Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: *"Розробка системи безпеки комп'ютерної мережі Тернопільскої ЗОШ №28"*

Виконав: студент (ка)
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Олександр ЮРЕЧКО
підпис (прізвище та ініціали)

Керівник *Марія Стадник*
підпис (прізвище та ініціали)

Нормоконтроль *Тарас ЛОБУР*
підпис (прізвище та ініціали)

Завідувач кафедри *Наталя ЗАГОРОДНА*
підпис (прізвище та ініціали)

Рецензент *Михайло ПЕТРИК*
підпис (прізвище та ініціали)

м. Тернопіль – 2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«23» Червня 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)
за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)
Студенту Юречку Олександру
(прізвище, ім'я, по батькові)
1. Тема роботи Розробка системи безпеки комп'ютерної мережі Тернопільської ЗОШ №28

Керівник роботи Стадник Марія Андріївна
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
Затверджені наказом ректора від « 03 » 04 2023 року № 4/7-349 .
2. Термін подання студентом завершеної роботи 22.06.2023
3. Вихідні дані до роботи Налаштовані компоненти системи для забезпечення безпеки мережі

4. Зміст роботи (перелік питань, які потрібно розробити)
Аналіз вимог та рішень до поставленого завдання.
Розгляд ефективних апаратних та програмних засобів захисту.
Моделювання та реалізація проектних рішень, налаштування маршрутиризаторів, брандмауерів, блокуваня при допомозі DNS, налаштування VPN, налаштування локальної безпеки
Безпека життєдіяльності та основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Підключення брандмауера. Схема роботи IDS. Схема роботи IPS. Схема організації контент фільтру. Схематична організація VPN з використанняс Ipsec. Принцип роботи хмарного VPN. Інтерфейс Налаштування MikroTik. Політики DNS ресуру Norton. Налаштування VPN. Налаштування ESET nod.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Пилипець М. І., д. т. н. професор.		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.02 – 19.02	*Виконано*
2.	Підбір джерел про мікропроцесори	20.02 – 27.02	*Виконано*
3.	Опрацювання джерел в галузі дослідження	28.02 – 16.03	*Виконано*
4.	Розроблення програмного коду	17.03 – 20.03	*Виконано*
5.	Тестування роботи програми та верифікація результатів	20.03 – 05.04	*Виконано*
6.	Оформлення розділу «Загальна частина»	06.03 – 17.04	*Виконано*
7.	Оформлення розділу «Розробка системи безпеки комп'ютерної мережі»	18.04 – 29.04	*Виконано*
8.	Оформлення розділу «Тестування системи від потенційних загроз»	30.04 – 13.05	*Виконано*
9.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	14.05 – 21.05	*Виконано*
10.	Оформлення кваліфікаційної роботи	22.05 – 05.06	*Виконано*
11.	Нормоконтроль	06.06 – 12.06	*Виконано*
12.	Перевірка на плагіат	10.06 – 15.06	*Виконано*
13.	Попередній захист кваліфікаційної роботи	16.06 – 19.06	*Виконано*
14.	Захист кваліфікаційної роботи	23.06.2023	

Студент _____ *Юречко О.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Стадник М.А..*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка системи безпеки комп'ютерної мережі Тернопільської ЗОШ №28 // Кваліфікаційна робота ОР «Бакалавр» // Юречко Олександр // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-41 // Тернопіль, 2023 // С. – 69 , рис. – 18, табл. – 0 , додат. – 0.

Ключові слова: ЗАХИСТ МЕРЕЖІ, БРАНДМАУЕР, VPN, MIKROTIK, НАЛАШТУВАННЯ.

Дана кваліфікаційна робота присвячена розробці системи безпеки комп'ютерної мережі Тернопільської загальноосвітньої школи №28 з метою захисту її інформаційних ресурсів та забезпечення надійності використання трафіку користувачами. Роль комп'ютерних мереж у сучасних школах надзвичайно важлива, оскільки вони забезпечують доступ до цифрових навчальних ресурсів, сприяють комунікації між учасниками навчального процесу та управлінню інформацією. Проте, разом зі зростанням використання комп'ютерних мереж збільшується ймовірність кібератак, витоку конфіденційної інформації та інших загроз безпеці.

У рамках проекту буде розроблено і впроваджено систему захисту, що включатиме налаштування брандмауера. Брандмауер є важливим елементом безпеки мережі, оскільки він контролює трафік, що входить і виходить з мережі, і визначає, які з'єднання допускаються і які блокуються. Використання брандмауера дозволить школі налаштовувати правила доступу до мережі, обмежувати певні типи трафіку (наприклад, блокувати небезпечні веб-сайти або певні порти), а також виявляти та блокувати небажаний або підозрілий мережевий трафік. Також додатковими налаштуваннями буде використання DNS серверу та налаштування VPN для певної категорії користувачів.

Проект також включатиме навчання учнів та вчителів комп’ютерної грамотності, та основам кібербезпеки.

В цілому, розробка системи безпеки комп'ютерної мережі школи є важливим кроком у забезпеченні захищеного та безпечного середовища для навчання та обміну інформацією.

ABSTRACT

Development of a security system for the computer network of Ternopil Secondary School No. 28 // Qualification work of Bachelor's degree // Yurchko Oleksandr // Ternopil Ivan Pul'uj National Technical University, Faculty of Computer and Information Systems, Department of Cybersecurity, Group SBs-41 // Ternopil, 2023 // P. - 69, fig. - 18, tab. - 0, app. - 0.

Keywords: NETWORK SECURITY, FIREWALL, VPN, MIKROTIK, CONFIGURATION.

This qualification work is dedicated to the development of a security system for the computer network of Ternopil Secondary School No. 28 aimed at protecting its information resources and ensuring reliable usage of traffic by users. The role of computer networks in modern schools is extremely important as they provide access to digital educational resources, facilitate communication among participants of the educational process, and information management. However, with the increasing use of computer networks, the likelihood of cyber attacks, confidential information leaks, and other security threats also grows.

Within the project, a protection system will be developed and implemented, which will include firewall configuration. A firewall is an essential network security component as it controls the incoming and outgoing network traffic and determines which connections are allowed and which are blocked. The use of a firewall will enable the school to configure access rules to the network, restrict certain types of traffic (e.g., blocking dangerous websites or specific ports), as well as detect and block unwanted or suspicious network traffic. Additional configurations will involve the use of a DNS server and setting up a VPN for a specific user category.

The project will also include computer literacy training for students and teachers, as well as the fundamentals of cybersecurity.

Overall, the development of the school's computer network security system is an important step in providing a secure and safe environment for learning and information exchange.

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ 10

ВСТУП 11
1 ЗАГАЛЬНА ЧАСТИНА 12
1.1 Аналіз вимог до системи захисту інформації 12
1.2 Аналіз можливих рішень поставленого завдання 12
1.2.1 Фізичний захист 13
1.2.2 Встановлення сильних паролів 14
1.2.3 Обмеження доступу до підозрілих сайтів 15
1.2.4 Резервне копіювання даних 17
1.2.5 Використання антивірусного програмного забезпечення, та систем (IDS/IPS) 18
2 ТЕОРЕТИЧНА ЧАСТИНА 19
2.1 Постановка завдання 19
2.2 Апаратні та програмні засоби захисту мережі 20
2.2.1 Служби фільтрування мережевого трафіку 20
2.2.2 Honeypot 22
2.3 Мережеві засоби інформації 28
2.3.1 Брандмауер 28
2.3.2 Системи захисту (IDS/IPS) 31
2.4 Веб фільтри 36
2.5 Віртуальні приватні мережі VPN 39
2.6 Системи виявлення та запобігання DDos-атак 45
3 РЕАЛІЗАЦІЯ ТА МОДЕЛЮВАННЯ ПРОЕКТНИХ РІШЕНЬ 48
3.1 Налаштування маршрутизатора 48
3.2 Налаштування брандмауера 51
3.3 Блокування за допомогою DNS 57
3.4 Налаштування VPN 59
3.5 Налаштування локальної безпеки 61
4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ 65
4.1. Оцінка розробленого технологічного процесу щодо умов безпеки, втомлюваності та продуктивності праці 65
4.2. Пожежна профілактика у приміщенні школи 68
ВИСНОВКИ 71
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 72

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

СКС – структурована кабельна система.

Firewall – міжмережевий екран.

ПК - персональний комп’ютер.

ОС - операційна система.

ПЗ - програмне забезпечення

ББЖ - блок безперебійного живлення

ACL - список прав доступу до об'єкта

IP (Internet Protocol) – Інтернет-протокол.

LAN (Local Area Network) – локальна мережа.

DNS (Domain Name System) - сервер доменних імен.

HTTP (Hypertext Transfer Protocol) - протокол передачі гіпертексту.

DHCP (Dynamic Host Configuration Protocol) - протокол динамічного конфігурування стеку протоколів TCP/IP робочих станцій.

NAT (Network Address Translation) – мережева трансляція адрес.

TCP/IP (Transmission Control Protocol/Internet Protocol) – протокол управління передачею/Інтернет протокол.

MAC (Media Access Control) - апаратна адреса ПК.

OSI (Open System Interface) – модель з’єднання відкритих систем.

SNMP (Simple Network Management Protocol) – протокол керування мережею.

MIME (Multipurpose Internet Mail Extension) – Багатоцільові розширення для інтернет-пошти

ВСТУП

Важною складовою сучасних навчальних закладів є безпечна комп'ютерна мережа, яка забезпечує безпечне користування ПК та інших пристроїв. Зараз існує багато способів захисту таких мереж. Серед найпоширеніших і простих методів можна виділити фізичний захист, встановлення міцних паролів, обмеження доступу до підозрілих веб-сайтів та резервне копіювання даних. Більш складні методи включають встановлення брандмауера, сегментацію мережі, налаштування системи виявлення та запобігання вторгнень (IDS/IPS), а також використання протоколів для валідації. Сучасні технології надають можливість захисту як мереж, так і окремих користувачів від зловмисників.

Наявність захищеної локальної мережі в загальноосвітній школі створює безпечне робоче середовище для користувачів завдяки налаштуванню безпеки на мережевому рівні. Захист локальної мережі дозволяє використовувати онлайн ресурси без ризику втрати або витоку персональних даних користувачів та використовувати спеціалізовані засоби та інструменти для вирішення професійних задач.

Під локальною мережею розуміється спільне підключення робочих станцій та мережевих пристроїв до єдиного каналу передачі даних. Завдяки локальним мережам та їх налаштуванням безпеки, ми отримуємо можливість безпечного одночасного використання мережевих ресурсів, таких як мережеві принтери, доступ до глобальної мережі без загрози шкідливого програмного забезпечення, а також доступ до баз даних для кількох користувачів одночасно.

1 ЗАГАЛЬНА ЧАСТИНА

1.1 Аналіз вимог до системи захисту інформації

Для розробки ефективної системи захисту інформації комп'ютерної мережі школи необхідно провести детальний аналіз вимог до безпеки даної системи. Вимоги можуть включати захист від несанкціонованого доступу, запобігання вторгнень, забезпечення конфіденційності даних, цілісності і доступності мережевих ресурсів.

Однією з основних вимог є забезпечення безпеки під час обміну інформацією між користувачами, серверами та іншими пристроями в мережі школи. Це може включати захист від шкідливих програм, фішингових атак та недобросовісних дій користувачів. Додатковою вимогою може бути забезпечення безпеки даних, яка включає їх резервне копіювання, шифрування та контроль доступу до них.

1.2 Аналіз можливих рішень поставленого завдання

У цьому розділі проводиться аналіз різних можливих рішень для забезпечення безпеки комп'ютерної мережі школи. Один з варіантів - фізичний захист, який включає контроль доступу до приміщень з серверним обладнанням та іншими цінними ресурсами. Інші варіанти включають встановлення сильних паролів, обмеження доступу до підозрілих веб-сайтів, використання антивірусного програмного забезпечення та систем виявлення та запобігання вторгнень (IDS/IPS).

Під час аналізу рішень варто врахувати їх ефективність, складність впровадження, вартість та зручність в користуванні. Важливо забезпечити баланс між безпекою і зручністю використання системи для користувачів.

На основі проведеного аналізу вимог і розглянутих можливих рішень буде розроблена система захисту інформації для комп'ютерної мережі школи, яка

відповідатиме потребам безпеки та забезпечить безпечне користування ПК та інших пристроїв в школі. Результати цього аналізу будуть використані для визначення оптимального набору заходів забезпечення безпеки, які будуть впроваджені в системі комп'ютерної мережі.

1.2.1 Фізичний захист

Фізичний захист є невід'ємною складовою ефективної системи захисту інформації комп'ютерної мережі школи. Він має на меті забезпечення безпеки фізичних ресурсів, таких як сервери, мережеві комутатори, маршрутизатори та інші важливі об'єкти, що забезпечують нормальне функціонування мережі.

Один з найважливіших аспектів фізичного захисту полягає в контролі та обмеженні доступу до приміщень, де розташовані серверні кімнати та інші цінні об'єкти. Для досягнення цієї мети використовуються спеціальні системи контролю доступу, такі як:

- Карткові читачі.
- біометричні пристрої.
- електронні замки.

Ці системи дозволяють обмежити доступ до серверних приміщень лише авторизованим особам, що ефективно запобігає несанкціонованому доступу та підвищує рівень безпеки.

Окрім контролю доступу, необхідно також забезпечити фізичну безпеку самого обладнання. З цією метою використовуються спеціальні стійки або шафи, які мають міцну конструкцію та механізми запобігання несанкціонованому доступу. Вони можуть бути оснащені замками або кодовими замками для додаткового забезпечення. Це дозволяє зберігати сервери та мережеве обладнання у безпечному середовищі і запобігати фізичному доступу неавторизованих осіб.

Додатковою складовою фізичного захисту є безпека кабелів, які з'єднують сервери, комутатори та інші пристрої в мережі. Ці кабелі можуть бути легко

пошкоджені або перервані, що може призвести до втрати зв'язку та недоступності мережі. Для запобігання цьому застосовуються спеціальні металеві труби або кабель-канали, які забезпечують захист кабелів від фізичних пошкоджень. Такі труби можуть бути вбудовані в стіни та підлоги, що забезпечує додатковий рівень безпеки та надійності мережі.

Фізичний захист також включає заходи щодо забезпечення електропостачання та вентиляції серверних приміщень. Блок безперебійного живлення (UPS) та резервне джерело електроенергії гарантують неперервну роботу серверу навіть у разі виникнення перебоїв в електропостачанні. Ефективна система вентиляції та охолодження допомагає підтримувати оптимальну температуру та вологість в серверних приміщеннях, що сприяє нормальному функціонуванню обладнання та запобігає його перегріву.

Фізичний захист є необхідною складовою безпеки комп'ютерної мережі школи, оскільки він забезпечує захист фізичних ресурсів та запобігає несанкціонованому доступу до них. Комбінація фізичного захисту разом з іншими заходами безпеки, такими як мережеві файрволи, антивірусне програмне забезпечення та системи виявлення вторгнень, створює надійну та комплексну систему захисту інформації, що відповідає потребам безпеки та забезпечує безпечне користування ПК та інших пристроїв у мережі школи.

1.2.2 Встановлення сильних паролів

Використання сильних паролів є важливим аспектом безпеки комп'ютерної мережі. Пароль є першою лінією оборони проти несанкціонованого доступу до системи і інформації, тому важливо приділяти належну увагу політиці стосовно паролів при розробці системи захисту інформації.

При встановленні політики паролів рекомендується вимагати від користувачів використовувати складні паролі, що складаються з комбінації великих і малих літер, цифр та спеціальних символів. Складний пароль повинен бути достатньо довгим і випадковим, що ускладнює його вгадування або підбір

шляхом перебору. Наприклад, пароль може містити більш ніж 8 символів і включати комбінацію букв верхнього і нижнього регістрів, цифр та спеціальних символів, таких як символи пунктуації.

Крім вимог до складності паролів, також необхідно забезпечити регулярну зміну паролів. Часта зміна паролів допомагає запобігти його викраденню або використанню недобросовісними особами. Рекомендується встановити періодичність зміни паролів, наприклад, раз на 3-6 місяців, а також заборонити використання попередніх паролів для певного періоду часу.

Додатковою вимогою є недопущення використання одного пароля для різних систем або облікових записів. Кожен обліковий запис повинен мати унікальний пароль, що знижує ризик масового порушення безпеки у разі компрометації одного пароля. Для досягнення цієї мети можна використовувати систему керування паролями, яка дозволяє зберігати та керувати паролями для різних систем і облікових записів.

Встановлення політики стосовно паролів є важливим кроком у забезпеченні безпеки комп'ютерної мережі школи. Відповідно до цієї політики, користувачі будуть зобов'язані створювати та використовувати сильні паролі, змінювати їх періодично та уникають використання одного пароля для різних систем або облікових записів. Це сприятиме підвищенню рівня безпеки мережі та захисту конфіденційної інформації в шкільній системі.

1.2.3 Обмеження доступу до підозрілих сайтів

Обмеження доступу до підозрілих або потенційно небезпечних веб-сайтів може використовуватись для запобігання вхідним загрозам інформаційної безпеки. Це можна досягти за допомогою фільтрації веб-трафіку або використанням програмного забезпечення, яке аналізує сайти на наявність шкідливого змісту або потенційно небезпечних елементів.

Запровадження політики використання сильних паролів є необхідним етапом в розробці системи захисту інформації комп'ютерної мережі школи. Для

досягнення цієї мети, необхідно встановити вимоги до паролів, які включатимуть в себе використання різноманітних символів, таких як великі і малі літери, цифри та спеціальні символи. Наприклад, пароль може складатись з комбінації великих та малих літер, цифр та спеціальних символів, і мати мінімальну довжину.

Крім того, для забезпечення безпеки системи важливо встановити політику щодо регулярної зміни паролів. Це може включати вимогу зміни пароля через певний період часу, наприклад, кожні 60 днів. Також необхідно недопустити використання одного пароля для різних систем або облікових записів, оскільки це може створити вразливість у системі.

При обмеженні доступу до підозрілих або потенційно небезпечних веб-сайтів можна використовувати різні підходи. Один з підходів - це фільтрація веб-трафіку, що передбачає використання спеціального програмного забезпечення, яке аналізує URL-адреси веб-сайтів і блокує доступ до тих, які вважаються підозрілими або небезпечними. Це програмне забезпечення може використовувати базу даних відомих шкідливих сайтів або використовувати алгоритми аналізу вмісту сторінок для виявлення потенційно шкідливого змісту.

Ще одним підходом є використання спеціалізованого антивірусного програмного забезпечення, яке може перевіряти веб-сайти на наявність шкідливого змісту. Це дозволяє виявляти й блокувати доступ до сайтів, які можуть містити віруси, троянські програми або інші шкідливі елементи. Таке програмне забезпечення може працювати на рівні клієнта або на рівні сервера.

Запровадження обмежень доступу до підозрілих або потенційно небезпечних веб-сайтів є важливим кроком у забезпеченні безпеки комп'ютерної мережі школи. Це допомагає запобігати вхідним загрозам, зберігати цілісність та конфіденційність даних, а також захищати користувачів від шкідливих програм та атак. Комбінація фільтрації веб-трафіку та використання антивірусного програмного забезпечення створює надійний шар захисту, що доповнюється іншими технічними і організаційними заходами безпеки.

1.2.4 Резервне копіювання даних

Резервне копіювання даних є невід'ємною складовою безпеки інформації в комп'ютерній мережі. Цей процес передбачає створення додаткових копій даних, що дозволяють відновити інформацію в разі її втрати, пошкодження або несправності системи. Резервне копіювання є важливим засобом захисту від незапланованих подій, таких як технічні помилки, хакерські атаки, випадкові видалення файлів або природні катастрофи.

При розробці системи захисту інформації необхідно врахувати резервне копіювання даних і встановити ефективну стратегію для його здійснення. Існує декілька підходів до резервного копіювання, включаючи використання зовнішніх носіїв даних, хмарні сервіси та спеціалізоване програмне забезпечення для автоматичного резервного копіювання.

Один з підходів - це використання зовнішніх носіїв даних, таких як вінчестери, флеш-накопичувачі або жорсткі диски, для створення резервних копій інформації. Ці носії можуть бути підключені до комп'ютерної системи і періодично зберігати копії важливих файлів та даних. Однак, цей підхід може вимагати ручного копіювання і збереження даних, що може бути часом затратно.

Іншим підходом є використання хмарних сервісів для збереження резервних копій даних. Хмарні сервіси надають можливість зберігати дані на віддалених серверах через Інтернет. Це забезпечує доступ до резервних копій з будь-якого місця та забезпечує високий рівень надійності, оскільки дані резервної копії розміщуються на кількох серверах з реплікацією. Хмарні сервіси також можуть пропонувати автоматичне резервне копіювання за заданою графіком, що забезпечує зручність та безперервність процесу.

Також можна використовувати спеціалізоване програмне забезпечення для автоматичного резервного копіювання. Ці програми дозволяють налаштувати параметри резервного копіювання, включаючи розклади, типи даних, які потрібно копіювати, та засоби збереження. Вони здатні автоматично виконувати

резервне копіювання в задані часи або після виявлення змін у системі, що дозволяє забезпечити постійну актуалізацію резервних копій.

Вибір методу резервного копіювання залежить від специфіки мережевої інфраструктури, обсягу даних, доступності ресурсів та вимог до часу відновлення інформації. Незалежно від вибраного методу, важливо встановити регулярний графік резервного копіювання, перевіряти цілісність і доступність резервних копій та зберігати їх у безпечному місці, що забезпечить ефективну відновлення даних у разі потреби.

1.2.5 Використання антивірусного програмного забезпечення, та систем (IDS/IPS)

Використання антивірусного програмного забезпечення та систем виявлення та запобігання вторгнень (IDS/IPS) є важливими аспектами безпеки комп'ютерної мережі.

Антивірусне програмне забезпечення допомагає виявляти та усувати шкідливе програмне забезпечення, а системи IDS/IPS виявляють та блокують вторгнення в мережу, сповіщаючи адміністраторів про потенційні загрози.

Після ретельного аналізу різних можливих рішень забезпечення безпеки, буде обрано оптимальні заходи забезпечення безпеки для комп'ютерної мережі школи, які відповідатимуть вимогам безпеки та забезпечать безпечне користування ПК та інших пристроїв. Результати аналізу вимог та розглянутих рішень будуть використані для розробки подальших розділів кваліфікаційної роботи.

2 ТЕОРЕТИЧНА ЧАСТИНА

2.1 Постановка завдання

Отже основним завданням роботи є розробка системи безпеки Тернопільської загальноосвітньої школи №28 для захисту даних та забезпечення стійкості роботи системи, в якому присутня реалізація використання firewall та технологія (IDS/IPS), встановлення антивірусного програмного забезпечення та проведення подальшого аналізу системи.

Реалізація програмного середовища для захисту даних школи повинна задовольняти наступні вимоги:

- Забезпечення конфіденційної інформації авторизованих користувачів.
- Забезпечення цілісності інформації яка передається мережею.
- Безперебійне функціонування мережі для авторизованих користувачів у будь-який час.
- Аутентифікація користувачів.
- Авторизація користувачів.
- Забезпечення реєстрування та аналізування подій що стосуються безпеки мережі.
- Забезпечення захисту від вторгнень.

Ці вимоги є основними складовими елементами системи захисту інформації для комп'ютерної мережі школи. У наступних підрозділах цього розділу будуть розглянуті деталі розробки моделі безпеки, що включатиме у себе політики та засоби безпеки, необхідні для задоволення цих вимог.

2.2 Апаратні та програмні засоби захисту мережі

Засоби захисту інформації складаються з різноманітних пристроїв, пристосувань, приладів, технічних систем і інших виробів, які використовуються для вирішення різних завдань, пов'язаних із захистом інформації.

Технічні (апаратні) засоби захисту інформації є різноманітними пристроями, що функціонують на рівні обладнання і вирішують завдання, пов'язані з захистом інформації.

Існує кілька програмних технологій, що можуть використовуватись для захисту даних навчального закладу:

- Служби фільтрування контенту.
- Honeypot.

2.2.1 Служби фільтрування мережевого трафіку

Фільтрація трафіку є популярною технологією, яку використовують різні інструменти та системи для захисту від різноманітних загроз і небажаного використання мережевих ресурсів. Вона застосовується антивірусами, фільтрами спаму, засобами захисту від несанкціонованого доступу та системами захисту від витоків.

На сьогоднішній день, у більшості мереж широко застосовується контентна фільтрація яка забезпечує інформаційну безпеку не тільки у сучасних мережах а й у інших проектних рішеннях. Впровадження інтернет-фільтрації суттєво підвищує рівень безпеки внутрішньої мережі, оскільки це дає можливість контролювати завантаження та блокувати доступ до непотрібних зловмисних ресурсів. Крім того, фільтруючи контент можна встановлювати блокування доступу до веб-сайтів які потенційно є не потрібні для роботи. (рис.).

В загальності існує два варіанти фільтрування мережевого контентного трафіку:

- Фільтрування даних веб-контенту.
- Фільтрування даних електронних скриньок.

Обумовлено це тим, тому що основними каналами які доставляють контент безпосередньому користувачу є саме вони.

Варто зазначити, чим саме відрізняються фільтр контент від фільтру антивірусного. Відрізняються вони тим що функціонал контент-фільтру спрямований безпосередньо на роботу з інформацією, яка призначена для кінцевого користувача системи. Він працює з контентом, що міститься в електронних листах або на веб-сторінках, і виконує фільтрацію засновану на змісті інформації, а не на кодах файлів, як у випадку з антивірусним фільтром.

Основних прикладів завданнь контент-фільтра може бути неймовірно багато. Тому завдання які виконують основну функцію, блокування повідомлення або сторінки представлені далі:

- Складання чорного і білого списків веб-сторінок - це один з способів фільтрації контенту. У разі, коли категоріальний фільтр є недостатнім або коли сайт помилково віднесений до неправильної категорії, адміністратор може скласти списки заборонених або дозволених сайтів.
- Антиспам - це найпоширеніший модуль контент-фільтра. За його існування розробниками рішень інформаційної безпеки задля боротьби зі спамом, було розроблено в рази складніші технології. В основі антиспамового модуля лежить використання заданого алгоритму, який на базі отриманих електронних повідомлень оцінює їх за певними параметрами, щоб визначити, чи є вони спамом за там чи є вони корисними для користувача.
- Блокування веб-сторінок за словами або фразами які були використані. Цей механізм дозволяє адміністратору вказувати слова або фрази які потенційно були заборонені. Якщо повідомлення містить такі слова, система вживає відповідних заходів, наприклад, блокує доставку або видаляє повідомлення. Таким же методом система розпізнає намагання користувача

відкрити веб-сайт з забороненим вмістом, зокрема також з забороненими словами, і одразу ж блокує до нього доступ.

- Блокування різного роду та формату файлів, які вкладені в повідомлення або які були завантажені з посторонніх веб-ресурсів, за критеріями їх назви та розширення. Адміністратор має можливість вказати певну частину назви файлу або його розширення, за якими буде відбувається розпізнавання та блокування. Для прикладу можна узяти такі розширення, як .com і .exe, багато контентних фільтрів блокують файли з певними розширеннями на різних ресурсях, оскільки це найпростіший та найпоширеніший спосіб завантаження на комп'ютер вірус.
- Блокування повідомлень та файлів з різних сайтів, які відрізняються за форматом. Є певний список форматів, якими користуються зловмисники для надсилання такого роду повідомлень які відносяться до підозрілих. Для прикладу, це можуть продубльовані розширення файлів (.exe.exe), некоректні типи MIME тобто Багатоцільові розширення для інтернет-пошти, файли архіви та інше [1].

2.2.2 Honeypot

Honeypot – це комп'ютерна система, яка створена для того, щоб заманити кіберзлочинців, а також виявляти, відхиляти або вивчати спроби отримати несанкціонований доступ до інформаційних систем. [2] З метою збору інформації про дані мережі, зловмисники намагаються атакувати спеціально створену пастку, розроблену фахівцями. В свою чергу, фахівці використовують цю можливість, щоб викрити дії зловмисників.

Пастка являє собою комп'ютерну систему з застосунками та інформаційними даними, і злочинці приймають її за справжню ціль,на яку вони сподіваються. Наприклад, клієнтам компанії може бути надана Honeypot, що імітує систему для виставлення рахунків. Цей вид пастки є популярною ціллю для кіберзлочинців, які намагаються отримати номера кредитних карт. Можна

спостерігати за хакерами, які потрапили у такі пасти, для того щоб від слідкувати їхні дії та розробити більш ефективних захисних методів для справжніх систем.

Часто такі пости роблять доволі простими, щоб зловмисникам було легше обійти захист та попастися, тай метод є більш привабливим для зловмисників ніж взламувати великий код захисту. Наприклад, одним із таких пасток є використання портів, які можна виявити через сканування, а також використання ненадійних паролів. Часто фахівці залишають вразливі порти відкритими, тим самим збільшуючи ймовірність, що приманка спрацює і зловмисник буде відвернений від реальних меж, які є надійно захищеними.

Пастка не є антивірусом або мережевим екраном, вона точно не призначена для вирішення справжніх, конкретних проблем з безпекою. Вона скоріше виступає як інструмент інформаційної безпеки, який спрямований на їх визначення або ж наявних проблем з безпекою. Також паска призначена для того щоб виявляти нові види потенційних загроз. Зібрані дані дозволяють пріоритезувати проблеми та ефективно розподілити ресурси інформації.

Для виявлення загроз використовують різні види кіберпасток . Їх можливості залежать від того яка загроза присутня та з якою ціллю вона була створена. Кожна пастка виконує свою своєрідну роль в стратегії усунення кібербезпеки.

Один із різновидів Honeypot є Поштові пастки, відомі також як спам-пастки, їхній принцип у прихованні місця розташування підробленої електронної адреси, та лише для збирачів які автоматично отримують ці адреси. Завдяки фальшивості цієї адреси, ми можемо бути абсолютно впевнені, що абсолютно усі листи, надісланий на цю адресу, є спамом. Усі отримані повідомлення таким методом в пастку можна одразу ж заблокувати, а IP-адресу відправника відповідно додавати до чорного списку.

Приманка використовується для моніторингу уразливих програмних засобів та виявлення атак, які використовують ненадійну архітектуру систем або методи SQL-ін'єкції, які зловживають SQL-сервісами або привілеями.

Шкідлива програмна пастка імітує додатки та API, що надихають атаки шкідливих програм. Програми які власне атакують передаються одразу для аналізу та ефективної розробки захисту мережі або системи усунення дір у системі.

Приманка для пошукових роботів, таких як "павуки", приваблює шахраїв шляхом створення веб-сторінок і покликань, доступних лише для цих роботів. Крім того, пастка для пошукових роботів надає можливість:

- Зібрати інформацію про поведінку та характеристики пошукових роботів, таких як їхні агенти користувача, протоколи, які вони використовують, і частота їхніх запитів.
- Виявити недозволені дії від пошукових роботів, такі як надмірне сканування або спроби отримати незаконний доступ до вмісту.
- Встановити обмеження на доступ пошукових роботів до певних частин веб-сайту або ресурсів.
- Перевірити відповідність пошукових роботів відповідним стандартам і протоколам.
- Виявити і блокувати спамові або шкідливі пошукові роботи, які можуть завдати шкоди веб-сайту або збирати недозволену інформацію.

Усе це сприяє покращенню безпеки сайту та оптимізації його взаємодії з пошуковими системами, забезпечуючи належний контроль і захист від шкідливих або небажаних пошукових ботів.

Аналізуючи трафік, що надходить до пастки, можна здійснити наступні дії:

- Визначити місцезнаходження кіберзлочинців.
- Оцінити ступінь загрози.
- Вивчити методи, використовувані зловмисниками.
- Дізнатися, які дані або програми цікавлять злочинців.
- Оцінити ефективність заходів захисту від кібератак.

Кібернетичні пастки є спеціальними "скриптами", подібними до макросів, які створені хакером і автоматично активуються безсвідомими діями персоналу служби технічного обслуговування, такими як перемикання, увімкнення або

вимкнення прихованого зловмисного програмного забезпечення. Хакер стратегічно планує дії обслуговуючого персоналу, з метою забезпечення тривалості кібер-фізичної атаки навіть після того, як хакер втратить доступ до вразливостей системи. Наприклад, якщо процедури відновлення на сервері, який був скомпрометований, відомі хакерам, вони можуть використати ці процедури проти нашої організації.

Кіберпастки поділяються на:

- Низько інтерактивні.
- високо інтерактивні.

Низько інтерактивні пастки – вимагають менше ресурсів та збирають базову інформацію про рівень загрози, тип загрози та її джерело. Для їх установки зазвичай потрібні мережеві служби та моделювання TCP- і IP-протоколи. Однак така система не затримає злочинця на довгий час та не дозволяє детально вивчити його звички або складні загрози. Якщо ж системі потрібно знайти більш кращий спосіб вивчити дії зловмисників, тоді використовують високо інтерактивні пастки.

Високо інтерактивні пастки – це системи, які змушують зловмисників витратити значно більше часу на пошкодження даних. Володіючи такою хитрою пасткою можна надовго змусити зловмисника застрягнути в базах системи, отож у фахівців буде більше часу, щоб розібратися у намірах зловмисника, відстежити де конкретно хакери можуть знайти конфіденційну інформацію, а також можна буде дізнатися цілі та конкретні методи пошкодження. Завдяки проробленню такої роботи можна буде знайти всі «прогалини» та зробити кращу безпеку будь-яких даних, також це підвищить рівень захисту, після чого випадок компрометації системи буде зведений практично до 0.

Низько інтерактивна та високо інтерактивна пастки також мають своє пряме призначення, кожну з них використовують для виявлення проблем з безпекою, але низько інтерактивну беруть тоді, коли потрібно надати базову інформацію про загрозу , а високо інтерактивна доповнює ці відомості ще

намірами та методи, які використовують злочинці, а також про будь які уразливості, які вони використовують, для проникнення у систему.

Ціллю хакерів є серйозне нанесення шкоди критичним системам, і для досягнення цієї мети вони використовують дуже складні шкідливі програми. Важливо розуміти, що ці хакери активно вдосконалюють свої методи і використовують продумані техніки для злому систем. Вони можуть експлуатувати вразливості в програмному забезпеченні, використовувати хитрі механізми обходу захисту і навіть створювати нові типи атак. Усвідомлення складності цих шкідливих програм допоможе зрозуміти, що боротьба з кіберзлочинцями вимагає постійного вдосконалення захисних заходів та пильного моніторингу мереж і систем безпеки.

Система аналізу загроз, яка використовує кіберпастки, допомагає компаніям ефективно розподіляти ресурси і виявляти уразливості в їхніх інформаційних системах. Використання кіберпасток має кілька переваг:

По-перше, це надійний метод виявлення вразливостей у важливих системах. Наприклад, пастка може продемонструвати, наскільки небезпечні можуть бути атаки на пристрої Інтернету речей і надати рекомендації щодо посилення захисту.

Існує кілька причин використовувати кіберпастки замість спроб виявити атаки на реальні системи. По-перше, кіберпастки завжди є несправжньою активністю - будь-які зафіксовані дії є спробою проникнення або злому системи. Таким чином, можна легко виявити характеристики атак, такі як подібність або походження з однієї країни, IP-адреси, що свідчать про проникнення в мережу. Ці ознаки атак можуть бути втрачені в масивному потоці нормального трафіку в реальній мережі. Крім того, кіберпастки споживають дуже мало ресурсів і трафіку, і для їхньої роботи не потрібне потужне обладнання.

Крім того, використання кіберпасток мінімізує кількість помилкових виявлень. Це дозволяє зосередити зусилля на вирішенні реальних проблем і не витрачати ресурси марно. Додатково, шляхом порівняння даних, зібраних кіберпастками, з журнальними даними системи і мережевим екраном, можна

налаштувати систему виявлення вторгнень (IDS) для пошуку найбільш актуальних загроз і зменшення кількості помилкових виявлень. Таким чином, кіберпастки сприяють вдосконаленню інших систем кібербезпеки.

Крім того, кіберпастки дозволяють отримати детальне уявлення про розвиток загроз, вектори атак, експлойти і шкідливі програми, а також про спамерів і фішингові кампанії, якщо використовуються пастки для спаму. У той же час, коли злочинці постійно вдосконалюють свої методи, кіберпастки допомагають виявляти нові загрози і формувати знання про них. Ефективне використання кіберпасток дозволяє усунути сліпі зони в системі кібербезпеки.

Також, такі системи є чудовим засобом тренування для співробітників відділу інформаційної безпеки, які можуть безпечно вивчати методи хакерів, шахраїв і різні типи загроз в контрольованому середовищі. Це дозволяє їм повністю сконцентруватися на атаках, не відволікаючись на реальні фактори.

Майстерність розміщення кібер-пастки полягає у вмінні використовувати природну поведінку людей, враховуючи знання соціальної психології. Це означає використання таких факторів, як звички, цікавість або допитливість, а також розуміння стандартних дій обслуговуючого персоналу, що можуть здатися простим вирішенням складної проблеми.

Хакери вивчають людську поведінку та використовують її для підманювання персоналу в пастку. Вони можуть створювати ситуації, які викликають в людей цікавість або натякують на можливість отримати швидке і просте рішення. Наприклад, це може бути надання фальшивої інформації, яка виглядає як вирішення проблеми, але насправді викликає запуск шкідливої програми або розкриває доступ до системи.

Розуміння того, як хакери використовують соціальну психологію та викликають довіру та недбалість, допомагає підвищити обізнаність персоналу і підготувати їх до виявлення та уникнення кібер-пасток. Додатково, освіта щодо безпеки та навчання персоналу щодо стандартних процедур безпеки можуть збільшити стійкість систем до цих видів атак.

2.3 Мережеві засоби інформації

Мережеві засоби інформації - це технологічні рішення, програми та пристрої, які використовуються для забезпечення передачі, обміну, зберігання та обробки інформації в комп'ютерних мережах. Вони дозволяють забезпечити ефективну та безпечну роботу мережі, забезпечують комунікацію між різними вузлами мережі та забезпечують доступ до інформаційних ресурсів.

До мережевих засобів інформації відносяться такі компоненти:

- Мережеве обладнання: це фізичні пристрої, такі як маршрутизатори, комутатори, маршрутизатори-брандмауери, хаби, мости та інші, які забезпечують з'єднання та комутацію мережевого трафіку.
- Сервери: це потужні комп'ютери, які забезпечують централізовану обробку даних та розподілення ресурсів мережі, таких як файли, друк, бази даних, електронна пошта тощо.

Мережеве програмне забезпечення: це програми та протоколи, які забезпечують керування, безпеку, маршрутизацію, комунікацію та інші функції в мережевому середовищі. До такого програмного забезпечення відносяться операційні системи для серверів та мережевих пристроїв, програми керування мережею, програми безпеки мережі тощо.

Системи зберігання даних: це пристрої та програми, які використовуються для зберігання і управління даними в мережевих середовищах, такі як файлові сервери, сховища даних (NAS), системи управління базами даних та інші.

Мережеві заходи безпеки: це засоби та програми, які захищають мережу.

2.3.1 Брандмауер

Брандмауер або firewall - це міжмережевий екран, який послідовно фільтрує дані, що протікають через нього. Він аналізує трафік згідно з певними правилами або шаблонами, які застосовуються до мережі або комп'ютера

користувача. У разі невдалої перевірки пакету, брандмауер перешкоджає його проходженню і забороняє доступ до Інтернету для пристрою користувача.

Брандмауери використовуються для розділення мереж з різними вимогами до безпеки, наприклад, Інтернету та внутрішньої мережі, в якій знаходяться сервери зі значущою інформацією. Організації повинні використовувати брандмауери там, де їх внутрішні мережі та системи взаємодіють з зовнішніми мережами та системами, а також там, де вимоги до безпеки відрізняються серед їх внутрішніх мереж. Цей розділ призначений для допомоги організаціям у визначенні місць розташування брандмауерів та мереж і систем у відношенні до брандмауерів.

Оскільки однією з основних функцій брандмауера є запобігання небажаному трафіку увійти в мережу (і, у деяких випадках, вийти з неї), брандмауери повинні розташовуватись на межі логічних мережевих меж. Зазвичай це означає, що брандмауери розташовуються або як вузол, де мережа розгалужується на кілька шляхів, або в лінії вздовж одного шляху.

Основні види атак від яких захищає брандмауер:

- Фішинг.
- Доступ через Back door.
- Злам з використанням віддаленого робочого столу.
- Переадресація пакетів.
- DDoS-атаки.

У маршрутизованих мережах брандмауер зазвичай розташовується безпосередньо на мережі неподалік від входу трафіку в роутер (місце входу), і іноді він співпрацює з роутером. Рідко розташовують брандмауер для багатошляхового вузла після роутера, оскільки пристрій брандмауера мусив би спостерігати за кожним з кількох вихідних шляхів, які зазвичай існують у таких ситуаціях.

Більшість пристроїв апаратного брандмауера мають можливості роутера, а в комутованих мережах брандмауер часто є частиною самого комутатора, щоб забезпечити захист якомога більшої кількості сегментів комутатора.

Виробники брандмауерів часто використовують різні терміни для логічного потоку трафіку брандмауера. Брандмауер приймає трафік, який не пройшов перевірку, перевіряє його відповідно до політики брандмауера і діє згідно з цим (наприклад, передає трафік, блокує його, передає з деякими змінами).

Оскільки весь трафік в мережі має напрямок, політики ґрунтуються на напрямку руху трафіку. З метою цього документа трафік, який ще не пройшов перевірку, йде з "незахищеної сторони" брандмауера і рухається до "захищеної сторони". Деякі брандмауери перевіряють трафік у обох напрямках, наприклад, якщо вони налаштовані для запобігання певному трафіку з локальної мережі організації до Інтернету. У таких випадках захищена сторона брандмауера є та, що спрямована на зовнішню мережу.[1]

Існують різні види брандмауерів, вони бувають:

- програмними (Software).
- програмно-апаратними (програмне забезпечення (ПЗ) і відповідно пристрій, на якому функціонує брандмауер).

Перші типи брандмауерів є більш доступними і придатними для використання звичайними користувачами. Вони вимагають лише обмежених ресурсів комп'ютера і можуть задовольнити потреби звичайного користувача. З іншого боку, другі типи брандмауерів, зазвичай, застосовуються в корпоративних середовищах з великими мережами і високими вимогами до безпеки. Ці рішення мають більший функціонал та надійність, але вони вимагають великих ресурсів та інфраструктури для ефективної роботи.

Задля захисту несанкціонованого доступу брандмауер налаштовується безпосередньо на маршрутизаторі між мережею загального користування та між мережею закладу освіти. При цьому увесь трафік проходить тільки через міжмережевий екран (Рис. 2.1)

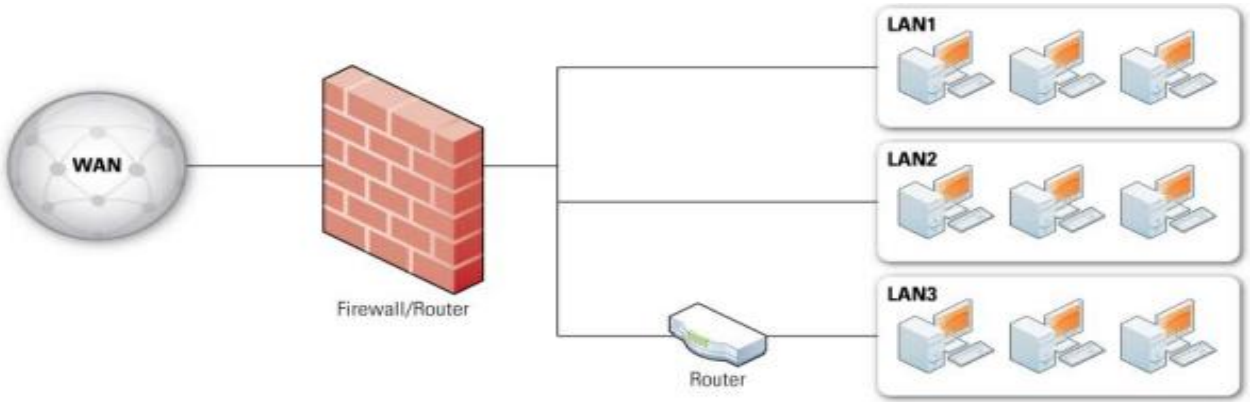

Рисунок 2.1 - Приклад підключення брандмауера у локальній мережі

Брандмауер, який підключений до всіх пристроїв локальної мережі, виконує такі основні завдання:

- Обмеження доступу зовнішніх засобів до пристроїв локальної мережі.
- Задачу розділення доступу користувачів внутрішньої мережі до зовнішніх інтернет ресурсів. [2]

2.3.2 Системи захисту (IDS/IPS)

Системи виявлення та запобігання вторгненням (IDS/IPS), являються надзвичайно потрібним компонентом для захисту мереж від атак зловмисників. Головна мета цих систем полягає у виявленні незаконного доступу до корпоративної мережі або незатвердженого керування нею, а також у вжитті відповідних заходів для запобігання таким вторгненням (наприклад, повідомлення адміністраторів про вторгнення, заборона з'єднання або налаштування брандмауера для блокування подальших дій зловмисника тощо).

IDS виявляє незвичайну або підозрілу активність у мережі, аналізує її і сповіщає адміністратора про потенційну загрозу. Він моніторить мережевий трафік, досліджує події та виявляє аномальну поведінку або підозрілі шаблони.

Коли виявляється вторгнення, IDS сповіщає адміністратора, щоб той міг прийняти відповідні заходи.

IPS, у свою чергу, забезпечує активний захист, перешкоджаючи атакам у реальному часі. Він може вживати додаткові заходи для блокування небезпечного трафіку або атакувати вторгнення, перенастроюючи брандмауер чи обриваючи з'єднання зловмисника.

Система IPS (Intrusion Prevention System) призначена для запобігання атак і є важливою складовою сучасних мережевих інфраструктур, забезпечуючи надійний рівень безпеки. Разом з IDS (Intrusion Detection System), вони утворюють комплексний захист мережі, виявляючи потенційні загрози та приймаючи необхідні заходи для їх усунення.

Основна функція системи IPS полягає в активному запобіганні атакам у реальному часі. Вона виявляє шкідливий трафік, зловмисні поведінкові шаблони або небезпечні вразливості в мережі та вживає автоматичних заходів для блокування чи мінімізації ризику. Це може включати заборону певних видів трафіку, перенастроювання брандмауерів, автоматичну блокування підозрілих IP-адрес або розірвання з'єднання зловмисника.

Завдяки використанню системи IPS, мережа отримує високий рівень захисту шляхом активного перехоплення та блокування потенційно шкідливих дій. Вона дозволяє організаціям реагувати на атаки в реальному часі, забезпечуючи безпеку мережі та захищаючи конфіденційні дані. Система IPS (Intrusion Prevention System) необхідна для того щоб уникати зовнішніх атак (рис.2.2). Дана система, головною метою якої є стежити за трафіком самостійно заблоковує потоки різного роду підозрілих даних. Основною метою цієї системи є – при виявленні несанкціонованих дій запобігти розповсюдженню в Інтернеті. У системи є певний набір правил, який вона використовує, та завдяки цим правилам блокуються всі прогалини у безпеці. Система IPS застосовується у хостах, які мають окрему мережу, або на межі мереж.

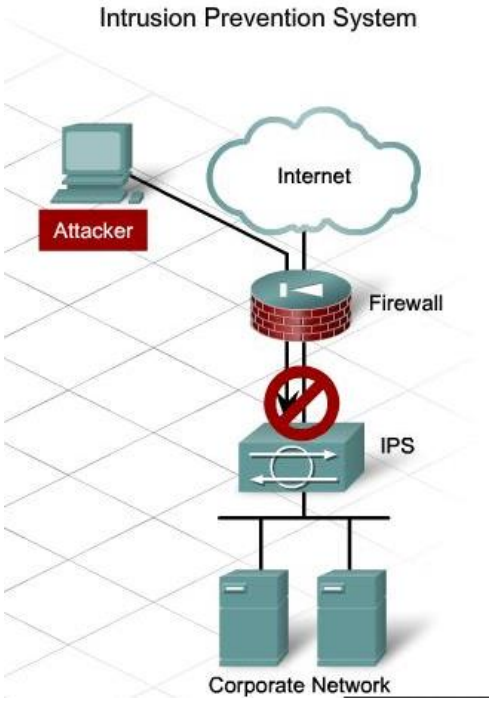

Рисунок 2.2 - Схема роботи системи IPS

Результати аналізу, отримані з обох категорій системи IPS, є важливою інформацією для адміністраторів і фахівців з інформаційної безпеки. Вони не зможуть оперативно реагувати на можливі загрози та отримати допомогу для запобігання атаці.

вибір визначення загроз, системи IPS також забезпечують інші важливі функції. Вони забезпечують контроль за мережевим трафіком, що дозволяє ідентифікувати незвичайну або помітну активність. Крім того, вони допомагають виявляти порушення політики безпеки з боку користувачів, наприклад, спроби доступу до недозволених ресурсів або недотримання правил використання мережі.

Система виявлення вторгнень IDS, у свою чергу, є доповненням до IPS і забезпечує роль постійного моніторингу стану безпеки мережі. Вони активно досліджують поточні загрози та атаки, а також аналізують поведінку користувачів та мережевий трафік для виявлення незвичайних або підозрілих дій.

Загалом, використання систем IPS та IDS створює важливий шар захисту мережі, дозволяючи виявити якісь загрози та отримати необхідні заходи для їх запобігання. Ці системи є невід'ємною частиною сучасних мережевих інфраструктур і забезпечують надійний рівень безпеки, що є особливим випадком у постійно змінюваному ландшафті кіберзагроз.

Система IDS (Intrusion Detection System) використовують к систему, яка виявляє дії нетипові в Інтернет та попереджає про них фахівця з Інформаційної безпеки (рис.2.3).

Повідомляється, це таким чином, що звістка про небезпеку відправляється фахівцю на електронну пошту або ж телефон, а також може з'явитися на панелі управління.

Основною метою системою IDS є надання постійного моніторингу мережевого трафіку з виявленням встановлених мережевих атак. Ця система досліджує різноманітні види активності в мережі та аналізує їх на предмет відповідності встановленим правилам та шаблонам поведінки.

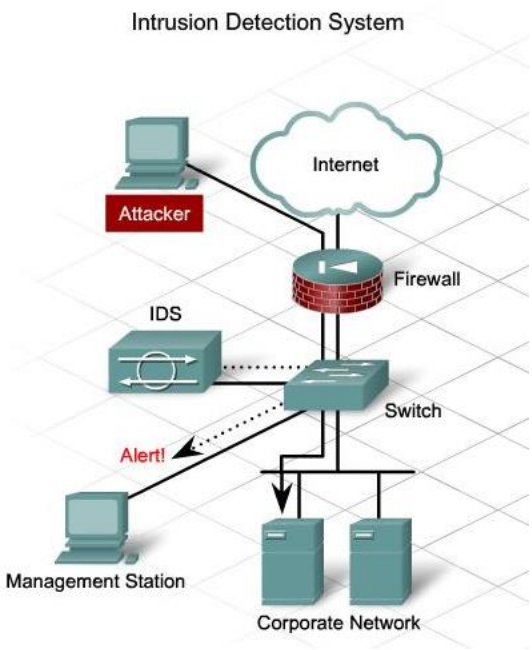

Рисунок 2.3 - Схема роботи системи IDS

Незалежно від того, системи IDS виявляють порушення політики безпеки користувачів. Вони аналізують дії користувачів і виявляють незвичайні,

усвідомлені або неприпустимі дії, які можуть стати загрозою безпеці мережі. Це дозволяє оперативно реагувати на порушення та приймати відповідні заходи для їх запобігання.

Система виявлення вторгнення IDS забезпечує важливу функцію відслідковування стану безпеки. Вони сприяють перевірці ефективності застосованих заходів безпеки, виявляють популярні невразливості та слабкі місця в мережі. Збираючи інформацію про незвичайну активність та можливості загрози, системи IDS допомагають адміністраторам зрозуміти стан безпеки мережі та отримувати відповідні запити для покращення її захисту.

Завдяки системам IDS можна ефективно виявляти вторгнення, реагувати на них і запобігати подальшим атакам. Вони є елементом комплексної стратегії безпеки мережі, сприяючи забезпеченню надійного рівня захисту від постійно зростаючих кіберзагроз.

Функції IDS-систем включають:

- Запис інформації: IDS-системи здатні записувати події та активність, що відбуваються в мережі. Ця інформація може бути відправлена до систем збору логів або SIEM-систем для подальшого аналізу та зберігання.
- Повідомлення про інциденти: IDS-системи генерують alert-повідомлення, що вказують на виявлені аномалії, підозрілу активність або потенційні вторгнення. Ці повідомлення можуть бути спрямовані до відповідальних осіб для подальшого аналізу та реагування на інциденти.
- Складання звітів: IDS-системи здатні підсумовувати дані про події та вторгнення, що відбулися. Це дозволяє згрупувати та систематизувати інформацію для подальшого аналізу, аудиту та звітування про стан безпеки мережі.

Архітектура IDS-систем зазвичай включає:

- Підсистему сенсорів: призначена для збору подій та моніторингу різних ділянок системи захисту. Сенсори активно відстежують мережевий трафік та реагують на потенційні загрози.
- Підсистему аналізу: відповідає за виявлення та класифікацію атак та підозрілих дій на основі даних, зібраних сенсорами. Вона використовує різні алгоритми та правила для виявлення аномалій та вторгнень.
- Сховище: забезпечує зберігання первинних подій та результатів аналізу. Це дозволяє здійснювати подальший ретроспективний аналіз та виконання досліджень в разі необхідності.
- Консоль управління: надає інтерфейс для конфігурації IDS-системи, спостереження за її станом, перегляду звітів про виявлені інциденти та інші дії адміністрування.

Існують два основні підходи до виявлення вторгнень:

Сигнатурний аналіз: схожий на принцип роботи багатьох антивірусних програм. Він полягає у порівнянні мережевого трафіку з базою даних сигнатур, що містить інформацію про відомі шкідливі програми. Якщо виявляється відповідність, система сповіщає відповідальну особу про потенційну загрозу.

Поведінковий аналіз: включена в мережу IDS вивчає нормальну поведінку та функціонування користувачів та додатків. На основі побудованої моделі система виявляє некоректну або аномальну активність, що може свідчити про вторгнення або загрозу безпеці. [3]

2.4 Веб фільтри

Фільтрація контенту є широко використовуваною технологією в сфері IT-безпеки. Вона використовується антивірусами, фільтрами спаму, захисними засобами від нецільового використання мережевих ресурсів та системами захисту від витоків. Сучасні технології контентної фільтрації знаходять своє застосування в різних рішеннях IT-безпеки.

Технології фільтрації контенту використовуються для наступних цілей:

- Виявлення шкідливого контенту: Вони допомагають ідентифікувати та блокувати шкідливий вміст, такий як віруси, троянські програми, шпигунське ПЗ та інші загрози безпеці. Це забезпечує захист систем та користувачів від потенційно небезпечного контенту.
- Фільтрація спаму: Технології контентної фільтрації допомагають виявляти та блокувати небажану електронну пошту, яка включає спам, фішингові повідомлення та інші небажані комунікації. Це забезпечує покращення ефективності роботи з електронною поштою та зменшення ризику впливу шкідливого спаму.
- Захист від нецільового використання ресурсів. Фільтрація контенту є широко використовуваною технологією в сфері IT-безпеки. Вона використовується антивірусами, фільтрами спаму, захисними засобами від нецільового використання мережевих ресурсів та системами захисту від витоків. Сучасні технології контентної фільтрації знаходять своє застосування в різних рішеннях IT-безпеки.
- Захист від витоків інформації: Технології фільтрації контенту дозволяють виявляти та блокувати витоки конфіденційної або небажаної інформації, такої як особисті дані, корпоративна інформація або інтелектуальна власність. Це допомагає попередити витоки даних та зберегти конфіденційність організації.

Технології контентної фільтрації є невід'ємною частиною сучасних рішень IT-безпеки, які допомагають забезпечити захист і безпеку інформаційних ресурсів та користувачів. Використання такої фільтрації допоможе заблокувати сайти, коли вони заважають роботі, забезпечить контроль адміністрації, блокує потенційно небезпечні ресурси, які нашкодять мережі, а також само собою система збільшує безпеку безпосередньо конкретної мережі. Ці та інші переваги додають впевненості замовникам, що впровадження контентної фільтрації буде корисною для поліпшення роботи.(рис.2.4).

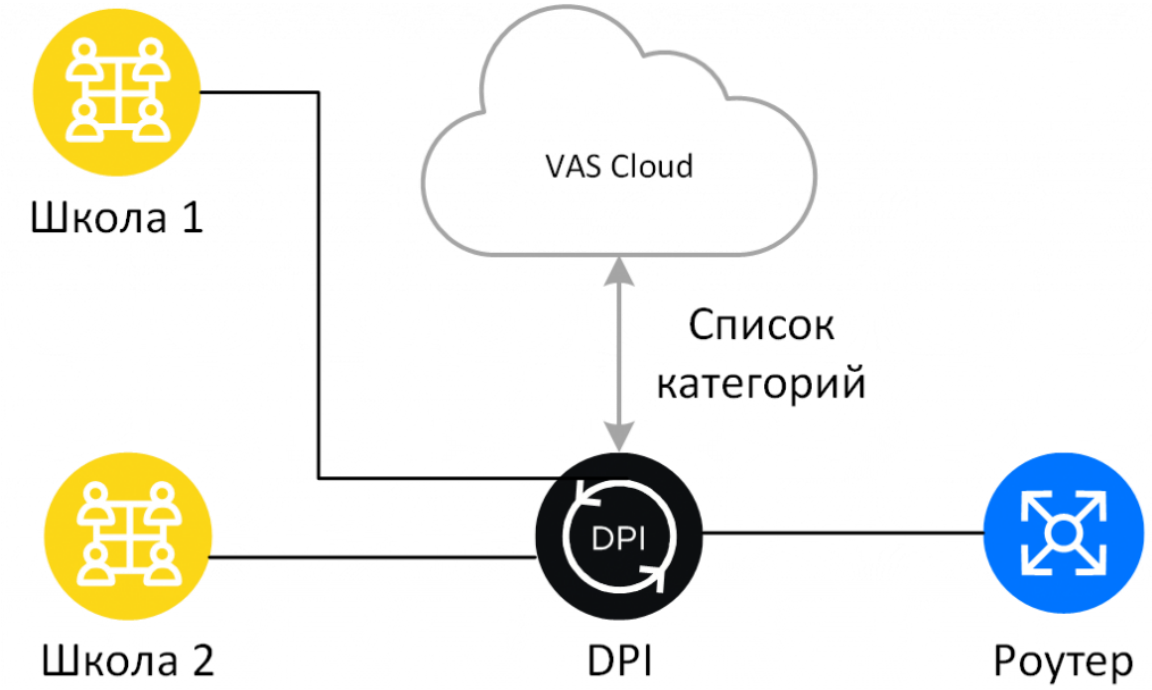

Рисунок 2.4 - Схема організації контент-фільтру на прикладі мережі

Існує два основних напрямки у фільтрації контенту: фільтрація веб-контенту і фільтрація електронної пошти. Такий поділ обумовлений тим, що ці канали є основними для передачі інформації до кінцевих користувачів.

Контент-фільтр відрізняється від антивірусного фільтра тим, що він працює безпосередньо з контентом, тобто інформацією, призначеною для людини, що міститься в електронних повідомленнях або на веб-сторінках, а не з файловими кодами, як у випадку з антивірусним фільтром. Головна мета контент-фільтра полягає в блокуванні електронних повідомлень або веб-сторінок, які відповідають або не відповідають певним умовам.

Основні умови, за якими працює контент-фільтр, включають наступні:

- Блокування веб-сторінок за чорним або білим списком: Крім використання категорій фільтрації, адміністратор може скласти список заборонених або дозволених сайтів, що дозволяє більш гнучко контролювати доступ до певного контенту.
- Антиспам: Цей модуль контент-фільтра широко поширений і використовується для боротьби зі спамом. За допомогою складних алгоритмів

оцінюється електронне повідомлення, і на основі різних параметрів виробляється висновок про його спамовий або корисний характер.

- Блокування за фразами або словами: Фільтр може блокувати електронні повідомлення або веб-сторінки, які містять певні слова або словосполучення у листах, сторінках або заголовках. Працює це таким чином, що адміністратор вказує фрази, слова або речення, які можуть бути небезпечними, а система буде блокувати весь контент, у якому буде присутнє все вище перераховане. Це допоможе прибрати потенційно небезпечний контент, що може нашкодити роботі.
- Блокування файлів за розширенням або назвою: Фільтр може блокувати вкладені в листи або завантажувані з веб-сторінок файли за їх назвою або розширенням. Наприклад, розширення .com і .exe часто блокуються, оскільки це поширений спосіб поширення вірусів.
- Блокування контенту, що не відповідає певним форматам: Багато рішень надають можливість блокувати певні формати файлів, які часто використовуються для поширення шкідливого контенту, такі як подвійні розширення файлів, некоректні типи MIME (Multipurpose Internet Mail Extension) або зашифровані архіви.

Такі умови дозволяють контент-фільтру ефективно виявляти та блокувати небажаний або потенційно небезпечний контент, забезпечуючи безпеку та захист інформаційних ресурсів та користувачів.

2.5 Віртуальні приватні мережі VPN

Virtual Private Network (VPN) - віртуальна приватна мережа, це загальна назва технологій, які дозволяють створити одну або кілька безпечних з'єднань поверх використовуваної мережі. Термін VPN почав широкого використовуватись коли вперше анонсували вихід операційної системи Windows 95. Основною ідєю було, забезпечити усіх співробітників безпечним доступом

до внутрішньої мережі їх організації, уникаючи того щоб її було відкрито для атак зовнішньої мережі.

Virtual Private Network (VPN) має три основних принципи, а саме: тунелювання, шифрування і аутентифікація, тому розглянемо їхні функції.

Тунелювання - це процес передачі приватної інформації через публічну мережу, таку як Інтернет, з використанням зашифрованого тунелю. Тунель у VPN створюється шляхом запаковування приватних даних в криптографічний протокол та передачі їх через публічну мережу, що забезпечує конфіденційність і захист інформації від небажаних перехоплювачів. Цей механізм дозволяє встановлювати безпечне з'єднання між віддаленими мережами або пристроями, що дозволяє користувачам здійснювати безпечний доступ до ресурсів та передавати дані через незахищені мережі. Тому, щоб захистити дані від проникнення через вузли відкритої публічної мережі, використовується механізм електронного цифрового підпису (ЕЦП). ЕЦП - це додаткова інформація, яка передається разом з пакетом даних і генерується з використанням спеціального криптографічного алгоритму та унікального для вмісту пакета та секретного ключа ЕЦП відправника. Цей блок є ЕЦП пакета і дозволяє отримувачу перевірити автентичність даних, використовуючи відкритий ключ ЕЦП відправника. Таким чином, забезпечується конфіденційність і цілісність інформації, що передається.

Крім трьох базових принципів, вона має додаткові важливі характеристики. Одна з них - маршрутизація. VPN може визначити оптимальний маршрут для передачі даних між вузлами мережі, що дозволяє ефективно використовувати ресурси та забезпечує швидку передачу інформації. Маршрутизація може бути здійснена на рівні мережевих пристроїв, які виконують функції маршрутизаторів для управління трафіком.

Інша важлива характеристика VPN - маскування IP-адрес. При використанні VPN IP-адреси вузлів мережі захищаються і приховуються, що забезпечує конфіденційність ідентифікації вузлів і захист від зовнішніх атак.

Додаткові протоколи можуть бути використані в рамках віртуальної приватної мережі (ВПМ), щоб забезпечити додаткові рівні безпеки. Наприклад, протоколи контролю доступу дозволяють керувати правами доступу до ресурсів мережі, а протоколи мережевої аутентифікації використовуються для перевірки ідентичності користувачів.

Завдяки цим характеристикам, ВПМ забезпечує надійний та захищений обмін даними між вузлами мережі, навіть через відкриту публічну мережу, таку як Інтернет. Вона знаходить широке застосування в комерційних організаціях, де конфіденційність та безпека даних є надзвичайно важливими, а також в особистому використанні для забезпечення безпеки та приватності під час підключення до віддалених мереж.

Крім того, віртуальна приватна мережа (ВПМ) може використовувати інші додаткові механізми для забезпечення безпеки та приватності. Наприклад, механізми мережевого брандмауера можуть бути впроваджені для контролю трафіку та блокування небажаних з'єднань. Також, можуть використовуватися механізми (IDS) та (IPS) для виявлення та блокування потенційних загроз безпеці мережі.

ВПМ також може підтримувати шифрування на рівні даних, що забезпечує конфіденційність інформації під час передачі. Шифрування даних забезпечує їх захист від несанкціонованого доступу та перехоплення.

Крім того, деякі ВПМ надають можливість встановлення віртуальних точок доступу, що дозволяють користувачам з'єднуватися з мережею з різних місць і пристроїв. Це особливо корисно для дистанційних робітників або користувачів, які часто перебувають в дорозі, оскільки вони можуть безпечно підключатися до внутрішньої мережі організації з будь-якого місця з доступом до Інтернету.

Узагалі, ВПМ є потужним інструментом для забезпечення безпеки, конфіденційності та приватності в мережах. Вона дозволяє організаціям та користувачам впевнено обмінюватися даними, зберігаючи їх захищеними від потенційних загроз.

Враховуючи все вище перелічене, можна сформулювати загальні вимоги до шкільної віртуальної приватної мережі (VPN):

- Централізоване адміністрування: Усі завдання адміністрування, включаючи управління розмежувальною політикою доступу до шкільних ресурсів і ключовою політикою (створення та поширення шифрувальних ключів мережі), мають бути вирішені з самим адміністратором безпеки за допомогою централізованої системи адміністрування безпеки, що включає робочий пристрій автоматизації для адміністратора.
- Обмеження доступу користувачів: Користувачі повинні бути виключені з процесу адміністрування і працювати в шкільній мережі відповідно до встановлених обмежень, які встановлює адміністратор. Користувачі мають обмежувати свою взаємодію тільки на тих користувачів або комп'ютерах, з якими вони мають дозвіл, і передавати дані тільки у форматі, який встановив адміністратор, чи то відкритий, чи зашифрований. Шифрування віртуальних каналів повинно відбуватися "непомітно" для користувача, і ключ шифрування користувача, який надається адміністратором, не повинен дозволяти розкриття конфіденційності даних користувача при їхньому незаконному доступі.

Загальна мета цих вимог полягає в тому, щоб забезпечити безпеку, конфіденційність та контроль доступу в корпоративній мережі через використання віртуальної приватної мережі (VPN).

Основними технологіями шифрування віртуальних приватних мереж є:

- IPsec (Internet Protocol Security): IPsec є набором протоколів, які забезпечують захист даних, що передаються через протокол IP. Цей набір протоколів забезпечує аутентифікацію, цілісність та шифрування IP-пакетів. Він також включає протоколи для безпечного обміну ключами в мережі Інтернет. IPsec забезпечує високий рівень безпеки шляхом застосування шифрування на рівні пакетів IP, що дозволяє захистити всі дані, які пересилаються через VPN.
- SSL (Secure Sockets Layer): SSL є протоколом безпеки, який шифрує дані, передані між клієнтом і сервером через мережу. Використовуючи SSL, VPN може забезпечити захищений канал комунікації і зашифрований обмін даними

між вузлами мережі. SSL широко використовується в комерційних веб-браузерах для захищеного підключення до веб-сайтів.

Обидві технології, IPsec і SSL, використовуються для забезпечення безпеки і захисту даних від несанкціонованого доступу, прослуховування і модифікації під час передачі через віртуальну приватну мережу (VPN). Вони є важливими і надійними засобами шифрування, які допомагають забезпечити конфіденційність та безпеку комунікацій в VPN.

IPsec є гнучким і добре налаштовуваним інструментом, який може бути використаний для створення з'єднання між двома мережами або між комп'ютером і корпоративною мережею. Використання VPN з IPsec дозволяє шифрувати трафік і захищати його паролем, що забезпечує конфіденційність та захист від несанкціонованого доступу протягом всього шляху від відправника до отримувача.

Проте варто врахувати, що IPsec, хоча є стандартизованою технологією, може мати несумісні реалізації між різними постачальниками та пристроями. Тому успішне впровадження IPsec вимагає наявності належних IT-ресурсів та кваліфікованого персоналу, який зможе підтримувати та налаштовувати такі протоколи.

IPsec може бути відмінним вибором для компаній, які прагнуть забезпечити безпеку з'єднань і захист конфіденційної інформації. Однак, перед впровадженням IPsec рекомендується звернутися до кваліфікованого фахівця або консультанта з мережевої безпеки, щоб належно налаштувати його і забезпечити сумісність з існуючою мережевою інфраструктурою. Налаштування IPsec вимагає досвіду та знань, щоб забезпечити оптимальний рівень безпеки та зручність використання для організації.

Крім того, IPsec забезпечує додаткові функції безпеки, такі як аутентифікація, цілісність даних та захист від повторного відтворення. Він використовує механізми шифрування, такі як шифрування ключами симетричного або асиметричного шифрування, для забезпечення захищеності переданих даних.

IPsec може бути налаштований в режимі тунелювання або застосовуватися в режимі транспорту. У режимі тунелювання весь пакет IP-даних, включаючи заголовок, шифрується і розміщується в новому пакеті IP, що забезпечує приватність і конфіденційність даних. У режимі транспорту шифрується лише навантаження пакета IP, що дозволяє забезпечити безпеку без зміни заголовка.

Одним з переваг використання IPsec є його можливість працювати на рівні мережевого протоколу, що означає, що він незалежний від додатків і може застосовуватися до будь-яких типів трафіку, які передаються через мережу. Це робить його універсальним рішенням для захисту даних в корпоративному середовищі.

Застосування IPsec вимагає наявності належної інфраструктури ключів, яка включає довірені центри сертифікації та керування ключами. Це дозволяє забезпечити безпеку обміну ключами та перевірку відповідності сертифікатів. Для оптимальної роботи IPsec необхідно належно налаштувати політику безпеки, включаючи параметри шифрування, алгоритми та ключі шифрування (рис. 2.5).

Загалом, IPsec є потужним і ефективним інструментом для забезпечення безпеки з'єднань і захисту конфіденційної інформації в мережах. Проте перед його впровадженням рекомендується провести аналіз потреб організації і залучити кваліфікованого фахівця з мережевої безпеки, щоб забезпечити належну конфігурацію та оптимальну працездатність IPsec.

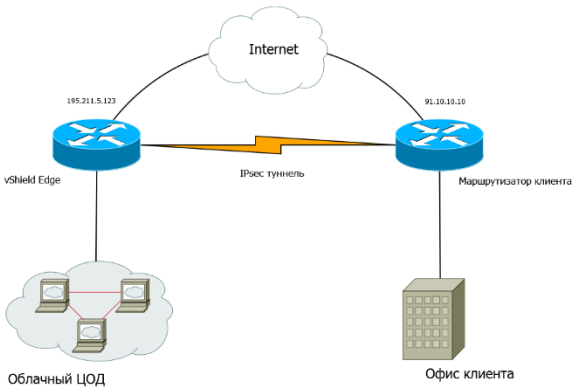

Рисунок 2.5 - Схематична організація VPN використовуючи IPsec

2.6 Системи виявлення та запобігання DDos-атак

SSL (Secure Sockets Layer) - Протокол на базі криптографічних обчислень, який призначений для забезпечення безпечного зв'язоку. Основний його функціонал, це для збереження конфіденційності він використовує симетричне шифрування. Використання асиметричної криптографії дозволяє використовувати повідомлення аутентифікаційних кодів для збереження цілісності у них, а також проводити аутентифікацію ключів обміну.

Віртуальні приватні мережі з використанням SSL на основі IPsec VPN перше початково розроблялися як технології для віддаленого доступу. Але надійність і низькі витрати, зробили SSL VPN привабливою технологією для організацій впровадження власної віртуальної приватної мержі. SSL віртуальної приватної мережі забезпечує з'єднання між окремим комп'ютером і корпоративною мережею через спеціальний шлюз.

Оскільки SSL VPN використовує браузер як інтерфейс, користувачу зазвичай не має необхідності для встановлення додаткового програмного забезпечення. Це спрощує процес встановлення, а також утворює мережу з пристроями, що працюють на різних операційних системах. Однак, недолік полягає в тому, що SSL VPN з'єднання використовують з додатками, які працюють безпосередньо з HTML/HTTP. Дане обмеження можна обійти, встановивши на клієнтський комп'ютер спеціальні додатки, але це зменшує гнучкість. Тому, можливо, IPSec VPN буде вигіднішим варіантом.

Часто співробітники компаній зобов’язані обмінюватись конфіденційною інформацію за межами офісу, для цього розроблено mVPN. Основна відмінність mVPN та VPN в тому, що точка, яка встановлюється в кінці з'єднання, не статична. Тому в такому випадку mVPN має можливість відновлювати безпечне з'єднання, коли користувач переміщується між мережами. Для цього використовується протокол IPsec, шифрування якого забезпечсує данні

всередині VPN-каналу. Підсумовуючи, в мережі з'єднання віддаленого комп'ютера і основного шлюзу залишається захищенним.

Завдяки розвитку хмарних технологій тепер єможливість створити власну систему VPN у хмарному сховищі (рис.2.6) – Таким чином з’являється можливість відмовитися від використання сервера і здійснювати всі налаштування віддалено.

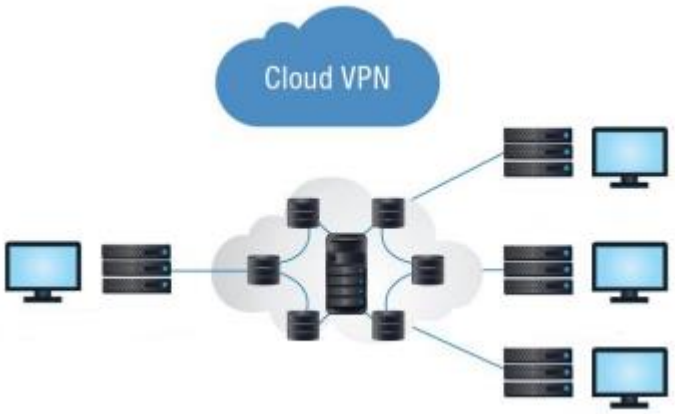

Рисунок 2.6 - Принцип роботи хмарного VPN

Крім того, зазвичай оплата за хмарні сервіси проводиться на годинній основі, що дозволяє будь коли припинити використання сервера і платити лише за обсяг зайнятого місця на диску. Хмарний сервер може без проблем масштабуватись, зменшуватись або збільшуватись відповідно до обсягу ресурсів сервера в залежності від зменшення або зростання числа користувачів.[4]

Використання VPN надає можливість безпечно поширювати інформацію мільйонам користувачів та компанім по всьому світі. Ця технологія володіє великим значенням і, очевидно, що в подальшому буде відігравати значну роль, доступну для подальших досліджень у майбутньому.

Загалом розроблка VPN дозволила подивитися на світ по-іншому та заставити IT-спеціалістів розглянути свої системи з різних боків, оскільки

змінивши просто IP-адресу можна отримати багато інформації, яка була обмежена для іншого користувача.

3 РЕАЛІЗАЦІЯ ТА МОДЕЛЮВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Налаштування маршрутизатора

Оскільки дана система призначена в майбутньому для безпечного використання мережі в навчальних цілях, то, першим та найбільш актуальним рішенням захисту мережі навчального закладу є налаштування міжмережевого екрану, або ж брандмауера для блокування шкідливого трафіку який потенційно може нашкодити користувачам.

Провівши аналіз використаної літератури можна дізнатись що брандмауер можна налаштувати як для одного персонального комп'ютера (ПК) так і одразу для цілої мереж, тому оптимальним рішенням буде налаштувати брандмауер одразу на всю мережу навчального закладу. Зробити це можна через налаштування локального маршрутиризатора mikrotik (рис. 3.1) який є наявний у даному закладі освіти.

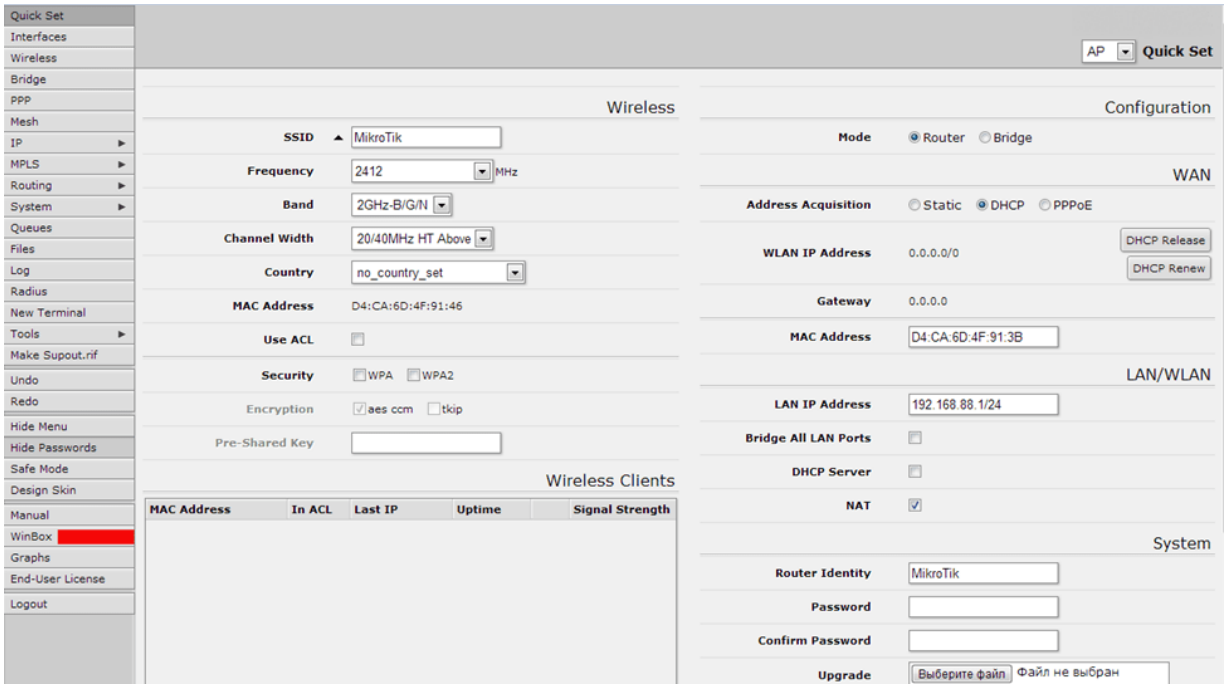

Рисунок 3.1 - Інтерфейс маршрутиризатора mikrotik

Перед налаштуванням необхідно увійти у програму Winbox, яку заздалегідь використовували при роботі з даним маршрутиризатором, та налаштувати його базові функції для подальшої роботи з ним. Наступним кроком необхідно перейти у розділ IP Service list, та для підключення до зовнішньої мережі необхідно спочатку налаштувати безпеку маршрутизатора, відключивши непотрібні сервіси, та оновивши застарілий пароль адміністратора. Послідовно виділяємо та вимикаємо послуги FTP, Telnet і WWW що зображені на (рис 3.2).

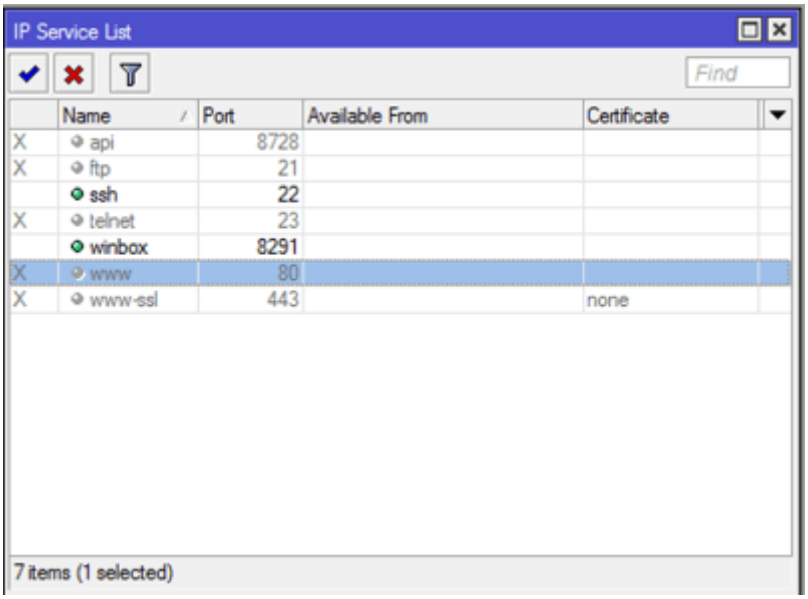

Рисунок 3.2 - Деактивація послуг маршрутиризатора mikrotik

Для налаштування NAT та WAN, необхідно здійснити кілька кроків. Спочатку необхідно перейти до розділу IP/Firewall у системі. У цьому розділі у розділі NAT, можна додати нове правило.

У розділі NAT, на вкладці General, обираємо параметри Chain/srcnat та Out Interface=WAN1. Це означатиме, що правило буде застосовуватися до трафіку, який йде через інтерфейс WAN1 (ваше зовнішнє під'єднання до Інтернету).

Далі, на вкладці Action, необхідно обирати опцію Masquerade. Це дозволить змінювати джерело пакетів із локальної мережі, щоб вони виглядали, як пакети, які виходять через інтерфейс WAN1. Це важливо для забезпечення коректного маршрутизації трафіку у мережі (рис. 3.3).

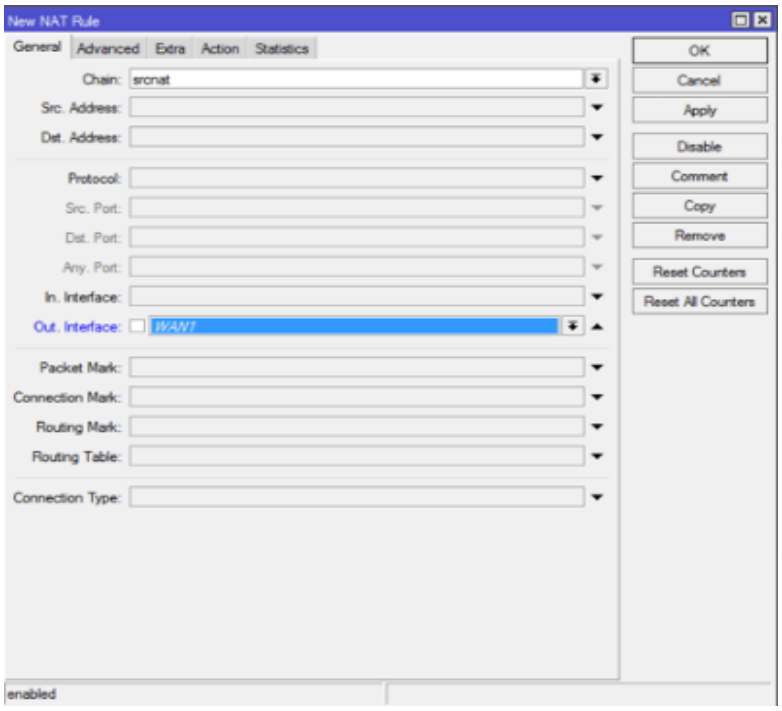

Рисунок 3.3 - Вікно налаштування NAT

Виконавши ці кроки, NAT та WAN успішно налаштуються в системі. Рекомендується повторно перевірити налаштування та забезпечити, щоб вони відповідали потребам та вимогам безпеки.

Для налаштування WAN потрібно виконати кілька кроків. Спочатку необхідно сконфігурувати IP-адресу, маску та шлюз, які відповідно були надані провайдером.

У розділі "Adress list" (Список адрес) в меню IP/Firewall, необхідно переконатися, що маска встановлена на значення 255.255.255.252. Ця маска відповідає довжині /30, яка є стандартною для таких типів з'єднань. Надалі ж у меню IP/Addresses (IP/Адреси) і вводим IP-адресу маршрутизатора. Переходим до меню IP/Routes (IP/Маршрути) і додаєм шлюз за замовчуванням. Шлюз за замовчуванням встановлюється за допомогою маршруту 0.0.0.0/0. Додаєм цей маршрут і вказуємо IP-адресу шлюзу, яка в нашому випадку складає 172.30.10.1. Це дозволить маршрутизатору знаходити шлях до всіх мереж, не вказаних явно в інших маршрутах (Рис. 3.4).

Після цього маршрутизатор буде мати належне з'єднання з інтернетом та здатність маршрутизувати трафік у мережі закладу освіти.

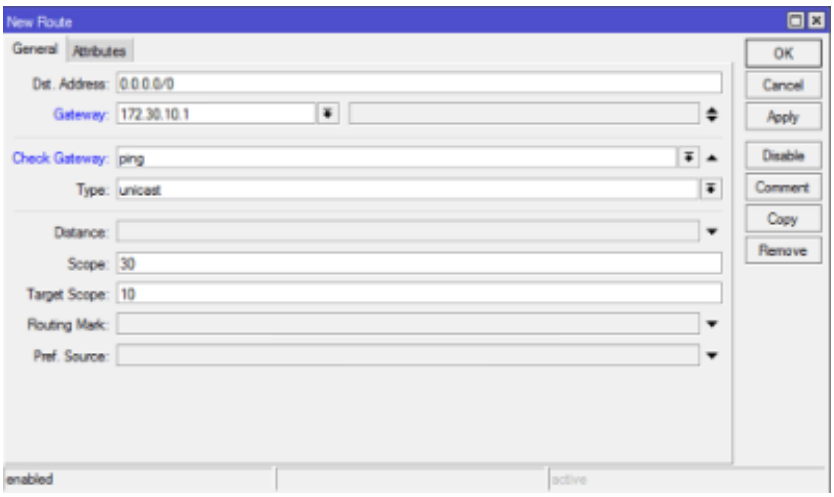

Рисунок 3.4 - Вікно налаштування маршрута

Описані налаштування мають ключове значення для подальшої роботи маршрутизатора та налаштування мережевого екрану в шкільній мережі.

3.2 Налаштування брандмауера

У рамках цього розділу розглядається процес налаштування брандмауера з метою забезпечення високого рівня безпеки в мережі школи. Брандмауер є важливим елементом інфраструктури мережі, який дозволяє контролювати, фільтрувати та моніторити мережевий трафік, що проходить через маршрутизатор. Цей процес має на меті запобігти несанкціонованому доступу, атакам та забезпечити конфіденційність, цілісність та наявність мережевих ресурсів.

Для цього у інтерфейсі маршрутиризатора необхідно перейти у розділ консоль та виконати наступні дії:

Створити Whitelist адрес які будуть мати доступ до маршрутиризатора;

Увімкнути доступ ICMP;

Налаштувати роботу з новими підключеннями щоб зменшити навантаження.

З цією метою, був написаний код зазначений на (рис 3.5), який відповідатиме вказаним вимогам:

/ip firewall filter

add action=accept chain=input comment="default configuration" connection-state=established,related

add action=accept chain=input src-address-list=allowed_to_router

add action=accept chain=input protocol=icmp

add action=drop chain=input

/ip firewall address-list

add address=192.168.88.2-192.168.88.254 list=allowed_to_router

Наступним кроком необхідно створити список адрес яку необхідно назвати наступним чином "not_online". Це необхідно щоб в подальшому задовільнити правила фільтрації брандмауера.

Код який відповідає заданому завданню:

/ip firewall address-list

add address=0.0.0.0/8 comment=RFC6890 list=not_online

add address=172.16.0.0/12 comment=RFC6890 list=not_online

add address=192.168.0.0/16 comment=RFC6890 list=not_online

add address=10.0.0.0/8 comment=RFC6890 list=not_online

add address=169.254.0.0/16 comment=RFC6890 list=not_online

add address=127.0.0.0/8 comment=RFC6890 list=not_online

add address=224.0.0.0/4 comment=Multicast list=not_online

add address=198.18.0.0/15 comment=RFC6890 list=not_online

add address=192.0.0.0/24 comment=RFC6890 list=not_online

add address=192.0.2.0/24 comment=RFC6890 list=not_online

add address=198.51.100.0/24 comment=RFC6890 list=not_online

add address=203.0.113.0/24 comment=RFC6890 list=not_online

add address=100.64.0.0/10 comment=RFC6890 list=not_online

add address=240.0.0.0/4 comment=RFC6890 list=not_online

add address=192.168.88.1/24 comment="6to4 relay Anycast [RFC 3068]" list=not_online

Після створення списку адрес необхідно налаштувати фільтрацію, що відповідає поставленим вимогам:

Тільки встановлені пакети з'єднання, які мають пов'язані дані та є частиною FastTrack, будуть пропускатись для поліпшення швидкодії передачі. Брандмауер буде застосовувати свої правила лише до нових з'єднань;

Виконати скидання неприпустимих підключень та зареєструвати їх, додаючи префікс "недійсний";

Відхиляти спроби доступу до приватних IP-адрес з вашої локальної мережі, застосовуючи попередньо визначений список адрес "not_in_internet". Цей процес буде застосований до "bridge" - інтерфейсу локальної мережі. Крім того, будуть реєструватись спроби з префіксом "!public_from_LAN" за допомогою опції "log=yes";

Будуть відхилятись вхідні пакети без NAT-перетворень, при цьому інтерфейс "ether1" виступатиме як загальнодоступний. Спроби будуть журналюватись з префіксом "!NAT";

Звернення до ланцюжка ICMP для виключення небажаних повідомлень ICMP;

Виконувати вилучення вхідних пакетів з Інтернету, які не належать до загальнодоступних IP-адрес, на інтерфейсі ether1, який є публічним. Зареєструвати спроби з префіксом "!public";

Відкидати пакети з локальної мережі, які не належать до IP-адреси підмережі локальної мережі 192.168.88.1/24.

Обмежити ланцюжок "icmp" на дозвіл лише необхідних кодів ICMP.

Згенерований код, який відповідає вказаним вимогам:

/ip firewall filter

add action=fasttrack-

connection chain=forward comment=FastTrack connection-state=established,related

add action=accept chain=forward comment="Established, Related" connection-state=established,related

add action=drop chain=forward comment="Drop invalid" connection-state=invalid log=yes log-prefix=invalid

add action=drop chain=forward comment="Drop tries to reach not public addresses from LAN" dst-address-list=not_in_internet in-interface=bridge log=yes log-prefix=!public_from_LAN out-interface=!bridge

add action=drop chain=forward comment="Drop incoming packets that are not NAT`ted" connection-nat-state=!dstnat connection-state=new in-interface=ether1 log=yes log-prefix=!NAT

add action=jump chain=forward protocol=icmp jump-target=icmp comment="jump to ICMP filters"

add action=drop chain=forward comment="Drop incoming from internet which is not public IP" in-interface=ether1 log=yes log-prefix=!public src-address-list=not_in_internet

add action=drop chain=forward comment="Drop packets from LAN that do not have LAN IP" in-interface=bridge log=yes log-prefix=LAN_!LAN src-address=!192.168.88.1/24

Код який відповідає обмежити ланцюжка "icmp" на дозвіл лише необхідних кодів ICMP:

```
/ip firewall filter
  add chain=icmp protocol=icmp icmp-options=0:0 action=accept \
    comment="echo reply"
  add chain=icmp protocol=icmp icmp-options=3:0 action=accept \
    comment="net unreachable"
  add chain=icmp protocol=icmp icmp-options=3:1 action=accept \
    comment="host unreachable"
  add chain=icmp protocol=icmp icmp-options=3:4 action=accept \
    comment="host unreachable fragmentation required"
  add chain=icmp protocol=icmp icmp-options=8:0 action=accept \
```

```
  comment="allow echo request"
add chain=icmp protocol=icmp icmp-options=11:0 action=accept \
  comment="allow time exceed"
add chain=icmp protocol=icmp icmp-options=12:0 action=accept \
  comment="allow parameter bad"
add chain=icmp action=drop comment="deny all other types"
```

Згідно зазначених параметрів, брандмауер буде налаштований з урахуванням встановлених параметрів для оптимального функціонування і безпеки. Це означає, що будуть встановлені певні параметри і конфігурації брандмауера, які відповідають вимогам та налаштуванням, необхідним для заданої мережевої інфраструктури та політики безпеки. [5]

Після успішної налаштування брандмауера, для забезпечення ефективної роботи працівників та учнів у програмі Winbox було використано параметр чорного списку. Основна мета цього списку полягає в блокуванні доступу користувачів до веб-ресурсів певного типу.

Початковим кроком було визначено та створено список потенційних сайтів, які можуть нанести шкоду або є неприйнятними для учнів та вчителів (рис 3.5).

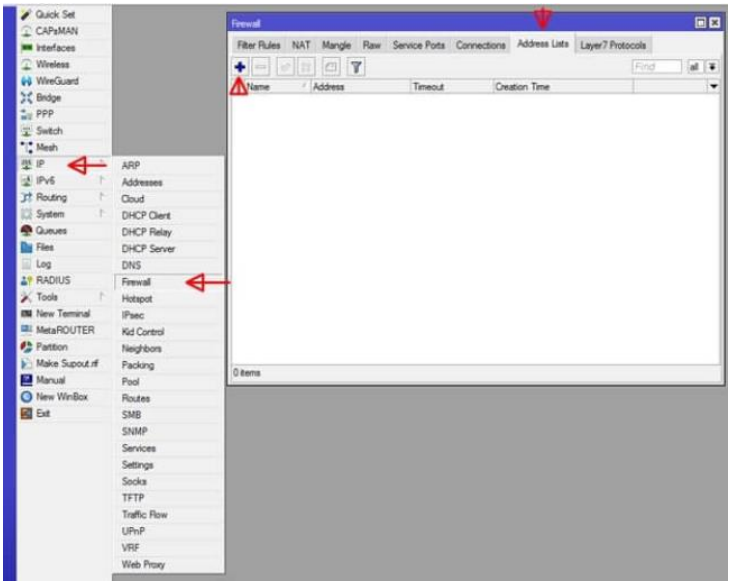

Рисунок 3.5 - Вікно списку адрес сайтів

Цей список включає веб-ресурси, які містять несанкціонований контент або можуть відволікати увагу від освітнього процесу. Шляхом використання чорного списку, доступ до цих сайтів ефективно блокується, що дозволяє забезпечити безпеку та відповідність освітнім стандартам.

Після того як список буде складений, наступним кроком буде пряме створення правила фільтрації. Цей підхід дозволяє керувати та обмежувати доступ користувачів до конкретних веб-ресурсів, створюючи безпечне та продуктивне середовище для роботи та навчання. Це можна здійснити у вкладці Filter rules у вкладці "Advanced" налаштовується поле "Dst. Address List - Blacklist", де вказується раніше створений список сайтів та адрес. Якщо ім'я сайту, на який користувач надсилає запит, збігається з ім'ям сайту в списку, то буде застосована визначена дія, яка встановлюється у вкладці "Action".

У вкладці "Action" встановлюється дія "reject" і параметр "Reject With - icmp network unreachable". Це означає, що запит буде відхилено, оскільки мережа недоступна (рис 3.6). Ця дія відрізняється від дії "drop" тим, що браузер отримає повідомлення про неможливість встановлення з'єднання, і як результат, браузер припинить надсилання запитів на встановлення з'єднання. Це призведе до зменшення навантаження на процесор.

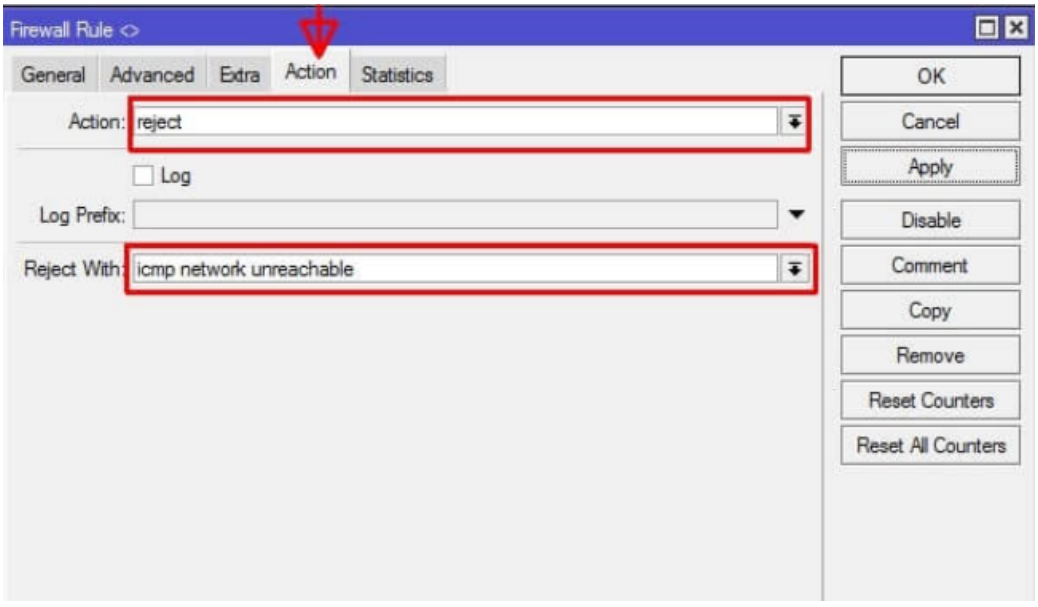

Рисунок 3.6 - Налаштування правил заборони

3.3 Блокування за допомогою DNS

Для забезпечення обмеженого доступу до підозрілих веб-сайтів для всіх користувачів мережі, був використаний другий метод блокування. Цей метод є більш практичним і ефективним, оскільки він ґрунтується на послугах зовнішньої компанії, відповідальної за пошук і оновлення списку шкідливих веб-сайтів. Для цих потреб буде використовуватись ресурс Norton який є безкоштовний для використання у мережі школи, та надає можливість використання його DNS-серверів. На (рис. 3.6) позначений перелік політик які можна використати у мережі навчального закладу.

Політика	IP-адреси	Опис
1. Безпека	199.85.126.10 199.85.127.10	Блокує шкідливі програми та фішингові/шахрайські сайти.
2. Безпека + вміст порнографічного характеру	199.85.126.20 199.85.127.20	Поміж блокуванням небезпечних сайтів, також обмежує доступ до сайтів з контентом сексуальної природи.
3. Безпека + вміст порнографічного характеру та інше	199.85.126.30 199.85.127.30	Це ідеальний варіант для мережі якою користуються діти, оскільки, окрім блокування небезпечних і порнографічних сайтів, він також перешкоджає доступу до веб-ресурсів з дорослим контентом, абортами, алкоголем, злочинами, культами, наркотиками, азартними іграми, нетерпимістю, сексуальною орієнтацією, самогубствами, курінням та насильством.

Рисунок 3.6 - Політики ресурсу Norton

Найбільш оптимальним варіантом є обрати третю опцію, оскільки вона надає більш широкі обмеження щодо шкідливого контенту. Тому в конфігурації маршрутизатора MikroTik буде використано саме цей варіант.

Після вибору DNS-сервера ми вводимо його налаштування у маршрутизаторі. Це можна зробити через головне меню, перейшовши в IP, далі DHCP Server, потім вкладку Networks. Вибираємо потрібну мережу подвійним кліком і вводимо DNS-сервер у поле DNS Server (рис. 3.7).

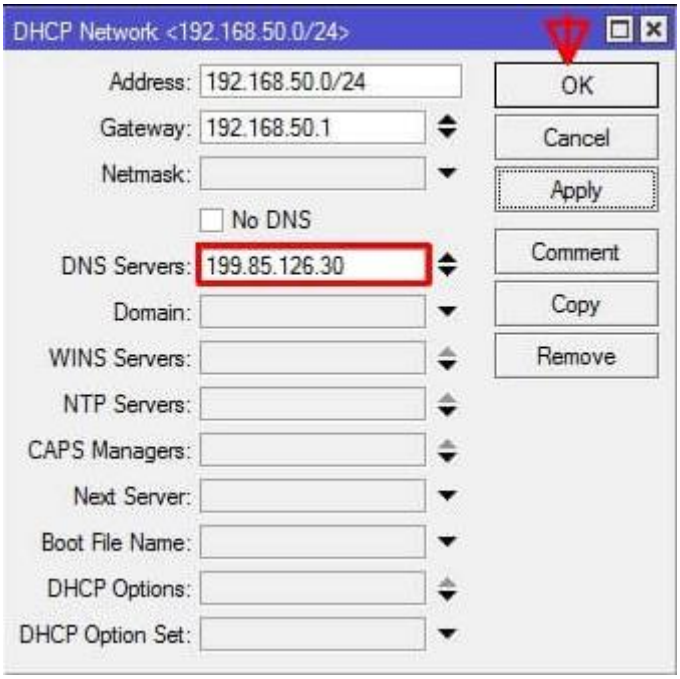

Рисунок 3.7 - Блокування ресурсів за допомогою політики DNS

Тепер, при відвідуванні шкідливого веб-сайту, користувач отримує сповіщення про його блокування. Щоб змінити налаштування на інтерфейсі, до якого підключені користувачі, необхідно перейти до головного меню і обирати "Interfaces", якщо всі порти об'єднані в один "Bridge". Після двократного клацання на вкладці "Bridge" у меню керування маршрутизатором, потрібно перейти на вкладку "General". На цій вкладці знаходяться параметри, пов'язані з ARP (адресною протокольною таблицею). Важливо змінити ці параметри на режим "reply-only". Це означає, що маршрутизатор буде відповідати лише на

ARP-запити, а інші ARP-пакети, що містять інформацію про IP-адреси, будуть проігноровані.

3.4 Налаштування VPN

У цьому розділі кваліфікаційної роботи буде розглянуто процес налаштування віртуальної приватної мережі (VPN) у локальній мережі кабінету персоналу. Основною задачею є захищений веб пошук без ризику втратити інформацію цінного роду, таку як бухгалтерську документацію, паролі, скани документів, тощо. Перед тим, як підключитися через VPN, необхідно прописати винятки для фаєрвола.

Оскільки шкільна мережа налаштовується з використанням маршрутизатора MikroTik, подальші кроки налаштування будуть виконуватися саме на ньому. Проте налаштування будуть задіяні лише для певних робочих місць. Перед цим необхідно налаштувати фаєрвол. З офіційного ресурсу рекомендується підключення у режимі "Safe Mode", оскільки інакше може бути втрачено доступ з'єднання з маршрутизатором.

Тому, у меню керування роутером потрібно перейти до розділу "IP" і вибрати "Firewall" з випадаючого списку. Потім відкриється розділ, потрібно перейти у першу вкладку під назвою "Filter Rules", щоб додати нове правило.

У розділі буде наявний параметр "Chain", де слід обрати значення "input". У рядку "Protocol" потрібно встановити "tcp". В полі "Dst. Port" вказується порт 1723, який зазвичай використовується для налаштування VPN-тунелю (рис.3.8).

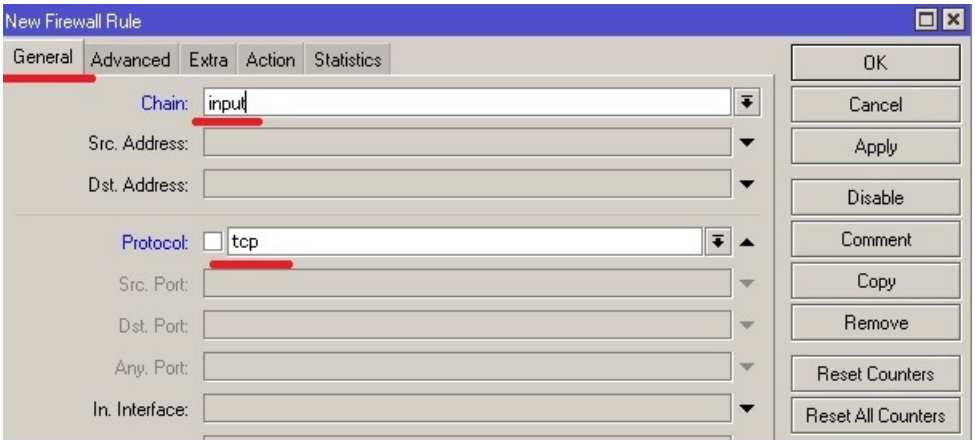

Рисунок 3.8 - Налаштування VPN-тунелю

У тій же вкладці, потрібно вибрати параметр "accept" зі списку в дії (Action), що дозволить трафіку пройти через VPN. Наступним кроком є дозвіл протоколу GRE. Це виконується шляхом створення нового правила, але цього разу в полі "Protocol" слід вибрати "gre", а в дії (Action) дозволити трафік. В розділі "Firewall" нові правила слід перемістити вгору, щоб вони перебували над забороняючими правилами, інакше вони не будуть працювати.

Після налаштування фаєрволу і дозволу трафіку для VPN, останнім кроком завершення розділу налаштування VPN для локальної мережі є налаштування самого VPN-сервера.

У меню управління маршрутизатором необхідно перейти в розділ "IP" і обрати "Services". Відкрити вкладку "PPTP Server", увімкнути PPTP-сервер, встановити IP-адресу, яка буде назначена клієнтам VPN. Вибирати діапазон IP-адрес для VPN-клієнтів. Налаштувати параметри аутентифікації, включаючи імена користувачів та паролі. Встановити необхідні параметри шифрування та інші опції та зберегти налаштування і в кінці перезавантажити маршрутизатор.

Після цих кроків налаштування VPN для локальної мережі у рамках певних користувачів буде завершено. Користувачі шкільної мережі зможуть підключатися до VPN-сервера з використанням налаштованих параметрів аутентифікації і користуватися безпечним з'єднанням зі шкідливими веб-ресурсами обмеженого доступу.

3.5 Налаштування локальної безпеки

Останнім завершальним пунктом налаштування мережі Тернопільської загальноосвітньої школи №28 є налаштування локальної безпеки, зокрема:

Налаштування користувачів.

Встановлення антивіруса.

Першим пунктом як зазначено вище є налаштування користувачів, зокрема встановлення паролів на персональні комп'ютери (ПК). Даний навчальний заклад на своїх комп'ютерах використовує операційну систему Windows 10, яка передбачає створення декількох облікових записів. Для цього у меню налаштувань необхідно обрати параметр облікові записи та елементи та додати користувача без облікового запису Microsoft. Обираємо та вказуємо ім'я користувача (Student), після створення нового користувача необхідно буде вказати на користувача адміністратора. Для цього переходим тим самим методом у "налаштування", обираємо першого користувача з якого ми проводили всі дії та обираємо тип облікового запису (Адміністратор).

Надалі необхідно буде створити паролі для обох користувачів. Для цього компанія Microsoft попіклувалась про користувачів та зробила зміну паролю максимально доступною для кожного свого клієнта. Щоб налаштувати пароль потрібно у тому ж розділі "обліковий запис" перейти до елементу пароль, та встановити необхідний нам пароль. Задля безпеки користувача рекомендується встановити пароль з великими, та малими літерами а також символами, але оскільки студентськими обліковими записами будуть користуватись юні користувачі, варто встановити примітивні пароль, та залишити пароль підвищеної складності для адміністратора персонального комп'ютера (ПК)

Завершальним пунктом налаштування локальної безпеки є встановлення на персональний комп'ютер (ПК), систем захисту які візуально одразу будуть оповіщати працівників про потенційно небезпечні файли та зможуть стримати їх у карантинній зоні до моменту їх вилучення.

Підходячи до даного питання слід було уважно поставитись до підбору програм які можуть забезпечити захист комп'ютера у такому плані. У зв'зку з обставинами 22 лютого 2022 року на територію України зі сторони Російської федерації було здійснено повномасштабне вторгнення, тому слід з обачністю ставитись до програм походження яких має зв'зок з цією країною. Хорошим прикладом такого програмного забезпечення є антивірусна програма Kaspersky. Тому рекомендується уникати даного ПЗ та використовувати антивіруси по типу ESET nod32 які не мають ніякого відношення до країни агресора.

Для використання антивіруса ESED nod32 необхідно отримати установщик даного програмного забезпечення (ПЗ). Для цього адміністрацією школи був придбаний офіційний установщик який буде встановлений на всіх ПК даного закладу освіти. Після завантаження на Флеш носій для зручності даного ПЗ переходимо до безпосереднього встановлення на всі комп'ютери даного закладу. При встановленні в хаб USB 3.0 даного флеш носія і обирання потрібного нам файлу з розширенням (.exe) з'являється вікно установщика яке зображене на (рис 3.9).

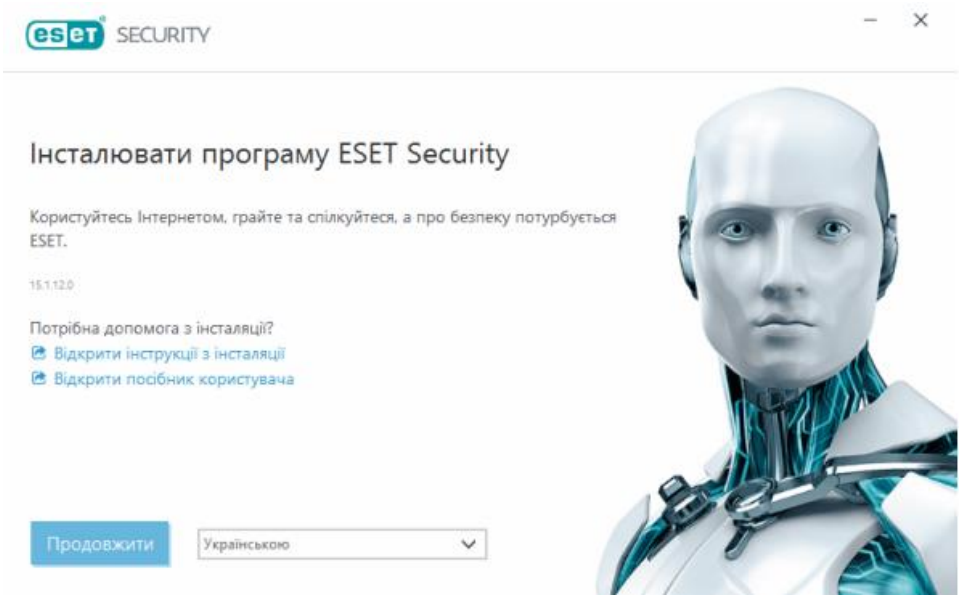

Рисунок 3.9 - Вікно установщика ESET nod 32

Дане програмне забезпечення захищене від встановлення спеціальним ліцензійним ключем який його активовує. Так як антивірус був офіційно придбаний необхідно ввести ключ який був даний для його активації та перейти для подальшого його налаштування. Даним антивірусом передбачено перегляд всіх активованих ліцензій та пристроїв ESET і керувати ними.[6] Тому створюєм робочу адресу електронної пошти Адміністратора та реєструємся у даному програмному забезпеченні. Обов'язково вказуємо мову користування «Українська» та успішно інстальовуємо дане програмне забезпечення на робочий комп'ютер.

Після встановлення у нас з'являється функціональне вікно з пропозицію просканувати комп'ютер на загрози. У разі успішного сканування без виявлення загроз антивірус видасть повідомлення такого типу (Ваш комп'ютер захищено). Процедуру сканування необхідно здійснювати на абсолютно кожному персональному комп'ютері яким користувались учні після закінчення робочого дня. У разі якщо антивірус видасть повідомлення про можливу загрозу (рис 3.10) слід помістити шкідливі файли до карантину для подальшого їх усунення. [6]

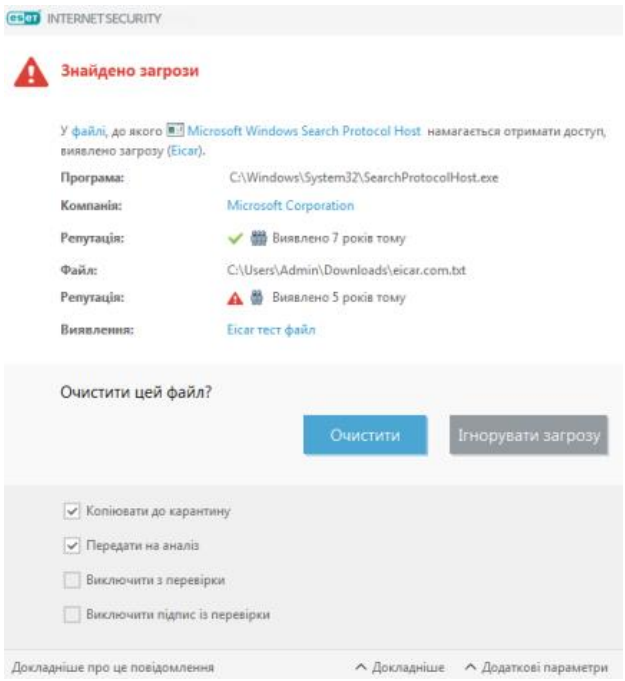

Рисунок 3.10 - Сповіщення ESET nod32 про виявлення загрози

Файли з карантину також можна відновити й повернути до початкових місць розташування за потреби. Але при виявленні невідомої загрози все ж слід її видалити за для збереження даних від загроз (рис. 3.11)

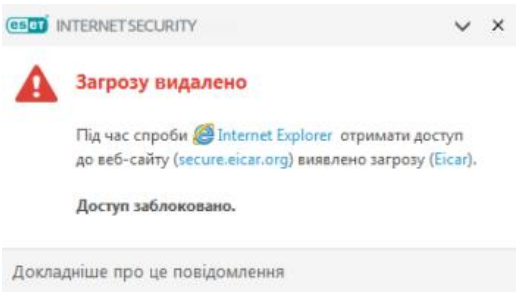

Рисунок 3.11 - Сповіщення про успішне усунення загрози.

4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

Науково-технічний прогрес приводить до суттєвих змін у характері та способах працевлаштування. Він приносить людству багато користі, зокрема, зменшує фізичне навантаження та робить працю більш інтелектуальною, захопливою та різноманітною. Крім того, він сприяє розвитку творчих здібностей людини та покращенню її професійних навичок.

Однак, сучасна техніка становить значну загрозу для безпеки та здоров'я працівника, його оточення та навколишнього середовища. Більшість дослідників вважає, що процес праці та умови безпеки повинні бути вивчені, з урахуванням особистісних і індивідуально-типологічних особливостей працівника, оскільки помилки на робочому місці (ціна яких надзвичайно висока), а також нещасні випадки, часто є наслідком несумісності між характеристиками людини та вимогами конкретної професійної діяльності.

4.1. Оцінка розробленого технологічного процесу щодо умов безпеки, втомлюваності та продуктивності праці

Оцінка розробленого технологічного процесу з точки зору умов безпеки в школі є надзвичайно важливим етапом, оскільки безпека учнів, вчителів та інших працівників школи є першочерговим завданням. Для досягнення цієї мети, було проведено дослідження, аналіз та оцінка всіх етапів технологічного процесу.

Втомлюваність є важливим аспектом оцінки розробленого технологічного процесу в школі. Для оцінки рівня втомлюваності були проведені аналіз та спостереження працівників та учнів під час виконання різних завдань за робочим місцем персонального комп’ютера.

Аналіз втомлюваності включав такі аспекти:

- час роботи за комп'ютером: було виміряно тривалість роботи працівників та учнів за комп'ютером, включаючи тривалість сеансів, перерви та загальний час, проведений у робочому середовищі.

- фізичні навантаження: були враховані рухи та позиції тіла працівників та учнів під час роботи за комп'ютером, а також вимоги до маніпуляційного простору, розташування обладнання та меблів.
- психологічний напруженість: було оцінено рівень стресу, концентрації та інших психологічних аспектів, що можуть впливати на втомлюваність працівників та учнів під час роботи за комп'ютером.
- система підтримки та зручність: була оцінена наявність необхідних засобів підтримки (наприклад, ергономічні стільці, підлокітники, підставки для документів) та зручність робочого місця, що впливає на рівень втомлюваності. [7]

Після проведення аналізу втомлюваності в Тернопільській загальноосвітній школі №28, отримано дані, які використовувалися для оцінки рівня втомлюваності працівників та учнів під час роботи за комп'ютером. Які не перевищують норми.

Дані цієї оцінки були порівняні з встановленими нормами та рекомендаціями щодо безпечних умов праці.

Помічено, що деякі фактори можуть призводити до підвищеної втомлюваності, такі як тривалість роботи за комп'ютером без перерв, незручна позиція тіла та некоректне освітлення робочого простору.

З метою зниження ризику втоми, запропоновані наступні заходи:

- регулярні перерви: рекомендується встановити регулярні перерви під час роботи за комп'ютером, що дозволить зменшити фізичне та психологічне напруження.
- організація робочого простору: слід забезпечити комфортне та ергономічне обладнання, яке враховує фізичні потреби працівників та учнів, зокрема, стільці з належною підтримкою спини та правильною регулюванням висоти.
- освітлення: варто забезпечити достатнє природне та штучне освітлення робочого простору, щоб уникнути напруження очей та забезпечити комфортні умови роботи.

Додатково, для оцінки продуктивності праці, були враховані такі фактори:

- швидкість та якість виконання роботи: оцінювалася ефективність технологічного процесу та час, необхідний для його виконання, а також якість отриманих результатів.
- система підтримки та навчання: оцінювалася доступність необхідних ресурсів, навчальних матеріалів та допомоги для працівників та учнів з метою підвищення продуктивності праці.

Оцінка розробленого технологічного процесу щодо умов безпеки, втомлюваності та продуктивності праці є важливим кроком у забезпеченні безпеки та ефективності праці в школі. Проведені дослідження та аналіз дозволили виявити ключові аспекти, які потребують уваги та вдосконалення.

Забезпечення умов безпеки є найвищим пріоритетом. Виявлені ризики та потенційні небезпеки були ідентифіковані та оцінені, а відповідні заходи були запропоновані для їх зменшення. Важливо постійно забезпечувати навчання персоналу та учнів правилам безпеки, а також підтримувати належний стан обладнання та інфраструктури.

Врахування втомлюваності є необхідним для збереження здоров'я та ефективності праці. Аналіз фізичного та психологічного навантаження дозволив виявити чинники, що сприяють втомлюваності, та запропонувати відповідні заходи для покращення умов праці. Включення регулярних перерв, організація комфортного та ергономічного робочого середовища та надання необхідних ресурсів та навчальної підтримки можуть допомогти знизити рівень втомлюваності та підвищити продуктивність праці. [7]

Встановлення ефективності роботи та якості результатів роботи допомагає виявити можливості для покращення. Надання належної підтримки та навчання сприяє підвищенню продуктивності праці та досягненню кращих результатів.

На основі проведеної оцінки були розроблені рекомендації та заходи для покращення умов безпеки, зниження втомлюваності та підвищення продуктивності праці в школі. Їх впровадження сприятиме забезпеченню

безпеки, здоров'я та ефективності праці всіх учасників навчального процесу в школі.

4.2. Пожежна профілактика у приміщенні школи

Перед розглядом заходів пожежної профілактики слід провести огляд приміщення школи з метою ідентифікації потенційних джерел загрози пожежі. Огляд повинен включати перевірку електропроводки, освітлення, опалення, кухонного устаткування та інших систем, які можуть стати джерелом виникнення пожежі.

Пожежна профілактика є важливим аспектом безпеки в школі, яка включає розробку та впровадження заходів для запобігання виникненню пожеж та забезпечення безпеки учасників навчального процесу. Дотримання пожежної профілактики допомагає мінімізувати ризик пожеж та забезпечує безпеку приміщення школи.

Розглянемо конкретні заходи пожежної профілактики, які можуть бути впроваджені у приміщенні школи:

- проведення регулярних перевірок пожежної сигналізації: забезпечення належного функціонування пожежної сигналізації є важливим аспектом пожежної безпеки. Регулярні перевірки допомагають виявляти потенційні проблеми з системою та вчасно їх усувати.
- навчання персоналу та учнів евакуаційним процедурам: проведення пожежних тренувань та навчання правилам евакуації є необхідними кроками для підготовки до можливих ситуацій пожежі. Персонал та учні повинні бути ознайомлені з процедурами евакуації та знати шляхи виходу.
- установка та перевірка пожежних вогнегасників: пожежні вогнегасники є важливими засобами пожежогасіння, тому їх установка та регулярна перевірка є необхідними. Переконайтеся, що вогнегасники розташовані на доступних місцях і їх термін придатності не минув.

Пожежна профілактика в приміщенні школи має на меті забезпечення безпеки всіх присутніх, включаючи учнів, вчителів і інший персонал. Для досягнення цієї мети необхідно впроваджувати ряд заходів, які спрямовані на запобігання виникненню пожеж та мінімізацію їх наслідків.

Одним з найважливіших аспектів пожежної профілактики є належна підготовка персоналу та учнів до евакуації в разі пожежі. Регулярні практичні тренування та навчання правилам евакуації допомагають забезпечити швидку та безпечну евакуацію у разі надзвичайної ситуації.

Крім того, важливо забезпечити належне функціонування систем пожежної безпеки, таких як пожежна сигналізація, системи пожежного гасіння та вентиляції. Регулярні перевірки та обслуговування цих систем гарантують їх належну роботу в разі потреби. Крім того, установка пожежних вогнегасників на доступних місцях та їх регулярна перевірка є важливим аспектом пожежної профілактики.

Окрім запобігання виникненню пожеж, також потрібно приділяти увагу безпеці під час проведення пожежних вправ і навчальних заходів, щоб уникнути нещасних випадків. Важливо дотримуватися інструкцій та встановлених правил під час проведення таких заходів і завжди мати план дій у разі непередбачених ситуацій.

Тому у такому випадку необхідний план евакуації приміщення, який є важливою складовою пожежної профілактики в школі. Він визначає послідовність дій, які необхідно виконати у разі виникнення пожежі або іншої надзвичайної ситуації, що загрожує безпеці учасників навчального процесу.

Основна мета плану евакуації полягає в тому, щоб усі присутні в школі люди могли швидко і безпечно покинути приміщення та зібратися на зазначеному місці збору. План евакуації повинен бути чітким, зрозумілим і добре відомим всім учасникам навчального процесу.

Ефективний план евакуації є важливою складовою безпеки школи та допомагає зменшити ризик у разі надзвичайної ситуації, такої як пожежа, землетрус або інший потенційно небезпечний інцидент. [8]

План евакуації повинен бути ретельно розроблений, чітким і зрозумілим для всіх учасників навчального процесу, включаючи учнів, вчителів, адміністрацію та інший персонал школи.

Основні етапи плану евакуації включають:

- визначення шляхів евакуації: у школі повинні бути встановлені та позначені шляхи евакуації, які ведуть до безпечних виходів з приміщення. Шляхи евакуації повинні бути чітко виділені, вільні від перешкод та легкодоступні для усіх учасників навчального процесу.
- установлення місця збору: в плані евакуації повинно бути визначене безпечне місце збору поза будівлею школи. Для прикладу це майданчик, спортивний майданчик, де учасники навчального процесу зможуть зібратися та бути під наглядом.
- навчання персоналу та учнів: всі учасники навчального процесу повинні бути ознайомлені з планом евакуації і знати свої ролі та обов'язки під час евакуації. Персонал школи повинен бути навчений керувати процесом евакуації та допомагати учням покинути приміщення.
- проведення тренувань: регулярні тренування плану евакуації допомагають усвідомити процес евакуації і навчитися діяти в умовах пожежі. Це можуть бути заплановані тренування або несподівані випробування для перевірки реакції учасників навчального процесу.
- оновлення та ревізія: план евакуації повинен періодично оновлюватися і переглядатися з метою врахування змін в структурі школи, нових загроз або інших факторів, що можуть вплинути на безпеку. Також важливо здійснювати огляд та підтримку шляхів евакуації та засобів пожежогасіння.

Загальні принципи пожежної профілактики, такі як чистота та порядок у приміщенні, раціональне використання електроприладів та систем опалення, також відіграють важливу роль у запобіганні пожежам. Особлива увага повинна бути приділена контролю за електропроводкою, забезпеченню належного освітлення, а також правильному зберіганню та використанню газового та електричного обладнання. [8]

ВИСНОВКИ

У результаті виконання даної кваліфікаційної роботи було розроблено систему безпеки комп'ютерної мережі Тернопільської ЗОШ №28. В рамках проекту було проведено аналіз, здійснено проектування, розробку та тестування системи з урахуванням актуальності теми і наявних рішень у цій сфері.

У загальній частині проекту було проведено обґрунтування актуальності теми кваліфікаційної роботи, виявлено необхідність розробки системи безпеки Тернопільської ЗОШ №28. Шляхом проведення аналітичного огляду існуючих рішень було здобуто розуміння переваг і недоліків наявних систем, що послужило фундаментом для подальшої розробки власного проекту.

У розділі теоретичної частини було виконано аналіз надійних та перевірених наявних рішень, що дало змогу чітко сформулювати вимоги до розробки системи безпеки для Тернопільської ЗОШ №28. Було здійснено опис існуючих рішень та визначено їх переваги при використанні для побудови безпечної мережі у навчальному закладі. На основі цього опису було розроблено послідовні кроки налаштування існуючих рішень з метою побудови комплексної системи захисту інформації мережі Тернопільської ЗОШ №28.

Основи охорони праці та безпеки життєдіяльності були ретельно розглянуті. Була розроблена оцінка технологічного процесу щодо умов безпеки, втомлюваності та продуктивності праці. Також була розглянута процедура пожежної профілактики у приміщенні школи.

Виконання даної кваліфікаційної роботи спричинило набуття значного практичного досвіду у розробці системи безпеки навчального закладу. Були використані перевірені та надійні методи захисту користувачів від зовнішніх втручань, а також забезпечення безпечного трафіку для захищеності користувачів від потенційних загроз. Результатом цієї роботи є функціональна система захисту мережі Тернопільської ЗОШ №28, яка має потенціал для успішного застосування в інших навчальних закладах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Aakanksha Chopra - Security Issues of Firewall // International Journal of P2P Network Trends and Technology (IJPTT) – Volume 22 Number 1 January 2016

2. Rathod, R.H., & Deshmukh, Prof. V.M. (2013). Role of Distributed Firewalls in Local Network for Data Security. International Journal of Computer Science and Applications, Vol. 6, No. 2, Apr 2013, ISSN: 0974-011 (open access), pp: 360-364

3. Sharad Gore et al, ― Importance of Intrusion Detection System‖ International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011.

4. Virtual Private Networking: An Overview, Sept, 2001, Microsoft:http://technet.microsoft.com/enus/library/bb742566.aspx accessed 01/June/2014

5. Settings MikroTik – URL: https://help.mikrotik.com/

6. Інтернет-справка – URL: https://help.eset.com/

7. Тамара Білько Євгенія Марчиниша Володимир Скібчик Михайло Мотрич Василь Хмельовський - Книга Охорона праці. Навчальний посібник для студентів ОС Бакалавр - видавництво “центр видавничої літератури” 2021 р.

8. Ярослав Бедрій - Охорона праці та пожежна безпека: навчальний посібник для студентів ВНЗ та інженерів-практиків - видавництво “навчальна книга - Богдан” 2014 р.