Вісник ЛДУБЖД
Bulletin of Lviv State University of Life Safety
https://journal.ldubgd.edu.ua/index.php/Visnuk
ISSN 2078-4643 (print), ISSN 2708-1389 (online)

UDC 004.056.5
DOI: 10.32447/20784643.29.2024.07

О. І. Полотай[1], Н. І. Федінець[1], Н. П. Кухарська[2]
[1]Львівський державний університет безпеки життєдіяльності, м. Львів, Україна
[2]Національний університет «Львівська Політехніка», м. Львів, Україна
ORCID: https://orcid.org/0000-0003-4593-8601 – О. І. Полотай
https://orcid.org/ 0000-0001-6811-3720 – Н. І. Федінець
https://orcid.org/0000-0002-0896-8361 – Н. П. Кухарська
orest.polotaj@gmail.com

ДОСЛІДЖЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА СПОСОБІВ ЇХ ВИРІШЕННЯ В КОМП'ЮТЕРНИХ МЕРЕЖАХ НА КАНАЛЬНОМУ РІВНІ

Постановка проблеми. Інформаційна безпека комп'ютерних мереж – це процес захисту комп'ютерних мереж від несанкціонованого доступу, зловживань, витоку конфіденційної інформації та інших загроз, що виникають через зловмисників або недбалість користувачів. Для захисту комп'ютерних мереж використовуються різні технології та методи, включаючи захист паролем, шифрування даних, мережеві брандмауери, системи виявлення вторгнень, антивірусне програмне забезпечення та аутентифікацію користувачів.

Мета. Метою статті є дослідження основних атак на комп’ютерні мережі, які зловмисник реалізовує, використовуючи слабкі місця другого (канального) рівня моделі OSI та способів нейтралізації цих атак за допомогою програмних інструментів мережевого обладнання компанії Cisco.

Результати. У статті детально описано суть канального рівня моделі OSI, який є другим рівнем. Описано характеристики цього рівня та показано, які основні функції він виконує. Проаналізовано основні загрози інформаційної безпеки комп’ютерних мереж, а також атаки на мережі, які зловмисник реалізовує, використовуючи усі «вузькі місця» канального рівня моделі OSI. Детально описано кожну з таких загроз і способи її реалізації. Також в статті детально описано основні способи захисту інформації комп’ютерної мережі на канальному рівні моделі OSI від атак. Наводяться детальні теоретичні кроки для реалізації блокування, нейтралізації або пом’якшення атак на мережі, які зловмисник здійснює на канальному рівні моделі OSI. У статті детально описані способи нейтралізації цих атак за допомогою програмних інструментів мережевого обладнання компанії Cisco.

Висновки. Безпека комп'ютерних мереж є важливим аспектом захисту важливої інформації та конфіденційних даних, а також забезпечення нормальної роботи комп'ютерних систем і мереж. Рівень безпеки комп'ютерних мереж варіюється від організації до організації та від компанії до компанії, але завжди важливо вживати найкращих можливих заходів для захисту критично важливої інформації та забезпечення стабільності системи.

Ключові слова: комп’ютерна мережа, канальний рівень моделі OSI, cisco, кібербезпека, інформаційна безпека, загрози.

O. I. Polotai[1], N. I. Fedynets[1], N. P. Kukharska[2]
[1]Lviv State University of Life Safet
[2]Lviv Polytechnic National University

STUDY OF INFORMATION SECURITY THREATS AND METHODS OF THEIR SOLUTION IN COMPUTER NETWORKS AT THE CHANNEL LEVEL

Introduction. Information security of computer networks is the process of protecting computer networks from unauthorised access, abuse, leakage of confidential information and other threats arising from malicious actors or user negligence. Various technologies and methods are used to protect computer networks, including password protection, data encryption, network firewalls, intrusion detection systems, anti-virus software, and user authentication.

Purpose. The purpose of the article is to study the main attacks on computer networks that an attacker implements using the weak points of the second (channel) level of the OSI model and how to neutralise these attacks with the help of Cisco network equipment software tools.

Results. The article describes in detail the essence of the channel layer of the OSI model, which is the second layer. The characteristics of this level are described and its main functions are shown. The main threats to the information security of computer networks, as well as attacks on networks implemented by an attacker using all the problems of the channel level of the OSI model, are analysed. Each of these threats and the methods of their implementation are described in detail. The article also describes in detail the main methods of protecting computer network information at the channel level of the OSI model from attacks. Detailed theoretical steps are given to implement blocking, neutralising or mitigating attacks on networks carried out by an attacker at the link layer of the OSI model. The article describes in detail ways to neutralise these attacks using Cisco network equipment software tools.

Conclusion. Computer network security is an important aspect of protecting important information and confidential data, as well as ensuring the normal operation of computer systems and networks. The level of security of computer networks varies from organisation to organisation and company to company, but it is always important to take the best possible measures to protect critical information and ensure system stability.

Keywords: computer network, link layer of the OSI model, cisco, cyber security, information security, threats.

Вступ. В умовах сьогодення інформація є важливим елементом та однією з основ сучасного суспільства. Інформаційно-комунікаційні системи та мережі відіграють важливу роль у розширенні доступу користувачів до інформаційних ресурсів та наданні різноманітних послуг. Однак інформаційно-комунікаційні системи та мережі не лише виконують корисні функції та надають різноманітні послуги, але й можуть бути шляхом несанкціонованого доступу до комп'ютерів користувачів. Тому питання комп'ютерних мереж та інформаційної безпеки нерозривно пов'язані між собою і потребують постійного вдосконалення, адже загрози стають все більш серйозними [10].

Важливим елементом для дослідження комп'ютерних мереж є модель взаємодії відкритих систем (OSI), запропонована Міжнародною організацією зі стандартизації (ISO) Модель OSI складається з семи рівнів, кожному з яких відповідає своя загроза інформаційній безпеці. Для побудови комплексної багаторівневої системи захисту інформації необхідно не тільки протидіяти загрозам на кожному рівні моделі OSI, але й розробити політику безпеки, інструкції та рекомендації для користувачів інформаційно-комунікаційних систем та мереж. Модель OSI, розроблена більше року тому, потребує розширення та доповнення для врахування питань інформаційної безпеки [2].

Питання інформаційної та кібербезпеки комп’ютерних мереж, розглядали такі вчені, як Грайворонський М.В., Михайлюта С.Л., Степанушко І.В., Бабич Б.О., Ткаченко В.Ю., Лавринович В.С., Вертузаєв М.С., Юрченко О.М. та ін. Проте дослідження цього питання ще перебуває в початковому етапі та потребує подальшого вивчення, особливо якщо враховувати таку вузьку спрямованість, як канальний рівень моделі OSI.

Існує низка підходів до класифікації загроз та можливих атак на комп'ютерні мережі. Враховуючи, що апаратне та програмне забезпечення комп'ютерних мереж працює на відповідному рівні моделі взаємодії відкритих систем (модель OSI), для аналізу методів і засобів захисту використовується класифікація, яка також орієнтована на модель OSI [8]. Найпоширеніші атаки найчастіше здійснюються на п'яти рівнях (фізичному, канальному, мережевому, транспортному та прикладному). Загрози сеансового та представницького рівнів в основному пов'язані з процедурами ідентифікації, аутентифікації та шифрування, алгоритми і протоколи яких реалізовані в операційній системі і мають мінімальний вплив на роботу мережевих адміністраторів. Ця стаття зосереджена на загрозах і технологіях захисту на канальному рівні моделі OSI.

Методи досліджень. Методологічну основу дослідження становлять принципи та основні категорії діалектичного пізнання соціальних явищ і процесів, розвитку та взаємозв’язку об’єктів реальної дійсності, системи загальнонаукових та спеціальних методів, які є засобами наукового пошуку в арсеналі гуманітарних, у тому числі й юридичних наук. Поряд із загальновідомими науковими та іншими методами дослідження у статті були використані такі: структурно-системний метод для дослідження взаємозв'язків між елементами механізму загроз інформаційної безпеки комп’ютерних мереж як системи та технологіями захисту інформації на цьому рівні, використовуючи програмні засоби мережевих пристроїв другого рівня компанії Cisco.

Результати досліджень. Канальний рівень – другий рівень мережної моделі OSI, призначений для передачі даних між вузлами, що перебувають в одному сегменті локальної мережі.

Канальний рівень моделі OSI, готує мережні дані для фізичної мережі. Він відповідає за зв'язок між мережними інтерфейсними картами.

Канальний рівень виконує такі функції:

- забезпечує верхнім рівням можливість отримати доступ до середовища передавання даних. Протокол верхнього рівня не має повної інформації про тип середовища, який використовується для пересилання даних;
- приймає дані, зазвичай пакети Рівня 3 (тобто IPv4 або IPv6), і інкапсулює їх у кадри другого рівня;
- контролює спосіб розміщення та отримання даних в/з середовища передавання даних;
- забезпечує обмін кадрами між кінцевими точками через середовище передавання даних;
- отримує інкапсульовані дані, зазвичай пакети мережевого рівня, і передає їх відповідному протоколу верхнього рівня;
- виявляє помилки і відкидає всі пошкоджені кадри.

Технології канального рівня складають основу локальних мереж, тому забезпечення безпеки їх роботи – наріжний камінь безпеки мережі в цілому, оскільки зламавши її на цьому рівні, зловмисник отримує можливості обійти заходи захисту на верхніх рівнях.

Мережеві адміністратори зазвичай розгортають рішення безпеки для захисту елементів 3-7 рівнів моделі OSI, таких як VPN, брандмауери та пристрої IPS. Однак порушення безпеки на канальному рівні також впливає на всі рівні, розташовані вище. Наприклад, якщо зловмисник, який має доступ до внутрішньої мережі, успішно перехоплює кадри на канальному рівні, всі засоби захисту на верхніх рівнях стають марними. Зловмисник може завдати значної шкоди інфраструктурі локальної мережі на другому рівні.

Загалом, усі атаки на канальний рівень можна поділити на атаки активного і пасивного типів. До активних атак відносяться такі атаки, які потребують від зловмисника певних конкретних дій (відмова в обслуговуванні, порушення роботи мережі або її ділянок), а до пасивних – атаки підслуховування, підміна довіреного суб'єкта [7].

Якщо розглянути всі атаки на канальний рівень, то їх можна згрупувати і виділити кілька типів загроз:

- спуфінг з метою прозорого перехоплення інформації;
- відмова в обслуговуванні якогось ресурсу системи;
- несанкціонований доступ до ділянок мережі;
- порушення правильної роботи мережі або її ділянок.

Найпоширенішими атаками канального рівня є перевантаження каналів передачі даних та комутаційного обладнання шляхом генерації широкомовних кадрів (так звані "широкомовні шторми" у великих комутаційних мережах мають той самий результат), підміна MAC-адрес вузлів, атаки на протоколи ARP та Spanning Tree Protocol [4]. Методи захисту канального рівня стосуються в першу чергу MAC-адрес вузлів, але їхня сфера застосування поширюється і на мережевий рівень, оскільки багато засобів захисту комутаторів також аналізують і використовують IP-адреси вузлів.

Першим кроком до зменшення ризику атак є розуміння основних функцій канального рівня та загроз, які несе в собі інфраструктура.

З точки зору інформаційної безпеки, канальний рівень добре вивчений і відповідає за формування та доставку безпомилкових кадрів. На цьому рівні використовуються апаратні обчислення MAC-адрес і контрольних сум; атаки підміни MAC-адрес, атаки на протоколи ARP і Spanning Tree широко використовуються зловмисниками, кінцевою метою яких є перехоплення трафіку і отримання доступу до більш чутливої інформації [10]. У таблиці 1 описані атаки на систему локальних мереж канального рівня.

Таблиця 1

Основні атаки на комп’ютерну мережу на канальному рівні

Вид атаки	Опис атаки
Атаки на таблиці MAC-адрес	До них належать атаки з переповнення таблиць MAC-адрес (MAC-флуд).
Атаки на VLAN	Включають атаки переходів між VLAN і VLAN з подвійними тегами. До них також належать атаки, що виникають між пристроями у спільній VLAN.
Атаки, пов'язані з DHCP	Включають атаки з виснаження та підроблення DHCP.
ARP-атаки	До них належать атаки з підміни ARP і отруєння ARP-кешу.
Підроблення адрес	Здійснюються через атаки з підміни MAC- і IP-адрес.
Атаки на STP	Покладаються на маніпуляції з протоколом Spanning Tree.

Переповнення таблиці MAC-адрес призводить до зниження швидкості передачі користувацького трафіку аж до повної непрацездатності мережі. Оскільки всі MAC-таблиці мають обмежений розмір, ресурси комутатора для зберігання MAC-адрес можуть бути вичерпані; атака переповнення MAC-адрес шляхом бомбардування комутатора кадрами, що містять підроблені MAC-адреси джерела, доки MAC-таблиці не будуть заповнені, Вона використовує це обмеження.

Як тільки ця умова досягнута, комутатор розглядає кожен кадр як невідомий одноадресний кадр і починає переповнювати весь вхідний трафік через всі порти в одній VLAN (віртуальній локальній мережі) без посилання на MAC-таблицю. У цій ситуації зловмисник може перехопити всі кадри, що надходять від одного хоста до іншого в локальній мережі або в локальній VLAN.

Лавинний трафік не може перетинати локальну мережу або VLAN. Зловмисник може перехоплювати трафік лише в локальній мережі або VLAN, до якої він підключений.

Атаки, пов'язані з VLAN – це найпопулярніший тип атак. Атаки цього типу передбачають отримання доступу до VLAN, який спочатку був нереалізований для атакуючого ПК. При неправильному налаштуванні комутатора зловмисник може отримати можливість пересилати трафік в інші VLAN, заздалегідь маркуючи кадри.

Існує декілька типів атак, які спрямовані на мережі VLAN. Сюди відносяться такі атаки: переміщення трафіку з однієї віртуальної локальної мережі в іншу без використання пристроїв маршрутизації інформації; атаки з подвійним тегуванням, які полягають в тому, що зловмисник може отримати доступ до вузлів або серверів в інших VLAN, добавивши в кадр додаткове поле з неправдивим тегом з інформацією про вигаданий VLAN;

З протоколом DHCP пов'язано два типи атак – це виснаження DHCP (DHCP starvation) і підроблення DHCP (DHCP spoofing), DHCP DoS.

Виснаження DHCP призначене для створення DoS-атаки для клієнтів, що під'єднуються. Сенс атаки «DHCP DoS»: при реалізації атаки «Виснаження DHCP» на DHCP сервер посилається велика кількість пакетів. Після цього сервер буде завантажений фальшивими запитами і тому справжні запити не будуть опрацьовані.

Атака з підроблення DHCP (DHCP-спуфінг) виникає, коли під'єднаний до мережі шахрайський DHCP-сервер надає законним клієнтам неправильні параметри IP-конфігурації. Шахрайський сервер може надавати різноманітну оманливу інформацію, таку як Неправильний шлюз за замовчуванням, Неправильний DNS-сервер, Неправильна IP-адреса.

ARP-атаки – тип атак, націлених на локальні мережі, метою яких є відправлення шкідливих ARP-пакетів на шлюз. Мета атаки — зміна пар «IP-адреса – MAC-адреса».

Аналіз протоколу безпеки ARP показує, що можна перехопити широкомовні ARP-запити на атакуючому вузлі в певному сегменті мережі та надіслати фальшивий запит (ARP-відповідь), в якому він видає себе за цільовий вузол (наприклад, роутер), активно відстежує мережевий трафік цього вузла.

Для проведення STP-атаки зловмисник може маніпулювати протоколом Spanning Tree Protocol (STP), підміняючи кореневий міст і змінюючи топологію мережі [14].

Захист на канальному рівні включає такі підходи:

- застосування MAC-фільтрації та прив’язок MAC-адрес до портів комутаторів (функція Portsecurity комутатора [1]);
- застосування додаткових функцій захисту комутатора, таких як DHCP snooping, Dynamic ARP inspection та IP SourceGuard [1];
- сегментація мережі на окремі зони (широкомовні домени) з використанням технології VLAN;
- автентифікація та авторизація на канальному рівні.

Ці рішення канального рівня не будуть ефективними, якщо не забезпечити захист протоколам керування. Наприклад, такі традиційні протоколи керування, як Syslog, SNMP, TFTP, telnet, FTP і багато інших поширених протоколів є незахищеними; тому рекомендовано дотримуватися таких стратегій:

- використовувати безпечні варіанти протоколів: SSH, Secure Copy Protocol (SCP), Secure FTP (SFTP) і Secure Socket Layer/Transport Layer (SSL/TLS);
- автономно керувати пристроями;
- використовувати спеціальні VLAN для керування, у яких немає нічого окрім службового трафіку;
- використовувати ACL (списки контролю доступу) для відсікання небажаного доступу.

В таблиці 2 описані методи та технології захисту канального рівня а також огляд рішень компанії Cisco для нейтралізації атак Рівня 2.

Таблиця 2

Основні способи захисту інформації комп'ютерної мережі на канальному рівні моделі OSI

Спосіб захисту	Опис
Захист портів (Portsecurity)	Запобігає багатьом типам атак, включно з атаками переповнення таблиці MAC-адрес і виснаження DHCP.
Відстеження DHCP (DHCP Snooping)	Допомагає запобігти атакам з виснаження і підроблення DHCP.
Динамічна перевірка ARP (DAI)	Запобігає атакам підміни й отруєння ARP.
Захист від підміни IP-адрес (IPSG)	Запобігає атакам підроблення MAC- і IP-адрес.
Сегментація на VLAN	Передача кадрів з будь-якими MAC-адресами отримувача тільки між вузлами окремих VLAN
Авторизація по протоколу 802.1x	Передача кадрів від вузла тільки після проходження автентифікації та авторизації кінцевого пристрою або користувача
Використання штучного інтелекту відстеження трафіку (ШІ)	Цей підхід базується на аналізі трафіка, що проходить через мережеве обладнання канального рівня. Аналіз трафіку та визначення його шкідливості здійснюється за допомогою штучного інтелекту [3].

Захист портів – функція комутатора, яка дозволяє адміністративно визначати MAC-адреси вузлів, підключених до певного порту (прив'язка портів), та обмежує кількість MAC-адрес на порту, яким дозволено надсилати дані через порт. Ця функція комутатора використовується для запобігання несанкціонованій підміні MAC-адрес мережевого пристрою, несанкціонованому підключенню вузла до мережі, запобіганням атак, які спрямовані на переповнення таблиці комутації.

DHCP snooping – функція комутатора для захисту від атак з використанням протоколу DHCP (наприклад, підміни або атаки DHCP-голодування, які додають несанкціоновані DHCP-сервери в мережу або роблять всі адреси на DHCP-сервері доступними для зловмисника).

Динамічна перевірка ARP (DAI) – це функція комутатора, призначена для захисту від ARP-атак. Такі атаки спрямовані на заміну легітимних MAC-адрес в ARP-записах вузла на фальшиві (підміна ARP), що дає змогу зловмисникам перехоплювати кадри від вузлів для доступу до конфіденційної інформації, перехоплювати зв'язок між атакованими вузлами для порушення нормальної роботи мережі, а також порушувати нормальну роботу мережі шляхом перехоплення зв'язку між атакованими вузлами. Щоб протистояти таким атакам, комутатори потребують механізмів, які гарантують, що між портами пересилаються лише легітимні ARP-повідомлення.

VLAN – це віртуальна локальна мережа, яка складається з групи мережевих вузлів, трафік яких, повністю відокремлений від інших мережевих вузлів на канальному рівні. [4]. Це означає, що передача кадрів між різними віртуальними мережами на основі MAC-адрес неможлива.

Обговорення результатів досліджень. Таким чином, існує низка загроз, які притаманні другому рівню моделі OSI. І кожна з них потребує вирішення або пом'якшення.

Наприклад, для пом'якшення атаки MAC-флуду, адміністратори мережі повинні запроваджувати захист портів, що дасть змогу встановити кількість MAC-адрес джерела, які можна вивчити на кожному порті.

Перестрибуванню між VLAN і атакам подвійних тегів можна запобігти, використовуючи правила безпеки магістральної лінії:

- виключати функцію trunking на всіх портах доступу;
- виключати автоматичне налаштування магістралі (auto trunking) на магістральних лініях і запроваджувати лише ручне увімкнення магістралі;
- забезпечувати використання native VLAN лише на магістральних лініях.

Атаки, які спрямовані на DHCP-сервер, нейтралізуються шляхом реалізації відстеження DHCP (DHCP snooping). Підміну та отруєння ARP можна нейтралізувати шляхом впровадження динамічної перевірки ARP (DAI). Спуфінг IP- і MAC-адрес, тобто їх підроблення можна нейтралізувати, впроваджуючи функцію обмеження IP-трафіку на інтерфейсах 2-го рівня – IP Source Guard (IPSG). STP-атаку можна пом'якшити шляхом впровадження захисту BPDU (BPDU Guard) на всіх портах доступу.

В даний час, популярними є системи виявлення атак [8] – це програмні або програмно-апаратні системи, які автоматизують процес аналізу подій в локальній мережі з міркувань безпеки. Крім виявлення всіх типів атак (і реальних і потенційних), такі системи здатні реагувати на атаки – від найпростіших звітів до активного втручання при визначенні проникнень. У наш час СВА вважаються необхідним

елементом інфраструктури безпеки локальних мереж, в тому числі і на канальному рівні.

Отже, для реалізації захисту інформації комп'ютерної мережі від атак, які зловмисник здійснює на канальному рівні моделі OSI, у комутаторах компанії Cisco передбачено ряд інструментів. Однак, для запровадження ефективного захисту, необхідно дотримуватися комплексного підходу та використовувати всі існуючі методи в сукупності.

Висновки. Отже, проблема захисту інформації в комп'ютерних системах є надзвичайно важливою в час, коли такі системи широко використовуються, а комп'ютерні мережі, що передають великі обсяги інформації, розширюються. Безпечна робота комп'ютерних мереж має важливе значення для всіх типів підприємств і організацій, від невеликих приватних компаній до державних установ, в тому числі і Державної служби України з надзвичайних ситуацій. Різниця полягає лише в засобах, методах і масштабах забезпечення безпеки.

Дотримання мережевим адміністратором, який працює з обладнанням Cisco, правил забезпечення інформаційної безпеки та використання інструментів для реалізації цих правил, зокрема на канальному рівні, дасть змогу більш ефективно розробити та реалізувати систему інформаційної безпеки комп'ютерної мережі.

Список літератури:

1. F.H.Y. Bhaiji, Network security technologies and solutions. Indianapolis, IN, USA: Cisco Press, 2008, ISBN: 978-1-58705-246-0].
2. Kachold Lisa. Layer 8 Linux Security: OPSEC for Linux Common Users, Developers and Systems Administrators // Linuxgazette.net, July 2009 (# 164).
3. Lisa Bock, Learn Wireshark: A definitive guide to expertly analyzing protocols and troubleshooting networks using Wireshark, 2nd Edition, 2022. 606 p.
4. R. Seifert and J. Edwards, The all-new switch book: the complete guide to LAN switching technology, 2nd ed. Indianapolis, IN, USA: Wiley Publishing, cop., 2008, ISBN: 978-0470287156.
5. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В. Ю., Складанний П. М. Технології забезпечення безпеки мережевої інфраструктури: підручник. Київ, КУБГ, 2019. 218 с.
6. Вертузаєв М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: навч. посіб. Київ: Європ. ун-т, 2001. 321 с.
7. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. Київ. Видавнича група BHV, 2009. – 608 с.
8. Жилін А.В., Шаповал О.М., Успенський О.А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Київ: Вид-во «Політехніка», 2021. 213 с.
9. Івченко О., Палагін В. Використання алгоритмів ШІ для аналізу шкідливого трафіку на канальному рівні (ARP SPOOFING). Інформаційна безпека та інформаційні технології: збірник тез доповідей VI Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів, м. Львів, 30 листопада 2023 року. Львів: ЛДУ БЖД, 2023. С. 87-89.
10. Корнієнко Б.Я. Дослідження моделі взаємодії відкритих систем з погляду інформаційної безпеки. Наукоємні технології, 2012. № 3 (15). С. 83-89.
11. Кучернюк П.В. Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні). Мікросистеми, Електроніка та Акустика : науково-технічний журнал. – 2017. – Т. 22, № 6(101). – С. 64-70.
12. Михайлюта С.Л., Степанушко І.В., Бабич Б.О., Ткаченко В.Ю., Лавринович В.С. Дослідження мережевих DOS-атак, що ґрунтуються на використанні протоколу ICMP. Вісник Інженерної академії України. К., 2009. № 2. С. 146–149.
13. Полотай О.І., Дубик А.-О.Ю. Особливості захисту інформації в комп'ютерних мережах. "Світ наукових досліджень" (матер. міжнар. мультидисциплінарної наук. інтернет-конф. (м. Тернопіль, Україна, м. Ополе, Польща, 24-25 жовтня 2023 р.). Вип. 23. С. 291-292.
14. Полотай О.І., Дубик А.-О.Ю. Загрози інформації в комп'ютерних мережах на канальному рівні. "Світ наукових досліджень" (матер. міжнар. мультидисциплінарної наук. інтернет-конф.(м. Тернопіль, Україна, м. Ополе, Польща, 21-21 березня 2024 р.). Вип. 28. С. 185-187.

References:

1. F.H.Y. Bhaiji, Network security technologies and solutions. Indianapolis, IN, USA: Cisco Press, 2008, ISBN: 978-1-58705-246-0].
2. Kachold Lisa. Layer 8 Linux Security: OPSEC for Linux Common Users, Developers and Systems Administrators // Linuxgazette.net, July 2009 (# 164).
3. Lisa Bock, Learn Wireshark: A definitive guide to expertly analyzing protocols and troubleshooting networks using Wireshark, 2nd Edition, 2022. 606 p.
4. R. Seifert and J. Edwards, The all-new switch book: the complete guide to LAN switching technology, 2nd ed. Indianapolis, IN, USA: Wiley Publishing, cop., 2008, ISBN: 978-0470287156
5. Buriachok V.L., Anosov A.O., Semko V.V., Sokolov V. Yu., Skladannyi P. M. (2019). Tekhnolohii zabezpechennia bezpeky merezhevoi

infrastruktury. [Technologies for ensuring network infrastructure security]. Kyiv: KUGB [in Ukrainian].

6. Vertuzaev M.C. & Yurchenko O.M. (2001). Zakhyst informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu [Protection of information in computer systems against unauthorized access]. Kyiv: Publishing House of the European University [in Ukrainian].

7. Graivoronsky M.V. & Novikov O.M. (2022). Bezpeka informatsiino-komunikatsiinykh system [Security of information and communication systems. Electronic scientific specialist publication]. Kyiv: VNV Publishing Group [in Ukrainian].

8. Zylin A.V. (2021). Tekhnolohii zakhystu informatsii v informatsiino-telekomunikatsiinykh systemakh [Information protection technologies in information and telecommunication systems]. Kyiv: KPI named after Igor Sikorsky [in Ukrainian].

9. Ivchenko O. & Palagin V. (2023) Vykorystannia alhorytmiv ShI dlia analizu shkidlyvoho trafiku na kanalnomu rivni (ARP SPOOFING) [Using AI algorithms to analyze malicious traffic at the channel level (ARP SPOOFING)]. *Informatsiina bezpeka ta informatsiini tekhnolohii – Information security and information technologies,* 87-89 [in Ukrainian].

10. Kornienko B.Ya. (2012). Doslidzhennia modeli vzaiemodii vidkrytykh system z pohliadu informatsiinoi bezpeky [Study of the interaction model of open systems from the point of view of information security]. *Naukoiemni tekhnolohii – Science-intensive technologies, 3*, 83–89 [in Ukrainian].

11. Kucherniuk P.V. (2017). Metody i tekhnolohii zakhystu kompiuternykh merezh (fizychnyi ta kanalnyi rivni) [The role of computer forensics in ensuring information security]. *Mikrosystemy, Elektronika ta Akustyka – Microsystems, Electronics and Acoustics*, *6(101)*, 64–70 [in Ukrainian].

12. Mykhailouta S.L., Stepanushko I.V., Babich B.O., Tkachenko V.Yu., Lavrynovych V.S. (2009). Doslidzhennia merezhevykh DOS-atak, shcho gruntuiutsia na vykorystanni protokolu ICMP [Research of network DOS-attacks based on the use of the ICMP protocol].Visnyk Inzhenernoi akademii Ukrainy – *Bulletin of the Engineering Academy of Ukraine*, *2*, 146–149 [in Ukrainian].

13. Polotai O.I. & Dubyk A.-O. (2023). Osoblyvosti zakhystu informatsii v kompiuternykh merezhakh [Peculiarities of information protection in computer networks]. *Svit naukovykh doslidzhen – The world of scientific research*, *23*, 291-292 [in Ukrainian].

14. Polotai O.I. & Dubyk A.-O. (2024). Zahrozy informatsii v kompiuternykh merezhakh na kanalnomu rivni [Information threats in computer networks at the channel level]. *Svit naukovykh doslidzhen – The world of scientific research*, *28*, 185-187 [in Ukrainian].

Науково-методична стаття.
Надійшла до редакції 02.04.2024.
Прийнято до публікації 12.06.2024.