SCIENTIFIC COLLECTION INTERCONF+

№ 84
November, 2021

THE ISSUE CONTAINS:

Proceedings of the 5th International Scientific and Practical Conference

THEORY AND PRACTICE OF SCIENCE: KEY ASPECTS

ROME, ITALY

7-8.11.2021

ISSN 2709-4685

InterConf
Scientific Publishing Center

SCIENTIFIC COLLECTION «INTERCONF»

№ 84 | November, 2021

THE ISSUE CONTAINS:

Proceedings of the 5th International Scientific and Practical Conference

THEORY AND PRACTICE OF SCIENCE: KEY ASPECTS

ROME, ITALY

7-8.11.2021

ROME
2021

UDC 001.1

INDEX COPERNICUS INTERNATIONAL

S 40 *Scientific Collection «InterConf»*, (84): with the Proceedings of the 5th International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects» (November 7-8, 2021). Rome, Italy: Dana, 2021. 478 p.

ISBN 978-88-32012-34-7
DOI 10.51582/interconf.7-8.11.2021

EDITOR COORDINATOR

EDITORIAL BOARD

If you have any questions or concerns, please contact a coordinator Mariia Granko.

The recommended styles of citation:

1. Surname N. (2021). Title of article or abstract. *Scientific Collection «InterConf»,* (84): with the Proceedings of the 5th International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects» (November 7-8, 2021) at Rome, Italy; pp. 21-27. Available at: https://interconf.top/...
2. Surname N. (2021). Title of article or abstract. *InterConf,* (84), 21-27. Retrieved from https://interconf.top/...

This issue of Scientific Collection «InterConf» contains the International Scientific and Practical Conference. The conference provides an interdisciplinary forum for researchers, practitioners and scholars to present and discuss the most recent innovations and developments in modern science. The aim of conference is to enable academics, researchers, practitioners and college students to publish their research findings, ideas, developments, and innovations.

TABLE OF CONTENTS

PART I

DOI 10.51582/interconf.7-8.11.2021.043

Чинчик Дмитро Михайлович
студент IV курсу, кафедра безпеки інформаційних технологій
Національний університет «Львівська політехніка», Україна

Коробейнікова Тетяна Іванівна
кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Україна

Захарченко Сергій Михайлович
кандидат технічних наук, доцент, доцент кафедри обчислювальної техніки
Вінницький національний технічний університет, Україна

МЕТОДИ ТА ЗАСОБИ КОМПЛЕКСНОГО ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

Анотація. *Тут будуть розглянуті деякі механізми мережевої безпеки, використання яких допоможе забезпечити надійний захист активів корпоративної мережі. Основним завданням під час розроблення подібних рішень захисту є розгляд загальновідомих механізмів та їх комбінацій із подальшим застосуванням окремого рішення.*
Ключові слова*: корпоративна мережа, захист мережі, протокол.*

Незважаючи на велику кількість публікацій [1-6] та чимало організацій, що займаються захистом комп'ютерних мереж, досі спеціалізованим механізмам захисту корпоративних мереж надається неабияке значення. Для того, щоб надійно захистити інформацію корпоративної мережі, потрібен систематичний комплексний підхід [7-8]. Його використання – це успіх, який передбачає забезпечення доступності, цілісності та конфіденційності інформаційних ресурсів та підтримуючої інфраструктури, відомих як тріада CIA та є керівним принципом забезпечення інформаційної безпеки для будь-якої корпорації. Комплексний підхід передбачає реалізацію захисту на законодавчому, адміністративному, процедурному та програмно-технічному

рівнях. Розглянемо деякі механізми захисту мереж та їх комбінації.

Заходи забезпечення безпеки інформації у корпоративних мережах. Перелік заходів, які використовують для забезпечення інформаційної безпеки містить правові, організаційно-адміністративні та інженерно-технічні заходи.

Правові заходи забезпечення безпеки інформації у корпоративних мережах. Ґрунтуються на положеннях міжнародних (до них належать: угоди, ліцензії, патенти, авторські права, договори) та національних (до їхнього складу входять: конституція, укази, нормативні акти, кодекси, інструкції, керівні документи) правових норм. Такі нормативні акти закріплюють відкритість, доступність, свободу обміну інформації, її достовірність та повноту, гарантують право на інформацію, а також визначають правомірність одержання, використання, поширення та зберігання інформації і т. д.

До правових заходів також відносять норми, які регулюють питання відповідальності за кіберзлочини, захист авторських прав розробників програм. До того ж, вони призначені для визначення пріоритету міжнародного права над внутрішньодержавним та економічної доцільності [9].

Організаційно-адміністративні заходи забезпечення безпеки інформації у корпоративних мережах. Вчасність та правильність прийняття стратегічних рішень, а також визначення засобів, методів та механізмів і їхнє впровадження у систему захисту інформації корпоративної мережі визначають роль організаційно-адміністративних заходів. Сюди також відносять дії загального характеру, що вживаються керівництвом організації. Головною метою є формування програми робіт в галузі інформаційної безпеки і забезпечення їх виконання. Організаційно-адміністративні заходи можна поділити на організаційні та адміністративні відповідно. Організаційні заходи забезпечення безпеки інформації у корпоративних мережах передбачають рішення, які стосуються пропускного режиму, зберігання документів, порядку обліку та знищення документів, навчання правилам роботи з таємною інформацією. У свою чергу, адміністративні заходи передбачають контроль журналів роботи, підтримку правильної конфігурації ОС, контроль зміни паролів, проведення тестувань засобів захисту інформації та ін.

Організаційно-адміністративні заходи містять планування захисту, керування системою захисту, безперервність процесу захисту інформації, гнучкість захисту, розділення доступу, багаторівневість захисту інформації та інші [9].

Інженерно-технічні заходи забезпечення безпеки інформації у корпоративних мережах. Їх вибір корелюється з потрібним рівнем захисту даних організації і буде унікальним для кожного окремого випадку. До інженерно-технічних заходів відносять використання шифрів для захисту, захист від несанкціонованого доступу, обладнання для захисту від різного роду витоку інформації, мережевого обладнання для перерозподілу ресурсів, при виході з ладу деякої частини мережної інфраструктури та ін. Окрім цього, у рамках впровадження інженерно-технічних заходів, можуть встановлюватися системи пожежогасіння, контролю і управління доступом, резервного електроживлення і т.п. [9].

Огляд засобів захисту корпоративних мереж.

Інженерно-технічні заходи забезпечення безпеки інформації у корпоративних мережах за призначенням можна поділити на такі групи:

– фізичні засоби – засоби, які повинні створювати фізичні перешкоди на шляху зловмисників;

– апаратні засоби – різні технічні конструкції, які можуть протидіяти розголошенню відповідної інформації корпоративної мережі, її витоку та спробам несанкціонованого доступу до неї;

– програмні засоби – програми чи програмні комплекси, що можуть забезпечити захист інформації самостійно чи разом з іншими засобами захисту інформації корпоративної мережі;

– криптографічні засоби – алгоритми, за допомогою яких шифрується інформація корпоративної мережі, яка захищається;

– стеганографічні засоби – спеціальні алгоритми, які використовуються для приховування факту присутності відповідної інформації [5, 10].

Фізичні засоби захисту корпоративних мереж. Основним принципом фізичного захисту є його неперервність. Потрібно вживати всіх можливих

заходів, щоб убезпечити будівлі, прилеглу територію, підтримуючу інфраструктуру, обчислювальну техніку та носії даних від ймовірних загроз. До фізичного захисту належать такі напрями:

– фізичне керування доступом – дозволяє контролювати і за необхідності обмежувати вхід або вихід працівників;

– захист підтримуючої інфраструктури – забезпечення цілісності (захист обладнання від пошкоджень та викрадень) та доступності (дублювання відповідних вузлів, забезпечувати належний ремонт вузлів) тепло-, водо-електропостачання, системи кондиціонування та засобів комунікацій;

– захист від перехоплення даних – максимально розширити контрольовану зону, контролювати лінії зв'язку;

– захист мобільних систем – захист портативних мобільних пристроїв від викрадення [5].

Апаратні засоби захисту корпоративних мереж. Апаратними засобами захисту називають технічні рішення, котрі можуть забезпечити безпеку інформації комп'ютерної мережі. Пристрої чи прилади, що відносяться до апаратних засобів повинні підтримувати безпечне середовище для ділової активності. На основі однотипних технічних пристроїв можна побудувати як прості, так і складні системи. Апаратні пристрої можуть займати досить багато місця, але й можуть бути надзвичайно малими. Так, наприклад, кейлоггери є досить мініатюрними тому, реєстрація натиснень клавіш на клавіатурі є непомітною навіть для фахівця, який проводитиме аудит. Окрім цього, кейлоггери можуть мати необмежений час роботи, оскільки мають великий об'єм внутрішньої пам'яті, а також не потребують додаткового живлення. Розрізняють внутрішні та зовнішні кейлоггери. Внутрішній кейлоггер може бути прикріпленими до материнської плати чи до мікросхеми клавіатури. Перевага внутрішніх кейлоггерів полягає у тому, що вони вмонтовуються в середину системного блоку чи ноутбука. Також існують клавіатури, які мають вже вбудований кейлоггер.

Поряд із внутрішніми кейлоггерами використовуються зовнішні. Такі кейлоггери встановлюють в місце під'єднання клавіатури, наприклад, у роз'єм

USB. Зовнішні кейлоггери можуть бути оснащеними Bluetooth-модулем або модулем Wi-Fi. Ці модулі призначені для передачі перехопленої інформації на відстані. До переваг зовнішніх кейлоггерів можна віднести їх низьку ціну, легке під'єднання, можливість зберігати велику кількість інформації на невеликих картах пам'яті.

Такі пристрої можуть використовуватися зловмисниками, тому важливо використовувати відповідні фільтри та екранування [9].

Існують цілі апаратні системи захисту. Одна з таких – SunScreen. Ця система може фільтрувати пакети, розпізнавати трафік та забезпечувати його приватність. SunScreen не може бути атакованою ззовні, оскільки, не має основних мережевих параметрів (IP-адреси та маска мережі). Пристрій SunScreen має 5 адаптерів Ethernet. До чотирьох під'єднуються сегменти мережі, а п'ятий адаптер призначений для провайдера. Кожен адаптер, до якого підключений певний сегмент мережі, може бути налаштований незалежно від інших, використовуючи потрібний сет правил для фільтрації трафіку. Система SunScreen володіє іще одною рисою – підтримкою протоколу SKIP. За допомогою цього протоколу, все «спілкування» між сегментами має вигляд повністю шифрованого (завдяки інкапсуляції зовнішнього трафіку сегментів) і на додачу до цього, маскується оцінка інтенсивності трафіку (шляхом використання «порожнього» трафіку) [5, 9].

Програмні засоби захисту корпоративних мереж. Саме програмні засоби є найпоширенішим видом захисту інформації в корпоративних мережах. Таким засобам притаманні універсальність, простота реалізації. До них не складно внести зміни та постійно розвивати у потрібному для організації напрямку. Розглянемо деякі найпоширеніші програмні інструменти захисту інформації.

Міжмережевий екран. Міжмережевий екран, (фаєрвол або брандмауер) – це програма, яка може захистити мережу, фільтруючи трафік відповідно до наперед встановленого набору правил безпеки. Фаєрвол ретельно аналізує вхідний трафік, що надходить з незахищених або підозрілих джерел, щоб запобігти атакам. Брандмауери аналізують трафік у вхідній точці комп'ютера

– на порту, де відбувається обмін інформацією із зовнішніми пристроями.

Міжмережеві екрани можуть полегшити управління безпекою, попереджати доступ неавторизованих користувачів та, навіть, блокувати шкідливі дані. Проте, існують шляхи обходу захисту, який забезпечує фаєрвол. Окрім цього, неправильно налаштований брандмауер може привести до небажаних наслідків (наприклад, стати єдиною точкою відмови) [2].

Антивірус. Антивірусами називають програмні засоби, котрі здатні виявляти та знищувати віруси, які можуть заразити всього один пристрій чи навіть усю комп'ютерну мережу (під «вірусом» тут потрібно розуміти будь-який шкідливий код). Є такі типи антивірусних програм як детектори, фаги (лікарі), ревізори та фільтри. Існують індивідуальні та корпоративні пакети антивірусного захисту. Перші – індивідуальні пакети – використовуються на індивідуальних комп'ютерах, а другі, зазвичай, використовують організації. Корпоративні пакети антивірусного захисту мають архітектуру «клієнт-сервер». Клієнтські програми встановлюються на окремих пристроях мережі, а сервер робить розсилку оновлень.

Для виявлення шкідливого коду, антивіруси використовують різні методи. Найпопулярнішими є метод сигнатур та евристичні методи. Метод сигнатур полягає у тому, що кожен тип вірусів містить у собі характерний лише для нього фрагмент коду, який, найвірогідніше, ідентифікує тип. Цей фрагмент коду і є сигнатурою. Зазвичай, антивіруси мають бібліотеку сигнатур, яка постійно оновлюється і з якою й порівнюється шкідливий код. Незважаючи на те, що метод сигнатур є надзвичайно поширеним, він має суттєвий недолік. За допомогою методу сигнатур неможливо виявити нові типи вірусів.

Евристичні методи виявляють віруси, ґрунтуючись на структурі шкідливого коду або поведінці вірусу. Якщо антивірусна програма виявить вірус, то помістить заражену програму до карантину, а далі користувач безпосередньо вирішує: чи видаляти вірус з програми, чи видалити програму цілком [1, 2].

IDS/IPS. Не менш важливу роль для безпечної роботи мережі організації

відіграють системи виявлення вторгнень (англ. Intrusion Detection System, IDS) та системи попередження вторгнень (англ. Intrusion Prevention System, IPS). IDS/IPS – це комплекс програмних засобів, які виявляють факти і запобігають спробам несанкціонованого доступу до корпоративної системи. Системи виявлення та запобігання вторгненням використовуються для ідентифікації та попередження користувачів про відому або підозрілу діяльність. IDS зазвичай носять пасивний характер, тоді як IPS активний. Зазвичай IDS та IPS працюють в парі. Спочатку IDS повинна виявити небезпечний або підозрілий мережевий трафік. Після того, як IPS отримала попередження про небезпеку (alert) від IDS, вона може приймати такі рішення:

– перевірка (на основі сигнатур та аномальної поведінки) та аналіз (підозрілої активності та підозрілих пакетів);

– певна дія (помістити деякі пакети до карантину або відкинути їх);

– ведення логів та надсилання звітів.

Системи виявлення і запобігання вторгнень можуть визначати шкідливу активність відповідно до наперед встановлених правил. Засновані на правилах IDS працюють за принципом: «ЯКЩО ситуація ТОДІ дія». Такі рішення потребують великої затрати праці від кваліфікованого фахівця для проведення налаштування [2].

SIEM-системи. Досить потужним програмним засобом для забезпечення безпеки у комп'ютерній мережі є SIEM-системи (Security information and event management – управління інформаційною безпекою та подіями безпеки). Це такий програмний продукт, який аналізує в онлайн режимі подій інформаційної безпеки, отримані від мережевих пристроїв і додатків. Так само як і IDS/IPS, SIEM-системи можуть використовуватися для запису даних у логи і створення звітів. SIEM-системи також призначені для зберігання інформації у зручному для користувача форматі. Сама SIEM порівнює отримані дані зі встановленим стандартом і намагається знайти невідповідності [11].У собі цей програмний продукт поєднує управління подіями безпеки (англ. Security event management, SEM) та управління інформаційною безпекою (англ. Security Information management, SIM). Такий

інструмент використовується тоді, коли звичні засоби не можуть впоратися із поставленими на них завданнями. Проте, у кожному конкретному випадку метод використання SIEM буде залежати від цілей корпорації [11].

Криптографічні засоби. Для підвищення рівня безпеки у корпоративних комп'ютерних мережах широко використовується шифрування. Зазвичай, в його основі лежать ключ та певний криптографічний алгоритм. Так, наприклад, для захисту веб-продуктів використовують протоколи SSL та HTTPS.

Протокол SSL – англ. Secure Sockets Layer – рівень захищених сокетів – шифрує дані на канальному рівні моделі OSI. Цей протокол забезпечує кодування на порту.

Протокол HTTPS призначений для забезпечення надійного захисту тільки гіпертекстових документів веб-сервера. Цей протокол гарантує авторизацію та захист веб-документів. Цей протокол не можна використати для захисту інших протоколів таких, як FTP чи SMTP.

Для того, щоб захистити електронну пошту, використовують протокол S/MIME. Цей протокол був розроблений компанією RSA Data Security Inc. Компанія використала багато криптографічних алгоритмів, щоб забезпечити надійне шифрування та цілісність повідомлення за допомогою відкритого ключа.

Стенографічні засоби. Для того, щоб створити електронний еквівалент звичайного ручного підпису, було розроблено електронний цифровий підпис (ЕЦП). За допомогою ЕЦП можна гарантувати цілісність надісланого повідомлення та підтвердження особи відправника цього повідомлення. Алгоритм використання ЕЦП досить простий:

– генеруються відкритий і закритий ключі (ці ключі генерує відправник);

– відкритий ключ передається одержувачу;

– повідомлення шифрується закритим ключем відправника і передається по каналу зв'язку;

– одержувач дешифрує повідомлення за допомогою відкритого ключа відправника [5, 9].

Спеціалізовані механізми захисту корпоративних мереж з точки зору мережевої безпеки. Для опису спеціальних механізмів захисту корпоративних мереж з точки зору мережевої безпеки визначимо основні поняття.

Безпека інформації – стан, в якому інформація перебуває в такому захищеному вигляді, у якому будь-які дестабілізуючі впливи не здатні протистояти йому.

Корпоративна мережа – це така мережа, яка надає послуги лише працівникам підприємства, яке має у власності цю мережу. Зазвичай, під поняттям корпоративна мережа мають на увазі, мережу великого підприємства, яка містить у собі локальні мережі та глобальну мережу, що об'єднує їх.

Об'єкти – фізичні і логічні інформаційні ресурси інформаційної системи.

Суб'єкти – сутності між якими розділяються інформаційні ресурси інформаційної системи.

Ідентифікація – це присвоєння об'єктам і суб'єктам інформаційної системи унікальних імен – ідентифікаторів.

Автентифікація – процедура встановлення належності інформації в системі користувачеві

Авторизація – процедура контролю доступу суб'єктів до об'єктів і надання кожному з них саме тих прав, які для них визначені правила доступу.

Опишемо деякі механізми захисту, що присутні у інструментах корпоративних мереж.

Frame Relay («ретрансляція кадрів») – протокол канального рівня моделі OSI. Основна його перевага – простота реалізації. Тут реалізований мінімальний набір послуг, які є необхідними для швидкої передачі кадрів у місце призначення. Працює за принципом «best efforts». Цей протокол, на жаль, не підтримує надійну передачу кадрів. Цю «відповідальність» Frame Relay перекладає на протоколи вищих рівнів, наприклад, на TCP. Технологія Frame Relay володіє такою властивістю як гарантія пропускної здатності з'єднань мережі.

Стандартним протоколом Інтернет є протокол точка-точка (англ. PPP – Point-to-Point Protocol) і він має складну процедуру обміну параметрами зв'язку: встановлення зв'язку, визначення автентичності користувача та виклик протоколу мережевого рівня. Між останніми двома етапи може бути ще один етап – контроль повторного виклику PPP, цей етап не є обов'язковим [12]. Досить цікавим, з точки зору безпеки, є етап визначення автентичності користувача. Для цього протокол PPP, за замовчуванням, може використовувати два протоколи. Одним із них є протокол автентифікації за паролем (англ. Password Authentication Protocol, PAP), який пересилає пароль у відкритому вигляді по лінії зв'язку. Іншим – протокол автентифікації за викликом квітування (англ. Challenge Handshake Authentication Protocol, CHAP). CHAP використовує передачу не паролів по каналу зв'язку, а лише непрямих відомостей про паролі. Алгоритм цього протоколу використовує хеш-функцію. Роботу цього протоколу можна описати так: спочатку CHAP-сервер надсилає клієнту запит, далі клієнт на основі цього запиту і свого паролю обчислює хеш і надсилає його серверу, і сервер виконує те ж саме і перевіряє надісланий хеш. Якщо є збіг, дані вважаються автентичними [13].

IPSec. Стек протоколів IPSec працює на мережевому рівні моделі OSI і є прозорим для додатків та може працювати у всіх мережах, оскільки базується на IP і може використовувати всі технології канального рівня. Механізм безпеки тут – протоколи AH, ESP, IKE, що виконують функцію «захищеного з'єднання». Стандарти IPSec дозволяють кінцевим точкам захищеного каналу використовувати засоби «захищеного з'єднання» для передачі трафіку через усі проміжні точки загальнодоступної мережі. Такий підхід також дає можливість вибирати потрібний рівень деталізації захисту [14].

Детальніше розглянемо функції вищезгаданих механізмів безпеки стеку протоколів IPSec. Протоколи AH, ESP та IKE утворюють ядро IPSec. Завданням протоколу AH (англ. Authentication Header – заголовок автентифікації) є гарантія цілісності та оригінальності даних. Протокол ESP (англ. Encapsulating Security Payload – інкапсуляція зашифрованих даних)

призначений для шифрування даних, які передаються, а також може виконувати ті ж функції що й протокол AH. Для автентифікації даних у цих протоколах використовують дайджест автентифікацію (один із методів автентифікації, який застосовує хеш-функцію, щоб захешувати пароль перед відправленням через мережу [2, 5]**Ошибка! Источник ссылки не найден.**) за допомогою MD5 або SHA-1. Функції протоколів AH та ESP частково перекриваються. Це пов’язано з тим, що, інколи, через відповідні обмеження в законодавстві деяких держав – шифрування використовувати не можна. Звісно, без використання протоколу ESP, захист інформації мережі може бути не достатнім, але й мережа на протоколі AH буде повністю працездатною. І, нарешті, протокол IKE (англ, Internet Key Exchange – обмін ключами Інтернету) виконує допоміжну роль – надає кінцевим пристроям доступ до захищеного каналу секретних ключів, які є потрібними для протоколів AH та ESP. Цей протокол використовує DES (англ. Data Encryption Standard – стандарт шифрування даних). Великою перевагою IPSec є те, що його можна розширювати шляхом додавання інших алгоритмів автентифікації чи шифрування. Наприклад, використовуються алгоритми Triple DES, Cast, RC5, Idea та інші [2, 5].

GRE (Generic Routing Encapsulation) – протокол інкапсуляції, що працює з IPSec для створення тунелів. Сам по собі GRE не забезпечує безпечного передавання даних, однак незамінний коли є завдання, пов'язані з динамічною маршрутизацією. Протокол не навантажує обладнання, проте навантаження при шифруванні великого обсягу даних істотне. Механізм безпеки тут – передавання даних від протоколів динамічної маршрутизації, причому, самі дані від цих протоколів можуть шифруватися. GRE може інкапсулювати різні типи протоколів у IPSec-тунелі (IPSec-тунель потрібний для безпечного з'єднання IP-мереж, які не мають прямого маршруту між собою, при цьому використовується основний протокол маршрутизації через проміжний транспортний зв'язок [5]). Схема інкапсульованого пакету протоколу GRE наведено на рис. 1.

Структура інкапсульованого пакету GRE складається із протоколу

доставки, що передає дані протоколу інкапсуляції, наприклад IP; протоколу інкапсуляції GRE та протоколу, який потрібно інкапсулювати («протокол-пасажир»). Зауважимо, що протокол GRE має відому проблему DF-біту [15].

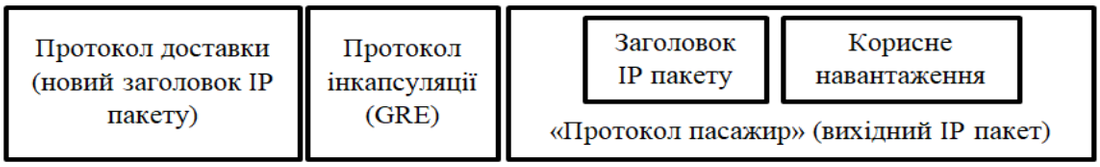

Рис. 1. **Схема інкапсульованого пакету протоколу GRE**

AAA (authentication, authorization, accounting). Цей сервіс ускладнює роботу для зловмисників і при цьому сприяє легітимним користувачам під час доступу до мережевих ресурсів. Автентифікація вимагає від користувачів доказів того, що вони дійсно є тими, за кого себе видають. Під час авторизації, сервіс вирішує, до яких ресурсів дозволяється доступ користувачеві і які в нього права. Ведення запису дій користувача здійснюється з метою обліку та контролю. Механізм безпеки тут – автентифікація, авторизація, облік [1-2].

Спочатку розглянемо процес автентифікації. Існує дві основних автентифікаційних моделі сервісу AAA для корпоративних мереж:

– двостороння модель. Процедура автентифікації виконується лише учасниками діалогу без послуг, які може надавати третя сторона. Таку модель, наприклад, описує автентифікація при віддаленому доступі до мережевих пристрої по протоколах доступу (SSH чи Telnet);

– тристороння модель. Її використовують для виконання автентифікації у великих мережах. Тристороння модель має такі складові:

а) користувач, що хоче автентифікуватися в мережі;

б) сервер доступу до мережі, який є «посередником» між користувачем та мережею;

в) AAA-сервер, який виконує перевірку облікових записів користувачів за запитами «посередника» [16, 17].

Процес автентифікації сервісу AAA показано на рис. 2 [16]. Спочатку користувач, що хоче автентифікуватися в мережі (постачальник

автентифікаційних даних), підключається до ААА-клієнта – пристрою доступу – AGW (англ. Access Gateway) або до сервера доступу до мережі – NAS (англ. Network Access Server) по протоколу доступу (Telnet, SSH, Serial) і вводить свої логін та пароль.

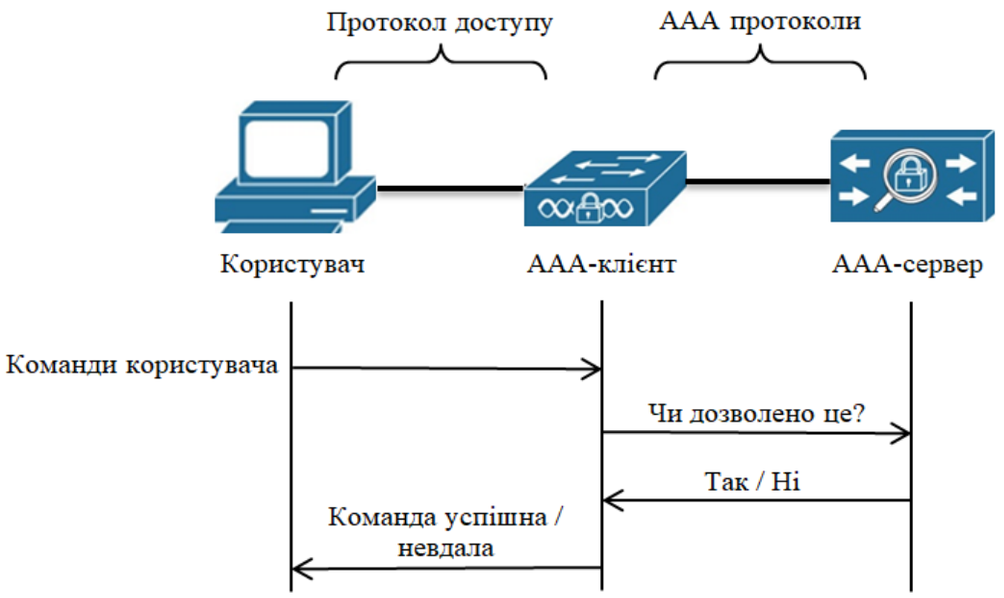

Рис. 2. **Схематичне зображення процесу автентифікації сервісу ААА**

ААА-клієнт формує і відправляє запит автентифікації до ААА-сервера і очікує відповіді. ААА-сервер перевіряє логін користувача і його пароль, використовуючи при цьому протокол RADIUS, TACACS+ або DIAMETER. Після перевірки ААА-сервер формує відповідь і відправляє її назад до ААА-клієнта. Якщо користувач пройшов автентифікацію, то ААА-клієнт надає йому доступ до мережі, але не надає йому доступу до послуг. Якщо користувач намагається отримати доступ до потрібних йому послуг, наприклад, до Інтернет, то ААА-клієнт формує новий запит і надсилає його до ААА-серверу для авторизації. Знову ж таки, ААА-сервер перевіряє отриману інформацію про послуги, які є доступними для цього користувача і надсилає позитивну або негативну відповідь ААА-клієнту. У свою чергу ААА-клієнт надсилає цю відповідь користувачеві. Який може або не може скористатися, наприклад, Інтернет [16].

Друга А абревіатури сервісу означає авторизацію. Під час процесу

авторизації визначаються повноваження доступу конкретного користувача до відповідних ресурсів. Для такого процесу потрібна певна інфраструктура. Розглянемо базовий її варіант (рис. 3).

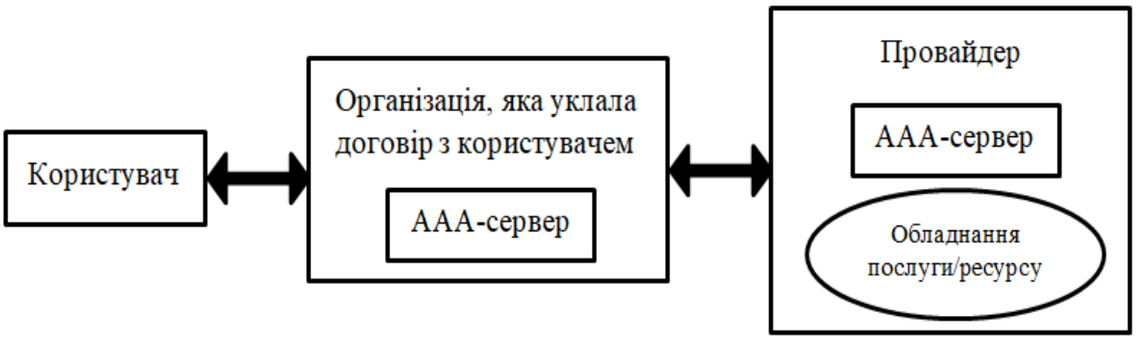

Рис. 3. **Базовий варіант інфраструктури процесу авторизації**

Існує користувач, який хоче отримати доступ до певного ресурсу чи послуги. Цей користувач укладає договір з організацією, яка перевіряє чи має він право доступу до необхідного ресурсу чи послуги. У свою чергу ця організація укладає договір із провайдером, AAA-сервер якого авторизує доступ до необхідної послуги чи ресурсу. Наступним в дію вступає обладнання послуги чи ресурсу, яке й надає її чи його (наприклад, принтер, маршрутизатор).

Остання літера А абревіатури AAA означає – облік (англ. accounting). Поняття облік будемо ототожнювати із збиранням інформації про використання ресурсу для аналізу, контролю та розподілу вартості. Архітектура системи обліку не є складною. Спочатку пристрої мережі збирають інформацію про використані ресурси і відправляють її, використовуючи протоколи аудиту, на сервер обліку. Сервер обліку обробляє отриману інформацію (об’єднує дані проміжного аудиту або ідентифікує записи, що повторюються). Цей сервер розділяє події внутрішніх доменів та міждоменні події, а також виконує відповідну маршрутизацію трафіку. Після того, як сервер обліку обробить отриману інформацію, він відправляє її по протоколу передачі на біллінг-сервер (біллінг – сукупність подій, необхідних для підготовки рахунків). Біллінг-сервер, зазвичай, оцінює вартість і генерує

рахунки. На локальний біллінг-сервер поступають події обліку внутрішніх доменів, а міждоменні події відправляються на сервери інших адміністративних доменів.

*VPN***.** Сервіс VPN (англ. Virtual Private Network – віртуальна приватна мережа) використовується для забезпечення захисту корпоративних мереж. Головною перевагою тут є значно ефективніший розподіл ресурсів мережі під час комутації пакетів, ніж при комутації каналів. Відсутність зв'язків із зовнішнім середовищем надійно захищає мережу від зовнішніх атак та істотно знижує ймовірність «прослуховування» мережевого трафіку. Механізм безпеки тут – шифрування трафіку, автентифікація користувачів, контроль доступу до мережі.

Тепер розглянемо деякі властивості віртуальних приватних мереж, які відіграють чималу роль у виборі сервісу. Сервіс VPN обмежує доступ до мережі, тобто обмінюватися пакетами можуть лише вузли цієї мережі, оскільки лише вони мають таку технічну можливість. Таке завдання є досить трудомістким для VPN. Це можна пояснити тим, що пакети віртуальної приватної мережі повинні пройти через ті ж канали та мережеві пристрої, що й пакети зовнішніх вузлів. Технологія VPN дозволяє адресацію вузлів мережі із всього діапазону IP-адрес, в тому числі й приватні адреси. Тобто обмеження на вибір IP-адреси вузлом віртуальної приватної мережі відсутні як такі. Вагомою перевагою VPN є окремі лінії зв’язку. Це дозволяє досить точно передбачити продуктивність мережі. Технологія віртуальних приватних мереж передбачає відсутність зв’язків із «зовнішнім світом». Доступ зовнішніх користувачів серйозно обмежується. Такі заходи допомагають істотно підвищити рівень захисту інформації у корпоративних мережах [18].

Висновки та комплексний захист ресурсів корпоративної мережі засобами сучасних технологій та їх комбінацій із подальшим застосуванням для окремого рішення. Систематичний комплексний підхід для захисту інформаційних, фінансових та матеріальних активів компанії полягає у запровадженні організаційно-адміністративних, інженерно-технічних, апаратних, програмних та криптографічних засобів захисту корпоративної

мережі, а також у застосуванні ще й спеціалізованих механізмів захисту корпоративних мереж. Розглянемо запропонований підхід на прикладі організації комплексного захисту корпоративної мережі компанії «Underdefense» (рис. 4).

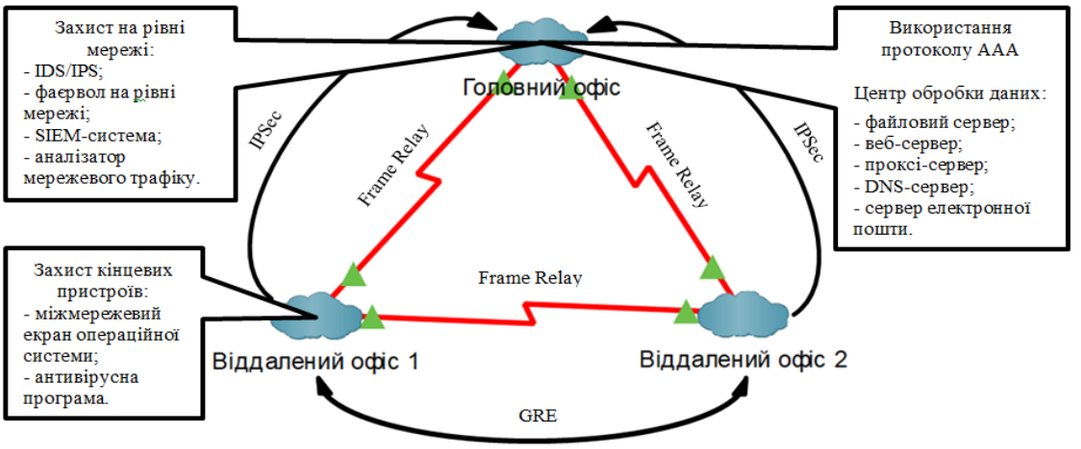

Рис. 4 **Схема комплексного підходу захисту корпоративної мережі**

На рисунку 4 показано приклад комбінації деяких технологій захисту корпоративних мереж. Так, наприклад, для з'єднання віддалених офісів (ВО) з головним офісом (ГО) та між собою, використовується технологія Frame Relay. Також пропонується впровадження окремо захисту на рівні мережі (IDS/IPS, фаєрвол на рівні мережі, SIEM-система, аналізатор мережевого трафіку) та на рівні хостів (міжмережевий екран операційної системи (ОС), антивірусна програма). У ГО застосовано сервіс AAA. Це забезпечить надійний захист активів компанії, що використовує протоколи динамічної маршрутизації. ВО мають з'єднання за допомогою GRE, а до ГО є зв'язок через стек протоколів IPSec. Не менш важливими є фізичне керування доступом та захист підтримуючої інфраструктури, а також обґрунтоване та обдумане впровадження політик безпеки. Чималу роль у захисті корпоративної мережі відіграє навчання персоналу, яке дозволяє істотно зменшити ймовірність виникнення інцидентів кібербезпеки.

Список джерел:

1. Технології захисту локальних мереж на основі обладнання CISCO : навч. пос.

/ Т. І. Коробейнікова, С. М. Захарченко. – Л.: Вид-во Львівської політехніки, 2021. – 188с.

2. Трояновська Т. І. Побудова захищених мереж на базі обладнання компанії Cisco. // Захарченко С.М., Трояновська Т. І., Бойко О.В. Навчальний посібник. Вінниця : ВНТУ, 2017. – 133 с.
3. Система обміну миттєвими повідомленнями в корпоративній мережі / Коробейнікова Т. І., Савицька Л. А., Карплюк С. В. // Актуальні досягнення сучасних наукових досліджень: XX Міжн. наук.-пр. конференція: тези доповідей, Дніпро, 17 вересня 2019 р. – Ч. 1. – Дніпро: ГО «НОК», 2019 – с. 19-24.
4. Методи та засоби безпечної передачі даних в корпоративних мережах / Коробейнікова Т. І., Куцак Ю. В. // Зб. мат.XLVIII наук.-техн. конф. ФІТКІ (2019). Реж. доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2019/paper/view/ 6606/5491.
5. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки. Навч. пос. – Вінниця: ВНТУ, 2009. – 268 с
6. Метод паралельного моніторингу параметрів корпоративних мереж / Коробейнікова Т.І., Каневський М. В. // Зб. мат. XLVIII Наук.-техн. конф. ФІТКІ (2019). Реж. доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-019/paper/view/6972/5687.
7. Коробейнікова Т. І. Комплексна система моніторингу корпоративної мережі / Коробейнікова Т. І., Каневський М. В. Зимові наукові підсумки 2018: XII Міжн. наук.-практич. конференція: тези доповідей, Дніпро, 25 грудня 2018 р. – Ч. 1. – Дніпро: НБК, 2018, с. 79-84.
8. Коробейнікова Т. І. Комплексний метод організації IP-телефонії в структурі захищеної корпоративної мережі підприємства / Коробейнікова Т. І., Ткачук В. Ю. Зимові наукові підсумки 2018: XII Міжнародна наук.-практич. конференція: тези доповідей, Дніпро, 25 грудня 2018 р. – Ч. 1. – Дніпро: НБК, 2018, с. 105-111.
9. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
10. Коробейнікова Т. І. Організація захисту інформації в корпоративній мережі за допомогою симетричних алгоритмів шифрування / Коробейнікова Т. І., Шостак С. В. Інноваційні підходи до розвитку сучасної науки: XIV Міжн. наук.-пр. інт.-конф.: тези доповідей, Дніпро, 28 лютого 2019 р. – Ч. 1. – Дніпро: НОК, 2019 – с. 51-57.
11. Поняття SIEM систем. [Електронний ресурс] // Софтліст. – 2019 – Реж. доступу: https://ua.softlist.com.ua/articles/chto-takoe-siem-sistema/.
12. PPP [Електронний ресурс] // Вікіпедія – вільна енциклопедія. – 2020. – Реж. доступу: https://uk.wikipedia.org/wiki/PPP.

13. CHAP [Електронний ресурс] // Вікіпедія – вільна енциклопедія. – 2020. – Реж. доступу: https://uk.wikipedia.org/wiki/CHAP.
14. Методи та засоби створення захищеної корпоративної мережі на базі обладнання компанії Cisco / Коробейнікова Т. І., Шостак С. В. // Збірник Матеріалів XLVIII Наук.-техн. конференції ФІТКІ (2019). Реж. доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2019/paper/view/6661/5569.
15. Проблема DF біта і фрагментації в GRE тунелях [Електронний ресурс] // OpenNET. – 2008. – Реж. доступу: https://www.opennet.ru/base/cisco/gre_fragment.txt.html.
16. Гольдштейн Б. С. Протоколи AAA: RADIUS і Diameter / Б. С. Гольдштейн, В. С. Єлагін, Ю. Л. Сенченко. – Санкт-Петербург: БХВ-Петербург, 2014. – 352 с.
17. Хазов В. Автентифікація, авторизація й облік (AAA) - RADIUS або TACACS+ [Електронний ресурс] / В. Хазов // VAS EXPERTS. – 2017. – Реж. доступу: https://vasexperts.ru/blog/autentifikaciya-avtorizaciya-i-uchet-aaa-radius-ili-tacacs/.
18. SunScreen SKIP User's Guide, Release 1.1 [Електронний ресурс] // Oracle Corporation and/or its affiliates. – 2010. – Реж. доступу: https://docs.oracle.com/cd/E19957-01/805-5743/index.html.