УДК 004.056.5:004.056.4.056.7

КІБЕРБЕЗПЕКА В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ ТА СИСТЕМАХ

У. П. Пановик

Українська академія друкарства,
вул. Під Голоском, 19, Львів, 79020, Україна

Досліджено проблеми кібербезпеки в телекомунікаційних мережах, акцентуючи на методах захисту від зростаючих кібератак. Розглянуто основні різновиди загроз, такі як DDoS-атаки, віруси, фішинг, а також основні категорії кіберзлочинців та їх методи атак. Проаналізовано сучасні методи захисту інформаційних ресурсів, зокрема шифрування даних та використання складних алгоритмів аутентифікації, таких як AES та RSA. Особливу увагу приділено налаштуванню роутерів Cisco як ключових елементів забезпечення кібербезпеки, зокрема встановлення базових параметрів та налаштування функцій аутентифікації. Розглянуто роль брандмауерів у системах кібербезпеки, їх основні функції та типи, а також етапи налаштування, зокрема конфігурацію політики безпеки, моніторинг трафіку, виявлення та блокування підозрілих активностей, оновлення правил безпеки. Описано методи постійного моніторингу мережевої активності та проведення регулярних аудитів безпеки, аналізу вразливостей та своєчасного виявлення загроз. Зроблено висновки про необхідність системного підходу до забезпечення кібербезпеки, який передбачає використання сучасних технологій, постійний моніторинг, навчання користувачів та координацію різних заходів безпеки.

Ключові слова: *кібербезпека, телекомунікаційні мережі, кібератаки, VMDR, роутери Cisco, брандмауери, шифрування, інформаційні системи.*

Постановка проблеми. Захист мереж стає дедалі важливішим через зростання хакерських атак та інших загроз. Це може призвести до втрати інформації та фінансів. Раніше інтернет був меншим і використовувався обмежено. Старі паролі і прості брандмауери були достатні для захисту даних. Проте сьогодні ситуація змінилася. Розвиток інтернету, нові технології та хакерські атаки ускладнили питання безпеки. Попри заходи безпеки, кібератаки залишаються загрозою через вразливості систем, фішинг, людські помилки та атаки на постачальників послуг. Статистика показує, що кібератаки стають дедалі частішими та серйознішими для компаній та держав.

Україна також зазнає численних кібератак. У січні 2022 року атакували урядові сайти, що викликало перебої в роботі державних установ. У лютому 2022 року платформа «Дія» зазнала DDoS-атаки, що ускладнило доступ до державних послуг. У грудні 2022 року хакери намагалися зламати системи управління електромережами. Влітку 2023 року кілька українських приватних компаній стали жертвами атак із використанням програм-вимагачів, що спричинило фінансові втрати. У

вересні 2023 року атакували інформаційні системи Національної поліції. Ці приклади підкреслюють серйозність загрози кібератак для України та необхідність вдосконалення систем кібербезпеки.

Безпека мереж має нейтралізувати загрози, даючи змогу користувачам, державним установам і бізнесу досягати своїх цілей. Вона має бути гнучкою та адаптивною до змін у топології мережі та технологіях. Сучасні системи 4G та експериментальні 5G успішно забезпечують безпечну співпрацю та комунікацію. Лідерами в цій галузі є мережі та комп'ютерні системи. Отже, вирішення проблем кібербезпеки в телекомунікаційних мережах потребує всебічного підходу: розробки нових методів захисту, вдосконалення наявних технологій, підвищення обізнаності користувачів та постійного моніторингу загроз.

Аналіз останніх досліджень та публікацій. Останні дослідження в галузі кібербезпеки телекомунікаційних систем виявили низку ключових проблем та способів їх вирішення. У працях [3, 9] автори акцентують на ідентифікації факторів, які впливають на безпеку, та моделях безпеки для зменшення ризиків у телекомунікаційних компаніях. Зокрема, у статті [3] наголошується на необхідності вдосконалення політики безпеки та впровадженні новітніх технологій у телекомунікаційних мережах, зокрема, для захисту від сучасних кіберзагроз. Автори [9] досліджують різні моделі безпеки для зменшення ризиків і загроз у телекомунікаційних компаніях, розглядають наявні методи захисту і пропонують інтегровані підходи для підвищення ефективності безпеки. Зокрема, рекомендується впроваджувати багаторівневі системи безпеки та постійно моніторити загрози для стабільної роботи телекомунікаційних служб.

Дослідження [5, 6, 10] розглядають сучасні кіберзагрози, їхні наслідки та методи захисту, зокрема, в контексті технології 5G. Публікація [6] висвітлює різноманітні методи атак, включаючи DDoS-атаки та фішинг, та підкреслює важливість етичного хакінгу для виявлення вразливостей. Автори [5] обговорюють специфічні загрози, які виникають із впровадженням технології 5G, і закликають до розроблення нових методів захисту. У праці [10] аналізуються алгоритми шифрування для безпеки комунікацій між телекомунікаційними та комп'ютерними мережами; проведена оцінка ефективності різних методів шифрування та їх придатність для сучасних телекомунікаційних систем.

У працях [2, 4, 8] автори пропонують методи оцінки рівня безпеки та аудиту телекомунікаційних систем, спрощуючи процес виявлення вразливостей та надаючи рекомендації щодо удосконалення захисту. Так, дослідження [2] вказують на важливість систематичного аудиту та тестування на вразливість для забезпечення загальної безпеки інформаційно-телекомунікаційних систем підприємств. У публікації [4] проводиться аналіз методів оцінки важливості інформаційних і телекомунікаційних систем для промисловості та пропонується модель для оцінки їхньої безпеки. Використовуючи метод аналізу ієрархій, створено модель для обчислення кількісних критеріїв безпеки, що спрощує вибір експертів та дає змогу оцінювати системи, навіть при обмежених даних. Це допомагає перейти від якісних до кількісних оцінок. Стаття [8] досліджує фактори, що

впливають на кібербезпеку спеціалізованих інформаційно-телекомунікаційних систем через кібератаки. Основна увага приділяється визначенню цих факторів та аналізу наслідків сучасних атак. У результаті запропоновано план покращення кібербезпеки та визначено ключові компоненти, що впливають на рівень безпеки.

Останні дослідження кібербезпеки телекомунікаційних систем виділяють кілька ключових моментів. Виявлення факторів і вразливостей мережі критично важливе для безпеки. Теперішні кіберзагрози, такі як DDoS-атаки та фішинг, потребують постійного вдосконалення захисту. Нові технології створюють нові вразливості, тому потрібний постійний моніторинг та адаптація захисту. Технічний аудит і тестування на вразливість допомагають виявляти та виправляти проблеми. Разом з удосконаленням політики безпеки і впровадженням нових технологій це сприяє покращенню загальної безпеки телекомунікаційних мереж.

Мета статті — комплексне дослідження проблем кібербезпеки в телекомунікаційних мережах та системах, аналіз сучасних загроз і вразливостей, а також розроблення заходів для ефективного захисту інформаційних ресурсів.

Виклад основного матеріалу дослідження. Телекомунікаційна мережа — це інфраструктура, що допускає обмін даними, інформацією та комунікаціями між різними пристроями та користувачами на великій відстані. Вона містить різноманітні технології передачі даних, такі як провідні, безпровідні та оптичні, і може бути побудована на різних рівнях — від локальних мереж (LAN) у межах будівлі чи кампусу до глобальних мереж (WAN), які охоплюють великі географічні області або весь світ, наприклад, інтернет (рис. 1). Телекомунікаційні мережі дають можливість передавати голос, дані, відео та інші види інформації за допомогою різних пристроїв і технологій зв'язку. Функціонування телекомунікаційних мереж забезпечується телекомунікаційними системами — комплексні технічні структури, які включають обладнання, програмне забезпечення, протоколи зв'язку та інфраструктуру зв'язку.

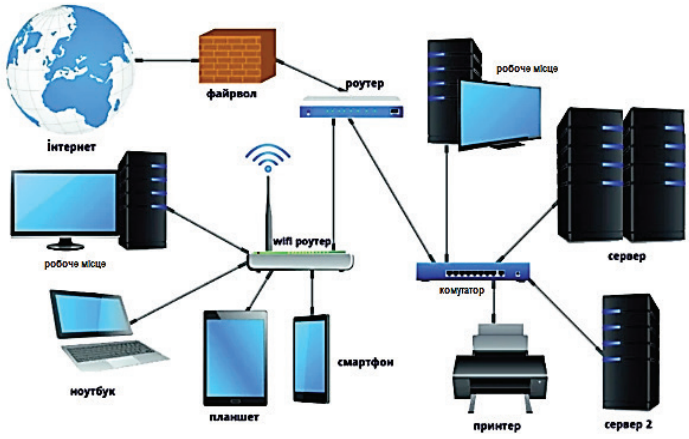

Рис. 1. Мережева схема телекомунікаційної системи

Телекомунікаційна мережа складається з різних пристроїв, які співпрацюють для забезпечення ефективного обміну інформацією. Ось деякі з них:

1. Кінцеві пристрої — це комп'ютери (ПК), ноутбуки, смартфони, сервери тощо. Це кінцеві точки в мережі, через які користувачі отримують доступ до інформації.

2. Комутатори — це пристрої, що об'єднують кілька пристроїв у мережі й керують передачею даних між ними. Вони використовують різні стандарти Ethernet, такі як Fast Ethernet і Gigabit Ethernet, для ефективної передачі даних зі швидкістю від 100 Мбіт/с до 10 Гбіт/с. Комутатори виявляють MAC-адреси для надсилання даних.

3. Маршрутизатори — це важливі пристрої в мережі, які з'єднують різні мережі, такі як LAN і WAN. Вони керують передачею даних між цими мережами, фільтрують непотрібні дані, захищають від інтернет-атак і дають змогу встановлювати VPN-з'єднання. Властивості маршрутизаторів включають кількість портів LAN і WAN, типи підтримуваних з'єднань, швидкість передачі даних (до 10 Гбіт/с) і протоколи маршрутизації, такі як RIP, OSPF, BGP.

4. Брандмауери (фаєрволи) — це пристрої, що захищають мережу від небажаних атак з інтернету. Вони контролюють трафік даних, блокуючи небезпечні джерела та налаштовуючи права доступу. Брандмауери також ведуть моніторинг мережевої активності. Основні характеристики брандмауерів включають різні типи підтримки (програмні, апаратні, хмарні), швидкість обробки пакетів даних і методи фільтрації трафіку, такі як за IP-адресою, портом чи застосунком.

5. Середовища передачі — це різні способи пересилання даних у мережі між пристроями, такі як кабельні з'єднання, оптичні кабелі (оптоволокно) і бездротові технології. Вони відрізняються за швидкістю передачі даних, дальністю зв'язку (для бездротового з'єднання) і стійкістю до перешкод.

У телекомунікаційних мережах ці пристрої спільно працюють, щоб забезпечити надійний, швидкий і безпечний обмін даними в телекомунікаційній мережі, використовуючи такі протоколи, як TCP/IP, UDP, HTTP, HTTPS, FTP, SMTP, IMAP, SSH, SNMP тощо.

Проблема трафіку в мережі виникає через обмежену пропускну здатність, збільшення часу доставки пакетів, можливі відмови пристроїв та зіткнення інформації. Концентратори та комутатори є ключовими пристроями, що допомагають у подоланні цих проблем. Концентратори скорочують відстань, але не розділяють мережу, тоді як комутатори забезпечують альтернативні маршрути та оптимізовану роботу мережі. У повністю комутованих мережах кожен вузол має свій сегмент, під'єднаний до комутатора, тоді як змішані мережі використовують як концентратори, так і комутатори для ефективного функціонування.

Важливим аспектом забезпечення безпеки в мережах є методологія обробки елементів безпеки та застосування брандмауерів. У разі проєктування максимально безпечної системи необхідно спочатку ретельно вивчити потенційні загрози. Це передбачає аналіз людей, які можуть намагатися зламати систему, різновиди атак та їх мета, щоб ідентифікувати найбільш критичні та вразливі моменти в мережі.

Кіберзлочинці — це особи або групи, які вчиняють злочинні дії в мережі «Інтернет», використовуючи комп'ютери, мережі та інші цифрові технології. Вони можуть вчиняти крадіжки даних, шахрайства, поширювати віруси, атакувати комп'ютерні системи, здійснювати шпигунство та інші злочинні дії. Кіберзлочинці можуть бути окремими злочинцями, членами організованих злочинних груп або навіть державними структурами. Їх мотивація може бути різноманітною — від особистої вигоди до політичних або геополітичних цілей. Їх можна розділити на кілька категорій: «Скріпт-Кідді», які використовують готові інструменти для атак; професійні хакери, що створюють складні загрози; зовнішні атакувальники, які намагаються проникнути в мережу ззовні через інтернет; та внутрішні загрози, що виникають від осіб із доступом до мережі, які використовують його недобросовісно.

Мережеві атаки проходять кілька етапів (рис. 2), що передбачають підготовку, вторгнення і активну фазу. Підготовка передбачає постійний моніторинг мережі для виявлення потенційних загроз та підготовку необхідних інструментів для атаки, таких як розроблення шкідливого програмного забезпечення або придбання фішингових компаній. Вторгнення передбачає етапи доставлення, експлуатації та інсталяції шкідливого коду на цільові системи, після чого розпочинається активна фаза, яка включає контроль і відпрацювання атаки, зокрема крадіжку даних або зміну конфігурації системи.

Кібератаки сьогодні є серйозною загрозою для державної безпеки та приватності громадян. Вони породжують низку проблем, таких як втрата конфіденційної інформації, фінансові втрати та порушення діяльності важливих інфраструктурних систем. Найбільш руйнівні та поширені атаки сьогодні включають DDoS (розподілена відмова в обслуговуванні), що перекриває нормальний трафік, перевантажуючи системи, та Ransomware (вимагання викупу), яке шифрує або блокує доступ до даних чи систем, вимагаючи викуп за їх відновлення. Також є інші різновиди атак, такі як фішинг, віруси тощо, які загрожують безпеці мереж та інформаційних систем.

Рис. 2. Модель мережевих атак

Україна за останні роки стала мішенню для різних типів кібератак, таких як DDoS, Ransomware та Phishing. Наприклад, атаки DDoS можуть спричинити

серйозні перешкоди в доступі до онлайн-ресурсів широкого спектра організацій. Такі загрози не тільки паралізують системи, а й можуть призвести до фінансових втрат та втрати конфіденційної інформації, як у випадку Ransomware. Фішингові атаки також залишаються серйозним ризиком, зловмисники намагаються здійснити доступ до конфіденційних даних, надсилаючи підроблені листи або повідомлення. Українські компанії вживають заходів, таких як використання антивірусного ПЗ та навчання персоналу для захисту від таких загроз.

Поглиблення розуміння цих загроз та розроблення ефективних стратегій захисту стають невідкладними завданнями для забезпечення стійкості та безпеки в цифровому світі [1]. Важливо використовувати різноманітні техніки та інструменти безпеки, такі як брандмауери, системи виявлення вторгнень та антивірусне програмне забезпечення. Крім того, регулярне навчання персоналу з питань кібербезпеки та впровадження політики безпеки допоможуть забезпечити високий рівень захисту мережі.

Відповідно до опитування SANS [7] для забезпечення безперервної безпеки та зниження ризиків в організації через ідентифікації та виправлення вразливостей до того, як їх можуть використати зловмисники, використовується VMDR. VMDR (Vulnerability Management, Detection and Response) — це інтегрований підхід до управління вразливостями, який охоплює процеси виявлення, оцінки, усунення та моніторингу вразливостей в інформаційних системах (рис. 3).

Рис. 3. Управління, виявлення та реагування на вразливості

Управління вразливістю, виявлення та реагування містить чотири основні компоненти. Управління активами організації включає ідентифікацію, класифікацію та моніторинг IT-активів. Програмне забезпечення, таке як Qualys AssetView та ServiceNow ITAM, сприяє у виявленні та управлінні активами. Управління вразливістю передбачає ідентифікацію, оцінку та впровадження заходів для зменшення ризиків, використовуючи інструменти, наприклад, Nessus або Qualys. Виявлення вразливостей та встановлення пріоритетів потребує сканування систем та використання моделей ризику, таких як CVSS. Усунення вразливостей передбачає впровадження виправлень або заходів для зменшення ризиків, використовуючи автоматизовані системи управління патчами. Це важливо для кібербезпеки в сучасних IT-системах, оскільки забезпечує надійний захист IT-ресурсів.

Захист мережі є важливою складовою безпеки в мережі «Інтернет» й одним із ключових інструментів для цього є брандмауер. Брандмауер — це важлива частина захисту мережі в інтернеті. Він допомагає знизити ризики за умови правильної конфігурації. Перш ніж його налаштовувати, треба з'ясувати, що саме ми хочемо захистити. Мережа може бути загрозою для наших даних і ресурсів комп'ютера, тому важливо їх захищати. Дані мають три основні властивості, які

потребують захисту: приватність, цілісність і доступність. Брандмауер аналізує та фільтрує трафік у мережі за набором правил безпеки, схожим на маршрутизатори. Його можна мати як апаратний пристрій або програмне забезпечення. Апаратні брандмауери надають кращий захист і не впливають на продуктивність мережевих пристроїв. Програмні брандмауери є дешевшими, але можуть потребувати ресурсів апаратних засобів.

Отже, роутери, зокрема роутери Cisco, і брандмауери — це важливі елементи будь-якої мережі, які забезпечують безпеку та захист від різних загроз. Вони використовуються для фільтрації та керування трафіком, захисту від несанкціонованого доступу та запобігання атакам. Програмне забезпечення Cisco IOS має велику кількість функціональних можливостей для забезпечення безпеки, зокрема пакетне фільтрування в списку доступу, набір функцій брандмауера, перехоплення TCP, автентифікацію, авторизацію та облік (AAA) і шифрування даних. Крім того, роутери Cisco можуть використовуватися для реалізації політики якості обслуговування (QoS), що допомагає контролювати пропускну здатність та пріоритезувати трафік у мережі.

Захист паролем — це процес обмеження доступу до облікових записів у мережі, забезпечуючи доступ лише авторизованим користувачам. Паролі гарантують, що тільки ті, хто має правильні облікові дані, можуть отримати доступ до захищених ресурсів. Шифрування є складнішим методом захисту, який перетворює інформацію в недоступний для читання формат, використовуючи криптографічні алгоритми та ключі. Це означає, що навіть якщо дані будуть перехоплені, без ключа їх не можна буде прочитати.

Захист паролем передбачає кілька важливих елементів: аутентифікація, яка перевіряє облікові дані користувача (ім'я користувача й пароль) для надання доступу до системи, гарантує доступ лише авторизованим користувачам; і обмеження доступу, яке захищає ресурси, даючи можливість тільки авторизованим користувачам переглядати або змінювати дані. Наприклад, захист паролем у системі може виглядати так: `User: admin, Password: ********.` Проте захист паролем має недоліки, такі як вразливість до атак методом перебору (brute force), фішинг-атак та інших методів компрометації. Якщо зловмисник отримає доступ до пароля, він зможе отримати доступ до всієї захищеної інформації. Натомість шифрування є важливим методом захисту даних, який передбачає використання криптографічних алгоритмів, таких як AES і RSA, для перетворення даних у зашифрований формат. Ці алгоритми гарантують, що дані будуть недоступні без ключа розшифрування (рис. 4). Ключі шифрування використовуються для шифрування та розшифрування даних, і без правильного ключа дані залишаються недоступними, навіть якщо їх буде перехоплено. Наприклад, оригінальні дані «ConfidentialInformation» після шифрування можуть виглядати як «SDF%43kjsdf@34ksdf#DFG». Основна перевага шифрування полягає в тому, що навіть якщо дані будуть перехоплені, вони залишаються недоступними без ключа розшифрування, забезпечуючи високий рівень безпеки і знижуючи ризики компрометації конфіденційної інформації. Порівняльні характеристики між цими методами наведено в табл. 1.

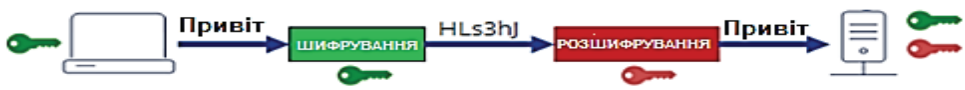

Рис. 4. Захист даних методом шифрування

Захист паролем обмежує доступ до даних, тоді як шифрування перетворює їх у недоступний формат, підвищуючи конфіденційність і безпеку. Одним із найважливіших аспектів безпеки є керування паролями, які відіграють ключову роль у захисті від несанкціонованого доступу. Рекомендується зберігати паролі на централізованому сервері аутентифікації, але багато роутерів усе ще мають локально налаштовані паролі. Важливо використовувати сильні паролі та регулярно їх змінювати, щоб запобігти уразливостям у мережі. Популярні програмні інструменти для шифрування, такі як BitLocker, VeraCrypt, AES Crypt, GnuPG, OpenSSL та PGP, допомагають забезпечити конфіденційність даних за допомогою сучасних алгоритмів шифрування. Користувачі мають обирати інструменти відповідно до своїх потреб та вимог безпеки.

Таблиця 1

Порівняння характеристик методів захисту даних

Шифрування пароля	Захист пароля
Процес приховування повідомлень у такий спосіб, що лише авторизований персонал може отримати доступ до інформації чи даних, що закодовані в повідомленнях	Захід безпеки для захисту конфіденційної та особистої інформації, яка доступна через телекомунікаційні мережі від несанкціонованого доступу
Конфіденційна інформація або дані шифруються або приховуються за допомогою алгоритму та ключа, а шифр є ключем до коду	Паролі — це просто набір символів і можуть містити букви, цифри, спеціальні символи або їх комбінацію
Шифрування бере інформацію або дані та робить їх нечитабельними для всіх, крім тих, для кого вони призначені	Паролі менш безпечні, ніж шифрування, і можуть бути легко зламані шкідливим програмним забезпеченням, оснащеним компонентами реєстратора ключів
Широко використовуються два типи шифрування: симетричне та асиметричне шифрування (шифрування з відкритим ключем)	Надійний пароль складається щонайменше із шести символів із комбінацією літер, цифр і символів

Для встановлення пароля, який забезпечує привілейований адміністративний доступ до системи IOS, використовується команда «enable secret». Порівнюючи зі старою командою «enable password», команда «enable secret» використовує більш надійний алгоритм шифрування і забезпечує вищий рівень захисту.

Метод налаштування пароля «enable password» використовує слабкий алгоритм шифрування, через що пароль зберігається у відкритому вигляді в конфігураційному файлі пристрою. Це робить його менш безпечним, оскільки пароль може бути легко

підібраний або переглянутий. Натомість метод «enable secret» використовує більш міцний алгоритм хешування (зазвичай MD5). Пароль зберігається в захешованому вигляді, що значно підвищує безпеку, оскільки важко відновити оригінальний пароль із хешу. Приклад налаштування: `Router(config)# enable secret mysecret-password.`

У разі налаштування пароля для команди «enable» на пристроях Cisco важливо також враховувати тип шифрування. Є два типи шифрування, які можна використовувати для захисту паролів: тип 8 (type 8) і тип 9 (type 9). Тип 8 використовує алгоритм DES (Data Encryption Standard), який є старим і ненадійним, оскільки вразливий до атак перебору. Шифрований пароль із типом 8 виглядає як рядок, що починається із числа 8, за яким є захешоване значення пароля. Тип 9 (type 9) використовує більш міцний алгоритм, такий як MD5, який є більш безпечним. Шифрований пароль з типом 9 виглядає аналогічно до попереднього, тільки починається з числа 9, наприклад:: `enable secret 9 encrypted_password`.

Команда «service password-encryption» в Cisco IOS використовується для шифрування паролів у конфігураційному файлі, що підвищує загальний рівень безпеки мережі. Введення цієї команди в режимі глобальної конфігурації активує шифрування для всіх незашифрованих паролів у конфігураційному файлі. IOS сканує конфігураційний файл, виявляючи всі паролі, встановлені командами, такими як «enable password», «line password», «username password» та іншими. Для кожного незашифрованого пароля застосовується шифрування типу 7, яке перетворює пароль на псевдошифрований рядок. Після шифрування паролі виглядають незрозуміло, але це шифрування легко розшифрувати за наявності відповідних інструментів. Зашифровані паролі зберігаються в конфігураційному файлі замість незашифрованих. Після збереження конфігурації (команди «write memory» або «copy running-config startup-config») зміни залишаються в постійній пам'яті маршрутизатора або комутатора. Приклад конфігураційного файлу після застосування команди «service password-encryption»:

```
enable password 7 0822455D0A16
line vty 0 4
password 7 045802150C2E
username admin password 7 060506324F41
```

Команда «service password-encryption» забезпечує мінімальний рівень захисту, перетворюючи паролі в псевдошифровану форму, яка не є надійною від досвідчених зловмисників. Для кращого захисту рекомендується використовувати «enable secret» з типами 8 або 9 шифрування, які застосовують міцні алгоритми хешування (SHA-256). Це допомагає забезпечити базовий рівень захисту паролів у конфігураційному файлі, зменшуючи ризик їх розкриття.

Консольний порт (Console port) на мережних пристроях, таких як маршрутизатори, комутатори або фаєрволи, забезпечує адміністраторам локальний доступ до консольного інтерфейсу пристроїв. Це корисний засіб керування та конфігурації, особливо у випадках, коли доступ через мережу недоступний. Консольний порт на пристроях з операційною системою Cisco IOS надає спеціальні привілеї

для забезпечення безпеки мережі. Надсилаючи сигнал BREAK на консольний порт у перші кілька секунд після перезавантаження, можна скористатися процедурою відновлення пароля, навіть без фізичного доступу або стандартних прав. Захист консольного порту Cisco на рівні привілейованого доступу до маршрутизатора важливий для безпеки будь-якого модему або мережевого пристрою.

Консольний порт використовується для різних цілей забезпечення безпеки мережі. Адміністратор може використовувати його для відновлення доступу до пристрою, якщо забув пароль. Також він використовується для аудиту безпеки та налагодження, щоб адміністратори могли під'єднатися до пристрою та виявити проблеми безпеки. У випадку критичних ситуацій, таких як атаки або аварії, консольний порт допомагає відновити пристрій. За допомогою перевірки безпеки налаштувань можна переглядати і змінювати налаштування безпеки пристрою. Моніторинг системних повідомлень дає можливість переглядати системні повідомлення та логи подій у реальному часі, щоб виявити потенційні загрози.

Ось кілька прикладів налаштування консольного порту для захисту у Cisco IOS:

Встановлення пароля для консольного порту	`Router(config)# line console 0`
	`Router(config-line)# password your_console_password`
	`Router(config-line)# login`

Активація відображення символів пароля	`Router(config)# line console 0`
	`Router(config-line)# password your_console_password`
	`Router(config-line)# login`
	`Router(config-line)# login enhancements`

Встановлення локального користувача для консольного порту	`Router(config)# username admin privilege 15 secret your_console_password`
	`Router(config)# line console 0`
	`Router(config-line)# login local`

Обмеження доступу до консольного порту за допомогою ACL	`Router(config)# access-list 10 permit host trusted_host_ip`
	`Router(config)# access-list 10 deny any`
	`Router(config)# line console 0`
	`Router(config-line)# access-class 10 in`

Встановлення тайм-ауту сесії консолі	`Router(config)# line console 0` `Router(config-line)# exec-timeout 10 0`

Використання банера для попередження про конфіденційність	`Router(config)# banner motd #`
	`Unauthorized access is prohibited. This system is for authorized users only.`
	`#`

Ці налаштування допоможуть забезпечити безпеку консольного порту в Cisco IOS, запобігаючи несанкціонованому доступу та підвищуючи загальний рівень захисту телекомунікаційної мережі.

Утримання безпеки стає ефективнішим, якщо зламники системи будуть проінформовані про будь-яке несанкціоноване використання. Із цією метою можна встановити попереджувальне повідомлення, сконфігуроване за допомогою команди «banner login», з детальними вимогами. Проте важливо уникати розголошення конкретної інформації про маршрутизатор, його ім'я, модель або власника, щоб уберегтися від зловмисного використання.

Наприклад, налаштування цих банерів у Cisco IOS:

Загальний попереджувальний банер	`Router(config)# banner login #` `Unauthorized access is prohibited. This system is for authorized users only. Any unauthorized access or use is prohibited and may be subject to criminal prosecution. #`
Попереджувальний банер із контактною інформацією	`Router(config)# banner login #` `Access to this device is restricted to authorized personnel only. If you are not an authorized user, disconnect immediately. For assistance, contact the IT department at example@example.com. #`
Банер із вимогою авторизації	`Router(config)# banner login #` `This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel. #`
Банер із правовою відповідальністю	`Router(config)# banner login #` `WARNING: Unauthorized access to this system is forbidden and will be prosecuted by law. By accessing this system, you agree that your actions may be monitored if unauthorized usage is suspected. #`

Ці попереджувальні банери можуть бути корисними для попередження потенційних зловмисників про недопустимість несанкціонованого доступу та можливих юридичних наслідків. Важливо пам'ятати про обмеження щодо розголошення конфіденційної інформації та забезпечити збалансованість між ефективним попередженням та захистом конфіденційності даних.

Заходи проти аналізаторів пакетів та інших загроз. Щоб убезпечити мережеві пристрої від атак, маршрутизатори мають уникати ведення журналу через незашифровані протоколи на ненадійних мережах. Рекомендується використовувати захищені протоколи, такі як SSH або Kerberized Telnet, для забезпечення безпеки ведення журналу, а також використовувати шифрування IPSec для забезпечення конфіденційності. У випадку віддаленого керування безпечніше використовувати одноразові паролі, які змінюються для кожної сесії, щоб уникнути ризиків. Для зменшення ризику зламу маршрутизатора через інтернет обмежте доступ лише

до відомих довірених хостів. Для безпечного ведення журналу усі хости мають використовувати надійні протоколи аутентифікації. Є також ризик зміни напрямку з'єднання TCP, яка може дозволити зловмисникові отримати контроль над користувачем. Хоча ці атаки складні, їхнє втілення можливе, якщо є чітка ціль. Для захисту від атак із відмови в обслуговуванні рекомендується використовувати окремий канал управління, наприклад, дозвіл на використання модема для екстрених ситуацій.

Висновки. Дослідження показують, що забезпечення надійної кібербезпеки в телекомунікаційних мережах потребує системного підходу, що передбачає використання сучасних технологій, постійний моніторинг, навчання користувачів та координацію різних заходів безпеки. Необхідність вдосконалення методів захисту зумовлена постійним зростанням складності та кількості кібератак. Системи кібербезпеки мають бути гнучкими та здатними адаптуватися до нових видів загроз. Використання сучасних технологій, таких як шифрування даних та складні алгоритми аутентифікації, є критично важливим для забезпечення безпеки інформації. Постійний моніторинг і аудит безпеки необхідні для зниження ризиків компрометації інформаційних систем. Підвищення обізнаності користувачів є важливим, оскільки людський фактор залишається одним із найслабших місць у системі безпеки. Застосування комплексного підходу до безпеки містить різноманітні методи захисту, такі як брандмауери, антивірусне програмне забезпечення, системи виявлення вторгнень тощо. Забезпечення надійної кібербезпеки в телекомунікаційних мережах потребує використання сучасних технологій, постійного моніторингу, навчання користувачів та координації різних заходів безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Пановик У. П., Ткачук Р. Л. Кібербезпека через призму системного аналізу. Комп'ютерні технології друкарства. 2023. № 1(49). С. 197–208. Doi: https://doi.org/10.32403/2411-9210-2023-1-49-197-208.
2. Якименко Ю. М., Рабчун Д. І. та інші. Технічний аудит захищеності інформаційно-телекомунікаційних систем підприємств. Кібербезпека: освіта, наука, техніка. 2023. № 4 (20). С. 45−61. DOI:10.28925/2663-4023.2023.20.4561.
3. Ancu A.-E., Barbu A. Identification of critical factors for improvinf the security of telecommunication systems. International Conference of Management and Industrial Engineering. 2023. 11. 239−246. DOI: 10.56177/11icmie2023.54.
4. Gnatyuk S. et al. The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems. *International Workshop on Intelligent Information Technologies & Systems of Information Security*. 2022. URL: https://ceur-ws.org/Vol-3156/paper29.pdf.
5. Mohan J. P., Sugunaraj N., Ranganathan P. Cyber Security Threats for 5G Networks. *IEEE International Conference on Electro Information Technology (eIT)*, Mankato, MN, USA, 2022. Pp. 446−454. DOI: 10.1109/eIT53891.2022.9813965.
6. Onyema Edeh Dinar, Amina Elbatoul et al. Cyber Threats, Attack Strategy, and Ethical Hacking in Telecommunication Systems. In book: Security and Privacy in Cyberspace (pp. 25−45) Publisher : Springer, 2022. DOI: 10.1007/978-981-19-1960-2_2.

7. SANS Vulnerability Management Survey. SANS Institute. URL: https://www.sans.org/white-papers/38900/ (дата звернення 04.04.2024).
8. Sova O. Analysis of conditions and factors affecting cyber security in the special purpose information and telecommunication system. *Technology Audit and Production Reserves*. 2022. 4 (2 (66)). 25–28. doi: http://doi.org/10.15587/2706-5448.2022.261874.
9. Toapanta S. M., Mafla Gallegos L. E. et al. Analysis of Models of Security to Mitigate the Risks, Vulnerabilities and Threats in a Company of Services of Telecommunications. *3rd International Conference on Information and Computer Technologies (ICICT)*, San Jose, CA, USA, 2020. Pp. 445−450. DOI: 10.1109/ICICT50521.2020.00077.
10. Yifeng He, Nan Ye, Rui Zhang. Analysis of Data Encryption Algorithms for Telecommunication Network-Computer Network Communication Security. *Wireless Communications and Mobile Computing*. Article ID 2295130, 19 pages. DOI: https://doi.org/10.1155/2021/2295130.

REFERENCES

1. Panovyk, U. P., & Tkachuk, R. L. (2023). Kiberbezpeka cherez pryzmu systemnoho analizu: Komp'iuterni tekhnolohii drukarstva, 1 (49), 197–208. Doi: https://doi.org/10.32403/2411-9210-2023-1-49-197-208 (in Ukrainian).
2. Yakymenko, Yu. M., & Rabchun, D. I. ta inshi. (2023). Tekhnichnyi audyt zakhyshchenosti informatsiino-telekomunikatsiinykh system pidpryiemstv: Kiberbezpeka: osvita, nauka, tekhnika, 4 (20), 45−61. DOI:10.28925/2663-4023.2023.20.4561 (in Ukrainian).
3. Ancu, A.-E., & Barbu, A. (2023). Identification of critical factors for improvinf the security of telecommunication systems. International Conference of Management and Industrial Engineering, 11, 239−246. DOI: 10.56177/11icmie2023.54 (in English).
4. Gnatyuk, S. et al. (2022). The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems. International Workshop on Intelligent Information Technologies & Systems of Information Security. Retrieved from https://ceur-ws.org/Vol-3156/paper29.pdf (in English).
5. Mohan, J. P., Sugunaraj, N., & Ranganathan, P. (2022). Cyber Security Threats for 5G Networks. IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA, 446−454. DOI: 10.1109/eIT53891.2022.9813965 (in English).
6. Onyema, Edeh Dinar, & Amina, Elbatoul et al. (2022). Cyber Threats, Attack Strategy, and Ethical Hacking in Telecommunication Systems. In book: Security and Privacy in Cyberspace (pp. 25−45) Publisher : Springer, DOI: 10.1007/978-981-19-1960-2_2 (in English).
7. SANS Vulnerability Management Survey. SANS Institute. Retrieved from https://www.sans.org/white-papers/38900/ (data zvernennia 04.04.2024) (in English).
8. Sova, O. (2022). Analysis of conditions and factors affecting cyber security in the special purpose information and telecommunication system: Technology Audit and Production Reserves, 4 (2 (66)), 25–28. doi: http://doi.org/10.15587/2706-5448.2022.261874 (in English).
9. Toapanta, S. M., & Mafla Gallegos, L. E. et al. (2020). Analysis of Models of Security to Mitigate the Risks, Vulnerabilities and Threats in a Company of Services of Telecommunications. 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, 445−450. DOI: 10.1109/ICICT50521.2020.00077 (in English).

10. Yifeng, He, Nan, Ye, & Rui, Zhang. Analysis of Data Encryption Algorithms for Telecommunication Network-Computer Network Communication Security. Wireless Communications and Mobile Computing. Article ID 2295130, 19 pages. DOI: https://doi.org/10.1155/2021/2295130 (in English).

doi: 10.32403/1998-6912-2024-1-68-122-135

CYBER SECURITY IN TELECOMMUNICATION NETWORKS AND SYSTEMS

U. P. Panovyk

Ukrainian Academy of Printing,
19, Pid Holoskom St., Lviv, 79020, Ukraine
ulianapanovuk@gmail.com

The article examines current cybersecurity issues in modern telecommunications networks, emphasizing the need to enhance protection methods due to cyberattacks' increasing frequency and complexity. It discusses the rise of cybersecurity threats in contemporary telecom networks, stressing the necessity for their study and resolution. A detailed analysis of recent trends and cyberattack statistics is conducted, particularly in Ukraine. It covers primary threats like DDoS attacks, viruses, phishing, and others, along with descriptions of cybercriminal categories and their attack methods.

Contemporary methods of protecting information resources are analyzed, including data encryption and the utilization of complex authentication algorithms. The advantages and disadvantages of various encryption methods, such as AES and RSA, are discussed. Special attention is given to configuring Cisco routers as key components of cybersecurity, detailing setup steps like establishing basic parameters, employing Access Control Lists (ACLs) to restrict access, and using authentication and authorization functions to enhance security. The role of firewalls in cybersecurity systems, their main functions, and their types are examined. The article describes firewall configuration stages, covering security policy configuration, network traffic monitoring, detecting and blocking suspicious activities, and support for security rule updates. Emphasis is placed on vulnerability analysis and timely identification of potential threats.

A conclusion is drawn regarding the necessity of a systematic approach to cybersecurity, incorporating modern technologies, continuous monitoring, user education, and coordination of security measures. The importance of flexible and adaptive security systems capable of responding to new threats is underscored.

Keywords: *cybersecurity, telecommunication networks, cyber-attacks, VMDR, Cisco routers, firewalls, encryption, information systems.*

Стаття надійшла до редакції 19.04.2024.
Received 19.04.2024.