, що містить державну таємницю. Державна таємниця - це інформація, несанкціоноване розповсюдження якої може завдати шкоди інтересам державних установ, організацій, суб'єктів господарювання та країни в цілому [1].

Під загрозами інформації, класифікацію яких представлено на рис. 1.2, розуміють потенційні або фактично можливі дії щодо інформаційних ресурсів, які призводять до незаконного отримання захищених даних. До таких дій належать:

- доступ до конфіденційної інформації різними методами та засобами, без порушення її цілісності;

- зміна інформації з кримінальними намірами як часткове або суттєве переформатування даних та їх змісту;

- знищення (ліквідація) інформації з метою завдання прямих матеріальних збитків.

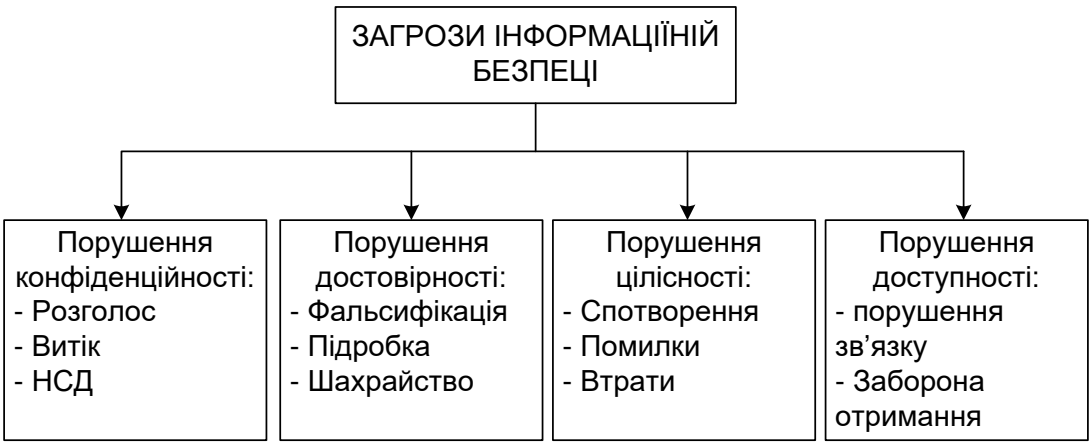

Рисунок 1.2 - Класифікація погроз інформації

1.2 Вимоги до захищеності інформації

Традиційно розроблена система класифікації державної інформації (даних) за ступенями необхідності її захисту зосереджена на врахуванні та забезпеченні виключно одного аспекту інформації - її таємності. Запити на забезпечення недоторканності та доступності інформації зазвичай включаються лише як непрямі вимоги до систем оброблення цих даних. Припускається, що обмежений доступ до інформації забезпечує мінімальний ризик її спотворення (несанкціонованого видалення). Обмежена довіра до інформаційних систем та перевага паперових носіїв інформації лише підсилюють обмеженість цього підходу [2].

Хоча така стратегія може бути частково виправдана через існуючу важливість безпекових атрибутів критичної державної інформації, це не означає, що її беззастережне застосування в інших сферах (з різними учасниками та їхніми інтересами) буде ефективним.

У багатьох областях діяльності частка таємної інформації є відносно невеликою. Для комерційної та особистої інформації, а також для державної інформації, яка не є конфіденційною, пріоритети безпекових характеристик можуть бути іншими. Для відкритої інформації, збитки від якої не є значними, ключовими можуть бути такі властивості, як доступність, недоторканність або захист від несанкціонованого розповсюдження. Наприклад, для фінансових документів найважливішою є гарантія їх недоторканності. Після цього, за ступенем значущості, йде доступність (втрата фінансового документа або затримка в платежах може бути дуже вартісною). Вимоги до забезпечення таємності окремих фінансових документів можуть і не ставитися взагалі [2].

Спроби вирішити проблеми захисту такої інформації, виходячи з традиційного зосередження лише на таємності, зазвичай зазнають невдачі. Головними причинами цього є обмеженість існуючої моделі захисту інформації, відсутність досвіду та спеціалізованих розробок у сфері забезпечення недоторканності та доступності не конфіденційної інформації. Удосконалення системи класифікації інформації за рівнями вимог до її захисту передбачає введення різноманітних ступенів (рівнів) вимог до забезпечення кожної з характеристик безпеки інформації: доступності, недоторканності,

таємності та захисту від копіювання. Приклад градацій вимог щодо захищеності:

- немає вимог;
- низькі;
- середні;
- високі;
- дуже високі.

Кількість дискретних градацій і вкладений у них сенс можуть різнитися.

В майбутньому будемо називати будь-який документ, який є функціонально повним і містить певну інформацію у формі знаків, незалежно від його фізичного носія, інформаційним пакетом.

Інформаційні пакети, що мають спільні характеристики, такі як структура, метод обробки або тип інформації, будемо класифікувати як належні до одного типу.

Метою є встановлення реального інтересу (високий, середній, низький або відсутній) сторін до дотримання вимог захисту для кожної характеристики різних типів інформаційних пакетів, які обігають у системі передачі даних.

Загальні вимоги до системи захисту (методи та засоби захисту) мають бути визначені на основі вимог до захисту різних типів інформаційних пакетів, що обробляються та зберігаються в системі, з урахуванням специфіки технологій їх обробки та передачі.

Типи інформаційних пакетів з однаковими пріоритетами та рівнями вимог до захисту (важливістю забезпечення їх безпеки: доступності, цілісності, конфіденційності) групуються в одну категорію.

Рекомендований порядок визначення вимог до захисту інформації в системі викладено нижче:

- спочатку формується перелік типів інформаційних пакетів, які циркулюють у системі (документи, таблиці), з урахуванням специфіки предметної області системи, класифікуючи інформаційні пакети за тематикою, функціональним призначенням, схожістю в технології обробки тощо. Це розбиття може бути уточнено на наступних етапах з урахуванням вимог до їх захисту;

- далі для кожного визначеного типу пакетів та кожної критичної властивості інформації (доступності, цілісності, конфіденційності) встановлюються:

а) перелік та значимість (за спеціальною шкалою) суб'єктів, чиї інтереси зачіпаються при порушенні цієї властивості;

б) рівень завданої шкоди (незначний, малий, середній, великий, дуже великий тощо) та рівень вимог до захисту.

- при оцінці завданих збитків враховуються:

а) потенційні втрати від отримання інформації конкурентом;

б) витрати на відновлення інформації у разі її втрати;

в) витрати на відновлення нормального функціонування системи передачі даних.

- якщо виникають складнощі через різницю оцінок для різних частин інформації одного типу, необхідно переглянути класифікацію на типи, повернувшись до попереднього етапу. Для кожного типу інформаційних пакетів, з урахуванням значущості суб'єктів і рівня збитків, встановлюється необхідний рівень захисту для кожної властивості інформації (при однаковій значущості суб'єктів вибирається найвищий рівень).

1.3 Організаційні заходи захисту інформації

Організаційний захист полягає у. встановленні правил для виробничої діяльності та відносин між учасниками на основі законодавства, що перешкоджає або значно ускладнює несанкціоноване доступ до інформації та виникнення внутрішніх чи зовнішніх загроз.

Організаційний захист повинен забезпечити:

- захист, встановлення режиму, роботу з персоналом, документацією;

- застосування технічних засобів безпеки та проведення інформаційно-аналітичної роботи для ідентифікації внутрішніх та зовнішніх загроз діяльності.

Організаційні заходи відіграють ключову роль у створенні ефективної системи захисту, оскільки ризики неавторизованого доступу до конфіденційної інформації часто залежать не від технічних засобів, а від неправомірних дій, недбалості співробітників або персоналу безпеки. Мінімізувати ці ризики технічними способами практично неможливо, тому потрібен комплекс

організаційно-правових та організаційно-технічних заходів, які б запобігали неавторизованому доступу до конфіденційної інформації.

Серед основних організаційних заходів виділяють:

- встановлення режиму та охорони. Їх завдання – запобігання несанкціонованому входу (як таємному, так і відкритому) на територію та до приміщень сторонніми особами; забезпечення контролю за переміщенням співробітників та гостей; створення спеціалізованих виробничих зон, наприклад, для роботи з конфіденційною інформацією, з окремими системами доступу; контроль за дотриманням часового режиму та перебуванням на території персоналу компанії; організація та підтримка ефективного пропускного режиму та контролю за співробітниками та відвідувачами;

- організацію роботи з співробітниками, що включає відбір та розміщення персоналу, ознайомлення з правилами роботи з конфіденційною інформацією, навчання та інформування про відповідальність за порушення правил захисту інформації;

- організацію роботи з документами, що охоплює створення, використання, облік, виконання, повернення, зберігання та знищення документів та носіїв інформації;

- використання технічних засобів для збору, обробки, накопичення та зберігання інформації;

- організацію аналізу внутрішніх та зовнішніх загроз конфіденційній інформації та розробку заходів для її захисту;

- організацію систематичного контролю за діяльністю персоналу, що працює з конфіденційною інформацією, порядком обліку, зберігання та знищення документів та технічних носіїв.

У кожному конкретному випадку організаційні заходи мають унікальну форму та зміст, адаптовані для забезпечення безпеки інформації в певних умовах.

Безсумнівно, для досягнення організаційних цілей необхідно забезпечити детальне планування, керування та виконання заходів за допомогою спеціально створеного структурного підрозділу, оснащеного кваліфікованими фахівцями у сферах безпеки, виробництва та інформаційного захисту. Зазвичай, цю роль виконує служба безпеки підприємства, до основних завдань якої відносяться:

- організація та забезпечення захисту. персоналу, матеріальних та фінансових активів, а також конфіденційної інформації;

- забезпечення контролю за дотриманням пропускного та внутрішнього режимів на території, у будівлях та приміщеннях, перевірка виконання встановлених правил співробітниками, партнерами та відвідувачами;

- управління процесами юридичного та організаційного регулювання у сфері захисту інформації;

- участь у створенні ключових документів для закріплення в них положень щодо забезпечення безпеки та захисту інформації, включаючи структуру підрозділів, трудові угоди, контракти, посадові інструкції та обов'язки керівництва та співробітників;

- розроблення та реалізація заходів з іншими відділами для забезпечення обігу документів, що містять конфіденційну інформацію;

- аналіз усіх аспектів виробничої, комерційної, фінансової діяльності для ідентифікації та протидії будь-яким спробам завдати шкоди, ведення обліку та аналізу порушень безпеки, збір та аналіз інформації про недоброзичливі дії конкурентів, діяльність підприємства та його клієнтів, партнерів, суміжників.

- організація та виконання службових розслідувань у випадках розголошення інформації, втрати документів, витоку конфіденційних даних та інших порушень безпеки підприємства;

- керування службами та підрозділами безпеки підпорядкованих структур з метою виконання умов захисту конфіденційної інформації, передбачених договорами;

- організація та систематичне проведення перевірок співробітників підприємства та служби безпеки з питань захисту інформації та забезпечення безпеки виробничих процесів;

- контроль та облік спеціально відведених приміщень для роботи з конфіденційною інформацією, технічних засобів, що використовуються в них, з метою запобігання витоку інформації та несанкціонованому доступу до захищених даних;

- здійснення заходів для запобігання будь-яким спробам завдати матеріальної чи моральної шкоди з боку внутрішніх та зовнішніх загроз.

Для забезпечення безпеки мовної інформації під час засідань рекомендується вжиття наступних організаційних заходів:

- перед засіданням важливо здійснити візуальний перевірку приміщення на предмет наявності прихованих пристроїв. Перевірка має бути систематичною та детальною, з особливою увагою до будь-яких, навіть незначних на перший погляд, деталей: присутності сторонніх об'єктів, побутових приладів чи елементів декору. По можливості, перевірку має проводити співробітник служби безпеки разом з особою, яка добре знає звичайний стан залу, наприклад, охоронцем;

- безпосередньо перед початком засідання охорона має перевірити приміщення, що межують з кімнатою для засідань на предмет видалення з них працівників або сторонніх осіб, які можуть здійснювати підслуховування через систему вентиляції або через стіну за допомогою спеціального обладнання; забезпечити закриття цих приміщень на час засідання та контролювати доступ до них;

- кількість учасників конфіденційних обговорень має бути зведена до мінімуму;

- доступ сторонніх осіб під час засідання має бути заборонений; також необхідно здійснювати спостереження за ситуацією на поверсі. з кімнати, оскільки в моменти, коли двері залишаються відчиненими, чіткість мовлення значно зростає. Більше того, виходячи або входячи, людина може залишити двері не повністю закритими, що також збільшить чіткість мовлення. слідкувати за тим, щоб сторонні не могли потрапити всередину;

- по можливості засідання слід переносити на час поза робочими годинами;

- будь-які роботи у кімнаті, що виконуються поза часом конфіденційних засідань, наприклад: прибирання, ремонт техніки, незначний косметичний ремонт, мають виконуватися за обов'язкової присутності співробітника служби безпеки. Це допоможе захистити приміщення від встановлення прослуховувальних пристроїв як співробітниками організації, так і сторонніми особами (електриками, робітниками, прибиральниками тощо);

- після засідання кімнату необхідно ретельно перевірити, закрити та опломбувати;

- між засіданнями кімната має залишатися закритою та опломбованою відповідальною особою.

- ключі до приміщення повинні бути вручені наступній зміні охорони з підтвердженням отримання та зберігатися у приміщенні для охорони, доступ до яких має контролюватися керівництвом [3].

Зазначені методи організаційного захисту в приміщенні для засідань визнані надзвичайно ефективними і не вимагають значних фінансових витрат чи викликають проблеми зі штатом, і можуть використовуватися як окремо, так і в комбінації, що істотно збільшить рівень захисту розглянутої інформації.

1.3.1 Оцінка ймовірного супротивника

Аналіз потенційного супротивника здійснюється перед початком пошукових заходів:

- у процесі визначення можливої моделі супротивника важливо враховувати його економічні та технічні ресурси, наявність кваліфікованих фахівців у команді;

- аналізуючи здатності потенційного ворога, потрібно формувати проміжні висновки, які допоможуть скласти первинне уявлення про супротивника;

- вивчення характеру дій дозволить зрозуміти його потенційні можливості;

- місцезнаходження та тип замаскованого пристрою, якщо вони були ідентифіковані до початку пошукових дій, допоможуть оцінити реальні здібності противника та виявити його зв'язки з співробітниками організації [3].

1.3.2 Оцінка умов розв'язання задачі захисту інформації

Для досягнення успіху у виконанні цілей здійснюється аналіз моделі поведінки та умов, в яких буде вирішено наступне завдання:

- дослідження території, де знаходиться об'єкт і положення інших об'єктів відносно нього;

- визначення контрольованої території та можливостей для збору інформації за її межами;

- інспектування захищеного об'єкта;

- під час перевірки об'єкта встановлюють взаємне розміщення контрольованих зон та прилеглих приміщень, режими доступу до них;

- фіксуються дані про час проведення ремонтних робіт, заміни меблів та елементів декору;

- створення планів приміщень з відображенням усіх комунікацій, що входять і проходять через них;

- аналіз конструктивних характеристик огороджувальних конструкцій, матеріалів і покриттів, з яких вони зроблені;

- у випадку щільної забудови особливу увагу звертають на прилеглі території, які можуть бути використані для паркування автомобілів з радіообладнанням, розгортання систем відеоспостереження або дистанційного аудіомоніторингу [3].

Після аналізу попередніх кроків визначаються типи та обсяги пошукових заходів, комплект вимірювальної апаратури та допоміжного устаткування. Потрібна кількість спеціалістів та робочих. Часовий проміжок для проведення операції. Розробляється сценарій проведення операції. Для керівника на першому етапі готується пакет документів з планом проведення пошукових дій.

1.4 Інженерно-технічні заходи захисту інформації

Інженерно-технічний захист визначається як комплекс спеціалізованих установ, технічних засобів та дій для їх застосування з метою охорони таємної інформації. Розподіл типів інженерно-технічного захисту інформації представлено нарис. 1.3

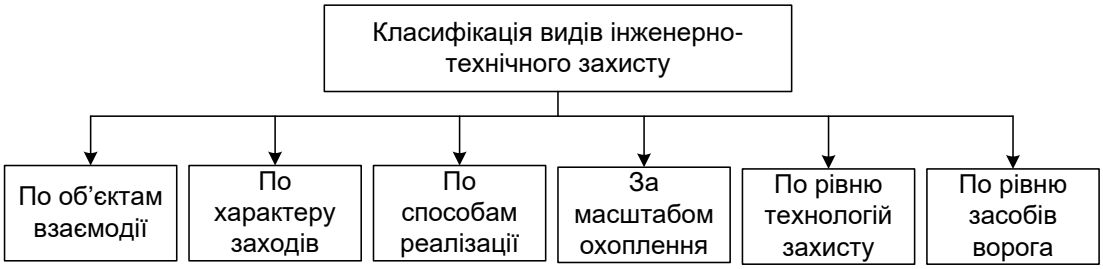

Рисунок 1.3 - Класифікація видів інженерно-технічної інформації

Розмаїття критеріїв класифікації дозволяє аналізувати інженерно-технічні засоби з погляду об'єктів впливу, типу дій, методів виконання, обсягу застосування, категорії засобів, проти яких ведеться боротьба з боку безпекових

служб. Залежно від функціонального призначення, засоби інженерно-технічного захисту поділяють на наступні групи:

- фізичні засоби – включають різноманітні пристрої та конструкції, які перепоною стоять на шляху фізичного проникнення зловмисників до захищених об'єктів або до носіїв конфіденційної інформації, а також забезпечують захист персоналу, матеріальних цінностей та фінансів від незаконних дій; до цієї категорії засобів захисту належать механічні, електромеханічні, електронні, електронно-оптичні, радіо- та радіотехнічні та інші пристрої, призначені для запобігання злочинним діям. Всі фізичні засоби захисту можна розділити на три основні категорії:

а) засоби попередження (системи охоронної сигналізації);

б) засоби виявлення (відеоспостереження, системи контролю доступу);

в) системи нейтралізації загроз (блокувальні пристрої).

- апаратні засоби – обладнання, пристрої та інші технічні рішення, що використовуються для захисту інформації. У діяльності компаній широко застосовуються різноманітні апарати, від телефонів до складних автоматизованих систем. Головна мета апаратних засобів – забезпечення надійного захисту інформації від витоку, розкриття та неавторизованого доступу через технічні пристрої, що використовуються у виробничому процесі;

- програмні засоби – спеціалізовані програми, програмні пакети та системи для захисту інформації у інформаційних системах різної спрямованості та обладнанні для обробки даних;

- криптографічні засоби – спеціальні математичні та програмні методи захисту інформації, яка передається через комунікаційні системи та мережі, зберігається та обробляється на електронно-обчислювальних машинах за допомогою різних методів шифрування [4].

1.5 Системи інформаційної безпеки

Основна ціль будь-якої системи захисту інформації полягає у забезпеченні безперебійної роботи об'єкта, уникненні загроз його безпеці, охороні законних інтересів Клієнта від незаконних втручань, запобіганні крадіжок фінансових активів, недопущенні витоку, втрати, спотворення чи знищення конфіденційної інформації, забезпеченні ефективної роботи усіх

відділів. Інша мета системи захисту інформації - підвищення рівня якості послуг та забезпечення гарантій безпеки майнових прав та інтересів клієнтів.

Реалізація поставлених завдань можлива через виконання наступних ключових задач:

- класифікація інформації як такої, що має обмежений доступ (конфіденційна інформація);

- прогнозування та оперативне виявлення загроз безпеці інформаційних активів, причин та умов, які сприяють збиткам фінансового, матеріального та морального характеру, порушенню їх нормальної роботи та розвитку;

- створення умов для роботи з мінімальною можливістю виникнення загроз безпеці інформаційних активів та нанесення різноманітних збитків;

- розробка механізму та створення умов для швидкого реагування на загрози інформаційної безпеки та прояви негативних тенденцій у роботі, ефективне припинення порушень за допомогою правових, організаційних та технічних заходів безпеки;

- забезпечення можливості для максимального відновлення та локалізації збитків, завданих незаконними діями фізичних та юридичних осіб, мінімізація негативного впливу порушень інформаційної безпеки на досягнення стратегічних цілей.

Модель створення системи захисту інформації.

У процесі виконання робіт може бути застосована наступна модель створення системи захисту інформації, представлена на рис. 1.4, яка базується на адаптації ОК (ISO 15408) та аналізі ризиків (ISO 17799).

Ця модель відповідає вимогам спеціальних регулятивних документів з питань забезпечення інформаційної безпеки, що були встановлені в міжнародному стандарті ISO/IEC 15408 «Інформаційні технології» - методики захисту - критерії для оцінювання інформаційної безпеки», а також стандарту ISO/IEC 17799 «Керування інформаційною безпекою», і враховує останні тенденції у розвитку національної нормативної безпеки [3].

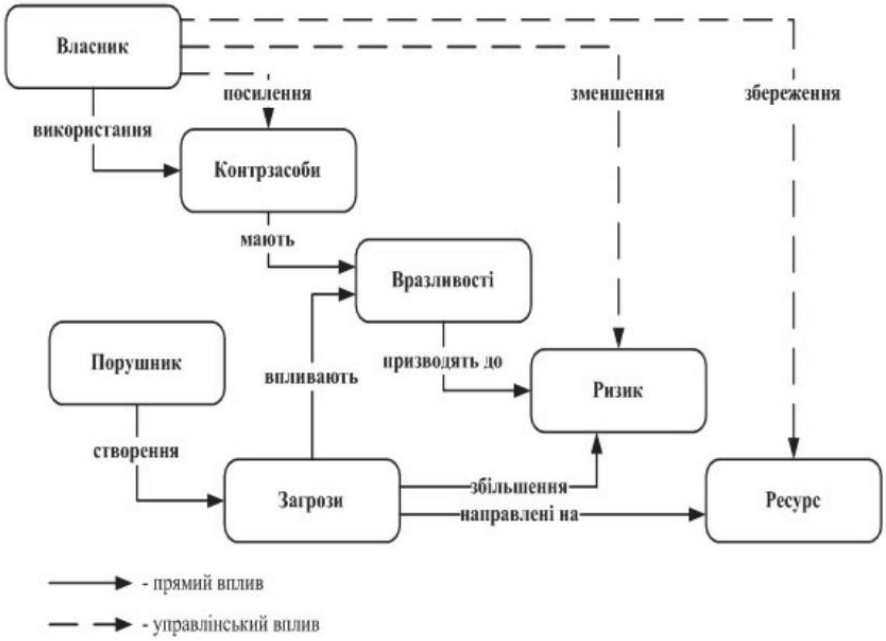

Рисунок 1.4 - Модель побудови системи інформаційної безпеки

Запропонована модель інформаційної безпеки представляє собою комплекс об'єктивних зовнішніх та внутрішніх чинників та їх вплив на рівень інформаційної безпеки об'єкта та на зберігання матеріальних або інформаційних активів.

Враховуються наступні об'єктивні чинники:

- загрози інформаційній безпеці, які оцінюються за ймовірністю їх виникнення та ймовірністю їх реалізації;

- вразливості інформаційної системи або системи заходів протидії (системи інформаційної безпеки), які впливають на ймовірність реалізації загрози;

- ризик - це чинник, що відображає потенційну шкоду для організації внаслідок реалізації загрози інформаційній безпеці: витоку інформації та її несанкціонованого використання (ризик у підсумку відображає потенційні фінансові збитки - безпосередні або опосередковані) [3].

1.6 Принципи побудови систем безпеки

Для створення ефективної системи інформаційної безпеки необхідно спершу здійснити аналіз потенційних ризиків у цій області. Наступним кроком є визначення прийнятного рівня ризику для організації, виходячи з обраних

критеріїв. Розроблена система інформаційної безпеки (заходи протидії) повинна бути націлена на досягнення цього рівня ризику.

Огляд ситуації в сфері захисту інформації свідчить про наявність вже сформованої концепції та структури захисту, яка базується на:

- розгалуженому наборі технічних засобів захисту інформації, що випускаються промисловим способом

- великій кількості організацій з необхідними ліцензіями, які займаються питаннями захисту інформації

- виразній системі поглядів на проблематику захисту інформації та наявності певного досвіду в цій галузі [3].

Проте, незважаючи на це, кількість зловмисних втручань в інформацію не зменшується, а навпаки, продовжує рости. Практика демонструє, що для протидії цій тенденції потрібна добре організована та цілеспрямована робота з захисту інформаційних ресурсів, до якої мають бути залучені професіонали, керівництво, співробітники та користувачі, що підкреслює важливість організаційного аспекту. Досвід різних установ та організацій показує, що:

- забезпечення безпеки інформації є не одноразовою дією, а постійним процесом, який включає обґрунтування та впровадження найефективніших методів, способів та підходів до вдосконалення системи захисту, її постійний моніторинг, виявлення слабких місць та незаконних дій;

- безпека інформації досягається лише за умови комплексного застосування усього спектру доступних засобів захисту на кожному етапі виробничого процесу та в усіх його структурних елементах. Максимальна ефективність виникає, коли всі використовувані засоби та методи інтегровані в єдину комплексну Систему Захисту Інформації (СЗІ), робота якої регулярно перевіряється, оновлюється та доповнюється відповідно до змін у зовнішніх та внутрішніх умовах;

- жодна система захисту не може забезпечити адекватний рівень інформаційної безпеки без належної підготовки користувачів та їх дотримання встановлених правил, спрямованих на її забезпечення [3].

Отже, систему захисту інформації можна охарактеризувати як добре організовану систему, що включає в себе спеціалізовані установи, інструменти, методики та заходи, спрямовані на забезпечення безпеки інформації перед внутрішніми та зовнішніми загрозами.

Розглядаючи зазначені вимоги, слід виокремити критерії, яким має відповідати система захисту інформації:

- охоплення всього інформаційного технологічного комплексу;

- різноманітність застосовуваних засобів, багаторівневість, з ієрархічним порядком доступу;

- можливість адаптації та доповнення заходів забезпечення безпеки інформації;

- унікальність, різноманітність. При виборі засобів захисту не можна покладатися на незнання зловмисників про можливості системи;

- простота у технічному обслуговуванні та зручність у використанні для користувачів;

- висока надійність;

- комплексність, цілісність, що передбачає неможливість вилучення будь-якої частини без шкоди для функціонування всієї системи [4].

Додатково, до системи захисту інформації висуваються такі вимоги:

- чітке визначення прав та обов'язків користувачів щодо доступу до певних видів інформації;

- надання користувачам лише мінімально необхідних прав для виконання покладених завдань;

- мінімізація кількості засобів захисту, спільних для декількох користувачів;

- реєстрація спроб та випадків несанкціонованого доступу до конфіденційної інформації;

- оцінка рівня конфіденційності інформації;

- контроль за цілісністю засобів захисту та оперативне реагування на їх несправності;

- система захисту інформації, як і будь-яка інша система, повинна мати власні засоби забезпечення, на які вона опиратиметься для досягнення своєї основної мети [4].

Враховуючи вищезазначені аспекти, система захисту інформації має включати:

- правове забезпечення, що охоплює законодавчі акти, правила, інструкції, методичні вказівки, дотримання яких є обов'язковим у межах їх застосування;

- організаційне забезпечення, яке передбачає реалізацію захисту інформації через певні структурні підрозділи, такі як служба захисту документації, служба контролю доступу та охорони, служба технічного захисту інформації, аналітична служба;

- технічне забезпечення, яке передбачає активне використання технічних засобів для захисту інформації та підтримки діяльності системи захисту;

- інформаційне забезпечення, що включає дані, інформацію, показники, параметри, необхідні для вирішення завдань системи;

- програмне забезпечення. Включає різноманітні програми для аналізу, обліку, статистики та розрахунків, які допомагають оцінити ризики витоку інформації та несанкціонованого доступу до конфіденційних даних;

- математичне забезпечення. Застосування математичних методик для аналізу ризиків, пов'язаних з технічними можливостями зловмисників, а також для визначення зон і стандартів необхідного захисту;

- лінгвістичне забезпечення, що включає правила та норми роботи органів і служб, забезпечуючих захист інформації, а також методики, які допомагають користувачам ефективно працювати в умовах високих вимог до безпеки інформації.

Отже, під СИСТЕМОЮ БЕЗПЕКИ визначають організований набір спеціалізованих установ, служб, засобів, методик та заходів, які гарантують охорону критично важливих інтересів індивіда, організації та країни проти внутрішніх і зовнішніх небезпек. Структурне представлення системи безпеки показано на рис. 1.5.

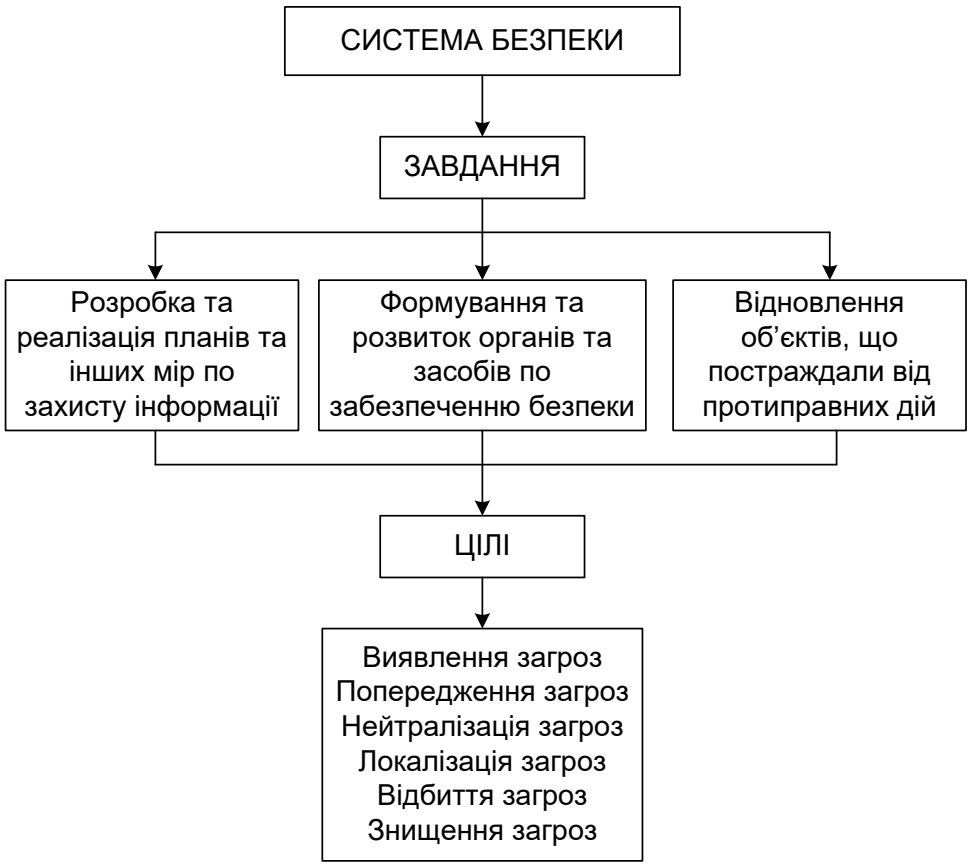

Рисунок 1.5 - Структурна схема системи безпеки

1.7 Захист комп'ютерної інформації

Основним захисним механізмом у сучасних системах обробки інформації є встановлення меж доступу для користувачів до ресурсів, що ґрунтується на розробці та впровадженні політики розподілу доступу та на наданні користувачам певних привілеїв (включаючи доступ до ресурсів, як-от використання взаємопосилань).

Для захисту інформації в комп'ютерних системах застосовуються комплексні підходи при створенні систем захисту інформації. Отже, можливо виокремити перелік програмних засобів та методик захисту інформації:

-програмні продукти для регулювання доступу до інформації;

-програми для ідентифікації та аутентифікації терміналів та користувачів за допомогою різноманітних критеріїв (паролі, спеціальні кодові слова, біометричні дані тощо), включаючи програми для підвищення надійності ідентифікації та аутентифікації;

- програми для перевірки роботи системи захисту інформації та моніторингу цілісності засобів захисту від несанкціонованого доступу;

- програми захисту з різними допоміжними функціями, зокрема антивірусні програми;

- програми для захисту операційних систем ПЕОМ (через модульну програмну інтерпретацію та інше);

- програми для контролю цілісності системного та прикладного програмного забезпечення;

- програми, що повідомляють про порушення використання ресурсів;

- програми для видалення залишкової інформації у запам'ятовувальних пристроях (оперативна пам'ять, відеопам'ять тощо) після її використання;

- програми для контролю та відновлення структури файлів даних;

- програми для імітації роботи системи або її блокування з метою виявлення несанкціонованого доступу;

- програми для виявлення несанкціонованого доступу та оповіщення (передачі повідомлень) про їх виявлення [4].

Засоби програмного захисту обробки інформації:

- пакети програмного забезпечення для автоматизованих робочих місць;

- бази даних в обчислювальних мережах;

- програмні засоби для автоматизованих систем керування;

- програмні засоби для ідентифікації виробника програмного (інформаційного) продукту, включно з засобами ідентифікації авторських прав.

1.8 Загрози несанкціонованого доступу до мережі

Під терміном загроза розуміємо можливість виникнення випадкових або умисних дій (або бездіяльності), які можуть призвести до порушення ключових характеристик інформації та систем її обробки: доступності, цілісності та конфіденційності. Володіння інформацією про різноманітні потенційні загрози захищеній інформації, здатність кваліфіковано та об'єктивно оцінювати ймовірність їх виникнення та рівень ризику кожної з них є ключовим елементом у складному процесі створення та підтримки захисту. Хоча визначити повний спектр загроз інформаційній безпеці (ІБ) є майже неможливим, детальне моделювання загроз може допомогти у досягненні повного опису їх щодо конкретного об'єкта [4].

Методи несанкціонованого доступу (НСД) до інформації в системах управління безпекою мережі, які знаходяться під захистом, включають:

- фізичний доступ. Це можливо через безпосередній або візуальний контакт з об'єктом захисту;

- логічний доступ. Він здійснюється шляхом подолання захисних систем за допомогою програмних засобів, що дозволяє логічно проникнути в структуру системи управління безпекою [5].

Шляхи реалізації несанкціонованого доступу до захищених даних системою управління безпекою мережі можуть включати:

- використання прямого стандартного шляху доступу. Це включає використання слабкостей в політиці безпеки та процесах адміністративного управління мережею, що може призвести до маскування під легітимного користувача;

- використання прихованого нестандартного шляху доступу. Тут використовуються недокументовані особливості (слабкості) системи захисту, такі як недоліки алгоритмів та компонентів системи захисту, помилки в реалізації проекту системи захисту [5].

Залежно від типу слабкостей системи управління інформаційною безпекою мережі, загрози несанкціонованого доступу до даних можуть проявлятися через такі недоліки, які зазвичай виникають на етапі проектування системи управління безпекою мережі:

- недоліки в політиці безпеки. Розроблена політика безпеки не відповідає критеріям безпеки, що використовуються для здійснення НСД;

- помилки в адміністративному управлінні. Недокументовані особливості системи безпеки, зокрема в програмному забезпеченні, – помилки, неоновлені операційні системи, вразливі служби, незахищені конфігурації за замовчуванням;

- недоліки в алгоритмах захисту. Алгоритми захисту, обрані розробником для створення системи захисту інформації, не враховують реальні аспекти обробки інформації та містять концептуальні помилки;

- помилки в реалізації проекту системи захисту. Втілення проекту системи захисту не відповідає принципам, закладеним розробниками системи [5].

Окрім цього, можемо визначити наступні принципи щодо потенційних методів та способів забезпечення неавторизованого доступу до мережі:

- аналізування мережевого трафіку, вивчення засобів захисту та їх вразливостей, а також аналіз алгоритмів роботи систем автоматизації. У системах із використанням окремого каналу зв'язку, повідомлення передаються безпосередньо від відправника до одержувача, оминаючи інші елементи системи. В такому випадку, без доступу до елементів передачі даних, неможливо здійснити аналіз мережевого трафіку;

- залучення до мережі неавторизованих пристроїв.

- перехоплення інформації, що передається з метою її крадіжки, зміни або перенаправлення;

- заміна довіреного елемента в системі автоматизації.

- втручання в мережу шляхом створення несанкціонованого маршруту (елемента) за допомогою нав'язування фальшивого маршруту для перенаправлення трафіку;

- створення в мережі помилкового маршруту (елемента) через використання слабкостей алгоритмів дистанційного пошуку;

- використання слабкостей системного та прикладного програмного забезпечення;

- криптоаналіз.

- використання недоліків у впровадженні криптографічних алгоритмів та програм.

- перехоплення, вгадування, заміна та прогнозування створених ключів та паролів;

- надання додаткових прав та зміна налаштувань системи захисту;

- використання програмних закладок;

- порушення функціонування системи інформаційної безпеки через перевантаження, знищення важливих даних, виконання помилкових операцій;

- доступ до комп'ютера в мережі, який отримує повідомлення або виконує функції маршрутизації [5].

Визначені та обґрунтовані класифікаційні характеристики описують як об'єкт захисту, так і комплекс загроз захищеним ресурсам. На їх основі можна розробити багато конфліктних ситуацій, які представляють завдання захисту інформації в системах управління мережевою безпекою.

1.8.1 Системи інформаційної безпеки мережі

Стратегії інформаційної безпеки в мережі націлені на охорону корпоративних процесів від загроз, що виникають через епідемії комп'ютерних вірусів та дії зловмисників, які можуть завдавати шкоди бізнес-операціям зовні та зсередини. Враховуючи темпи появи нових загроз, інформаційно-безпекові системи мережі розробляються з акцентом на проактивність, що дозволяє запобігати атакам замість боротьби з їхніми наслідками. Відмітною рисою такого підходу є вбудовування захисних механізмів безпосередньо в мережеву інфраструктуру, де кожен елемент, від персонального комп'ютера до мережевого устаткування, відіграє роль у забезпеченні безпеки та стабільності діяльності компанії [5].

Переваги систем інформаційної безпеки:

- платформа для інформаційної безпеки мережі. Забезпечує послідовний розвиток корпоративної мережі – згідно з планом оновлень, розробленим IT-відділом, та стратегічно – використовуючи існуючі ресурси для імплементації системи інформаційної безпеки в найбільш критичні моменти.

- моніторинг та захист від загроз. Дозволяє застосовувати передові технології в області інформаційної безпеки мережі, забезпечуючи своєчасний контроль та аналіз мережевого трафіку;

- захищений зв'язок. Надає можливість використовувати засоби передачі даних, голосу, відео та бездротового зв'язку в процесі ведення бізнесу, не хвилюючись про захист конфіденційності та цілісності важливих даних;

- ефективне керування та управління політиками безпеки: Дозволяє застосовувати комплекс інтегрованих та адаптованих інструментів для управління інформаційною безпекою, що сприяє розповсюдженню політик безпеки в складних та динамічних бізнес-умовах.

1.8.2 Принципи побудови систем безпеки мережі

Розробка системи безпеки зазвичай починається з створення концепції безпеки, яка включає узагальнення поглядів на безпеку об'єкта на різних стадіях та рівнях його діяльності, встановлення ключових засад системи, а також розробку стратегій та кроків для впровадження заходів безпеки.

Ключові засади створення систем безпеки включають:

- принцип законності, який передбачає суворе дотримання та застосування вимог чинного законодавства та нормативних актів при проектуванні та створенні систем безпеки;

- принцип своєчасності, що забезпечується шляхом впровадження профілактичних заходів для забезпечення безпеки;

- принцип поєднання комплексності, ефективності та економічної обґрунтованості, який реалізується через створення системи безпеки, що забезпечує надійний захист ресурсів підприємства від можливих загроз з мінімальними витратами, але не більше ніж 20% вартості захищених ресурсів;

- принцип модульності, який досягається за допомогою створення системи з урахуванням гнучких апаратних та програмних модулів, що дозволяє системі працювати в режимах чергування та налаштування, а також змінювати конфігурацію системи без заміни основного обладнання;

- принцип ієрархічності, який втілюється через створення багаторівневої структури, що включає обладнання центрального рівня, обладнання середньої ланки та об'єктове обладнання, дозволяючи розробляти системи безпеки для вищих організаційно-структурних рівнів;

- принцип переважно програмного налаштування, який реалізується через використання програмних модулів для перенастроювання обладнання;

- принцип сумісності технологічних, програмних, інформаційних, конструктивних, енергетичних та експлуатаційних елементів у використовуваних технічних засобах, що досягається через уніфікацію технологій виробництва компонентів системи та забезпечує технологічну єдність та взаємозамінність компонентів, а також оптимальну взаємодію підсистем безпеки при виконанні заданих функцій за допомогою стандартних засобів зв'язку з ЕОМ та строгої регламентації параметрів на всіх рівнях системи [5].

З огляду на невпинне зростання цін на програмне забезпечення для великих систем, яке значно перевищує витрати на апаратне забезпечення, стає критично важливим забезпечення програмної сумісності на різних рівнях та між рівнями обладнання.

Конструктивна сумісність гарантує єдність та взаємну відповідність геометричних розмірів, а також естетичних і ергономічних властивостей обладнання. Це досягається шляхом розробки єдиної конструктивної

платформи для функціонально схожих модулів на всіх рівнях, при цьому забезпечуючи відповідність конструкцій на нижчих рівнях до конструкцій на вищих рівнях.

Експлуатаційна сумісність забезпечує відповідність характеристик, які впливають на умови експлуатації обладнання, його тривалість служби, можливість ремонту, надійність та метрологічні властивості, а також дотримання вимог до електронно-вакуумної гігієни, умов технологічного мікроклімату та інше.

Енергетична сумісність гарантує відповідність типів використовуваних енергетичних ресурсів.

1.9 Апаратні засоби захисту даних, що передаються

Сучасні технології передачі інформації характеризуються складною структурою та архітектурними особливостями, що зумовлює необхідність впровадження ефективних заходів для захисту від несанкціонованого доступу до інформації, яка циркулює у мережах. Програмні засоби захисту інформації не завжди можуть гарантувати повну безпеку передачі даних, тому для забезпечення захисту мережевих структур активно використовуються різноманітні апаратні засоби контролю та захисту даних.

Для захисту даних, що передаються та отримуються в системах передачі інформації, як у внутрішніх, так і в загальнодоступних мережах, можна використовувати такі пристрої, як маршрутизатори.

Маршрутизатор - пристрій, що дозволяє з'єднувати мережі з різними архітектурами та протоколами. Він вибирає оптимальний маршрут для мережевого трафіку та здійснює фільтрацію широкомовних повідомлень для локальних мереж [6].

Маршрутизатор, в першу чергу, важливий для визначення маршруту даних, які надсилаються у великі та складні мережі. Користувач мережі відправляє дані та вказує адресу одержувача. Ці дані переміщуються через мережу до маршрутизаторів, розташованих у точках розгалуження маршрутів, які і визначають найкращий шлях. Вибір найкращого шляху базується на кількісних показниках, званих метриками. Оптимальний шлях – це той, що має

найменшу метрику, в якій можуть бути враховані різні фактори, такі як довжина шляху, час проходження, час існування пакету [6].

Маршрутизатори поділяються на пристрої:

- вищого класу;
- середнього класу;
- початкового класу.

Маршрутизатори вищого класу використовуються для інтеграції мереж великих підприємств. Вони підтримують широкий спектр протоколів та інтерфейсів, включаючи не лише стандартні, а й досить незвичайні. Такі пристрої можуть мати до 50 портів для підключення до локальних або глобальних мереж [6].

Маршрутизатори середнього класу використовуються для створення мережних об'єднань середнього розміру на рівні підприємства. Їх стандартна конфігурація включає два-три порти для локальних мереж та від чотирьох до восьми портів для глобальних мереж. Ці маршрутизатори підтримують найбільш розповсюджені протоколи маршрутизації та транспортні протоколи [6].

Маршрутизатори початкового класу призначені для локальних мереж відділів; вони з'єднують малі офіси з корпоративною мережею. Зазвичай мають один порт для локальної мережі (Ethernet або Token Ring) та два порти для глобальної мережі, призначені для повільних виділених ліній або комутованих з'єднань. Незважаючи на свої обмеження, такі маршрутизатори користуються попитом серед адміністраторів для розширення існуючих мережевих структур [6].

Наразі на ринку мережевих рішень існує велика кількість роутерів, що відрізняються за своїми можливостями. Однак, беззаперечним лідером у виробництві роутерів різноманітних типів та призначень виступає компанія Cisco.

Роутери з інтегрованими сервісами від Cisco забезпечують об'єднання передачі даних, голосу, відео та бездротового зв'язку в одному захищеному пристрої, забезпечуючи високу надійність та модульність, що дозволяє розширювати функціонал у відповідь на змінні потреби бізнесу [6].

Функціонал роутерів з інтегрованими сервісами Cisco включає:

- бездротові мережі. Забезпечують збільшення продуктивності та поліпшення співпраці завдяки доступу до мережі з будь-якого місця в офісі;

- голосовий зв'язок. Використовують передові засоби зв'язку, такі як управління дзвінками, голосова пошта, автоматичний секретар та конференц-зв'язок, що дозволяє оперативно відповідати на запити клієнтів та знижувати витрати на далекий зв'язок;

- відеозв'язок. Дозволяє використовувати більш ефективні системи контролю та забезпечення безпеки, а також надавати послуги передачі мультимедійних потоків на запит та в інтерактивному режимі;

- безпека. Допомагає знижувати бізнес-ризики, пов'язані з вірусами та іншими загрозами безпеки;

- віртуальні приватні мережі. Забезпечують безпечний доступ віддаленого персоналу та домашніх працівників до ресурсів компанії через захищене з'єднання;

- модульна архітектура. Дозволяє оновлювати мережеві інтерфейси для підтримки новітніх технологій завдяки широкому спектру доступних опцій для локальних та глобальних мереж. Роутери Cisco також пропонують різноманітні типи слотів для спрощення додавання з'єднань та сервісів у майбутньому, виходячи з концепції «інтеграція відповідно до зростаючих потреб»;

- гнучкість. Можливості підключення через DSL, кабельний модем, T1 або бездротовий 3G забезпечують широкий вибір варіантів для основних та резервних з'єднань [6].

У даній кваліфікаційній роботі для забезпечення мережевої безпеки в якості ключових елементів управління мережею будуть використовуватися роутери компанії Cisco, серій 2800 та 7200.

2 РОЗРОБКА СИСТЕМИ УПРАВЛІННЯ ОБ'ЄКТОМ ЗАХИСТУ ТА БЕЗПЕКИ

2.1 Постановка задачі проектування

Неперервний прогрес у сфері інфраструктури систем передачі даних сприяв створенню масштабних мережевих конструкцій, що вимагають особливого підходу до забезпечення безпеки. Важливим є впровадження комплексних заходів для захисту інформації в таких мережах.

Планування та реалізація систем управління безпекою мережі на етапі проектування будівлі та створення в ній системи передачі даних дозволяє ефективно захистити інформацію. На цьому етапі формується мережева архітектура об'єкта, проводиться аналіз потенційних загроз та розробляються заходи безпеки. Цей метод є витратним, але виправданим завдяки можливості уникнення багатьох вразливостей у системі безпеки мережі, які в подальшому складно усунути [7].

Оновлення та підсилення захисту інформації в існуючих системах управління безпекою мережі представляє собою складне завдання через можливі проблеми з плануванням мережі та інтеграцією або заміною ключових елементів системи [7].

У рамках кваліфікаційної роботи були визначені наступні цілі та завдання:

- виконати технічний огляд рівня захисту інформації в будівлі;
- ідентифікувати потенційні джерела витоку акустичної інформації;
- виявити потенційні джерела витоку візуальної інформації;
- аналізувати рівень захисту кабельної системи об'єкта;
- здійснити моніторинг мережі передачі даних об'єкта для виявлення потенційних вразливостей;
- розробити комплексний план посилення інженерно-технічного захисту об'єкта;
- провести модернізацію системи передачі даних за допомогою встановлення та налаштування мережевого обладнання від компанії Cisco;

- на основі аналізу доступних програмних рішень для захисту та зберігання інформації підібрати та інтегрувати в систему управління безпекою об'єкта відповідні програмні засоби.

Для розробки моделі мережі передачі даних та демонстрації процесу налаштування нових маршрутизаторів буде використано програму CiscoPacketTracer.

2.2 Аналіз об'єкта захисту

Об'єкт, що охороняється, представляє собою десятиповерхівку, розташовану на території, оточеній парканом. По обидва боки від неї розкинулися території інших компаній з прилеглими межами. На ділянці також облаштовано парковку для автомобілів.

Зона, де розміщено об'єкт захисту інформації, займає п'ятий поверх зазначеної споруди. До контрольованої зони відносяться наступні об'єкти та приміщення:

- кабінет проведення нарад;
- кабінет керівника;
- серверна;
- прилади та техніка, система обробки, зберігання та передачі даних.

Фізико-технічні характеристики приміщень мають такі властивості:

Стіни зовнішні:

- матеріал: залізобетонні;
- товщина (0,8 м);
- екранування та штукатурка: присутній;
- інші матеріали: з внутрішньої сторони стіни оздоблені під "Євростандарт".

Вікна:

- розмір отвору: ... 2,0 * 1,5 м;
- тип вікна: склопакет з подвійним потовщеним склом.

Двері:

- розмір отвору: 2,2*1,8м
- тип: одностулкові, залізні двері, механічний замок.

Система вентиляції:

- припливно-витяжна.

Система опалення:

- центральне водяне.

Система електроживлення (освітлення):

- мережа: 220 В/50 Гц;

- тип світильників: стельові галогенні світильники

Система заземлення: відсутня

Телефонні лінії:

- Тип ТА.

2.2.1 Контрольована зона

Контрольована зона означає ділянку в межах об'єкта, де доступ осіб строго регулюється і недопускається випадкове перебування без належного дозволу. Така зона може бути розширена понад межі охоронюваної території, забезпечуючи контроль за ділянками без охорони.

Згідно з нормами, об'єкти класифікують на універсальні, які поділяють на три категорії:

- об'єкти першої категорії потребують контрольовану зону в 50 метрів;

- для об'єктів другої категорії необхідно 30 метрів;

- об'єкти третьої категорії вимагають 15 метрів контрольованої зони.

Розглянутий об'єкт належить до другої категорії з контрольованою зоною в радіусі тридцяти метрів.

2.2.2 Можливі канали витоку інформації

Аналізуючи детальний план території, можемо зробити висновок, що особливо ризикованими для розміщення обладнання для перехоплення інформації за межами контрольованої зони виявляться:

- шляхи сполучення;

- місця для паркування;

- сусідні ділянки та адміністративні споруди, що на них розташовані.

Для ідентифікації найімовірніших місць несанкціонованого збору інформації та розміщення засобів розвідки в межах контрольованої зони, критично важливо аналізувати не лише локацію вивчаємої організації, а й

потенційні шляхи витоку конфіденційної інформації, що можуть виникнути через використання різноманітного обладнання.

Електромагнітні шляхи витоку інформації утворюються через непряме електромагнітне випромінювання:

- компоненти ОТСС (витік через непряме випромінювання терміналу, зчитування інформації з екрану та електромагнітного каналу), сигнал яких (струм, напруга, частота і фаза) зазнає змін аналогічно до інформаційного сигналу;

- ВЧ-генератори ОТСС та ВТСС (високочастотний канал витоку в побутовій техніці), який може несвідомо модулюватися електричним сигналом, що містить інформацію;

- НЧ-підсилювачі технічних засобів передачі інформації (ТЗПІ) через ненавмисне перетворення негативного зворотного зв'язку в неконтрольований позитивний, що може спричинити самозбудження та перехід підсилювача з режиму підсилення в режим генерації сигналів, модульованих інформаційним сигналом [7].

Канал витоку інформації через ланцюги живлення або передачі інформації виникає через наведення:

- електромагнітного випромінювання, що виникає під час передачі інформаційних сигналів компонентами ОТСС, а також через існування гальванічного зв'язку між з'єднувальними лініями ОТСС та іншими провідниками або лініями ВТСС (наведення на комунікаційні лінії та сторонні провідники);

- інформаційних сигналів у ланцюзі електроживлення (витік через мережу електроживлення) через магнітний зв'язок між вихідним трансформатором підсилювача та трансформатором системи електроживлення, а також через нерівномірне навантаження випрямляча, що веде до зміни споживаного струму відповідно до інформаційного сигналу;

- інформаційних сигналів у ланцюзі заземлення (витік через ланцюги заземлення) завдяки гальванічному зв'язку з землею різних провідників (включаючи нульовий провід мережі електроживлення, екрани) та металевих конструкцій, які виходять за межі контрольованої зони безпеки [7].

Велику увагу привертає можливість перехоплення даних під час їх передачі через комунікаційні канали, адже це відкриває шлях до

несанкціонованого доступу до передаваної інформації. Залежно від типу зв'язку, канали для перехоплення можуть бути класифіковані як електромагнітні, електричні та індукційні . Перший тип каналів виникає, коли сигнали комунікаційних систем перехоплюються за допомогою стандартного технічного обладнання, яке часто використовується для прослуховування телефонних дзвінків через різні радіоканали (мобільні, радіорелейні, супутникові). У другому випадку, для перехоплення даних, що передаються через кабельні лінії, використовуються телефонні пристрої з радіопередавачами. Індукційний канал базується на ефекті створення електромагнітного поля навколо кабелю під час передачі сигналів, які можна перехопити за допомогою спеціальних індукційних пристроїв. Цей метод відноситься до безконтактних способів отримання інформації і часто застосовується для перехоплення даних, що передаються по телефонних лініях [7].

Щодо каналів витоку акустичної інформації, у контрольованій зоні можна виділити наступні типи каналів:

- повітряні;
- вібраційні;
- електроакустичні;
- оптоелектронні;
- параметричні.

Проте найбільш розповсюдженим є повітряний канал для перехоплення даних, де застосовуються чутливі та спрямовані акустичні пристрої, такі як мікрофони, що підключені до диктофонів або спеціальних міні-передавачів. Акустична інформація, захоплена такими пристроями, може передаватися через радіоканали, мережу змінного струму, з'єднувальні лінії, проводи, труби тощо. Для прийому інформації зазвичай використовують спеціалізоване обладнання. Особливий інтерес представляють пристрої, які монтуються безпосередньо в корпус телефону або підключаються до телефонної лінії.

Вібраційний канал використовує як середовище поширення інформації конструктивні елементи будівель (стіни, стелі, підлоги тощо), а також трубопроводи водо- та теплопостачання, каналізацію. Для перехоплення акустичних сигналів зазвичай використовують контактні мікрофони з підсилювачем та радіо стетоскопи. У нашій контрольованій зоні не виключено

використання вібраційного каналу для збору інформації, проти чого будуть вжиті заходи для посилення ізоляції між стінами та стелями [7].

Електроакустичні канали створюються шляхом перетворення акустичних сигналів на електричні через «високочастотне нав'язування» або захоплення за допомогою ВТСС. Канал витоку, що виникає через неавторизоване підключення ВЧ-генератора до лінії, яка пов'язана з елементами ВТСС, дозволяє модулювати його інформаційним сигналом. У таких випадках для перехоплення розмов, що відбуваються у приміщенні, часто використовують телефон, який виходить за межі контрольованої зони. Також деякі ВТСС, як-от датчики системи протипожежної сигналізації, гучномовці та інші, можуть містити електроакустичні перетворювачі, що призводить до появи так званого мікрофонного ефекту [7].

Використовуючи лазерне випромінювання для освітлення вібруючих в акустичному полі відбивних поверхонь (таких як віконне скло, дзеркала, картини тощо), можливо створити оптоелектронний канал для витоку звукової інформації. Для перехоплення такої інформації використовуються локаційні системи, які зазвичай працюють у інфрачервоному діапазоні і відомі під назвою "лазерні мікрофони". Їх діяльність можлива на відстані до кількох сотень метрів [7].

Необхідно звернути увагу на канали витоку візуальної інформації, через які можна отримати зображення об'єктів або копії документів. Для цього застосовуються оптичні пристрої (біноклі, телескопи, монокуляри), відеокамери, прилади нічного бачення, тепловізори та інше. Для копіювання документів використовують електронні та спеціально закамуфльовані фотоапарати, а для дистанційного знімання візуальної інформації – відеопристрої-закладки.

Під час розробки системи безпеки для кваліфікаційної роботи особлива увага була приділена каналам витоку комп'ютерної інформації. Захист даних в комп'ютерних системах наразі є предметом інтересу лише вузького кола спеціалістів у нашій країні. Проблема захисту даних стала актуальною для державних, військових організацій та наукових кіл. Нині з'явилася значна кількість компаній і банків, чия робота неможлива без використання комп'ютерів. Як тільки керівництво цих організацій усвідомить це, вони одразу зіткнуться з необхідністю захисту своєї критично важливої інформації.

Аналізуючи потенційні шляхи витоку або спотворення інформації, можна виявити, що без спеціальних заходів захисту, які гарантують безпеку обчислювальної системи, можливі наступні ризики:

- дистанційне зчитування секретних повідомлень з моніторів ЕОМ та принтерів (через перехоплення електромагнітних випромінювань);
- витік інформації через електроживлення ЕОМ;
- акустичний або електроакустичний витік вводимої інформації;
- перехоплення даних у мережі зв'язку;
- введення неправдивої інформації;
- несанкціоноване зчитування (зміна) даних ЕОМ;
- крадіжка носіїв даних та виробничих відходів;
- доступ до залишкової інформації в пам'яті системи після виконання запитів;
- копіювання носіїв даних;
- несанкціоноване використання терміналів зареєстрованих користувачів;
- імітація зареєстрованого користувача шляхом викрадення паролів та інших даних для доступу;
- маскування неавторизованих запитів під системні запити (обман системи);
- використання програм-ловушок;
- доступ до захищених даних через серію дозволених запитів;
- використання слабкостей мов програмування та операційних систем;
- навмисне додавання до програмних бібліотек блоків типу «троянські коні»;
- умисне виведення з ладу захисних механізмів [7].

Окремо слід виділити спеціальні пристрої для знімання інформації з комп'ютерів. Мініатюрний радіомаяк, вмонтований у корпус, дозволяє відстежувати маршрут комп'ютера, передаючи сигнали на спеціальний приймач. Знаючи місцезнаходження системи, можна перехоплювати будь-яку інформацію, оброблену комп'ютером, через спеціально вбудовані електронні модулі, які не є частиною ЕОМ, але беруть участь у її роботі. Найкращий захист від такого пристрою – це екрановане приміщення для обчислювального центру. Під час аналізу каналів витоку інформації, особливу увагу потрібно

зосередити на захисті систем та комунікаційних ліній комп'ютерної інформації. Структурну схему системи підприємства можна побачити на рис. 2.1.

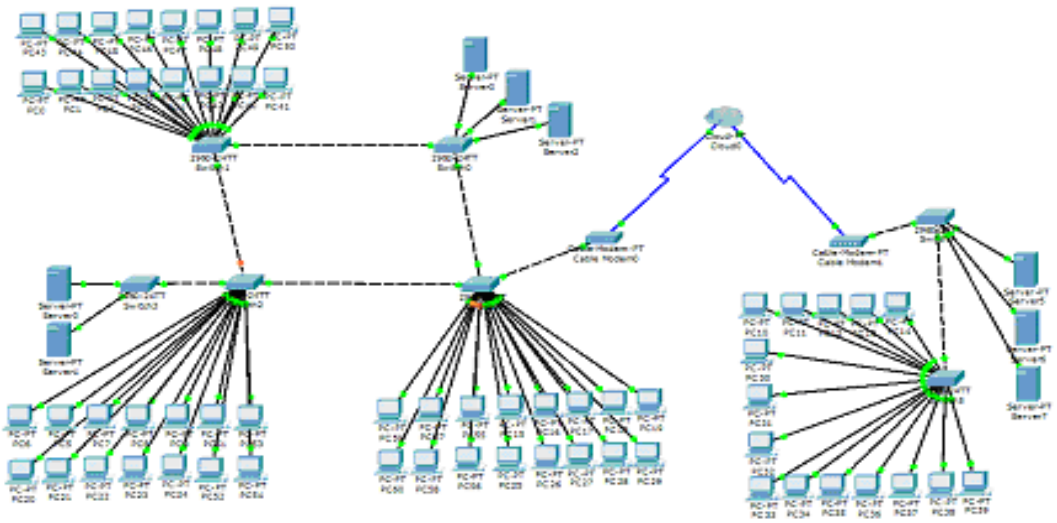

Рисунок 2.1 - Система передачі комп'ютерних даних

Експерти Cisco створили систему захисту, представлену на рис. 2.2, яка допомагає структурувати процес втілення та застосування інструментів безпеки мережі. Описаний на схемі процес відомий як аналіз рівня захищеності.

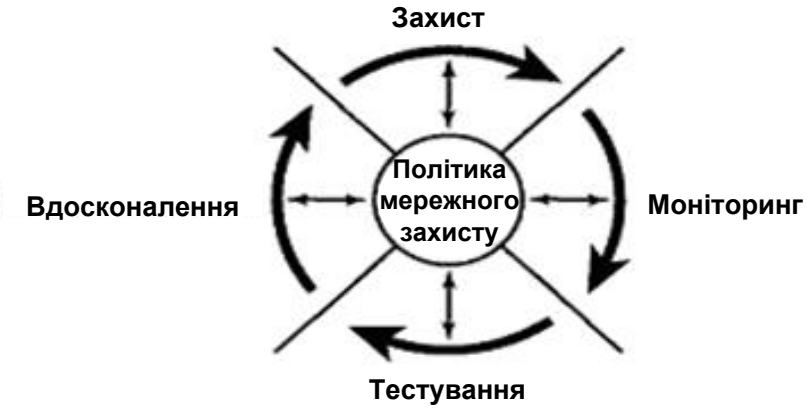

Рисунок 2.2 - Цикл захисту

Він представляє собою неперервні дії фірми, які регулярно повторюються і мають на меті охорону ключових ресурсів з мінімальними затратами, щоб зменшити ризик втрат до прийнятного рівня.

Враховуючи складний і повторюваний характер завдань забезпечення безпеки компанії, для того щоб компанія залишалася в безпеці від нових загроз,

процес має бути безперервним. Описаний цикл включає в себе чотири основні етапи.

Захист. Необхідно забезпечити захист корпоративної інформації. На цьому етапі компанії зазвичай впроваджують захисні технології (наприклад, файрволи та системи аутентифікації), які підвищують рівень безпеки мережі.

Моніторинг. Відстеження активності (як зовнішньої, так і внутрішньої) у критичних точках доступу до мережі. Також необхідно постійно здійснювати моніторинг мереж для виявлення вторгнень і випадків недозволеного використання, а також мати механізми автоматичного припинення неавторизованої активності, які працюють у режимі реального часу. Моніторинг може здійснюватися системами виявлення вторгнень. Такі системи повинні автоматизувати процес виявлення мережевих вторгнень. CiscoSecure IDS є системою виявлення вторгнень, яка працює в режимі реального часу, при цьому система не впливає на потік легітимних даних і дозволених дій у мережі. CiscoSecure IDS складається з двох елементів: датчиків та керівних пристроїв. Датчики CiscoSecure IDS, які є швидкодіючими мережевими пристроями, аналізують вміст окремих пакетів для виявлення ознак загроз або вторгнень у мережевому трафіку. Якщо поведінка потоку даних викликає занепокоєння, датчики CiscoSecure IDS у режимі реального часу фіксують порушення політики та відправляють сигнали тривоги до керівної консолі CiscoSecure IDS, щоб своєчасно від'єднати порушника від мережі та запобігти подальшому розвитку атаки. Керівний пристрій CiscoSecure IDS є високоефективною програмною системою управління, яка забезпечує централізоване керування великою кількістю датчиків CiscoSecure IDS, розташованих у локальних або віддалених сегментах мережі [7].

Тестування. Аналіз ефективності оборонних механізмів проти можливих кібератак.

Оптимізація. Впровадження передових технологій захисту та оновлення існуючих систем. Ключовим є централізоване керування захисними механізмами та політиками для забезпечення високої ефективності та оперативності внесення змін.

Оцінювання рівня безпеки вказує на шляхи удосконалення системи захисту компанії. В цьому процесі визначаються безпекові ролі та обов'язки працівників управлінської ланки та IT-підрозділів, а корпоративні дані

класифікуються за ступенем конфіденційності та встановлюються припустимі ризики для кожної категорії. У серці циклу захисту лежить ключовий елемент — політика мережевої безпеки, яка включає директиви для забезпечення необхідного рівня захисту компанії та охоплює такі аспекти.

Критично важливі активи компанії, які потребують захисту:

- ресурси (фінансові, людські, часові), які компанія готова інвестувати в захист своїх цінностей;

- рівень ризику, на який компанія готова піти.

Ключ до успішного створення системи захисту полягає в знаходженні балансу між легкістю використання захисних механізмів та рівнем наданого захисту. Невідповідність витрат на захист реальній загрозі може завдати шкоди бізнесу. Занадто суворі обмеження для користувачів можуть спонукати їх шукати способи обходу цих заходів, що знищить всі переваги від їх впровадження.

Для аналізу стану інформаційної безпеки мережі застосовують спеціалізоване програмне забезпечення. У проектах аудиту інформаційної безпеки та під час тестування на проникнення системний інтегратор пропонує рішення, засновані на програмах для аналізу безпеки – мережевих сканерах. Вибір продукту залежить від архітектури мережі організації:

- мережевий сканер безпеки "XSpider" від "Positive Technologies";

- мережевий сканер безпеки "Internet Scanner" від "Internet Security Systems".

Мережеві сканери безпеки представляють собою широко доступні та часто використовувані інструменти для оцінки захищеності. Вони працюють, імітуючи дії потенційного нападника для виявлення вразливостей у мережі. Принцип дії цих пристроїв демонструється на рис. 2.3.

XSpider аналізує потенційні слабкі місця без врахування програмного чи апаратного забезпечення вузлів: робочі станції на Windows, сервери Unix, Linux, Solaris, Novell, Windows, AS400, мережеве обладнання Cisco тощо. XSpider функціонує під управлінням операційної системи Microsoft Windows.

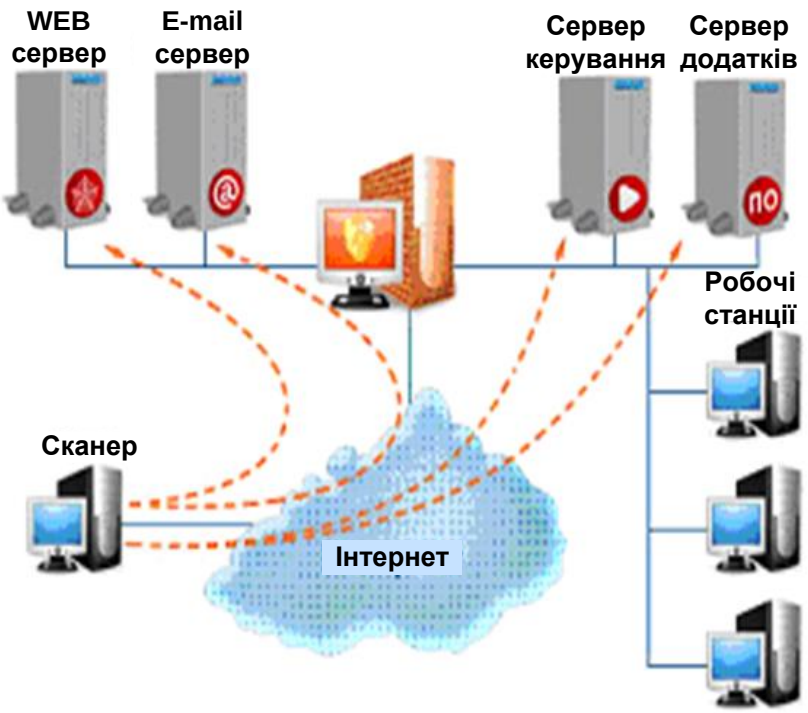

Рисунок 2.3 - Принцип роботи аналізатора стану безпеки системи безпеки мережі

Основні завдання програми для аналізу рівня безпеки:

- виявлення сервісів на нестандартних портах;
- евристичний підхід до визначення типів та назв серверів (HTTP, FTP, SMTP, POP3, DNS, SSH) незалежно від їх відповідей на звичайні запити;
- аналіз RPC-сервісів (Windows, Unix, Linux) з детальною ідентифікацією;
- перевірка надійності парольної захисту;
- аналіз вмісту WEB-сайтів;
- аналіз структури HTTP-серверів;
- тестування на вразливість до DoS-атак;
- щоденне оновлення бази вразливостей та методів їх перевірки;
- планувальник для автоматизації процесів;
- одночасне сканування великої кількості комп'ютерів (зазвичай обмежується швидкістю мережі);
- ведення логу перевірок;
- надання рекомендацій для виправлення вразливостей;
- створення звітів з різним ступенем деталізації [7]

Система аналізу безпеки Internet Scanner призначена для виявлення слабких місць у програмному та апаратному забезпеченні корпоративної мережі, визначення місця розташування вразливостей у мережі та рекомендацій щодо їх виправлення або усунення [7].

Завдання, які виконує програма для аналізу рівня безпеки:

- інвентаризація необмеженої кількості вузлів;
- аналіз рідко використовуваних сервісів;
- аналіз безпеки робочих станцій;
- виявлення нових вразливостей з моменту останнього сканування;
- виявлення конфігурацій «за замовчуванням»;
- аналіз налаштувань мережевого обладнання;
- аналіз налаштувань міжмережевих екранів;
- аналіз безпеки віддалених офісів;
- динамічне управління перевірками;
- автоматизація повторюваних процесів;
- розподіл завдань між відділами IT та інформаційної безпеки;
- виявлення модемів у корпоративній мережі;
- виявлення нерозпізнаних пристроїв;
- врахування часу існування вразливості;
- надання рекомендацій для виправлення вразливостей;
- створення звітів з різним ступенем деталізації [7].

Аналіз цієї мережевої структури виявив наступні вразливості та загрози інформаційній безпеці переданих даних:

- в цій системі передачі даних ключові елементи управління мережею є комутаторами без можливості аналізу вхідного та вихідного трафіку;
- система не має можливості створення приватного каналу передачі даних для двох або більше учасників;
- відсутній надійний захист серверів для зберігання та обробки даних;
- відсутні багатофункціональні мережеві пристрої для організації голосового зв'язку та створення широкосмугових підключень до зовнішніх мереж;
- в системі передачі даних також відсутнє спеціалізоване програмне забезпечення для захисту збережених і переданих даних;

- не забезпечено належний рівень інформаційної безпеки на станціях користувачів [7].

2.3 Розробка політики захисту контрольованої зони

Щоб забезпечити надійний захист периметра контрольованої території, я розробив наступні заходи та методики, які потрібно впровадити:

- замки та двері. Ефективний замок на вході в центр обробки даних є основою фізичного захисту. Рекомендується використовувати кодовий замок, що дозволяє ідентифікувати користувача. Важливо призначати унікальні комбінації для кожного співробітника та регулярно їх оновлювати. Запровадьте механізм блокування доступу для співробітників, які покидають компанію. Звичайні механічні замки або кодові замки з однією комбінацією не є безпечними через обмежені можливості контролю та легкість, з якою можна втратити ключ або підібрати код. Краще використовувати замки з захисним кожухом, що дозволяє лише користувачу, який вводить код, бачити клавіатуру. Також замок має бути налаштований на ведення журналу реєстрації входів у захищену зону. Існують системи блокування, що дозволяють вести реєстрацію. Такі замки оснащені інфрачервоним портом (IR), який можна використовувати для виведення журналу подій та списку користувачів. Також можливе використання замків на магнітних картках та ідентифікаційних бейджах (proximity badges), що підтримують фіксацію подій. Головний ризик для будь-якої системи, що вимагає від користувачів введення коду, наявності картки або ключа, полягає в тому, що особи без прав доступу можуть отримати доступ;

- потрібно посилити дверну раму та обшивку, встановити петлі таким чином, щоб зловмисники не могли зняти двері з зовнішньої сторони або використовувати незнімні петлі. Для кріплення петель та каркасу використовувати довгі гвинти, які закріплюються у стіні. Зварювати гайки зовнішніх болтів на металевих дверях;

- стелі та підлоги. Для блокування можливості несанкціонованого доступу зловмисників, на стінах, що примикають до справжнього стельового покриття та підлоги, встановлюють датчики руху. Стіни, підлогу та стелю необхідно заекранувати металом;

- електроенергія. У випадку, якщо основні панелі управління знаходяться поруч з центром даних (наприклад, за дверима), їх слід перемістити або заблокувати [6].

Одним із потенційних методів проникнення в систему є відключення електроенергії з метою деактивації сигналізації та іншого обладнання захисту периметра. Встановлення UPS для серверів та розміщення систем контролю доступу таким чином, щоб забезпечити захист під час відключення електроенергії, є важливим.

2.3.1 Забезпечення захисту приміщення керівника

Норми захисту приміщення керівника включають в себе положення для забезпечення безпеки кімнати, де проводяться наради.

Однак, враховуючи присутність у даному офісі персонального комп'ютера з таємною інформацією на ньому, до існуючих методів підвищення безпеки для кімнати нарад додаються наступні заходи:

- для оберігання від неконтрольованого розповсюдження інформації через параметричний канал рекомендується використання антистатичних браслетів та спеціалізованих гумових ущільнювачів;

- за можливості налаштувати розташування екрану монітора так, щоб уникнути ризику перехоплення візуальної інформації через вікна або двері;

- інсталяція на персональний комп'ютер спеціалізованого програмного забезпечення для надійного захисту інформації [6].

2.3.2 Забезпечення захисту приміщення серверної

Згідно з нормами TIA/EIA 568A, серверне приміщення є місцем розташування головного кросу для магістрального та горизонтального кабельного зв'язку. Також тут розміщується комунікаційне обладнання, кінці кабелів і кросова проводка.

Відповідно до зазначеного стандарту, основні принципи проектування захисту серверних приміщень, які використано для підвищення рівня захисту інформації, включають:

- на вхідних дверях встановлено охоронну сигналізацію для попередження несанкціонованого проникнення та електронний замок, щоб запобігти неавторизованому доступу;

- згідно з вимогами до організації серверних приміщень, цей проект передбачає розташування серверної кімнати у центрі поверху без зовнішніх стін;

- для забезпечення конфіденційності розташування серверної, на дверях не розміщено жодних вказівників чи інформаційних знаків;

- у приміщенні встановлені детектори руху та системи відеоспостереження;

- на шляху телефонних ліній до розподільчого панелі монтується захисний пристрій для телефонних ліній SEC-2003;

- на вході електроживлення та електропостачання до розподільчого панелі встановлюється генератор перешкод для мережі 220 В – SELSP- 41/C;

- для захисту ліній електропостачання використовуються мережеві фільтри;

- здійснюється обов'язкове заземлення серверних шаф згідно з наведеною схемою заземлення на рис. 2.5;

- розроблено політику доступу для довірених осіб до серверного приміщення [6].

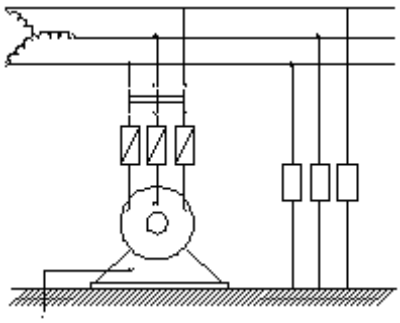

Рисунок 2.5 - Схема захисного заземлення

2.4 Розробка політики безпеки мережі та комунікацій

Організаційна політика безпеки (англ. Organizational security policies) - це комплекс керівних принципів, правил, процедур та методів застосування в сфері безпеки, які встановлюють управління, захист та розподіл важливої інформації [5].

Основною причиною створення політики безпеки зазвичай є вимога до наявності такого документу з боку регулятора - організації, що встановлює

норми роботи компаній певної галузі. У такому разі відсутність політики може призвести до репресивних заходів щодо компанії або навіть до її зупинки. Крім того, існують певні вимоги (рекомендації) від галузевих чи загальних, локальних чи міжнародних стандартів. Зазвичай це проявляється у вигляді зауважень зовнішніх аудиторів, які перевіряють діяльність компанії [5].

Відсутність політики призводить до негативної оцінки, яка, у свою чергу, впливає на публічні показники компанії - позиції в рейтингах, рівень довіри.

На підставі виявлених недоліків у захисті системи передачі даних була розроблена наступна політика безпеки мережі.

Аудит - розділ, присвячений аудиту в рамках політики безпеки, окреслює типи подій, які моніторяться у всіх системах. До стандартних подій належать:

- спроби входу в систему управління інформаційною безпекою мережі (успішні або невдалі);
- вихід з системи;
- помилки доступу до файлів або системних ресурсів;
- спроби віддаленого доступу (успішні чи невдалі);
- дії привілейованих користувачів (адміністраторів), успішні чи невдалі;
- системні події (вимкнення та перезавантаження) [5].

Кожна подія має включати таку інформацію:

- ID користувача (якщо доступний);
- дату та час;
- ID процесу (якщо доступний);
- виконану дію;
- успішне або невдале завершення події.

У розроблюваній політиці безпеки встановлюється термін зберігання записів аудиту та методика їх перегляду. За можливістю вказуються спосіб і частота перевірки цих записів.

У цій політиці мережевої безпеки для кожного типу з'єднань у мережі описано правила встановлення мережевих з'єднань та застосовувані механізми захисту:

- зєднання набірного доступу. Вимоги до цих з'єднань включають технічні правила автентифікації, в тому числі автентифікаційні правила для кожного типу з'єднання. Вони представлені у розділі аутентифікації політики і можуть передбачати більш суворі методи аутентифікації, ніж зазвичай. Також,

політика встановлює вимоги до аутентифікації при використанні набірного з'єднання. Для компанії корисно встановити строгий контроль над дозволеними точками доступу, аби відповідати вимогам авторизації в мережі;

- виділені лінії. У компаніях використовуються різноманітні типи виділених ліній, і для кожного з них потрібно визначити захисні пристрої. Зазвичай це міжмережеві екрани. Просте вказівка типу пристрою не гарантує певного рівня захисту. Політика безпеки має окреслити основні правила контролю доступу, що застосовуються до пристрою, а також процедуру запиту та отримання доступу, яка не є частиною стандартної налаштування;

- віддалений доступ до внутрішніх систем. Часто організації надають своїм працівникам можливість доступу до внутрішніх систем із, політики безпеки мають чітко окреслювати методи доступу до систем ззовні. Важливо, щоб кожне з'єднання було захищено за допомогою шифрування, і слід детально описати використовувані методи шифрування. З огляду на зовнішній доступ, рекомендується застосування ефективних способів автентифікації. Також політика безпеки повинна включати деталізовані інструкції щодо процесу авторизації. Що стосується бездротових мереж, їх популярність зростає, і встановлення бездротового зв'язку без узгодження з IT-відділом стає звичайним. Політика безпеки має встановлювати правила використання бездротових мереж та процедури авторизації в них. У разі дозволу на використання бездротових мереж, потрібно визначити спеціальні вимоги до автентифікації та шифрування. Бездротові мережі слід розглядати як зовнішні та незахищені, а не як частину внутрішньої мережі, і це має бути чітко вказано у політиці;

- виділені лінії. У структурах застосовуються різноманітні види спеціалізованих ліній, і для кожного виду потрібно вибрати захисні пристрої. Зазвичай це міжмережеві захисні стіни. Проте сама наявність такого пристрою не гарантує захист на певному рівні. Безпекова політика має окреслити основні правила контролю доступу, які будуть застосовані до пристрою, а також процедури подання запитів та надання доступу, які не входять до стандартної налаштування;

- доступ на відстані до внутрішніх систем. Часто організації надають можливість своїм працівникам отримувати доступ до внутрішніх систем з зовнішніх локацій. Безпекова політика мусить встановлювати механізми, що

використовуються для такого доступу. Важливо зазначити, що всі з'єднання мають бути захищені шифруванням, і окреслити деталі, пов'язані з типом шифрування. Враховуючи, що підключення відбувається ззовні, рекомендовано використовувати надійні методи аутентифікації. Також безпекова політика має встановлювати процедуру авторизації для такого доступу. Бездротові мережі. Бездротові мережі набувають популярності, і встановлення бездротового зв'язку без згоди IT-відділу стало звичайним. Безпекова політика має визначати умови використання бездротових з'єднань та процедуру авторизації в такій мережі. Якщо дозволяється використання бездротової мережі, потрібно вказати додаткові вимоги до аутентифікації чи шифрування. Бездротові мережі слід розглядати як зовнішні незахищені мережі, а не як частину внутрішньої мережі організації. Якщо це так, цей аспект мусить бути відображений у політиці [5].

Основними компонентами політики в області безпеки є ідентифікація, цілісність та активне аудитування.

Ідентифікація має на меті запобігти ризику анонімності та неавторизованого доступу до ресурсів і даних. Цілісність забезпечує захист від перехоплення та зміни даних, зберігаючи конфіденційність і недоторканність переданої інформації. І, нарешті, активне аудитування (перевірка) забезпечує контроль за дотриманням елементів політики безпеки та допомагає виявляти несанкціоновані втручання в мережу та атаки типу DoS [5].

Механізми ідентифікації слід впроваджувати з обережністю, оскільки навіть найкраща політика може бути знецінена, якщо її важко застосовувати. Типовим прикладом є запис пароля на листочку паперу і прикріплення його до монітора - це рішення для користувача, якому потрібно запам'ятати багато паролів для доступу до різних частин мережі. Складні або надмірно повторювані системи верифікації та авторизації можуть викликати невдоволення користувачів, тому їх варто уникати. Методи ідентифікації можуть базуватися на протоколі S/Key або використовувати спеціальні апаратні засоби (токен-автентифікація). А для модемного доступу часто використовується механізм ідентифікації за протоколом Point-to-Point Protocol (PPP), що включає Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) і Extensible Authentication Protocol (EAP) [5].

Цілісність включає в себе захист інфраструктурного обладнання мережі (доступ як фізичний, так і логічний), захист периметра та збереження

конфіденційності інформації. Захист від фізичного доступу можливий через розташування мережевого обладнання у спеціалізованих шафах з обмеженим доступом [5].

Захист логічного доступу зосереджений на впровадженні механізмів ідентифікації та авторизації перед наданням доступу до мережевих засобів зв'язку, таких як Telnet або термінали, до ключових компонентів загальної мережевої інфраструктури, наприклад, роутерів чи міжмережевих шлюзів. Захист периметра асоціюється з роботою міжмережевих шлюзів, які регулюють дозволений та заборонений трафік між різними зонами мережі, зазвичай між інтернетом та основною мережею або між користувачами віддаленого доступу та основною мережею [5].

Конфіденційність інформації може бути забезпечена за допомогою протоколів безпеки на транспортному рівні, таких як SSL та Secure Shell Protocol (SSH), які забезпечують безпечне обмін даними між клієнтом та сервером. Безпечний протокол передачі гіпертексту (S-HTTP) пропонує надійний механізм для Web-транзакцій, але SSL залишається найбільш використовуваним рішенням. Протокол SOCKS створює структуру, що дозволяє клієнтським та серверним програмам у доменах TCP та UDP безпечно використовувати мережеві послуги через міжмережевий шлюз. Протокол безпеки IP (IPSec) представляє собою набір стандартів для забезпечення цілісності та конфіденційності даних на рівні IP-мереж. X.509 є стандартом для підтримки структур безпеки та ідентифікації в електронному інформаційному обміні [5].

Основним елементом системи безпеки є аудит, який необхідний для моніторингу та перевірки дотримання політики безпеки. Аудит системи безпеки має проводитися регулярно, щоб оцінити її ефективність, включаючи перевірку нових систем, методи виявлення потенційних загроз від внутрішнього персоналу, наявність специфічних проблем, таких як атаки типу "відмова в обслуговуванні", та загальне дотримання політики безпеки.

При розробці політики безпеки критично важливо знайти баланс між легкістю доступу до інформації та належними механізмами ідентифікації авторизованих користувачів для забезпечення цілісності та конфіденційності даних. Ефективність політики безпеки забезпечується її обов'язковим впровадженням як на технічному, так і на організаційному рівні.

Отже, для підвищення рівня інформаційної безпеки системи передачі даних необхідно вжити наступні заходи:

- інтеграція в існуючу мережу ключових елементів для управління адресацією;

- організація мережі на сегменти, що включають сервери зберігання даних, поштові сервери, користувацькі мережі, web-сервери, віртуальні приватні мережі для віддаленого доступу та вихід в інтернет;

- детальний аналіз характеристик маршрутизаторів від Cisco для вибору оптимального центрального маршрутизатора для розроблюваної системи управління інформаційною безпекою;

- впровадження розумних маршрутизаторів від CISCO у ключових сегментах мережі;

- персоналізована конфігурація маршрутизаторів для кожного сегмента мережі;

- вибір та налаштування програмного забезпечення для захисту передаваних даних. Налаштування Outpost Firewall Pro.

Інтернет-шлюз + фаєрвол як основа системи управління

Виклик встановлення шлюзів та фаєрволів у мережі полягає у тому, що вся локальна мережа вважається довіреною, і шлюз, що розміщений на кордоні з довіреною мережею та інтернетом, стає потенційно слабкою ланкою. Якщо зловмисник вдасться захопити шлюз через інтернет, він зможе проникнути в довірену мережу компанії та взяти під контроль інші комп'ютери у локальній мережі, отримавши доступ до конфіденційної інформації. Таким чином, до сучасних шлюзів пред'являються особливо високі вимоги.

Інтернет-шлюз розміщений поряд з іншими готовими рішеннями, як це демонструється на рис. 2.6.

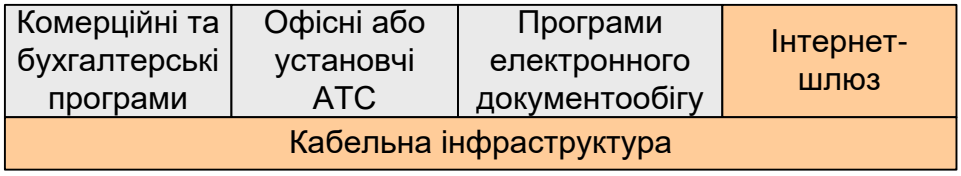

Рисунок 2.6 - Функції інтернет-шлюзу

Інтернет-шлюз має відповідати основним вимогам:

- багатофункціональність (підходить для різноманітних організацій);

- ефективність (забезпечує всі потрібні функції для виконання завдань);

- забезпечення безперебійної роботи в будь-яких ситуаціях);

- доступність утримання (мінімізація витрат на встановлення та обслуговування; легкість в обігу та керуванні) [4].

Проте, нинішні інтернет-шлюзи часто не відповідають сучасним потребам, тому вибір шлюзу для систем безпеки мережі вимагає детального аналізу вимог до інформаційної безпеки та можливостей шлюзу, який інтегрується. У таблиці представлено загальні типи інтернет-шлюзів з їх перевагами та недоліками.

Таблиця 2.1 - Основна градація інтернет шлюзів

Програми та служби під ОС Windows	+ низька вартість - низька безпека та надійність - використовуються в малих мережах
Власні розробки на базі ОС Linux/FreeBSD	+ хороша безпека - складність в обслуговуванні - слабка функціональність
Апаратний маршрутизатор	+ висока надійність та безпека - висока вартість впровадження та супроводу - слабка функціональність по роботі з користувачами

2.5 Вибір та конфігурування апаратних засобів захисту даних

Cisco Systems розробляє архітектурні рішення для забезпечення безпеки мереж, надаючи можливість інтегрувати системи управління інформаційною безпекою разом з продуктами від інших виробників. Це дозволяє створювати ефективні системи управління безпекою мережі, використовуючи програмно-апаратні платформи Cisco, що підтримують різноманітні політики та заходи для забезпечення надійного управління безпекою мережі:

- отримують сертифікацію як VPN-продукти;

- застосовують сертифіковані криптографічні бібліотеки від третіх сторін;

- реалізують користувацькі інтерфейси та підтримують VPN-протоколи продуктів Cisco;

- управляються через платформу CiscoWorks;

- підтримують єдину інфраструктуру ключів та можливість роботи з декількома PKI одночасно;

- дозволяють передавати байт ToS у заголовку пакета IPSec, що сприяє передачі даних про потрібну якість обслуговування (QoS) з внутрішніх пристроїв до зовнішніх мереж;

- забезпечують резервування для шлюзів та серверів;

- підтримують протоколи RADIUS, SSL, EAP/ TTLS [7].

Інтегруючи ці засоби з компонентами рішень Cisco, такими як:

- розширене фільтрування пакетів;

- підтримка зовнішніх систем ідентифікації;

- засоби виявлення вторгнень;

- системи моніторингу безпеки;

- фільтрація небажаного контенту;

- антивірусний захист;

- управління політиками безпеки мережі та окремих пристроїв;

- налаштування конфігурацій пристроїв – дозволяє створювати на основі програмно-апаратної платформи Ciscoпотужні системи управління інформаційною безпекою [7].

Огляд характеристик міжмережевих брандмауерів

Міжмережевий брандмауер Cisco Secure Private Internet Exchange (PIX) Firewall надає можливість захистити корпоративні мережі на високому рівні, будучи при цьому легким у обслуговуванні. PIX Firewall забезпечує повний захист внутрішньої мережі, ефективно ізолюючи її від зовнішнього світу. Відрізняючись від традиційних proxy-серверів, які обробляють кожен мережевий пакет окремо, навантажуючи процесор, PIX Firewall використовує спеціалізовану не UNIX подібну операційну систему реального часу для забезпечення вищої продуктивності. Висока продуктивність міжмережевого брандмауера PIX Firewall досягається завдяки застосуванню алгоритму адаптивної безпеки (adaptive security algorithm – ASA), який ефективно приховує адреси користувачів від несанкціонованого доступу. Цей надійний алгоритм забезпечує безпеку на рівні з'єднань, контролюючи інформацію про адреси відправника та одержувача, послідовність нумерації пакетів TCP,

номери портів та додаткові прапори TCP. Вся ця інформація зберігається у таблиці, через яку проходить перевірка всіх вхідних пакетів [6].

Доступ через PIX можливий тільки після успішної ідентифікації з'єднання. Цей метод надає безперешкодний доступ для внутрішніх та авторизованих зовнішніх користувачів, надійно захищаючи внутрішню мережу від нелегального входу. Використання технології «прозорого посередника» (Cut-Through Proxy) дозволяє міжмережевому брандмауеру Cisco PIX Firewall забезпечити значне підвищення продуктивності у порівнянні з проксі-серверами на базі ОС UNIX. PIX, подібно до звичайних проксі-серверів, керує встановленням з'єднань на програмному рівні. Після того, як користувач успішно пройде авторизацію доступу згідно з встановленими правилами безпеки, PIX забезпечує контроль за потоком даних між учасниками на рівні сесії. Такий підхід дозволяє міжмережевому брандмауеру PIX працювати набагато швидше, ніж традиційні проксі-екрани [6].

Окрім зростання продуктивності, використання спеціалізованої вбудованої операційної системи реального часу також сприяє підвищенню рівня безпеки. Виключається ризик єдиної точки потенційного збою. У випадку паралельної роботи двох PIX-екранів, при виході одного з них з ладу, другий автоматично та непомітно перебере на себе всі функції забезпечення безпеки.

Висока ефективність. Міжмережевий брандмауер Cisco Secure PIX Firewall підтримує понад 500 тисяч одночасних з'єднань і забезпечує обслуговування сотень та тисяч користувачів без втрати продуктивності [6].

Легкість використання. Міжмережевий брандмауер Cisco Secure PIX Firewall забезпечує низькі витрати на використання та обслуговування. Користувачі без спеціальної підготовки можуть легко налаштувати його за допомогою простого графічного інтерфейсу PIX Device Manager (PDM), доступ до якого здійснюється через звичайний веб-браузер. PDM - це програма, що використовує вбудований у PIX http-сервер і підтримує базовий набір команд для первинного налаштування міжмережевого брандмауера. За допомогою PDM можна налаштовувати PIX Firewall з будь-якого комп'ютера, а для захисту пристрою від несанкціонованого доступу під час конфігурації можна використовувати протокол SSL [6].

Рішення проблеми обмеженості IP-адрес. Міжмережевий брандмауер Cisco Secure PIX Firewall допомагає уникнути проблеми нестачі адрес при

розширенні та зміні IP-мереж. Технологія Network Address Translation (NAT) дозволяє використовувати в приватній мережі як існуючі, так і резервні адресні простори. Наприклад, можна використовувати одну зовнішню IP-адресу для 64 тисяч вузлів внутрішньої приватної мережі. PIX також можна налаштувати для використання як трансльованих, так і не трансльованих адрес, дозволяючи використовувати як адресний простір приватної IP-мережі, так і зареєстровані IP-адреси. Наразі користувачам Firewall доступні такі моделі апаратно-програмних міжмережевих брандмауерів Cisco Secure PIX Firewall - PIX 501, 506E, 515E, 525 та 535 [6].

Порівняльні характеристики CISCO PIX FIREWALL наведені у таблиці 2.2

Таблиця 2.2 - Порівняльні характеристики маршрутизаторів компанії Cisco

	Pix 501	Pix 506E	Pix 515	Pix 525	Pix 535
Продуктивність, Мбіт/сек	60	100	190	330	1667
Максимальна кількість з'єднань	7500	25 000	130 000	280 000	500 000
Кількість сесій, що одночасно підтримуються	19 500	53 000	176 000	625 000	1000000
Підтримувані фізичні інтерфейси	1x10/100 Ethernet та 4-портовий комутатор 10/100	2x10/100 Ethernet	До 6x10/100 Ethernet	До 8x10/100 Ethernet	До 10x10/100 Ethernet
Підтримувані логічні інтерфейси VLAN 802.1q	0	0	8	10	24
Продуктивність VPN (Triple DES/AES-128), Мбіт/сек	3/4,5	16/30	135*/130*	145*/135*	425*/495*
Максимальна кількість VPN-тунелів	10	25	2000*	2000*	2000*

Основні можливості CISCO PIX FIREWALL:

- розгалужена система оборони від неавторизованого входу на етапі підключення забезпечує надійний захист внутрішніх мережевих ресурсів;

- за допомогою технології CutThroughProхуможливе керування як вхідними, так і вихідними з'єднаннями, використовуючи такі протоколи безпеки, як TerminalAccessControllerAccessControlSystem (TACACS+) чи Remote Access Dial- In User Service (RADIUS);

- наявність до шести мережевих інтерфейсів для впровадження складних правил захисту. Інтерфейс адміністрування Security Manager дозволяє налаштовувати до 100 міжмережевих брандмауерів PIX з однієї консолі;

- динамічна та статична трансляція IP-адрес. Підтримується протокол управління мережею SNMP;

- збір облікових даних за допомогою системи ведення журналу подій (Syslog);

- прозора підтримка усіх ключових мережевих служб, таких як World Wide Web (WWW), File Transfer Protocol (FTP), Telnet, Archie, Gopher;

- підтримка мультимедійних додатків, включно з Progressive Networks RealAudio & ReadVideo, Xing StreamWorks, White Pines CU-SeeMe, Vocal Tec Internet Phone, VDOnet VDOLive, Microsoft NetShow і VXtreme Web Theater;

- підтримка взаємодії Microsoft Networking сервер-клієнт, Oracle SQL Net сервер-клієнт;

- захищена вбудована операційна система в реальному часі;

- відсутність потреби в оновленні програмного забезпечення на робочих станціях та маршрутизаторах;

- повний доступ до інтернет-ресурсів для авторизованих користувачів внутрішньої мережі;

- сумісність з маршрутизаторами, що управляються Cisco IO;

- підтримка відеоконференцій за протоколом H.323, включаючи Microsoft NetMeeting, Intel Internet Video Phone і White Pine Meeting Point;

- різноманітність програмної та апаратної комплектації;

- засоби централізованого управління;

- сповіщення про критичні події через пейджер або електронну пошту;

- підтримка інтерфейсів Ethernet, Fast Ethernet, Token Ring та FDDI;

- підтримка віртуальних приватних мереж (VPN) з використанням стандарту IPSec;

- висока ефективність;

- інтеграція з іншими продуктами компанії Cisco, зокрема з сервером ідентифікації користувачів Cisco Secure ACS [6].

В роботі також розглядаються маршрутизатори Cisco 2800 Series ISR для інтеграції в наявну мережу, оскільки вони пропонують високий рівень ефективності, що дозволяє задовольнити потреби навіть найвимогливіших компаній.

Маршрутизатори Cisco 2800 Series з інтегрованими сервісами пропонують різноманітність можливостей:

- вбудовані засоби безпеки: файєрвол, шифрування та захист від хакерів;

- вбудований запасний порт живлення для більшості моделей, що підвищує надійність;

- інтеграція з Cisco Unified Communications Manager Express, що дозволяє обслуговувати до 96 користувачів;

- інтеграція з Cisco Survivable Remote Site Telephony (SRST) для надання локальних голосових послуг у випадку відсутності зв'язку;

- збільшена надійність та адаптивність, що дозволяє встановлювати пріоритети для передачі голосу та даних, адаптуючи обслуговування до потреб компанії;

- підтримка з'єднань з віртуальними приватними мережами для співпраці з партнерами та філіями;

- підтримка бездротових мереж з повним покриттям офісу, захищеним доступом, можливістю гостьового підключення та відповідністю до сучасних стандартів бездротового зв'язку IEEE 802.11a/b/g/n;

- різноманітність опцій підключення до стандартних та широкосмугових мереж;

- можливості для живлення мережевих пристроїв через Ethernet-з'єднання, що дозволяє зменшити витрати на кабелювання [7].

Основні параметри маршрутизаторів Cisco серії 2800 у стандартному виконанні наведено у табл. 2.3.

Таблиця 2.3 - Характеристики маршрутизаторів сімейства 2800

Модель маршрутизатора	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
DRAM	128Mb(384Mb)	256Mb(768Mb)	256Mb(1Gb)	256Mb(1Gb)
Compact Flash	64Mb(128Mb)	64Mb(256Mb)	64Mb(256Mb)	64Mb(256Mb)
USB 1.1 Ports	1	2	2	2
Інтегровані LAN порти	2-10/100	2-10/100	2-10/100/1000	2-10/100/1000
Слоти для мережевих модулів	0	1 NME	1 NME або NME-X	1 NME, NMD, NME-X або NME-XD
Слоти для інтерфейсних карт	4 slots; 2 slots support HWIC, WIC, VIC, або VWIC type modules 1 slot supports WIC, VIC, or VWIC type modules1 slot supports VIC or VWIC type modules	4 slots, один slot може підтримувати HWIC, WIC, VIC, або VWIC type modules	4 slots, один slot може підтримувати HWIC, WIC, VIC, або VWIC type modules	4 slots, один slot може підтримувати HWIC, WIC, VIC, або VWIC type modules
Слот для голосового модуля розширення	0	0	1	1
Форм фактор	1U	1U	2U	2U

Керування роутерами можливе через WEB-інтерфейс або за допомогою Cisco IOS Software – командного інтерфейсу, включаючи віддалений доступ. Існує набір стандартних налаштувань, які спрощують процес адміністрування.

Структура роутерів інтегрованих сервісів родини Cisco 2800 ґрунтується на архітектурі потужних мультисервісних роутерів доступу серії Cisco 2600, пропонуючи додаткові вбудовані опції безпеки, значне підвищення продуктивності та збільшений обсяг пам'яті, а також нові інтерфейси високої щільності. Завдяки покращенням у продуктивності, доступності та надійності, роутери серії Cisco 3800 є незамінними для критично важливих бізнес-додатків, що використовуються в найважчих умовах роботи.

Характеристики продуктивності та щільності портів роутерів інтегрованих сервісів серії Cisco 2800 відповідають потребам середніх підприємств, а також малих та середніх відділень великих компаній щодо захищених, одночасно наданих сервісів, а також вимогам до керованих сервісів, які ставлять оператори зв'язку – без залучення операторів зв'язку [7].

Під керуванням програмного забезпечення Cisco IOS, роутери серії Cisco 2800 підтримують концепцію самозахищеної мережі Cisco Self-Defending Network – завдяки розширеним можливостям безпеки та управління, таким як апаратне прискорення шифрування, підтримка IPSec VPN (з використанням алгоритмів шифрування AES 3, систем виявлення вторгнень (IPS), контролю доступу до мережі (NAC) та фільтрації за URL. На всіх роутерах серії Cisco 2800 присутня інтуїтивно зрозуміла система управління через Web-інтерфейс Cisco Router and Security Device Manager (SDM), що значно спрощує управління та налаштування роутера [7].

Отже, базуючись на даних, отриманих в результаті моніторингу мережі даних та аналізі роутерів компанії Cisco, модернізуємо систему передачі даних, описану в розділі 2.2, до моделі, представленої на рис. 2.7.

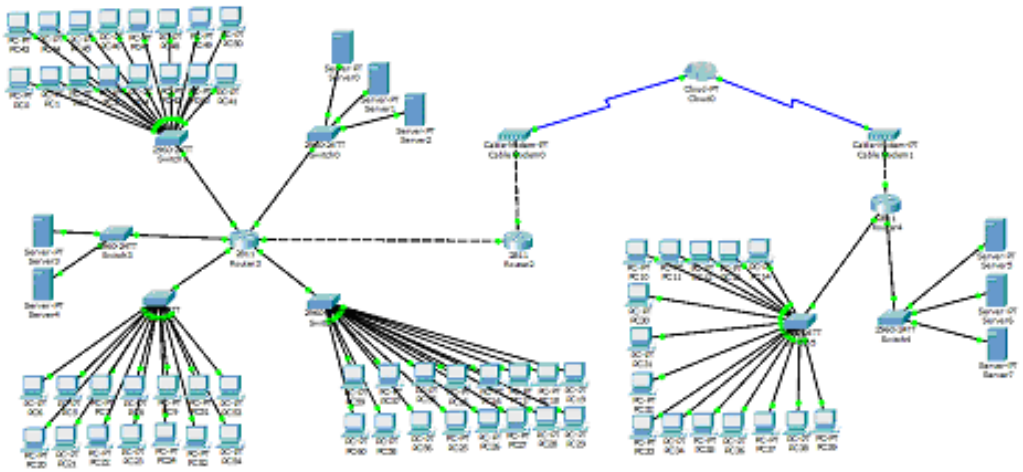

Рисунок 2.7 - Змінена структура мережі передачі

Інтеграція в систему безпеки компонентів, таких як маршрутизатори від Cisco серії 2800, допоможе досягти високого рівня захисту завдяки використанню спеціалізованого обладнання для захисту даних. Вбудовані в маршрутизатор функції безпеки допоможуть вирішити ряд критичних питань захисту даних у системі:

- поділити робочу мережу на окремі сегменти з можливістю моніторингу трафіку з обох боків;

- моніторити вхідні та вихідні дані;

- покращити ефективність системи та зменшити навантаження на комутатори.

2.6 Захист даних засобами захисту інформації та спеціального ПЗ

Захист програмної інформації є ключовим для запобігання неавторизованому доступу та модифікації особистих та бізнес-даних. Стратегія та концепція захисту інформації спрямовані на забезпечення безпеки даних, що містяться на жорстких дисках та магнітних стрічках. Лідери галузі пропонують свої рішення для захисту інформації на серверах та магнітних носіях. Програмний захист включає моніторинг доступу до зовнішніх і внутрішніх комп'ютерних пристроїв. Системи захисту інформації надають широкий спектр опцій для збереження даних та аутентифікації користувачів. При створенні програм захисту особлива увага приділяється побудові захисного бар'єру проти хакерських атак. Високий рівень безпеки досягається лише при адекватному впровадженні всіх заходів.

У роботі використовуватимуться вбудовані функції захисту операційних систем, а також інтеграція в мережу програмних засобів брандмауерів. Ці заходи, разом з іншими засобами захисту інформації, дозволять створити інтегровану систему управління безпекою інформації.

Брандмауер - це програма, що забезпечує додатковий рівень безпеки для комп'ютера при підключенні до інтернету. Вона спроектована для моніторингу неавторизованих спроб підключення ззовні, включаючи віруси та інші шкідливі програми [6].

Брандмауер працює безперервно, відслідковуючи спроби впровадження сторонніх програм, що значно підвищує безпеку комп'ютера, фільтруючи весь трафік. Він розділяє трафік на дозволений та заборонений. Правила, за якими відбувається фільтрація, налаштовуються в параметрах брандмауера.

Існують різні брандмауери: деякі вимагають складної настройки з гнучкими параметрами, інші пропонують мінімальні налаштування, а треті знаходяться десь посередині. Варто спробувати кілька програм, щоб вибрати найбільш підходящу, зосереджуючись на безпеці комп'ютера [6].

Брандмауер, вбудований у Windows, задовольняє потреби більшості користувачів, деякі навіть не знають про існування такого захисника, який захищає їхній комп'ютер від небажаних програм з інтернету. Він надійно блокує всі несанкціоновані запити, але якщо на комп'ютері є програми, яким потрібно отримувати дані, брандмауер запитує дозволу у користувача. Однак у

цій роботі використовується брандмауер від стороннього розробника Outpost Firewall Pro [7].

Ключові особливості цього програмного забезпечення включають:

- попередження спроб будь-якого програмного забезпечення взяти під контроль інші програми. Користувачі мають можливість налаштувати перелік програм, яким дозволено здійснювати вихідну передачу даних, щоб уникнути непомітних спроб доступу від шкідливих процесів, прихованих за легітимними програмами;

- блокування спроб запустити браузер із параметрами командного рядка. Деякі програми можуть відкривати вікно браузера, коли користувач натискає на посилання (Outlook, Microsoft Office, ICQ та інші). Для запобігання небажаним запускам від шкідливих процесів, користувач може налаштувати перелік програм, яким дозволено відкривати вікно браузера;

- моніторинг пам'яті програм. Користувач може створити список надійних програм, щоб запобігти використанню адресного простору легітимних програм шкідливими процесами для виконання шкідливого коду;

- контроль Active Desktop. Компоненти Active Desktop можуть містити шкідливий код, який може передавати конфіденційну інформацію від імені Windows Explorer. Outpost перешкоджає спробам встановлення та активації такого коду;

- попередження спроб керування вікнами інших програм. Шкідливі програми можуть імітувати натискання клавіш користувачем у інших вікнах та проводити неавторизований обмін даними між цими вікнами. Outpost перешкоджає таким діям, перевіряючи програми на легітимність і блокуючи всі неавторизовані спроби передачі даних;

- попередження спроб зміни критичних параметрів реєстру. Реєстр зберігає налаштування всіх програм. Користувач може визначити список програм, яким дозволено вносити зміни до реєстру;

- подвійна перевірка дозволу DNS-імен. Складні хакерські методи, які дозволяють викрасти дані через DNS-запити, ефективно блокуються;

- контроль низькорівневого мережевого доступу. Шкідливий код, встановлений у системі, може імітувати звичайну активність системи для встановлення вихідного з'єднання. Outpost виявляє такі спроби, інформуючи користувача та запитуючи його рішення;

- покращена продуктивність. Застосовано новий метод порівняння програм з базою spyware-сигнатур, що значно прискорює процес сканування;

- додатковий захист через параметр "сканування перед запуском". Без винятку всі програми перевіряються на легітимність перед їх запуском. Outpost імітує запуск програми та перевіряє її перед тим, як дозволити виконання або заблокувати її реальний запуск. При цьому продуктивність системи не знижується;

- новий аналізатор spyware-сигнатур. Удосконалений алгоритм виявлення підвищує захист користувача від відомих та невідомих шкідливих програм [7].

3 РЕАЛІЗАЦІЯ МОДЕЛІ МЕРЕЖІ ОБ'ЄКТА ЗАСОБАМИ ПРОГРАМИ PACKET TRACER

3.1 Опис програми налаштування маршрутизаторів Cisco

Для опису процесів та параметрів налаштування маршрутизаторів компанії Cisco, було прийнято рішення спроектувати модель мережі у програмі моделювання роботи мережі Cisco Packer Tracer, основне вікно якої наведено рис. 3.1.

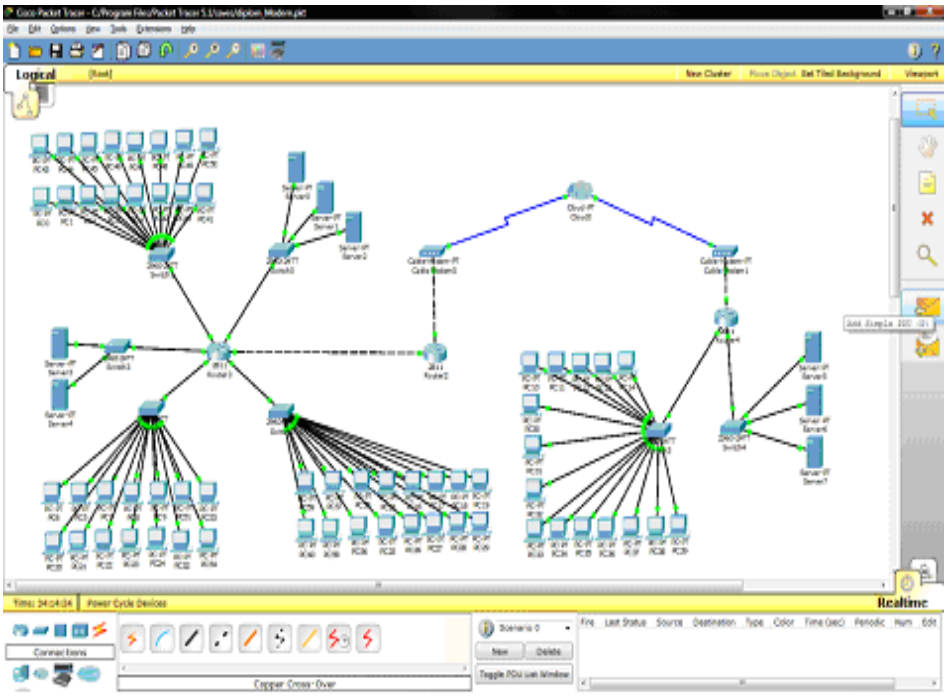

Рисунок 3.1 - Робоча область Cisco Packet Tracer

На зображенні показано оновлену та покращену з точки зору безпеки мережу. В критичних точках інфраструктури передачі даних розміщено маршрутизатори від Cisco.

До налаштувань конфігурації робочої станції належать дані про IP-адресу та маску підмережі, у випадку, коли не застосовується метод динамічного призначення адрес. Параметри конфігурації робочої станції показані рис. 3.2 і 3.3.

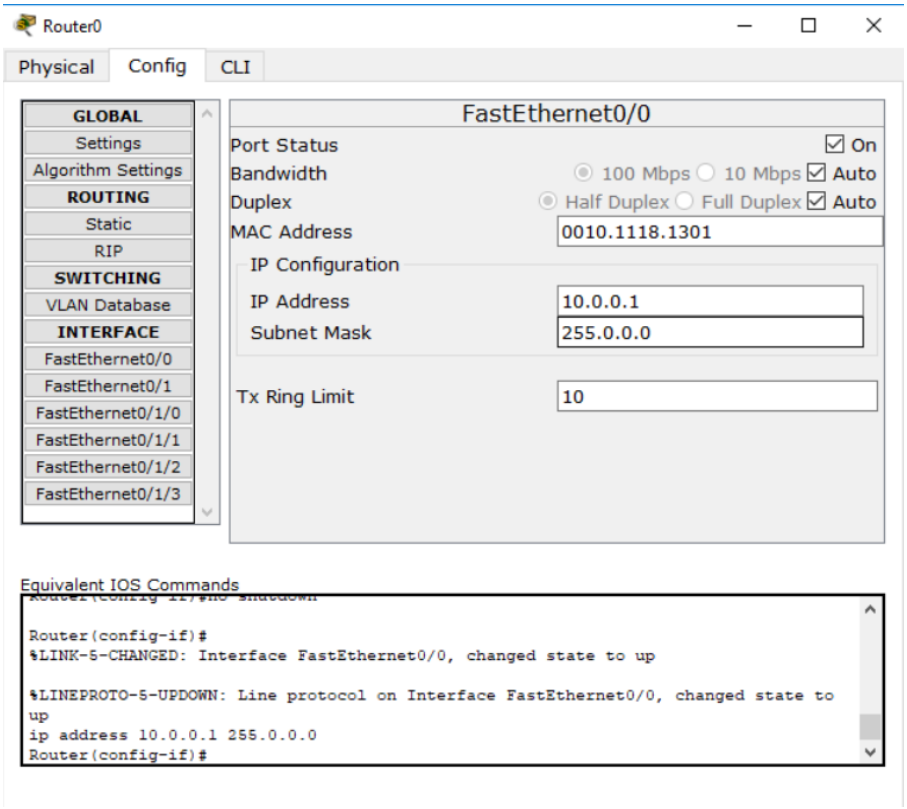

Рисунок 3.2 - Статичне завдання адресації

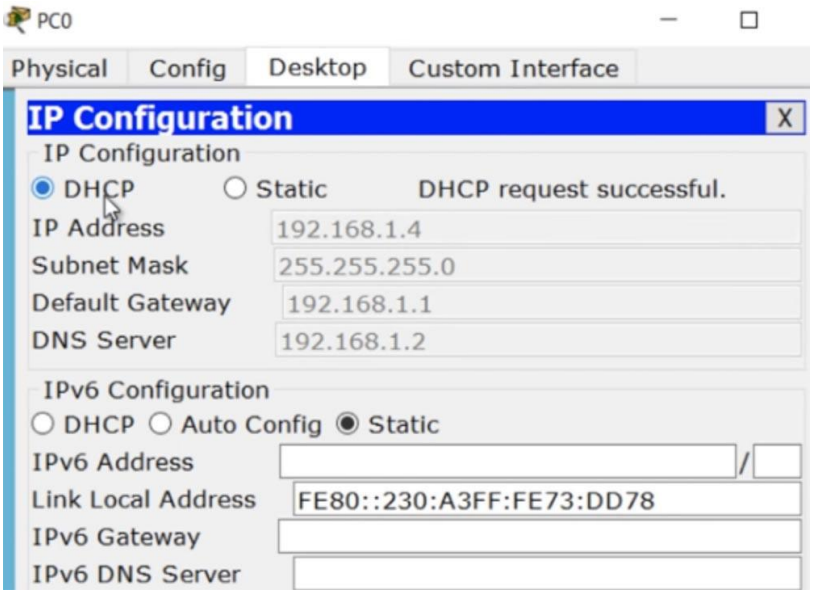

Рисунок 3.3 - Динамічний розподіл адрес у мережі

Процедура конфігурації комутаторів та їх портів полягає у налаштуванні віртуальних мережевих середовищ.

Конфігурацію можливо здійснити за допомогою графічного інтерфейсу користувача або через інтерфейс командного рядка терміналу управління системою IOS комутатора. На рис. 3.4 представлено приклад налаштування

мережевого зв'язку між комутатором і хостом, який є частиною мережі, що обслуговується цим комутатором.

```
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to
up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to
up


Switch>en
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```

Рисунок 3.4 - Налаштування роботи комутатора

На рис. 3.5 здійснюється перевірка стану з'єднання за допомогою команди ping.

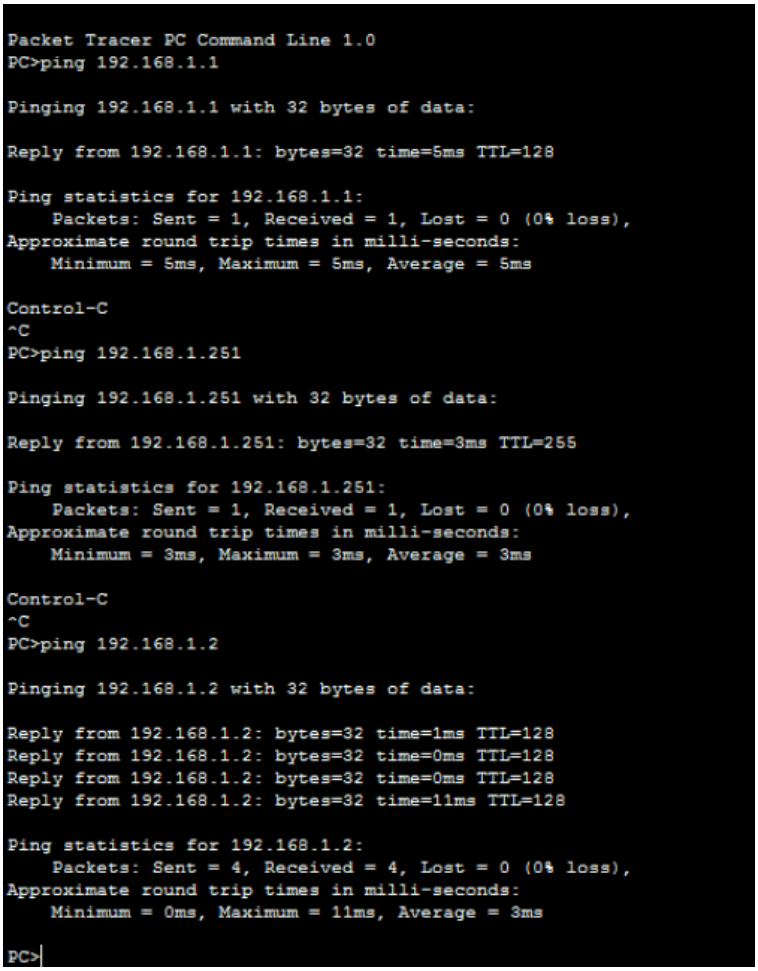

Рисунок 3.5 - Перевірка стану з'єднання

3.2 Опис налаштування спеціального програмного забезпечення захисту даних

Увімкнення та вимкнення захисту

Стандартно, Outpost Firewall Pro стартує автоматично при вмиканні системи, надаючи захист з самого початку її роботи. Про активність Outpost Firewall Pro свідчить іконка у формі білого запитання на синьому щиті, стандартний символ продукту, який з'являється в системному треї в нижньому правому кутку панелі задач Windows. Видіння цієї іконки гарантує, що Outpost Firewall Pro функціонує та охороняє вашу систему.

Двічі натисніть на іконку, щоб відкрити основне вікно Outpost Firewall Pro. Для закриття основного вікна, натисніть на хрестик у верхньому правому куті. Варто зазначити, що це не призводить до вимкнення програми. Основне вікно мінімізується до іконки, яка сигналізує про активну роботу та забезпечення безпеки вашої системи Outpost Firewall Pro.

Для повного відключення роботи продукту (при цьому Outpost Firewall Pro припинить захищати вашу систему), клацніть правою кнопкою миші на іконку продукту в системному треї, оберіть Вихід, виберіть зі списку Вийти з Outpost Firewall Pro і зупинити службу та натисніть OK.

Режим завантаження

Outpost Security Suite Pro пропонує налаштувати режим завантаження при старті системи. Для вибору одного з доступних режимів, натисніть Параметри на панелі інструментів. На сторінці Загальні в групі Параметри роботи доступні наступні режими завантаження:

- звичайний. Стандартний режим завантаження. Outpost Firewall Pro запускається автоматично при старті системи, іконка продукту з'являється в треї;

- фоновий. У Фоновому режимі завантаження Outpost Firewall Pro функціонує непомітно, не показуючи ні іконку в системному треї, ні спливаючі вікна. Це робить продукт повністю невидимим для користувача, дозволяючи таким чином батькам або системному адміністратору таємно блокувати небажаний трафік або вміст сторінок для користувача. Ще одна причина обрати Фоновий режим – це економія системних ресурсів.

Ви завжди можете запустити Outpost Firewall Pro вручну, натиснувши Пуск > Програми > Agnitum > Outpost Firewall Pro та обравши Outpost Firewall Pro. Вікно налаштувань мережевого брандмауера показано на рис. 3.6.

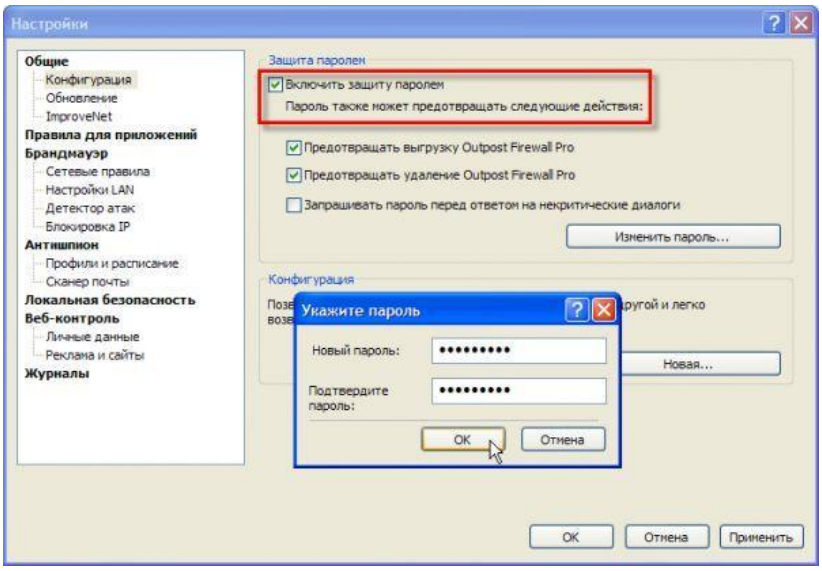

Рисунок 3.6 - Основне вікно налаштувань

Outpost Firewall Pro надає можливість тимчасово вимкнути захист на визначений період. Це стане в нагоді, коли вам потрібно не зупиняти продукт повністю, а лише припинити захист системи на короткий час, щоб уникнути небажаних сповіщень, наприклад, під час інсталяції перевіреного програмного забезпечення від сторонніх розробників, тестування додатків або проведення дій, які можуть бути визначені продуктом як підозрілі.

Коли захист Outpost Firewall Pro вимкнено, він не моніторить жодних дій; під час відновлення захисту застосовується конфігурація, що використовувалася до призупинення.

Для тимчасового вимкнення захисту, натисніть правою кнопкою миші на іконку продукту в системному треї та оберіть Призупинити захист, як це зображено на рис. 3.7.

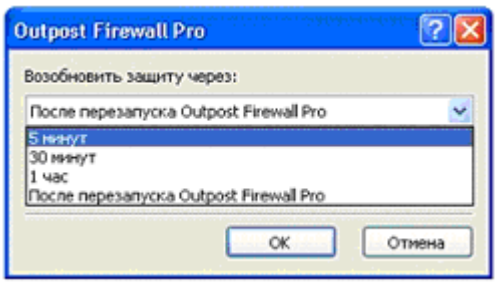

Рисунок 3.7 - Налаштування таймера захисту

Ви завжди можете поновити захист, натиснувши на іконку продукту в системному треї правою кнопкою миші та обравши опцію Відновити захист.

Замість того, щоб вимикати весь захист Outpost Firewall Pro, можливо деактивувати окремі його елементи для здійснення потрібних дій: - для відключення брандмауера перейдіть у Налаштування через панель інструментів, відкрийте вкладку Брандмауер і зніміть галочку біля опції Включити брандмауер

- для деактивації компонента Детектор атак перейдіть у Налаштування через панель інструментів, оберіть вкладку Детектор атак і зніміть галочку біля опції Увімкнути детектор атак;

- для відключення компонента Локальна безпека перейдіть у Налаштування через панель інструментів, відкрийте вкладку Локальна безпека та зніміть галочку біля опції Включити Локальна безпека;

- для вимкнення постійного захисту від шкідливих програм перейдіть у Налаштування через панель інструментів, оберіть вкладку Антишпигун і зніміть галочку біля опції Увімкнути постійний захист;

- для деактивації компонента Веб-контроль перейдіть у Налаштування через панель інструментів, відкрийте вкладку Веб-контроль та зніміть галочку біля опції Увімкнути веб-контроль;

- для відключення внутрішнього захисту Outpost Firewall Pro перейдіть у Налаштування через панель інструментів і зніміть галочку біля опції Увімкнути внутрішній захист.

Зазвичай налаштування локальної мережі на вашому комп'ютері встановлюються автоматично під час інсталяції Outpost Firewall Pro. Однак, ви маєте можливість активувати функцію виявлення мережі в будь-який час, щоб безперешкодно взаємодіяти з іншими комп'ютерами. Для перегляду списку мереж, до яких належить ваш комп'ютер, натисніть Установки на панелі керування та оберіть вкладку Установки LAN, як показано на рис. 3.8:

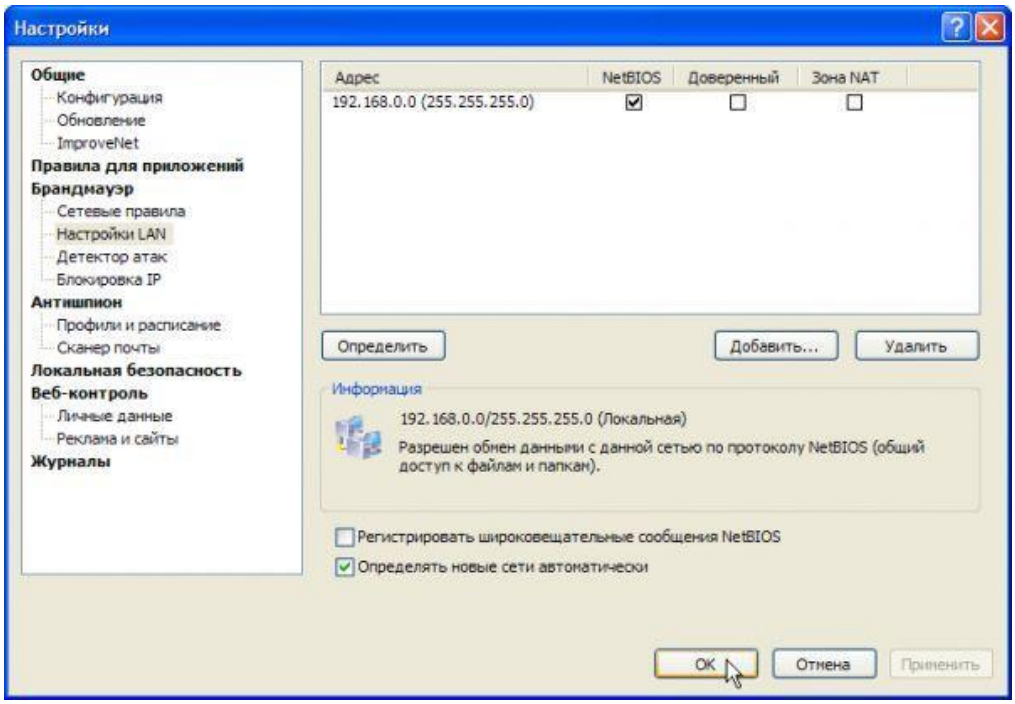

Рисунок 3.8 - Налаштування мережевого захисту

У розділі Налаштування LAN натисніть на опцію Визначити, і Outpost Firewall Pro самостійно знайде мережі, до яких підключений ваш комп'ютер, після чого покаже перелік їх IP-адрес з вказаними стандартними рівнями доступу. Потім ви зможете налаштувати бажаний рівень доступу для кожної

мережі. Щоб Outpost Firewall Pro мав змогу сам виявляти нові мережі, що звільнить вас від необхідності додавати їх вручну, активуйте опцію Визначати нові мережі автоматично, а далі натисніть кнопку OK для збереження налаштувань. Якщо ви бажаєте внести в список нову мережу або віддалений вузол, щоб призначити спеціальний рівень доступу, або в разі, коли Outpost Firewall Pro не зміг автоматично ідентифікувати вашу мережу, це можна зробити вручну. Для цього в розділі Налаштування LAN натисніть кнопку Додати та у вікні Вибір адреси вкажіть потрібний формат для введення адреси, як описано на рис. 3.9.

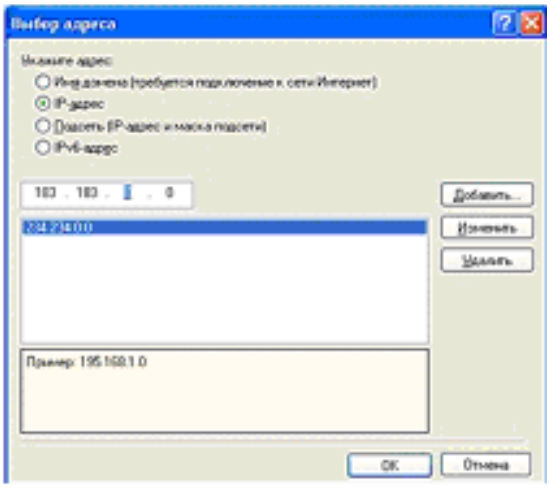

Рисунок 3.9 - Завдання адресації

Назва домену, наприклад, http://www.agnitum.com. Для цього потрібно мати з'єднання з Інтернетом, адже IP-адреси визначаються через мережу. IP-адреса зберігається разом із вказаним вами доменним іменем, і саме ця IP-адреса буде в основному використовуватися Outpost Firewall Pro. IP-адреса, наприклад, 216.12.219.12. Підмережа (IP-адреса та маска підмережі), наприклад, 216.12.219.1 - 216.12.219.255

Адреса IPv6, наприклад, 2002::a00:1.

Вкажіть потрібну адресу у обраному форматі (можливе використання масок) та натисніть Додати. Таким чином можна додати декілька адрес поспіль. Натисніть кнопку OK для їх додавання до списку в діалоговому вікні. Встановіть необхідний рівень доступу для кожної мережі та натисніть OK для збереження налаштувань.

Кожен ПК у локальній мережі може мати один з трьох рівнів доступу до вашого ПК:

- NetBIOS. Надає можливість спільного доступу до файлів та принтерів між ПК у локальній мережі. Для активації цього рівня відмітьте відповідний пункт NetBIOS для цієї адреси;

- довірені. Усі з'єднання до та з цієї мережі дозволені. Для активації цього рівня відмітьте пункт Довірені для цієї адреси;

- зона NAT. Виберіть цей параметр, якщо використовуєте Internet Connection Sharing або інші мережеві рішення, що надають доступ до Інтернету через ваш ПК;

- обмежений доступ до LAN. З'єднання NetBIOS блокуються, усі інші з'єднання обробляються згідно з загальними правилами та правилами для програм;

Для активації цього рівня зніміть обидва прапорці NetBIOS і довірені адреси. Важливо знати, що вузол у статусі Довірених має найвищий пріоритет і до нього можуть підключатися навіть заблоковані програми.

Рекомендується додавати до списку Довірених лише ПОВНІСТЮ БЕЗПЕЧНІ ПК. Якщо вам необхідний лише спільний доступ до файлів та принтерів, краще обрати рівень NetBIOS замість довірених.

Якщо ви не хочете перевантажувати журнали даними про широкомовні пакети NetBIOS, можна вимкнути їх реєстрацію для кожного виявленого вузла чи мережі. Виберіть адресу зі списку та зніміть прапорець Реєструвати широкомовні повідомлення NetBIOS. Це допоможе зробити інформацію в журналі подій більш чіткою та може підвищити продуктивність ПК.

При налаштуванні конфігурації Outpost Firewall Pro виявляються всі інстальовані програми та створюються правила для відомих програм на основі заздалегідь встановлених параметрів.

Кожна програма має відображені дві колонки з іконками, які вказують на тип правил, що використовуються брандмауером (Мережеві правила) та модулем Локальної безпеки (Anti-Leak). Іконка зеленого кольору демонструє, що до програми застосовані тільки дозвільні правила; червоний колір іконки означає застосування тільки заборонних правил; жовтий колір іконки свідчить про використання обох типів правил; якщо іконка відсутня - це означає, що до програми не застосовані жодні правила відповідним компонентом.

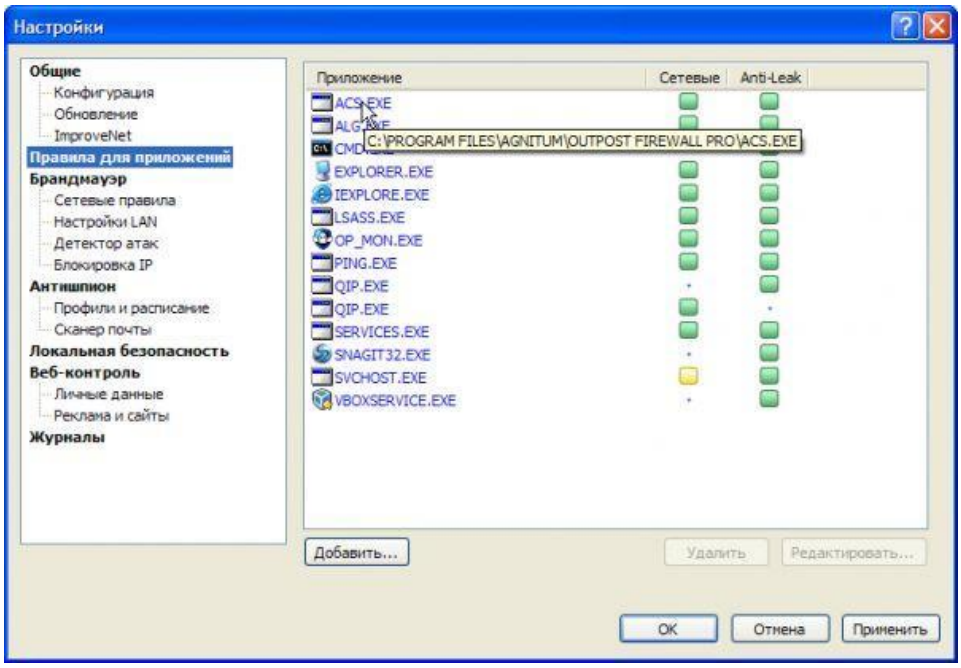

Рисунок 3.10 - Налаштування правил додатків

Також є можливість управління списком програм, додаючи або видаляючи їх вручну. Для додавання програми клікніть на кнопку Додати. Вам буде запропоновано обрати виконуваний файл програми у вікні. Оберіть його та натисніть Відкрити, після чого програма з'явиться у списку. Для призначення програмі індивідуальних правил, виберіть її та натисніть Редагувати. У вікні Редактор правил встановіть необхідні правила та підтвердіть вибір, натиснувши OK. Більше інформації про створення та редагування правил для програм можна знайти у розділі Налаштування правил для програм. Для видалення програми зі списку, натисніть кнопку Видалити.

Для перегляду переліку вже існуючих правил програми, клікніть Параметри на панелі інструментів та оберіть сторінку Мережні правила. Виберіть програму та двічі клікніть на неї лівою кнопкою миші. Перейдіть на вкладку Мережні правила. Для додавання нового правила клікніть Нове, як показано на рис. 3.11.

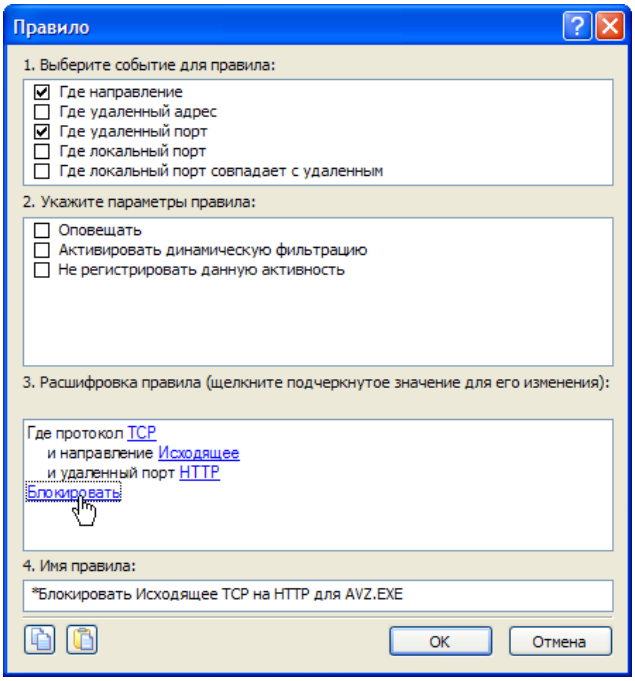

Рисунок 3.11 - Створення правил додатків

У налаштуваннях редактора правил вам знадобиться встановити наступні параметри:

Доступні для вибору критерії:

- напрямок з'єднання - вхідний чи вихідний;

- віддалена адреса – це може бути IP-адреса або доменне ім'я;

- віддалений порт – конкретний порт на віддаленій машині для здійснення з'єднання;

- де локальний порт - конкретний порт на вашому пристрої, який буде використовуватись для підключення;

- коли локальний порт співпадає з віддаленим – обидва пристрої використовують той самий порт для підключення. У випадку вказівки діапазонів портів для віддаленого та локального портів, правило буде застосовуватися до всіх портів, що входять в область їх перетину. Якщо перетин відсутній, правило не буде застосовуватися.

Оберіть критерій для події та налаштуйте необхідні параметри, натиснувши на підкреслене значення в полі Опис правила. Вкажіть параметри для правила.

Ви маєте можливість вибрати такі дії:

- сповіщення - інформує, коли правило активовано;

- увімкнення динамічної фільтрації - активує «динамічну фільтрацію» для даної програми (після того, як програма встановлює з'єднання з віддаленим сервером, усі вхідні дані з сервера до порту, відкритого програмою, будуть дозволені або заблоковані згідно з правилом);

- не зберігати цю активність - відключає логування активності для цього правила. Якщо ця опція вибрана, то дані при активації цього правила не будуть записуватися в журнал.

Після вибору дій на попередніх етапах відповідні інструкції з'являться у полі Розшифровка правила. За вказаними критеріями для правила вам потрібно буде вирішити, дозволити чи заборонити зазначене з'єднання, натиснувши на посилання зі стандартним значенням Дозволити. Переконайтеся, що в полі Розшифровка правила не залишилося невизначених параметрів. Outpost Firewall Pro автоматично створить Ім'я правила на основі введених параметрів. Натисніть кнопку OK для збереження правила. Правило з'явиться у списку. Деталі вибраного правила будуть показані в нижній частині діалогового вікна.

Для модифікації існуючого правила, перейдіть до списку та натисніть Змінити. Внесіть необхідні корективи, слідуючи вищезазначеним інструкціям, та натисніть OK для збереження змін. Обрані правила активні (включені) та обробляються програмою. Зніміть прапорець поруч з правилом, якщо ви не хочете, щоб Outpost Firewall Pro застосовував це правило, але не хочете його видаляти. Ви можете знову активувати правило, поставивши прапорець. Правила застосовуються в порядку від верху до низу. Зауважте, що Outpost Firewall Pro застосовує перше відповідне правило зі списку та ігнорує всі інші. Щоб змінити порядок застосування правил, виберіть правило зі списку та скористайтеся кнопками Вгору/Вниз.

Глобальні правила Outpost Firewall Pro стосуються всіх процесів та програм на вашому комп'ютері, які потребують доступу до мережі. Наприклад, створивши відповідні правила, ви можете блокувати весь трафік за певним протоколом або з певного віддаленого вузла. Деякі з налаштувань глобальних правил, оптимально підібрані, Outpost Firewall Pro встановлює за замовчуванням. Щоб переглянути список глобальних правил, натисніть на панелі інструментів кнопку Налаштування, оберіть сторінку Мережеві правила та натисніть кнопку Системні Правила, як показано на рис. 3.12.

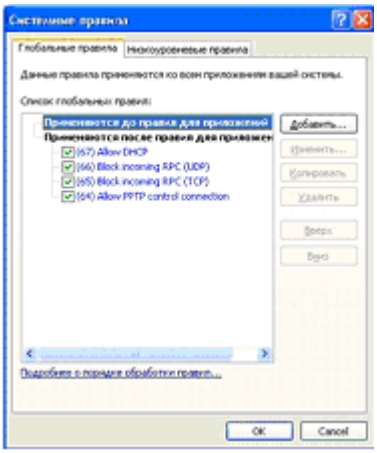

Рисунок 3.12 - Налаштування системних правил

Активовані правила зараз увімкнені та обробляються системою захисту. Якщо ви не хочете, щоб Outpost Firewall Pro застосовував певне правило, зніміть галочку поруч з ним, не видаляючи його повністю. Ви завжди маєте можливість знову активувати правило, встановивши галочку знову.

Правила застосовуються в порядку від верху до низу. Важливо пам'ятати, що Outpost Firewall Pro застосовує перше відповідне правило зі списку та ігнорує решту. Щоб змінити послідовність правил, виберіть потрібне правило та використовуйте кнопки Вгору/Вниз. Зверніть увагу, що ви маєте можливість налаштувати застосування глобальних правил брандмауера до або після застосування правил для окремих додатків, розмістивши їх у відповідній групі.

Outpost Firewall Pro надає можливість контролювати мережевий трафік, який передається через драйвери протоколів, що використовують IP протоколи, відмінні від TCP і UDP, а також транзитні пакети та інші дані, що не можуть бути контрольовані на рівні окремих додатків.

Для перегляду списку правил низького рівня натисніть Установки > Мережні правила > Системні правила та оберіть вкладку Низькорівневі правила. Додавання, зміна та видалення низькорівневих правил відбувається аналогічно до правил для додатків. Особливості управління правилами включають:

- критерії для правила включають тип IP-протоколу, напрямок, віддалену та локальну адресу;

- опція Позначити правило як Правило з високим пріоритетом дозволяє низькорівневому правилу мати перевагу над правилами додатків та глобальними правилами, які за замовчуванням мають вищий пріоритет;

Активовані правила зараз увімкнені та обробляються системою захисту. Якщо ви не хочете, щоб Outpost Firewall Pro застосовував певне правило, зніміть галочку поруч з ним, не видаляючи його повністю. Ви завжди маєте можливість знову активувати правило, встановивши галочку знову. Правила застосовуються в порядку від верху до низу. Важливо пам'ятати, що Outpost Firewall Pro застосовує перше відповідне правило зі списку та ігнорує решту.

Протокол контролю повідомлень Інтернет (Internet Control Message Protocol, ICMP) використовується для надсилання попереджувальних повідомлень та повідомлень про помилки між комп'ютерами в мережі. Outpost Firewall Pro дозволяє налаштувати типи та напрямки дозволених повідомлень ICMP. Для налаштування параметрів ICMP перейдіть до Параметри на панелі інструментів > Мережеві правила та натисніть кнопку Параметри ICMP. У діалоговому вікні Налаштування ICMP представлено список основних типів ICMP-повідомлень; Ви можете дозволити вхідні або вихідні повідомлення, встановивши відповідну галочку. Якщо галочки немає, це з'єднання блокується. Налаштування ICMPпредставлене на рис. 3.13.

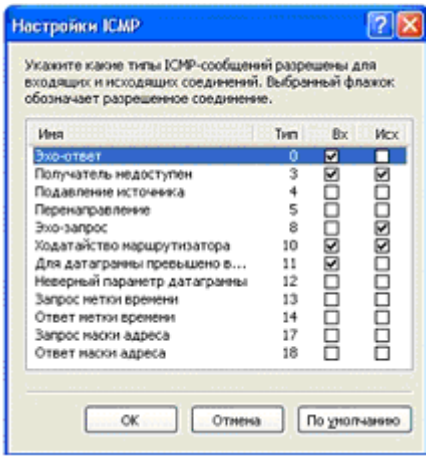

Рисунок 3.13 - Настроювання ICMP повідомлень

За допомогою Outpost Firewall Pro, окрім використання глобальних правил брандмауера та налаштувань для окремих програм, ви маєте можливість ефективно обмежувати небажаний трафік через Блокування IP. Цей інструмент дозволяє фільтрувати вхідні та вихідні інтернет-з'єднання на основі IP-адрес, надаючи досвідченим користувачам змогу детально контролювати мережеву активність свого комп'ютера шляхом блокування обраних адрес.

Цей модуль ефективно захищає від хакерів, шкідливих веб-сайтів та рекламних мереж, використовуючи чорні списки з IP-адресами, пов'язаними з такими загрозами. Ви маєте можливість створювати персоналізовані списки зловмисних IP-адрес, включаючи цілі діапазони, які ви вважаєте небезпечними, або користуватися готовими списками, доступними онлайн, без потреби вручну налаштовувати правила.

У Блокуванні IP найвищий пріоритет серед усіх механізмів обробки трафіку, перевищуючи навіть довірені програми та мережі. Це означає, що жоден додаток, включно з операційною системою, не може відправляти або отримувати дані через IP-протокол або його варіації до або з адрес, вказаних у списку блокувань.

Для активації блокування адрес, перейдіть до налаштувань Outpost Firewall Pro, оберіть вкладку Блокування IP та активуйте функцію Блокування IP. Outpost Firewall Pro не включає готових списків IP-адрес за замовчуванням, але ви можете завантажити спеціалізовані або універсальні списки з інтернету або створити власний список. Програма підтримує різноманітні формати списків. Для імпорту завантаженого списку натисніть Імпорт на вкладці Блокування IP, знайдіть файл із списком адрес і натисніть Відкрити. Список зберігатиметься у конфігурації продукту і може бути експортований або збережений як зовнішній файл разом з усіма налаштуваннями при зміні конфігурації. Для збереження списку як окремого файлу натисніть Експорт, оберіть папку для збереження та натисніть Зберегти. Для ручного додавання адреси натисніть Редагувати, введіть адресу у одному з можливих форматів, додайте коментар (щоб пам'ятати, чому ця адреса була додана) і натисніть Додати. Запис з'явиться у списку. Для видалення запису зі списку оберіть його та натисніть Видалити. Для очищення всього списку натисніть Видалити все.

Ви маєте на вибір чотири формати для введення адреси:

- доменне ім'я, наприклад, http://www.agnitum.ru. Для перетворення імені домену в IP-адресу потрібне інтернет-з'єднання. IP-адреса зберігається разом з введеним іменем домену і використовується Outpost Firewall Pro для блокування трафіку;

- IP-адреса, наприклад, 216.12.219.12;

- IP-адреса з маскою підмережі, наприклад, 216.12.219.1/216.12.219.255;

- Діапазон IP-адрес, наприклад, 203.1.254.0-203.1.254.255.

Фільтрування вхідних даних є ключовим елементом захисту через систему безпеки, служачи для моніторингу вхідних звернень та перешкоджання діям хакерів та вірусів, коли вони намагаються атакувати ваш ПК. Функція Виявлення атак ідентифікує, запобігає та інформує про будь-які потенційні напади, спрямовані на вашу систему через Інтернет або локальну мережу, до якої підключено ваш комп'ютер. Цей компонент аналізує вхідні дані, визначаючи їх легітимність, або порівнюючи хеші з відомими нападами, або проводячи аналіз поведінки. IP-адреси та інше, включаючи потенційні майбутні загрози. Для активації функції Виявлення атак, перейдіть до Установки > Виявлення атак і встановіть галочку на опції Увімкнути виявлення атак, після чого з'явиться вікно, яке демонструється на рис. 3.14.

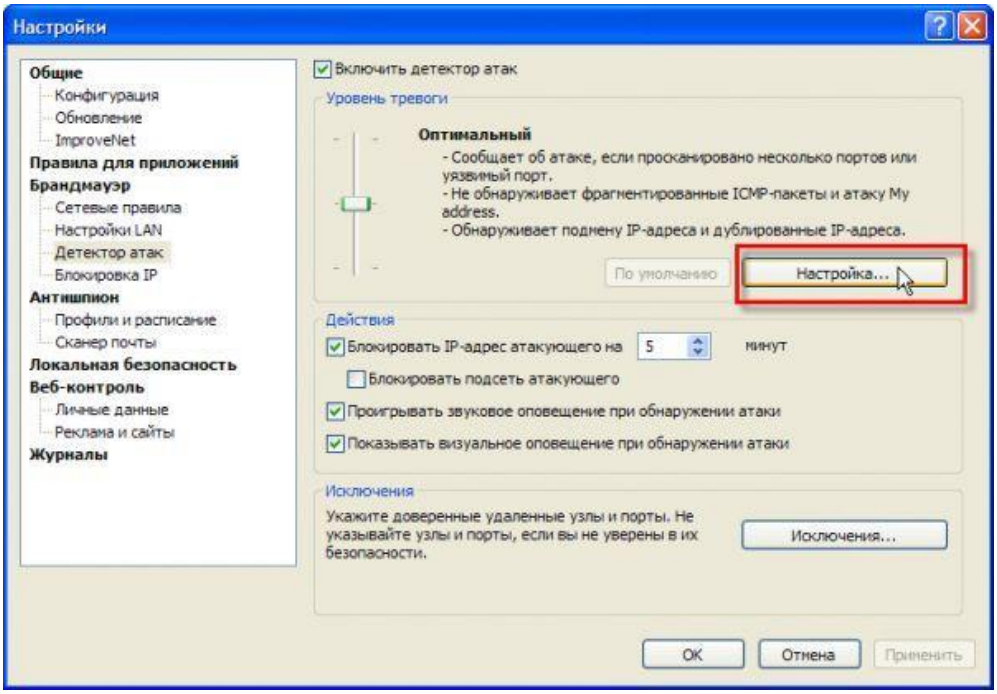

Рисунок 3.14 - Налаштування детектора атак

Встановіть бажаний рівень сповіщень Outpost Firewall Pro для реагування на атаки, обравши відповідний рівень тривоги. Цей рівень визначає, скільки підозрілих дій буде зафіксовано перед тим, як Outpost Firewall Pro сповістить про атаку:

- максимальний. Сповіщення про атаку з'являється при будь-якому скануванні портів; захист від усіх типів атак, як ззовні, так і зсередини мережі, забезпечений;

- оптимальний. Сповіщення про атаку активується при скануванні декількох портів або одного порту, який Outpost Firewall Pro вважає часто використовуваним для нападів; забезпечується захист від усіх зовнішніх атак, окрім Фрагментованих ICMP-пакетів та атак типу My address;

- низький. Сповіщення про атаку з'являється лише при кількох спробах атак типу 'Фрагментовані ICMP-пакети' та 'My address', а атаки зсередини мережі не виявляються.

Адаптуйте рівень тривоги залежно від ризику для вашого комп'ютера або встановіть максимальний рівень у разі підозр. Можливо також налаштувати індивідуальний рівень безпеки через кнопку Налаштування. Вкладка Ethernet дозволяє налаштувати параметри для Ethernet-атак, а вкладка Додатково - визначити список виявлених атак та вразливі порти для детальнішого аналізу. Після виявлення атаки Outpost Firewall Pro може автоматично адаптувати свої налаштування для захисту від майбутніх атак з тієї ж адреси. Для цього активуйте опцію Блокувати IP-адресу нападника, і всі дані з атакуючого комп'ютера будуть блоковані на вказаний час. За замовчуванням цей період становить 5 хвилин.

Також можливе блокування цілої підмережі, до якої належить атакуючий комп'ютер, за допомогою опції Блокувати підмережу нападника.

Для отримання візуальних та аудіо сповіщень про атаки активуйте відповідні параметри Програвати звукове сповіщення при виявленні атаки та Показувати візуальне сповіщення при виявленні атаки.

Під час передачі даних між комп'ютерами через мережу, відбувається відправлення ARP-запитів для визначення MAC-адреси цільового комп'ютера за його IP-адресою. У період між відправленням запиту та отриманням відповіді, дані можуть бути змінені, вкрадені або перенаправлені третім особам. Компонент Детектор атак забезпечує захист від вторгнень у локальну мережу, виявляючи та запобігаючи деяким Ethernet-атакам, таким як підробка IP-адрес (IP spoofing), ARP-сканування, ARP-флуд та інші, захищаючи вашу систему від небажаних вторгнень. Щоб налаштувати параметри для виявлення Ethernet-атак, перейдіть до Установки > Детектор атак > Настройка рис. 3.15.

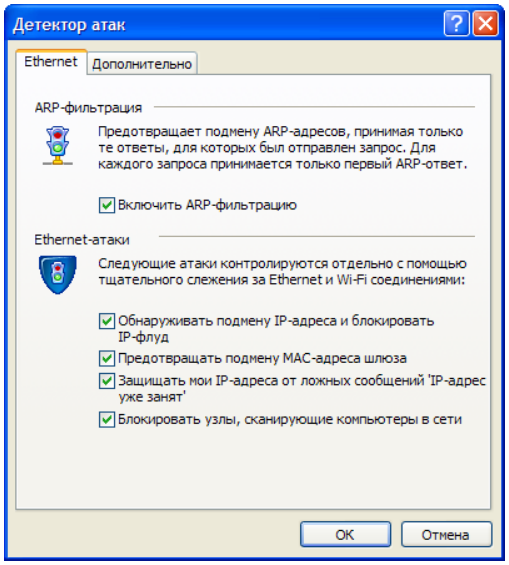

Рисунок 3.15 - Налаштування детектора атак

Налаштування включають наступні параметри:

- відключення ARP-фільтрування допомагає уникнути ARP-спуфінгу (ARP spoofing) - це коли пристрій відсилає безліч ARP-відповідей з різними MAC-адресами за короткий час, спробуючи завантажити мережеве обладнання, яке намагається встановити, яка з цих адрес дійсно належить даному пристрою. З активованою функцією, Outpost Firewall Pro прийматиме тільки ті ARP-відповіді від інших пристроїв, на які було зроблено запит раніше. Для кожного запиту приймається тільки перша ARP-відповідь. ARP-фільтрація також захищає від так званого отруєння ARP-кешу (ARP cache poisoning), що відбувається, коли хтось перехоплює Ethernet-трафік, використовуючи фальшиві ARP-відповіді, з метою замінити адресу мережевого адаптера на адресу, яку контролює нападник. Окрім того, це також запобігає ARP-флуду (ARP flood) - ситуації, коли велика кількість несправжніх ARP-відповідей надсилається на цільовий комп'ютер з метою «зависнути» систему;

- виявлення підміни IP-адрес та блокування IP-флуду Виявляє підміну IP-адрес (IP spoofing) нападника та блокує великий потік трафіку, який може завантажити комп'ютер. Цей параметр не може запобігти флуду в мережі, але може захистити комп'ютер від перевантаження;

- запобігання зміні MAC-адреси шлюзу Виявляє спроби нападника асоціювати IP-адресу мережевого адаптера шлюзу зі своєю MAC-адресою, щоб перехоплювати пакети. Зловмисник може замінити MAC-адресу на свою і перенаправити трафік на комп'ютер, який він контролює, замінюючи ARP-

відповіді, які Outpost Firewall Pro виявить та заблокує. Це дозволяє йому переглядати пакети і бачити всі передані дані. Також це дозволяє перенаправляти трафік на неіснуючі комп'ютери, спричиняючи затримки у доставці даних або відмову в обслуговуванні. Замінюючи MAC-адресу на Інтернет-шлюзі, спеціалізовані хакерські утиліти-сніфери можуть також перехоплювати трафік, включаючи чат-сесії та інші конфіденційні дані, такі як паролі, імена, адреси та навіть зашифровані файли;

- захист моїх IP-адрес від помилкових повідомлень 'IP-адреса вже використовується'. Виявляє випадки, коли два або більше комп'ютерів використовують одну і ту ж IP-адресу. Це може статися, якщо нападник намагається отримати доступ до мережевого трафіку або заблокувати комп'ютеру доступ до мережі, але також може відбуватися і легітимно, якщо провайдер використовує кілька серверів для розподілу навантаження. З активованим параметром Outpost Firewall Pro блокує ARP-відповіді з однаковими IP-адресами (але різними MAC-адресами) і таким чином захищає комп'ютер від наслідків дублювання IP-адрес;

- блокування вузлів, що сканують комп'ютери в мережі, обмежує кількість ARP-запитів, що перебирають IP-адреси, з однієї MAC-адреси за вказаний проміжок часу, що може бути скануванням локальної мережі. Деякі віруси, що масово розповсюджуються, перебирають вузли для поширення з одного комп'ютера на інший, інфікуючи їх по черзі. Цей метод також використовується сканерами мережі та аналізаторами уразливостей [8].

Елемент Outpost Firewall Pro Функція детекції атак виконує два окремі завдання: блокування атак та виявлення спроб сканування портів, які є відкритими в вашій системі до моменту атаки. Коли надходить запит на підключення (коротке повідомлення на мові комп'ютерів, що має на меті створення з'єднання через один з портів вашого комп'ютера), функція детекції атак зберігає «Запит на підключення», але для уникнення помилкових спрацювань, не розглядає одиничний віддалений компонент . вас буде попереджено про "Сканування портів" [8].

Чутливість Outpost Firewall Pro до виявлення сканувань портів (тобто кількість запитів на підключення, які спричиняють виведення повідомлення про «Сканування портів») налаштовується у вкладці Додатково (Установки >

Детектор атак > Налаштування > Додатково > Атаки), як це зображено на рис. 3.16.

Ви маєте можливість вказати, які атаки Outpost Firewall Pro повинен виявляти та блокувати. За замовчуванням, програма ідентифікує понад 25 типів атак та вторгнень, проте ви маєте можливість відключити деякі з них для зменшення використання ресурсів вашої системи або для зниження кількості помилкових або надто частих сповіщень, які можуть з'являтися, наприклад, коли довірена служба у вашій мережі була невірно розцінена як джерело атаки.

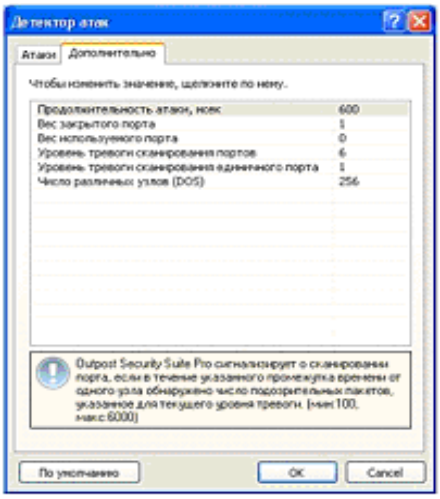

Рисунок 3.16 - Налаштування детектора атак

Щоб настроїти список здійснених атак, клацніть Установки > Детектор атак > Налаштування, а потім натисніть кнопку Атаки на вкладці Додатково, як показано на рис. 3.17.

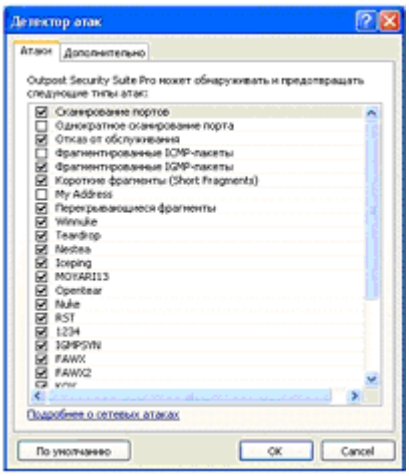

Рисунок 3.17 - Налаштування списку атак

Всі обрані види атак розпізнаються фаєрволом. Щоб відмовитися від будь-якого виду, зніміть галочку поруч з його назвою. Для повернення до стандартних налаштувань, натисніть кнопку Повернути до стандарту.

Не виключено, що у вашій мережі є комп'ютери, яким ви абсолютно довіряєте і які, на вашу думку, не можуть становити загрозу.

Ви також можете бути переконані, що деякі порти вашої системи не слугуватимуть точкою для атак. Тобто, ви вважаєте непотрібним моніторинг цих вузлів та портів і бажаєте зекономити ресурси системи, припинивши їхній моніторинг. Детектор атак надає можливість створення списків виключень, до яких можна додавати вузли та порти, моніторинг за якими ви бажаєте припинити. Щоб додати вузли, підмережі або порти до списку довірених, перейдіть до Установки > Детектор атак > Виключення.

На сторінці Вузли та мережі натисніть кнопку Додати та в діалоговому вікні Вибір адреси оберіть формат введення адреси. Надано такі опції:

- доменне ім'я. Наприклад, http://www.agnitum.com. У цьому разі необхідне з'єднання з Інтернетом, адже IP-адреси розв'язуються через Інтернет. IP-адреса зберігається разом з вказаним вами доменним ім'ям, і саме ця IP-адреса буде використовуватися Outpost Firewall Pro у більшості випадків.

IP-адреса. Наприклад, 216.12.219.12;

- підмережа (IP-адреса та маска підмережі). Наприклад, 216.12.219.1 – 216.12.219.255;

- IPv6-адреса. Наприклад, 2002::a00:1;

- макроадреса. Наприклад, LOCAL_NETWORK.

Заповніть необхідну адресу в обраному форматі, використовуючи маски за потреби, та натисніть кнопку Додати. Таким же способом можливо додати декілька адрес послідовно. Для додавання їх до списку довірених натисніть OK. Щоб вилучити адресу зі списку, оберіть її та натисніть Видалити. Якщо вам не потрібно, щоб Outpost Firewall Pro реагував на атаки з мереж, вказаних у вкладці Налаштування LAN як Довірені, зніміть галочку з пункту Виявляти атаки з довірених мереж. Для відключення функції виявлення атак з шлюзів, зніміть галочку з пункту Аналіз трафіку від шлюзів. Вкажіть усі вузли та підмережі, які ви розглядаєте як довірені, і натисніть OK для збереження налаштувань.

Оберіть вкладку TCP-порти або порти UDP, залежно від типу порту, який ви хочете додати до довіреного списку. Введіть номер порту або діапазон портів, розділяючи їх комами, або виберіть потрібний порт зі списку, клацнувши по ньому двічі для додавання у відповідне поле. Для видалення порту зі списку просто видаліть його назву або номер у текстовому полі. Після внесення всіх портів натисніть OK для збереження налаштувань.

ВИСНОВКИ

Наразі проблема інформаційної безпеки є дуже важливою не тільки для бізнесу, але й для кожної особи, що живе у сучасному суспільстві. В епоху, коли автоматизація охоплює все більше сфер нашого життя, несанкціонований доступ до інформаційних систем може призвести до непоправних наслідків. Тому важливо приділяти значну увагу захисту інформації.

Проте, ідеальний захист - це міф. Подолання захисних механізмів - лише питання ресурсів і мотивації. При створенні системи захисту важливо враховувати вартість захищеного об'єкта. Важливо також не зупинятися на досягнутому, адже те, що сьогодні здається непробивним, завтра може стати лише незначною перепоною для зловмисників.

У кваліфікаційній роботі створено систему безпеки для офісу однієї з компаній. Було детально розглянуто ключові аспекти інженерно-технічного захисту об'єкта та підвищення рівня його інформаційної безпеки. Проаналізовано телекомунікаційні системи об'єкта та проведено моніторинг основних елементів системи передачі даних. Виконано аналіз мережі для ідентифікації потенційних слабких місць у захисті передаваних даних. На основі аналізу було розроблено проект удосконаленої системи безпеки, складено план поетапного впровадження нових захисних елементів та методів для зміцнення інформаційної безпеки. Проведено вибір сучасного мережевого обладнання для створення надійної системи передачі даних. Розроблено мережеву модель з використанням ключових елементів мережі від Cisco, налаштування маршрутизаторів та створення моделі в програмі модуляції мережі – Cisco Packet Tracer.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Безпека інформаційних систем і технологій : навчальний посібник [для студентів вищих навчальних закладів, які навчаються за напрямами підготовки «Безпека інформаційних і комунікаційних систем»] / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632 с. ISBN 978-966-623-927-6

2. Безпека інформаційно-комунікаційних систем. - К.: Видавнича група BHV, 2009. — 608 с.

3. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий - Триумф. 2004. - с351.

4. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: Підручник. – К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с.

5. Волокитин А.В., Маношкин А.П., Солдатенков А.В., Савченко С.А., Петров Ю.А. Информационная безопасность государственных организаций и коммерческих фирм. Справочное пособие (под общей редакцией Реймана Л.Д.) М.: НТЦ «ФИОРД-ИНФО», 2002г.-272с.

6. Гапак О. М. Захист інформації в комп’ютерних системах: Підручник призначено для студентів інженерно-технічного факультету ДВНЗ «УжНУ» спеціальності 123-«комп’ютерна інженерія» / Ужгородський національний університет – Ужгород, 2021. – 184 с.

7. Вишняков, В. М. Захист інформації в комп'ютерних системах : навч. посібник / В. М. Вишняков ; Київ. нац. ун-т буд-ва і архіт. - Київ : КНУБА, 2022. - 119 с.

8. Погребняк А.В. Технології комп’ютерної безпеки. Монографія. МЕГУ, Рівне, 2011.-117 с

9. Остапов С.Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

10. Попов І.І., Максимов Н.В. Комп'ютерні мережі: навчальний посібник. - М.: ФОРУМ: ІНФРА - М, 2015. – 365 с.

11. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. З-38 Захист інформації в комп’ютерних системах: підручник. – Ніжин: ФОП Лук’яненко В.В., ТПК «Орхідея», 2020. – 236с.