https://doi.org/10.31891/2307-5732-2025-357-99
УДК 004.49

ГАВРИШ ОЛЕКСАНДР
Черкаський державний технологічний університет
https://orcid.org/0000-0003-4621-9510
e-mail: o.havrysh@chdtu.edu.ua
ЧЕПИНОГА АНАТОЛІЙ
Черкаський державний технологічний університет
https://orcid.org/0000-0003-3921-6557
e-mail: a.chepynoha@chdtu.edu.ua
ГОНЧАРОВ АРТЕМ
Черкаський державний технологічний університет
https://orcid.org/0000-0003-4043-5300
e-mail: a.honcharov@chdtu.edu.ua
КАТАЄВ ДМИТРО
Черкаський державний технологічний університет
https://orcid.org/0009-0001-3055-6451
e-mail: d.kataiev@chdtu.edu.ua

ОРГАНІЗАЦІЙНА СТРУКТУРА ЗАХИСТУ РОЗПОДІЛЕНОЇ МЕРЕЖІ ПІДПРИЄМСТВА НА ОСНОВІ ШЛЮЗІВ БЕЗПЕКИ CISCO

В роботі запропоновано модель захисту інформації розподіленої корпоративної мережі для забезпечення конфіденційності при обміні даними на основі шлюзів безпеки Cisco. Пропонується використовувати апаратний міжмережевий екран Cisco ASA 5505, за допомогою якого можна реалізувати демілітаризовану зону для корпоративних серверів і створити віртуальну приватну мережу.

Ключові слова: інформаційна безпека, міжмережевий екран, демілітаризована зона, технологія VPN, симулятор Cisco Packet Tracer.

HAVRYSH OLEKSANDR, CHEPYNOGA ANATOLII, HONCHAROV ARTEM, KATAIEV DMYTRO
Cherkasy State Technological University

ORGANIZATIONAL STRUCTURE OF PROTECTION OF A DISTRIBUTED NETWORK OF THE ENTERPRISE BASED ON CISCO SECURITY GATEWAYS

When building a corporate network of an organization, the task of uniting its segments that are spread over a long distance often arises. In this case, part of the traffic passes through an unsecured public network, which can cause the leakage of confidential information. To solve this problem, there are standard approaches, one of which is the use of firewalls with VPN technology. With their help, you can build secure communication channels, filter external traffic based on certain rules or templates, ensuring the required level of protection. In this work, it is proposed to use the Cisco ASA 5505 hardware inter-network screen, which can be used to implement a demilitarized zone for corporate servers and create a virtual private network. A description of the structure of the organization is given, which includes the main office with workplaces and a remote branch that is connected remotely via a global network. Hardware based on Cisco equipment was selected, a practical model of the organization's distributed network was created, access lists were configured, allowing to receive responses to requests to servers, and equipment was configured in the Cisco Packet Tracer environment. The proposed configuration of the network, which contains two firewalls, allows to ensure a high level of its security and provides an opportunity for employees of the organization to conduct work remotely, having a confidential access channel to the resources of the company's corporate network. The demilitarized zone is implemented by configuring the security levels on the ports of the ASA 5505 security gateway. The assigned numerical values determine the security level in different directions of traffic exchange. The results of this work can be practically useful to small companies or individual users who seek to increase the level of network security by using the Cisco ASA 5505 hardware firewall.

Keywords: information security, firewall, demilitarized zone, VPN technology, Cisco Packet Tracer simulator.

Стаття надійшла до редакції / Received 23.08.2025
Прийнята до друку / Accepted 15.09.2025

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Стрімка цифровізація суспільства призвела до глобалізації інформаційного середовища, в якому обмін корпоративною інформацією відбувається в публічній мережі Інтернет, яка є вразливою з точки зору інформаційної безпеки. Однією із багатьох задач цієї сфери є забезпечення такої властивості інформації при передачі як конфіденційність, що особливо важливо для інноваційного та конкурентного розвитку компанії [1]. Розв'язання саме цієї задачі вимагає індивідуального та ризик-орієнтованого підходу залежно від складності корпоративних комп'ютерних систем та мереж, затверджених політик інформаційної безпеки, складності та критичності бізнес-процесів [2]. Для забезпечення конфіденційності для даних під час передачі на сьогоднішній день пропонується безліч рішень: від простих – для малих офісів, до комплексних – для середніх та великих за розміром компаній, які, як правило, вимагають складних налаштувань [3]. Проте безумовним лідером по застосуванню в корпоративних системах є міжмережні екрани (нім. Brandmauer, англ. firewall). Вони представляють собою комплекс програмних або програмно-апаратних засобів, що інтегруються в комп'ютерну мережу для контролю і фільтрації мережного трафіку, який проходить через брандмауер

відповідно до заданих правил [4]. Міжмережні екрани також називають шлюзами безпеки або фільтрами, оскільки їх основна задача зводиться до фільтрації (заборони пропуску певних пакетів, що не задовольняють вимогам налаштованої політики безпеки) [5].

Аналіз досліджень та публікацій

Загальні принципи функціонування брандмауера в корпоративному середовищі визначаються політикою безпеки організації, відповідно один і той самий пристрій може зовсім по-різному фільтрувати трафік, залежно від критеріїв, що визначені в конфігурації [6]. Для пересічних користувачів цілком вистачає програмних брандмауерів на основі вузла, які можуть бути як складовою частиною операційної системи так і окремим програмним забезпеченням. Вони доступні, але менш надійні та використовують частину ресурсів комп'ютера.

В даній роботі досліджується питання реалізації інформаційної безпеки корпоративної мережі організації для забезпечення конфіденційності при обміні даними з віддаленими філіалами із застосуванням міжмережних екранів. Зважаючи на це, доцільно використовувати корпоративні рішення на базі програмно-апаратних брандмауерів, які представляють собою окремий пристрій з власною операційною системою і спеціалізованим програмним забезпеченням. Такі пристрої дозволяють забезпечити підвищені вимоги до безпеки, високу продуктивність мережі та відмовостійкість, проте потребують фахового підходу до налаштувань.

Виходячи з нормативних документів, політика безпеки організації розробляється згідно з положеннями [7, 8]. А це в свою чергу буде впливати на побудову системи захисту інформації з використанням міжмережевих екранів. Для забезпечення безпеки мережі по периметру необхідно визначитися з класом обладнання, за допомогою якого можна вирішити цю задачу. Аналіз показує, що майже кожна корпоративна мережа має в своєму складі крайовий маршрутизатор, який також може виконувати певні функції міжмережного екрану. В свою чергу останній може реалізовувати також і маршрутизацію, якої зазвичай достатньо для забезпечення всіх функцій корпоративної мережі. Проте, функціональні можливості міжмережевих екранів з точки зору підвищення безпеки значно ширше, тому для корпоративних рішень варто використовувати саме їх. Компанія Cisco Systems [9] пропонує велику кількість моделей шлюзів для під'єднання до мережі та покращення рівня її безпеки. Cisco ASA (Adaptive Security Appliance) представляє собою серію апаратних міжмережевих екранів, розроблених компанією Cisco Systems. Для невеликих організацій доцільно використовувати модель Cisco ASA 5505 з відмінним співвідношенням ціна-якість, яка забезпечує надійний захист мережі від зовнішніх атак, вторгнень, вірусів, спаму, шпигунських програм, надає можливість фільтрації трафіку користувачів за типом контенту [10].

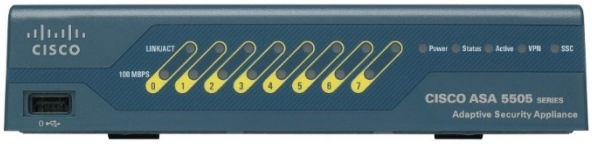

Рис. 1. Зовнішній вигляд апаратного мережевого екрану Cisco ASA 5505

Крім функцій міжмережевого екрану пристрій ASA 5505 має вбудований механізм NAT для організації спільного доступу користувачів до Інтернету, використовується як VPN сервер з протоколом IPSec для безпечного віддаленого доступу до локальних ресурсів мережі. Складовою частиною пристрою є вбудований комутатор на вісім портів, два з яких мають підтримку PoE, що спрощує підключення зовнішніх пристроїв [11].

Синтаксис командного рядка для міжмережевих екранів відрізняється від команд інтерфейсу CLI маршрутизаторів. Керувати шлюзом безпеки можна за допомогою мережевих протоколів telnet або SSH, веб-інтерфейсу або за допомогою програми Cisco *Adaptive Security Device Manage*.

Формулювання цілей статті

Мета дослідження: побудова моделі захисту інформації розподіленої корпоративної мережі для забезпечення конфіденційності при обміні даними на основі шлюзів безпеки Cisco.

Задачі дослідження:

1) проаналізувати структуру організації (установи) з точки зору вимог до її інформаційної безпеки;

2) побудувати модель розподіленої корпоративної мережі з провадженням технології міжмережевих екранів;

3) провести практичну реалізацію налаштувань мережі з демілітаризованою зоною з використанням технології VPN за рахунок налаштування портів шлюзу.

Виклад основного матеріалу

В роботі розглядається умовна організація невеликого розміру з головним офісом, що складається з трьох відділів та серверної, і віддаленим філіалом. Для додаткового забезпечення кіберзахисту в моделі використано також окремі VLAN для кожного відділу в головному офісі (рис.2).

Дана модель конфігурації мережі організації представляє собою модернізацію моделі, що досліджувалася в роботі [12]. Коротко охарактеризуємо головні сегменти мережі, представленої на рис. 2.

- Локальна мережа організації LAN (виділена салатовим кольором знизу ліворуч) містить три відділи, представлені кожний одним робочим місцем, та сервер з ресурсами головного офісу, об'єднані за допомогою комутаторів.
- Філіал організації, який представляє собою віддалене робоче місце працівника, що працює дистанційно Branch (виділений блакитним кольором знизу праворуч).
- Демілітаризована зона, яка містить DNS та веб-сервери (виділена червоним кольором вгорі схеми).
- Маршрутизатори Cisco 2901, що об'єднують різні сегменти мережі в загальну топологію.
- Шлюзи безпеки Cisco ASA 5505, що фільтрують трафік, відповідно до правил безпеки організації.

Зв'язок між офісом та філіалом було вирішено шифрувати за допомогою технології VPN "точка-точка", що забезпечить безпечний обмін пакетами через відкритий канал зв'язку.

Для забезпечення належного рівня безпеки, було вирішено впровадити демілітаризовану зону для серверної, котра у разі проникнення зловмисників на її ресурс не дозволить розповсюдитись їм по мережі.

Практична реалізація налаштування VPN та DMZ. Налаштування мережі відбуватиметься в розробленому Cisco Systems середовищі Cisco Packet Tracer, яке представляє собою симулятор мережі передачі даних. Він дозволяє розробляти та перевіряти моделі мережі, налаштовувати (командами Cisco IOS) маршрутизатори та комутатори, взаємодіяти між кількома користувачами [13, 14]. В даній роботі буде розглянуто тільки ті налаштування, які стосуються саме роботи каналу VPN з опущенням інших налаштувань.

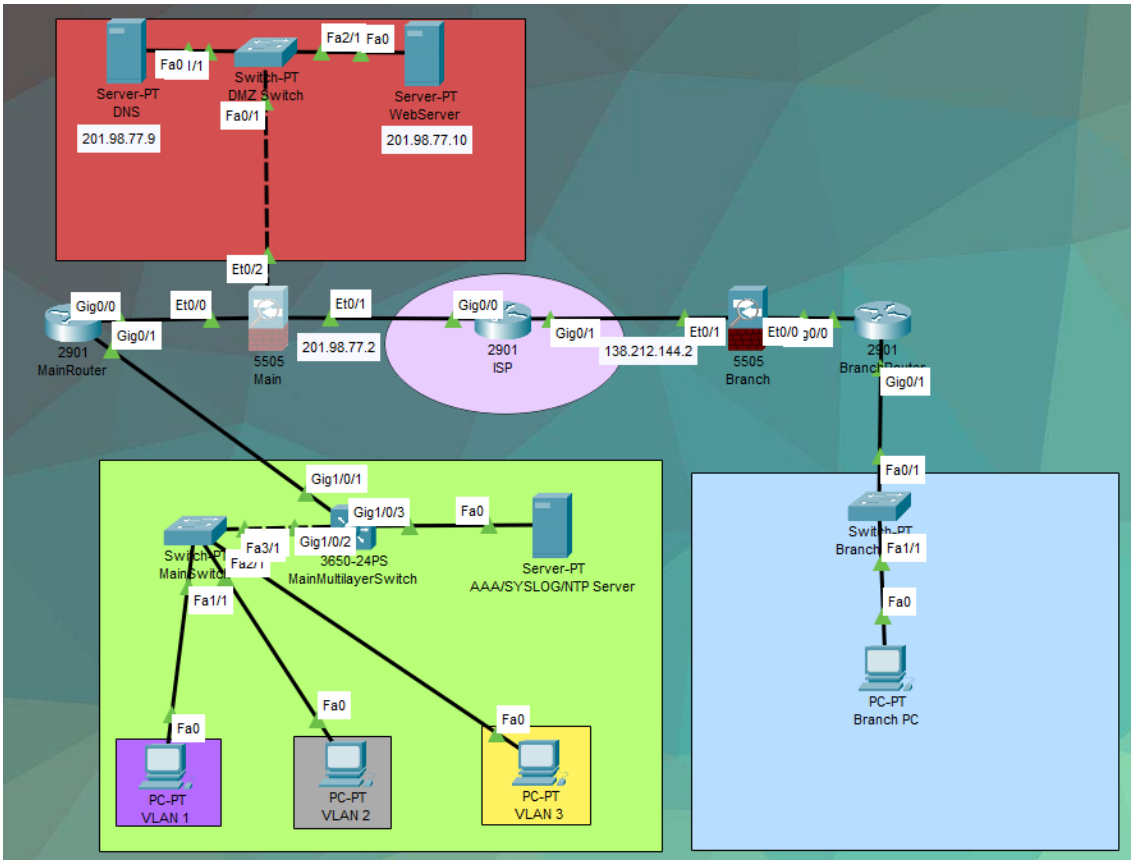

Рис. 2. Схема розподіленої мережі організації

Питання впровадження демілітаризованої зони було вирішено за допомогою налаштування рівнів безпеки на портах шлюзу безпеки ASA 5505. Рівень безпеки – це числова константа, від значення якої визначається куди пропускається трафік в залежності від того, звідки він надходить. В даному випадку порт з назвою "inside", що відповідає за внутрішню мережу офісу, має значення рівня безпеки 100, а порт, що відповідає за DMZ – 70. Це означає, що трафік з офісу в DMZ проходить вільно, але не навпаки.

На рис.3 показано створені VLAN для портів шлюзу безпеки із заданими значеннями рівня безпеки. Необхідно зауважити що найвищий рівень безпеки відповідає значенню 0 і встановлений для локальної мережі організації.

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 201.98.77.5 255.255.255.252
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 201.98.77.2 255.255.255.252
!
interface Vlan3
 nameif DMZ
 security-level 70
 ip address 192.168.3.1 255.255.255.0
```

Рис. 3. Налаштування портів для демілітаризованої зони

На початковому етапі було створено список доступу який буде пропускати шифрований трафік з Main до Branch:

access-list VPN_MAIN extended permit ip 201.98.77.32 255.255.255.224 host 138.212.144.10
access-list VPN_MAIN extended permit udp host 201.98.77.9 host 138.212.144.10
access-list VPN_MAIN extended permit ip host 201.98.77.10 host 138.212.144.10
access-list VPN_MAIN extended permit ip host 201.98.77.11 138.212.144.0 255.255.255.0

Для доступу до серверів демілітаризованої зони із філіалу було налаштовано такі списки доступу:

access-list DMZ_OUT extended permit tcp host 138.212.144.10 host 192.168.3.3
access-list DMZ_OUT extended permit udp host 138.212.144.10 host 192.168.3.2

Показані списки дозволяють проходження трафіку з вузлів 192.168.3.3 та 192.168.3.2, що є веб-сервером та DNS сервером, за портами TCP та UDP для внутрішньої мережі в офісі.

Також необхідно створити політику обміну ключами (рис.4) та налаштувати тунельну групу.

```
crypto ikev1 policy 1
encr aes
authentication pre-share
group 2
crypto ikev1 enable outside
tunnel-group 138.212.144.2 type ipsec-l2l
tunnel-group 138.212.144.2 ipsec-attributes
 ikev1 pre-shared-key CHDTU
```

Рис. 4. Налаштування політики обміну ключами тунелю VPN

Після створення списків доступу, вказуються методи та перетворення трафіку, налаштовується криптографічна мапа, час життя сесії та інтерфейс роботи. Наступним кроком визначають метод шифрування, автентифікації та метод передачі ключа (рис.5).

```
crypto ipsec ikev1 transform-set l2l esp-aes esp-sha-hmac
crypto map VPN 10 match address VPN_MAIN
crypto map VPN 10 set peer 138.212.144.2
crypto map VPN 10 set security-association lifetime seconds 86400
crypto map VPN 10 set ikev1 transform-set l2l
crypto map VPN interface outside
```

Рис. 5. Налаштування криптографічної мапи, часу життя сесії та інтерфейсу

Випробування впровадженої системи захисту інформації. Для перевірки працездатності VPN-тунелів, скористаємося командою show crypto ipsec sa, що покаже скільки статистику роботи створеного каналу. Результати виконання цієї команди та роботи тунелю VPN показані на рис.6.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Для забезпечення бажаного рівня захисту інформаційної безпеки організації пропонується використовувати шлюз безпеки Cisco ASA 5505. За його допомогою можна налаштувати зв'язок між офісом та філіалом за допомогою VPN-з'єднання формату точка-точка, що дозволить забезпечити конфіденційність трафіку через відкритий канал зв'язку. Відокремлення демілітаризованої зони здійснено за допомогою налаштування рівнів безпеки на портах шлюзу безпеки ASA 5505, що визначають типи зон. Для цього задані числові значення, які визначають рівень безпеки в різних напрямках обміну трафіком. Також створено списки доступу, що дозволяють фільтрувати отримувачів інформації при запитах до серверів.

```
Main#sh cry ipse sa

interface: outside
    Crypto map tag: VPN, seq num: 10, local addr 201.98.77.2

      permit ip 201.98.77.32 255.255.255.224 host 138.212.144.10
      local  ident (addr/mask/prot/port): (201.98.77.32/255.255.255.224/0/0)
      remote  ident (addr/mask/prot/port): (138.212.144.10/255.255.255.255/0/0)
      current_peer 138.212.144.2
      #pkts encaps: 24, #pkts encrypt: 24, #pkts digest: 0
      #pkts decaps: 328, #pkts decrypt: 328, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors 0, #recv errors 0

      local crypto endpt.: 201.98.77.2/0, remote crypto endpt.:138.212.144.2/0
      path mtu 1500, ip mtu, ipsec overhead 78,  media mtu 1500
      current outbound spi: 0x2CE2DDAA(753065386)
      current inbound spi: 0x5C2CAE62(753065386)

     inbound esp sas:
      spi: 0x5C2CAE62(1546432098)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, }
         slot: 0, conn id: 2008, crypto map: VPN
         sa timing: remaining key lifetime (k/sec): (4525504/83857)
         IV size: 16 bytes
         replay detection support: N
         Anti replay bitmap:
          0x00000000 0x0000001F
     outbound esp sas:
      spi: 0x2CE2DDAA(753065386)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, }
         slot: 0, conn id: 2009, crypto map: VPN
         sa timing: remaining key lifetime (k/sec): (4525504/83857)
         IV size: 16 bytes
         replay detection support: N
         Anti replay bitmap:
          0x00000000 0x00000001
  Crypto map tag: VPN, seq num: 10, local addr 201.98.77.2

    permit ip host 201.98.77.11 138.212.144.0 255.255.255.0
    local  ident (addr/mask/prot/port): (201.98.77.11/255.255.255.255/0/0)
    remote  ident (addr/mask/prot/port): (138.212.144.0/255.255.255.0/0/0)
    current_peer 138.212.144.2
    #pkts encaps: 306, #pkts encrypt: 306, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
    #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 201.98.77.2/0, remote crypto endpt.:138.212.144.2/0
    path mtu 1500, ip mtu, ipsec overhead 78,  media mtu 1500
    current outbound spi: 0x2CE2DDAA(753065386)
    current inbound spi: 0x5C2CAE62(753065386)

   inbound esp sas:
    spi: 0x5C2CAE62(1546432098)
       transform: esp-aes esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, }
       slot: 0, conn id: 2008, crypto map: VPN
       sa timing: remaining key lifetime (k/sec): (4525504/83857)
       IV size: 16 bytes
       replay detection support: N
       Anti replay bitmap:
        0x00000000 0x0000001F
   outbound esp sas:
    spi: 0x2CE2DDAA(753065386)
       transform: esp-aes esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, }
       slot: 0, conn id: 2009, crypto map: VPN
       sa timing: remaining key lifetime (k/sec): (4525504/83857)
       IV size: 16 bytes
       replay detection support: N
       Anti replay bitmap:
        0x00000000 0x00000001
```

Рис. 6 Перевірка статистики роботи тунелю VPN

В даній роботі брандмауер застосовано для захисту від атак типу «Людина посередині», від зламу сеансів підключень віддаленого робочого столу, що може надати доступ сторонній особі до комп'ютера, який знаходить у локальній мережі і керування ним. Додатково міжмережний екран

використано як аналізатор трафіку у вигляді системи запобігання вторгненню, що не дозволить інфікованому трафіку потрапити із зовнішньої публічної мережі в мережу організації та при компрометації серверів демілітаризованої зони. Використовуючи потужний інструмент у вигляді симулятора Cisco Packet Tracer, створено практичну комп'ютерну модель розподіленої мережі умовної організації, та проведене налаштування устаткування та перевірка працездатності моделі мережі.

В результаті виконання поставлених завдань було досліджено модель мережі організації, що містить шлюз безпеки, за допомогою якого було організовано захищений канал зв'язку з використанням технології Site-to-site VPN та створено відокремлену мережу DMZ, до якої входять серверні системи організації, що в комплексі вирішує проблему захисту інформації.

Наукова новизна дослідження полягає в подальшому розвитку методів та моделей побудови захисту інформації на мережевому рівні з використанням шлюзу безпеки Cisco, який дозволяє шляхом налаштування портів створити демілітаризовану зону, організувати VPN-тунель для забезпечення можливості дистанційного під'єднання віддалених офісів та співробітників компанії до всіх ресурсів корпоративної мережі.

Практична значущість отриманих результатів полягає у створенні моделі мережевої взаємодії віддалених співробітників організації, яка містить шлюз безпеки Cisco, що забезпечує захист інформації як в самій корпоративній мережі так і при приєднанні до неї через глобальну мережу.

Перспективи подальших досліджень. Запропонована модель захисту інформації в організації за допомогою шлюзу безпеки Cisco, дасть можливість частині працівників працювати дистанційно з дотриманням вимог безпеки. Придбання додаткової ліцензії може розширити функціональні можливості обладнання і при потребі мережа може бути модифікована під конкретні запити замовника. Розглянуті принципи практичної реалізації захищеної мережі, налаштування портів шлюзу безпеки, VPN-каналу, створення списків доступу, визначення методів шифрування даних, налаштування криптографічної мапи та перевірка правильності налаштувань є методологічною основою проєктування додаткових захищених елементів та сегментів мережі, що дозволяє зберігати її властивості.

Література

1. Ткач, Ю.М., Базилевич, В.М., Гур'єв, В.І., & Усов, Я.Ю. (2018). Аналіз вразливостей корпоративних інформаційних систем. *Захист інформації*, *20*(1), 61-66.
2. XSTR-SUSS Successful use of security standards (2021) – Режим доступу https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTSS-2020-3-PDF-E.pdf
3. Yan, F., Jian-Wen, Y., Lin, C. (2015) Computer Network Security and Technology Research, *Seventh International Conference on Measuring Technology and Mechatronics Automation, Nanchang*, China, 293-296, doi: 10.1109/ICMTMA.2015.77.
4. Mohan V. (2015) Network Security and Types of Attacks in Network. *International Conference on Intelligent Computing, Communication & Convergence*. Procedia Computer Science 48, 503 – 506.
5. Aakanksha Chopra (2016) Security Issues of Firewall. *International Journal of P2P Network Trends and Technology (IJPTT)* – Volume 22 Number 1, 4-9.
6. 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, 360-364.
7. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806) – Режим доступу https://tzi.com.ua/downloads/1.1-002-99.pdf
8. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах, наказ ДСТСЗІ СБУ від 04.12.2000 № 53 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806) – Режим доступу https://tzi.com.ua/ downloads/1.4-001-2000.pdf
9. Cisco IOS Quality of Service Solutions Configuration Guide (2019) – Режим доступу https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/command/qos-cr-book.pdf
10. Cisco ASA 5500-X Series Firewalls. – Режим доступу https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/series.html
11. QoS on the Cisco ASA Configuration Examples – Режим доступу https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/82310-qos-voip-vpn.pdf
12. Havrysh, O.S., Obruch, Yu.Yu., Chepinoha, A.V., Goncharov, A.V., Panasco, O.M. (2023) Organizational structure of technical protection of information at the network level using VPN technology. *Bulletin of ChDTU*, No.3, 5-15.
13. Мельник, Г.М., Вербовий, С.О., Возняк С.І. (2018) Методичні рекомендації до виконання лабораторних робіт з дисципліни «Комп'ютерні мережі» для студентів освітнього ступеня бакалавр спеціальності 123 «Комп'ютерна інженерія». Тернопіль: ТНЕУ, 71 с.
14. Cisco Packet Tracer - Режим доступу https://www.netacad.com/ru/courses/packet-tracer

References

1. Tkach, Yu.M., Bazilevich, V.M., Guriev, V.I., Usov, Ya.Yu. (2018). Analysis of vulnerabilities of corporate information systems. *Information Protection*, 20(1), 61-66.
2. XSTR-SUSS Successful use of security standards (2021) – Retrieved from https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTSS-2020-3-PDF-E.pdf
3. Yan, F., Jian-Wen, Y., Lin, C. (2015) Computer Network Security and Technology Research, *Seventh International Conference on Measuring Technology and Mechatronics Automation, Nanchang*, China, 293-296, doi: 10.1109/ICMTMA.2015.77.
4. Mohan V. (2015) Network Security and Types of Attacks in Network. *International Conference on Intelligent Computing, Communication & Convergence*. Procedia Computer Science 48, 503 – 506.
5. Aakanksha Chopra (2016) Security Issues of Firewall. *International Journal of P2P Network Trends and Technology (IJPTT)* – Volume 22 Number 1, 4-9.
6. 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, 360-364.
7. ND TZI 1.1-002-99 General provisions on the protection of information in computer systems against unauthorized access, order of the DSTSZI of the SBU dated 04/28/99 (Amendment No. 1 order of the State Special Communications Administration dated 12/28/2012 No. 806) – Retrieved from https://tzi.com.ua/downloads/1.1-002-99.pdf
8. ND TZI 1.4-001-2000 Standard provisions on the information protection service in automated systems, order of the DSTSZI of the SBU dated 04.12.2000 No. 53 (Amendment No. 1 order of the Administration of State Special Communications dated 28.12.2012 No. 806) – Retrieved from https://tzi.com.ua/ downloads/1.4-001-2000.pdf
9. Cisco IOS Quality of Service Solutions Configuration Guide (2019) – Retrieved from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/command/qos-cr-book.pdf
10. Cisco ASA 5500-X Series Firewalls. – Retrieved from https://www.cisco.com/c/ en/us/support/security/asa-5500-series-next-generation-firewalls/series.html
11. QoS on the Cisco ASA Configuration Examples – Retrieved from https://www.cisco.com/ c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/82310-qos-voip-vpn.pdf
12. Havrysh, O.S., Obruch, Yu.Yu., Chepinoha, A.V., Goncharov, A.V., Panasco, O.M. (2023) Organizational structure of technical protection of information at the network level using VPN technology. *Bulletin of ChDTU*, No.3, 5-15.
13. Melnyk H.M., Verbovy S.O., Voznyak S.I. (2018) *Methodological recommendations for performing laboratory work in the discipline "Computer networks" for students of the bachelor's degree in specialty 123 "Computer engineering"*. Ternopil: TNEU, 71 p.
14. Cisco Packet Tracer - Retrieved from https://www.netacad.com/ru/courses/packet-tracer