ВСТУП

Актуальність теми. Актуальність розробки методу побудови корпоративних мереж зумовлена стрімким зростанням вимог до надійності, безпеки та масштабованості сучасної інфраструктури. Поширення хмарних технологій, збільшення обсягів трафіку та зростання кількості кіберзагроз потребують системних підходів до проектування мереж, здатних забезпечити стабільну роботу підприємств. У цих умовах формування ефективних методів побудови корпоративних мереж набуває особливого практичного значення.

Платформа MikroTik надає значний набір функцій, залишаючись при цьому досить бюджетною, і вона дедалі частіше використовується в багатьох корпоративних IT-інфраструктурах. Водночас зростаючі вимоги до кібербезпеки потребують можливостей, які виходять за рамки базового брандмауера, а інтеграція Suricata додає глибоку інспекцію пакетів, виявлення вторгнень та функції поведінкового аналізу, яких у MikroTik не реалізовано.

Оскільки автоматизованої процедури об'єднання MikroTik з Suricata не існує, створення методу проектування мереж за моєю темою задовольняє актуальні потреби мережевих фахівців. Злиття MikroTik та рішення Suricata суттєво підвищує здатність виявляти інциденти безпеки та головне реагувати на них, пропонуючи поглиблене розуміння потоків даних, що дає можливість захоплювати та аналізувати небезпечний трафік. Крім того, для розробленого методу доступна масштабованість, що робить його актуальним для корпорацій різного масштабу. Спроектована мережа підтримує подальше зростання через розгортання VPN серверу, відкриття дочірніх філій, впровадження хмарних технологій, механізмів відмовостійкості та методу сегментації мережі.

Таким чином, поєднання обладнання MikroTik та програмного комплексу Suricata дозволяє реалізувати сучасні механізми захисту мережевого трафіку з урахуванням техніко-економічної доцільності, поєднуючи доступність, функціональність і можливість гнучкого масштабування, що робить запропонований підхід практично придатним для широкого кола підприємств.

Мета роботи – розроблення та обґрунтування методу побудови захищеної корпоративної мережі підприємства з використанням обладнання MikroTik та програмного комплексу Suricata, який забезпечує підвищення рівня інформаційної безпеки, керованості та масштабованості мережевої інфраструктури.

Об'єкт дослідження – корпоративна комп'ютерна мережа підприємства малого та середнього бізнесу як процес організації, передавання та захисту мережевого трафіку в розподіленій інформаційній інфраструктурі.

Предметом дослідження – метод побудови захищеної корпоративної мережі підприємства з використанням мережевого обладнання MikroTik та програмного комплексу Suricata.

Методи дослідження включають аналіз і узагальнення науково-технічних джерел, системний і структурно-функціональний аналіз мережевих архітектур, методи мережевого проектування, моделювання логічної сегментації та зон безпеки, а також експериментальне налаштування та аналіз роботи IDS/IPS Suricata. У результаті застосування зазначених методів обґрунтовано архітектуру корпоративної мережі, визначено оптимальну VLAN-сегментацію, розроблено правила виявлення мережевих атак і механізми автоматизованого реагування.

Наукова новизна одержаних результатів. У ході дослідження розроблено метод побудови корпоративної мережі підприємства малого та середнього бізнесу, який поєднує функціональні можливості обладнання MikroTik та програмного комплексу Suricata в єдину архітектуру. А також запропоновано методи моніторингу та реагування на мережеві інциденти за допомогою власних правил.

Практична значущість роботи полягає у можливості використання розробленого методу під час проектування та модернізації корпоративних мереж малого і середнього бізнесу з підвищеними вимогами до інформаційної безпеки.

ВСТУП

Актуальність теми. Актуальність розробки методу побудови корпоративних мереж зумовлена стрімким зростанням вимог до надійності, безпеки та масштабованості сучасної інфраструктури. Поширення хмарних технологій, збільшення обсягів трафіку та зростання кількості кіберзагроз потребують системних підходів до проектування мереж, здатних забезпечити стабільну роботу підприємств. У цих умовах формування ефективних методів побудови корпоративних мереж набуває особливого практичного значення.

Платформа MikroTik надає значний набір функцій, залишаючись при цьому досить бюджетною, і вона дедалі частіше використовується в багатьох корпоративних IT-інфраструктурах. Водночас зростаючі вимоги до кібербезпеки потребують можливостей, які виходять за рамки базового брандмауера, а інтеграція Suricata додає глибоку інспекцію пакетів, виявлення вторгнень та функції поведінкового аналізу, яких у MikroTik не реалізовано.

Оскільки автоматизованої процедури об'єднання MikroTik з Suricata не існує, створення методу проектування мереж за моєю темою задовольняє актуальні потреби мережевих фахівців. Злиття MikroTik та рішення Suricata суттєво підвищує здатність виявляти інциденти безпеки та головне реагувати на них, пропонуючи поглиблене розуміння потоків даних, що дає можливість захоплювати та аналізувати небезпечний трафік. Крім того, для розробленого методу доступна масштабованість, що робить його актуальним для корпорацій різного масштабу. Спроектована мережа підтримує подальше зростання через розгортання VPN серверу, відкриття дочірніх філій, впровадження хмарних технологій, механізмів відмовостійкості та методу сегментації мережі.

Таким чином, поєднання обладнання MikroTik та програмного комплексу Suricata дозволяє реалізувати сучасні механізми захисту мережевого трафіку з урахуванням техніко-економічної доцільності, поєднуючи доступність, функціональність і можливість гнучкого масштабування, що робить запропонований підхід практично придатним для широкого кола підприємств.

Мета роботи – розроблення та обґрунтування методу побудови захищеної корпоративної мережі підприємства з використанням обладнання MikroTik та програмного комплексу Suricata, який забезпечує підвищення рівня інформаційної безпеки, керованості та масштабованості мережевої інфраструктури.

Об'єкт дослідження – корпоративна комп'ютерна мережа підприємства малого та середнього бізнесу як процес організації, передавання та захисту мережевого трафіку в розподіленій інформаційній інфраструктурі.

Предметом дослідження – метод побудови захищеної корпоративної мережі підприємства з використанням мережевого обладнання MikroTik та програмного комплексу Suricata.

Методи дослідження включають аналіз і узагальнення науково-технічних джерел, системний і структурно-функціональний аналіз мережевих архітектур, методи мережевого проектування, моделювання логічної сегментації та зон безпеки, а також експериментальне налаштування та аналіз роботи IDS/IPS Suricata. У результаті застосування зазначених методів обґрунтовано архітектуру корпоративної мережі, визначено оптимальну VLAN-сегментацію, розроблено правила виявлення мережевих атак і механізми автоматизованого реагування.

Наукова новизна одержаних результатів. У ході дослідження розроблено метод побудови корпоративної мережі підприємства малого та середнього бізнесу, який поєднує функціональні можливості обладнання MikroTik та програмного комплексу Suricata в єдину архітектуру. А також запропоновано методи моніторингу та реагування на мережеві інциденти за допомогою власних правил.

Практична значущість роботи полягає у можливості використання розробленого методу під час проектування та модернізації корпоративних мереж малого і середнього бізнесу з підвищеними вимогами до інформаційної безпеки.

РОЗДІЛ 1 ДОСЛІДЖЕННЯ СУЧАСНОГО СТАНУ ТА ТЕНДЕНЦІЙ РОЗВИТКУ КОРПОРАТИВНИХ МЕРЕЖ І ЗАСОБІВ ЇХ ЗАХИСТУ

1.1 Огляд сучасних методів побудови корпоративних комп'ютерних мереж

Корпоративна комп'ютерна мережа є інтегрованим середовищем, що поєднує декілька взаємозалежних підсистем: мережу доступу для робочих станцій і мобільних пристроїв, серверну та дата-центрову інфраструктуру, мережі зберігання даних (NAS/SAN), підсистеми голосового та відеозв'язку, а також мережі керування й моніторингу. У системному підході така мережа розглядається як цілісна, де зміна в одній підсистемі має бути узгоджена з пропускною здатністю магістралі, схемами маршрутизації та політиками безпеки. [3]

У практичній реалізації корпоративну мережу варто описувати як поєднання трьох взаємопов'язаних площин: площини передавання даних (data plane), де відбувається комутація та маршрутизація трафіку; площини керування (control plane), що забезпечує побудову таблиць маршрутизації, узгодження станів протоколів та конвергенцію після відмов; та площини керування й експлуатації (management plane), яка охоплює адміністрування, моніторинг, облік конфігурацій і журнали подій. Таке розділення допомагає коректно інтегрувати підсистеми різного призначення та визначити, де саме мають виконуватися функції ідентифікації, сегментації, пріоритезації трафіку й контролю доступу.

До типових підсистем, що інтегруються в корпоративній мережі малого або середнього підприємства, належать:

– підсистема доступу користувачів (дротова та бездротова), що об'єднує робочі місця, POS-термінали, сканери, принтери та мобільні пристрої
– серверна або хмарна підсистема прикладних сервісів (файлові ресурси, доменні служби, облікові системи, CRM/ERP, внутрішні вебзастосунки)
– підсистема відеоспостереження та периферійних пристроїв (IP-камери,

реєстратори, контролери доступу, IoT-обладнання), для яких важливі ізоляція та керований доступ

– підсистема безпеки та експлуатації (фаєрвол, VPN-доступ, централізоване журналювання, моніторинг доступності, часові служби), яка забезпечує контроль і відновлення працездатності

Ключовою технічною ознакою корпоративної мережі є керована сегментація на рівні L2/L3: логічні домени формуються за допомогою VLAN, а передавання кількох сегментів між комутаторами та маршрутизатором реалізується через транкові з'єднання з тегуванням кадрів. Для забезпечення коректної роботи в ієрархічних топологіях використовуються механізми запобігання петлям (сімейство STP), а для підвищення пропускної здатності та надійності – агрегація лінків (LACP) і резервування шляхів. З практичної точки зору сегментація дозволяє мінімізувати широкомовний трафік, обмежити бічне переміщення зловмисника між зонами та спростити застосування політик безпеки на межі сегментів. [1]

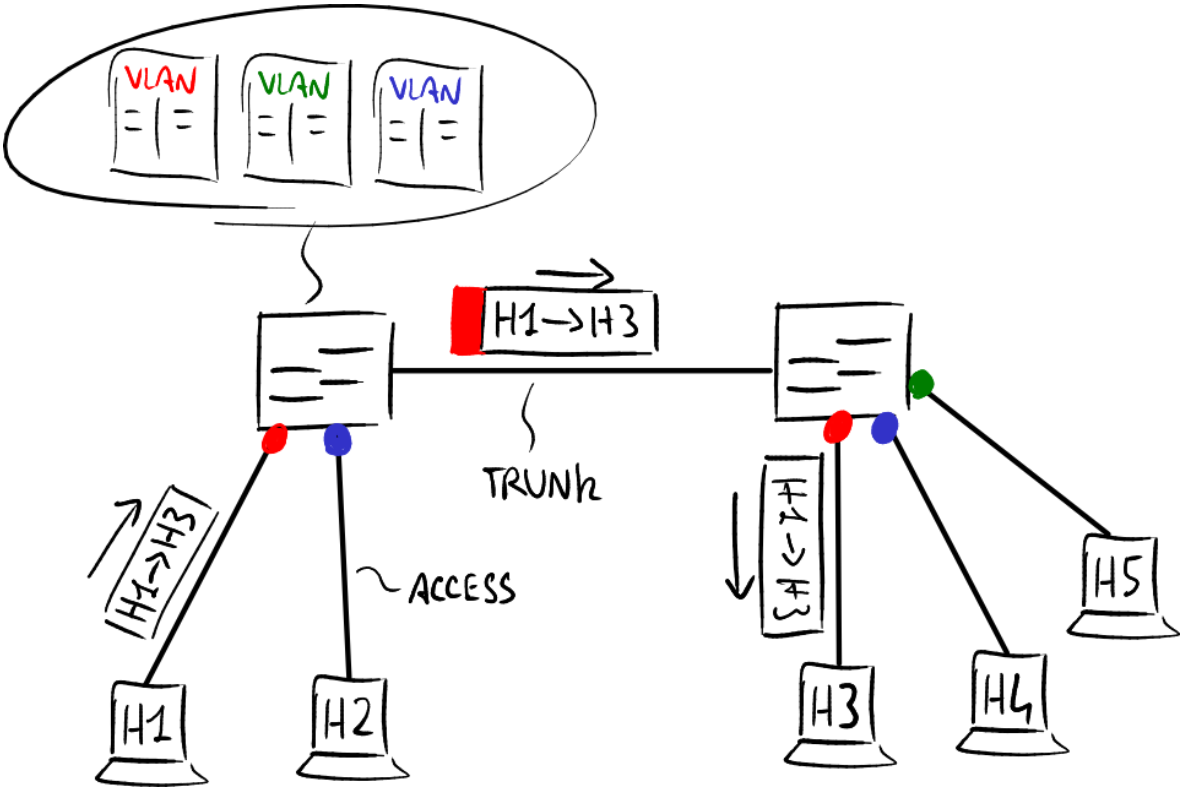

Рис. 1.1 Узагальнена схема інтегрованих підсистем SMB-мережі

У класичному підручнику з комп'ютерних мереж за авторством Ендрю

Стюарта Таненбаума розглядається побудова корпоративних мереж через багаторівневу модель, де фізичний, канальний, мережевий, транспортний та прикладний рівні виконують різні функції й спілкуються між собою через стандартизовані інтерфейси. Під "незалежною еволюцією протоколів" тут розуміють ситуацію, коли, наприклад, перехід від Fast Ethernet до Gigabit Ethernet відбувається на фізичному та канальному рівнях без зміни протоколу IP і прикладних сервісів, а використання IPv6 допускає збереження логіки роботи протоколів прикладного рівня (HTTP/HTTPS, SMTP, DNS тощо) за умови тому підтримки на транспортному рівні. Таким чином, розвиток фізичної інфраструктури, мережевих протоколів і прикладних сервісів може відбуватися окремими шарами, не вимагаючи повної перебудови всієї мережі.

З позиції експлуатації "незалежна еволюція" протоколів означає можливість поетапних міграцій: наприклад, розширення пропускної здатності мережі доступу (заміна комутаторів і лінків) може виконуватися без зміни IP-адресації та прикладних сервісів, тоді як перехід до нових механізмів сегментації чи маршрутизації можна реалізувати спочатку в окремому домені (наприклад, для гостьового Wi-Fi або відеоспостереження), не зачіпаючи критичні сервіси. Практично це вимагає підтримки режимів сумісності (dual-stack, тунелювання, перехідні шлюзи) та акуратного планування меж між L2 і L3 рівнями, щоб модернізація окремого шару не спричиняла зупинки всієї мережі.

При використанні підходу проектування мережі "згори донизу" акцент робиться на прикладних сервісах, які має підтримувати мережа: веб-додатки, електронна пошта, потокове відео, сервіси спільної роботи, хмарні застосунки тощо. Спочатку для кожного сервісу визначаються вимоги до пропускної здатності, затримок, надійності та безпеки, а вже потім приймаються рішення щодо топології (ієрархічна, фабрична, зірка, частково сітчаста), вибору протоколів маршрутизації, схем адресації та використання механізмів сегментації (VLAN, VPN). Такий підхід дозволяє одразу передбачити у проекті можливість інтеграції нових сервісів (наприклад, відеоконференцій або хмарних платформ) без необхідності суттєво перебудовувати вже побудовану архітектуру. [2]

Оскільки корпоративна мережа обслуговує різні класи трафіку, проектування має враховувати механізми якості обслуговування (QoS): класифікацію та маркування потоків (наприклад, за портами, адресами або ознаками застосунків), керування чергами, пріоритезацію трафіку реального часу та обмеження некритичних потоків. Для сервісів голосу й відео критичними є затримка, джитер і втрата пакетів, тому на магістральних і агрегаційних ділянках зазвичай застосовують політики пріоритетних черг і контроль перевантаження, тоді як для резервного копіювання або оновлень – політики обмеження швидкості (shaping і policing).

Системний підхід до мереж, запропонований у сучасних роботах, наголошує на тому, що корпоративна мережа має розглядатися як сукупність взаємодіючих компонентів: маршрутів, черг, механізмів відновлення після відмов, політик безпеки та управління трафіком. Типові методи побудови включають ієрархічні архітектури з виділенням рівнів доступу, агрегації та ядра, використання протоколів динамічної маршрутизації (OSPF, BGP) для побудови відмовостійких маршрутів і застосування механізмів контролю черг (QoS) для підтримки сервісів у реальному часі. Особлива увага приділяється проектування механізмів відновлення – резервним лінкам, дублюванню вузлів та використанню протоколів швидкої конвергенції.

Відмовостійкість у корпоративних мережах досягається поєднанням резервних каналів і протоколів, що швидко перебудовують маршрути. На рівні L3 для балансування та резервування часто використовуються рівноцінні шляхи (ECMP) у поєднанні з динамічною маршрутизацією, а для безперервності роботи кінцевих пристроїв на шлюзі – протоколи резервування першого стрибка (наприклад, VRRP). На рівні L2 резервування реалізують через дублювання комутаторів доступу/агрегації, кільцеві або частково сітчасті схеми, а також агрегацію лінків, що забезпечує як підвищення пропускної здатності, так і швидке відновлення при відмові окремого фізичного з’єднання.

Організація корпоративної мережі також залежить від вимог до безпеки: розподілом на внутрішні й зовнішні зони, виділенням демілітаризованих зон

(DMZ), гостьових сегментів, сегментів адміністрування та критично важливих систем. У літературі, орієнтованій на корпоративну безпеку, наголошується важливість того, щоб уже на етапі побудови мережі були передбачені політики доступу, зони різного рівня довіри, точки контролю трафіку й механізми централізованого логування. Такий підхід дозволяє відразу інтегрувати в архітектуру засоби виявлення вторгнень, системи управління подіями безпеки (SIEM) та резервні канали для критичних сервісів. [4]

Важливим елементом архітектури є виділення керівного (адміністративного) контуру: доступ до мережевого обладнання, систем моніторингу та серверів керування варто виносити в окремий сегмент, обмежувати за принципом найменших привілеїв і фіксувати в журналах. Для цього застосовуються окремі облікові записи адміністрування, контроль доступу за списками, багатофакторна автентифікація, обмеження керівних протоколів (SSH/HTTPS) та централізоване зберігання логів. Такий підхід підвищує керованість мережі та зменшує ризик компрометації критичних налаштувань у випадку інцидентів.

Окремим напрямком сучасних методів побудови є інтеграція мережевих рішень з хмарними сервісами й мобільними клієнтами, де мережа має забезпечити єдиний політично керований доступ до внутрішніх і зовнішніх ресурсів. Серед вимог – підтримка VPN-з’єднань, сегментації трафіку між офісними, гостьовими та віддаленими користувачами, а також узгоджені політики доступу до ресурсів незалежно від точки підключення. Саме такі вимоги формують підґрунтя для розгляду сучасних тенденцій розвитку корпоративних мереж.

1.2 Сучасний стан та тенденції розвитку корпоративних мереж

Сучасні корпоративні мережі розвиваються під впливом зростання ролі прикладних сервісів, які повинні працювати будь-де і будь-коли – від класичних офісних застосунків до хмарних сервісів, відеоконференцій і мобільних клієнтів. У такому середовищі мережа має не лише забезпечувати базову зв’язність, а й

підтримувати диференційовану якість обслуговування для різних класів трафіку, масштабованість для збільшення кількості користувачів та інтеграцію з інтернет-сервісами й API. З погляду архітектури це означає перехід від жорстко фіксованих схем до гнучких конфігурацій, здатних швидко адаптуватися до змін у наборі сервісів. [2]

Додатковим чинником є зміна характеру корпоративного трафіку: поряд із "північ-південь" потоками до Інтернету/хмари збільшується частка "схід-захід" взаємодії між сервісами всередині організації (мікросервіси, взаємодія застосунків із базами даних, резервне копіювання). Це підсилює вимоги до пропускної здатності внутрішніх сегментів, якості маршрутизації між VLAN/підмережами та до стабільності затримок, особливо якщо критичні застосунки рознесені між локальними серверами й хмарними компонентами.

З позиції експлуатації мультидоменна архітектура передбачає наявність спільної мови політик: правила сегментації, доступу та якості обслуговування мають застосовуватися узгоджено в кампусі, у WAN і в дата-центрі, щоб зміна сервісу або поява нового майданчика не вимагали ручного дублювання конфігурацій у кожному домені. На технічному рівні це реалізується через уніфіковані шаблони адресації, стандартизовані профілі VLAN/VRF, єдині принципи маркування трафіку та централізовані механізми збору телеметрії й журналів.

Системний погляд на розвиток мереж підкреслює важливість віртуалізації, хмарних обчислень і програмно-визначених мереж (SDN), які дозволяють відокремити логіку керування від площини пересилання трафіку. Завдяки цьому маршрутизація, фільтрація, балансування навантаження та інші мережеві функції можуть задаватися програмно й розподілятися між фізичними та віртуальними пристроями залежно від поточних потреб. Такі підходи роблять можливим швидке використання нових сервісів, автоматизоване масштабування ресурсів і централізоване застосування політик безпеки для великих розподілених інфраструктур. [3]

З практичного погляду SDN-підходи та віртуалізація стимулюють

автоматизацію експлуатації: конфігурації дедалі частіше описуються як набір шаблонів і політик, які застосовуються централізовано, а не налаштовуються вручну на кожному пристрої. Для цього використовують API, телеметрію, системи керування конфігураціями та принципи "інфраструктура як код", що зменшує кількість помилок і полегшує аудит змін. З погляду технічної ефективності це особливо важливо для розподілених мереж із філіями, де повторюваність конфігурацій і швидкість розгортання є ключовими показниками.

З точки зору безпеки та захисту даних особливої уваги потребують мобільні й віддалені користувачі, які отримують доступ до корпоративних ресурсів через несегментовані або частково керовані мережі. Сучасні підходи описують перехід від моделі "жорсткого периметра" до багаторівневих архітектур, де контроль доступу, шифрування, автентифікація й моніторинг трафіку розподілені по всій мережі. У таких умовах зростає роль мережевих рішень, які підтримують політики "нульової довіри", сегментацію трафіку й постійний аналіз мережевої активності для виявлення аномалій. [5]

У сфері захисту даних спостерігається зростання частки шифрованого трафіку (TLS), що з одного боку підвищує конфіденційність, а з іншого ускладнює мережеве виявлення загроз лише за вмістом пакетів. Відповідно, збільшується роль сегментації, контролю доступу до сервісів і аналізу мережевої поведінки на основі метаданих (контекст користувача, напрямки з’єднань, частота та об’єм сесій), а також кореляції мережевих подій із подіями на хостах і прикладних системах.

Проектні рекомендації щодо побудови кампусних мереж вказують на тенденцію до конвергованих архітектур, де на одній інфраструктурі співіснують дані, голос, відео, служби керування та гостьовий доступ. Для цього застосовується ієрархічна модель "доступ – розподіл – ядро", механізми віртуальних локальних мереж (VLAN), політики QoS для різних типів трафіку та резервування вузлів і лінків для забезпечення безперервності сервісів. Особливий акцент робиться на стандартизації шаблонів конфігурації, що дозволяє розгортати великі кампусні мережі з повторюваною структурою. [6]

У рекомендаціях з проектування мережевих сервісних архітектур для великих підприємств відзначається розвиток мультидоменних рішень, які об’єднують кампус, філії, дата-центри й WAN під єдиною політикою. Тут основними тенденціями є використання SD-WAN для гнучкого використання різних типів каналів зв’язку, інтеграція з хмарними дата-центрами та використання централізованих контролерів для керування маршрутизацією, сегментацією та безпекою. Такі архітектури дозволяють узгоджувати вимоги до продуктивності й захисту для різних сегментів мережі, не втрачаючи цілісності управління. [7]

Референс-архітектури для корпоративних WAN-мереж додатково підкреслюють перехід від суто MPLS-базованих рішень до гібридних моделей, де поєднуються MPLS, інтернет-канали та мобільний доступ із накладеними політиками шифрування й пріоритезації трафіку. Відповідні документи описують, як за допомогою політик на рівні додатків (application-aware routing) можна забезпечити кращу якість обслуговування для критичних сервісів, використовуючи при цьому більш доступні транспортні мережі для некритичного трафіку. У підсумку корпоративні мережі еволюціонують до гнучких, програмно керованих і економічно оптимізованих інфраструктур. [8]

Для мереж малого та середнього бізнесу окремою тенденцією є спрощення побудови корпоративної WAN за рахунок поєднання кількох транспортів (провідний Інтернет, резервний мобільний канал, інколи – MPLS) з політиками вибору траси на рівні застосунків. Такий підхід дозволяє підвищити доступність критичних сервісів (VPN у головний офіс, доступ до хмарних застосунків) без суттєвого зростання витрат, оскільки менш дорогі канали можуть використовуватися як резерв або для некритичного трафіку.

1.3 Класифікація корпоративних мереж та їх типові архітектури

Класичні підручники класифікують мережі за масштабом на локальні (LAN), міські/регіональні (MAN) та глобальні (WAN), що в корпоративному

контексті відповідає офісним/кампусним сегментам, міжбудинковим з’єднанням та міжрегіональним або міжнародним зв’язкам між філіями. Локальні мережі зазвичай будуються на основі Ethernet і забезпечують високу пропускну здатність та низькі затримки для користувачів і серверів у межах одного майданчика, тоді як WAN-мережі орієнтовані на забезпечення зв’язності між географічно рознесеними точками з урахуванням обмежень по пропускній здатності й вартості каналів. Така класифікація дозволяє розділити завдання внутрішньої комутації та магістральної маршрутизації на різні рівні проектування. [1]

Системний підхід пропонує додаткову класифікацію за функціональним призначенням: кампусні (офісні) мережі, мережі центрів обробки даних, мережі зберігання, мережі керування та моніторингу, а також сервісні та гостьові сегменти. Кампусна мережа зосереджується на підключенні користувачів і кінцевих пристроїв; дата-центрова – на взаємодії серверів, віртуальних машин і сховищ; мережі зберігання забезпечують гарантовану доставку даних між масивами й обчислювальними вузлами; мережі керування й моніторингу дозволяють ізолювати службовий трафік від користувацького. Такий поділ спрощує масштабування та спільне планування ресурсів для різних типів навантажень.

У рекомендаціях Cisco щодо побудови кампусних мереж виділяється ієрархічна архітектура з трьома основними рівнями: доступ, розподіл та ядро. На рівні доступу розміщуються комутатори й точки бездротового доступу, що підключають робочі станції й мобільних користувачів; рівень розподілу агрегує трафік, реалізує політики маршрутизації, фільтрації та QoS; на рівні ядра забезпечується високошвидкісна магістраль між основними сегментами мережі та вихід до WAN. Додатково виділяються зони DMZ, окремі серверні сегменти та сегменти віддаленого доступу, що дозволяє реалізувати багаторівневий підхід до безпеки та сегментації. [6]

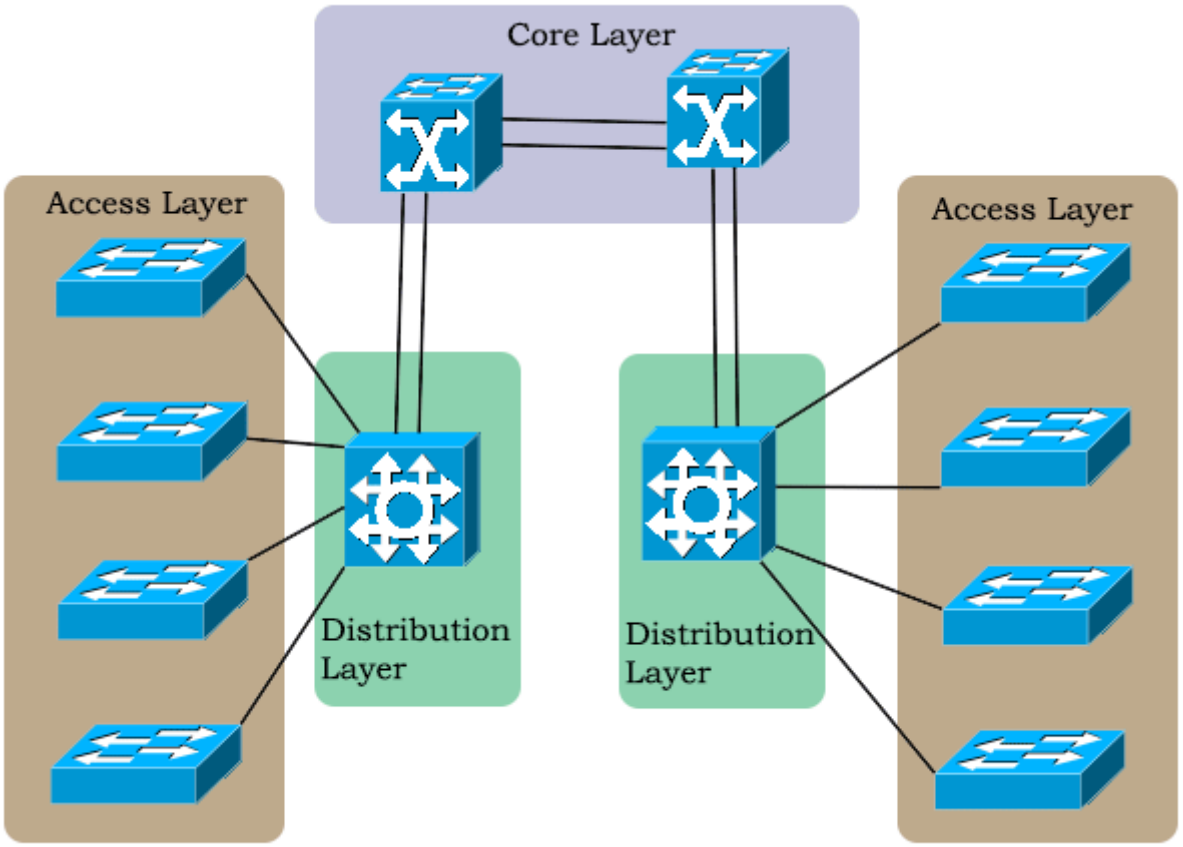

Рис. 1.2 Типова кампусна ієрархія: access – distribution – core

На практиці корпоративні кампусні мережі реалізуються не лише у "повній" трирівневій формі, а й у вигляді спрощених варіантів – наприклад, "collapsed core", де функції рівнів ядра та розподілу об’єднані в одну пару продуктивних комутаторів. Типове рішення для середнього офісу передбачає два комутатори агрегації з резервованими з’єднаннями до комутаторів доступу, динамічну маршрутизацію або статичні маршрути між сегментами, а також виділення окремих VLAN для користувачів, серверів, гостьового Wi-Fi і керування. Таке компонування спрощує масштабування (додавання нових комутаторів доступу) та підвищує відмовостійкість без надмірної складності конфігурації.

У книгах з проектування мережевих сервісних архітектур Cisco Press описується розвиток класичної трирівневої моделі в напрямку мультидоменних архітектур, які охоплюють кампус, філії, дата-центри, WAN та домен безпеки. Для таких архітектур характерне використання фабричних топологій у дата-центрах

(spine–leaf), overlay-технологій (наприклад, VXLAN) для віртуальної сегментації та SDN-контролерів для централізованого керування політиками маршрутизації й безпеки. Це дозволяє формувати єдині архітектурні шаблони для різних типів майданчиків, зменшуючи складність управління великою корпоративною мережею. [7]

Для мереж центрів обробки даних характерною є фабрична топологія spine–leaf, де кожен leaf-комутатор має рівноцінні підключення до всіх spine-комутаторів. За рахунок цього досягається передбачувана затримка та можливість паралельного використання кількох маршрутів (ECMP) для трафіку між серверами та сервісами. Поверх такої фізичної "underlay" мережі часто розгортається логічна "overlay" сегментація, яка дозволяє ізолювати середовища різних сервісів або клієнтів, не прив’язуючись жорстко до фізичної топології, і спрощує перенесення віртуальних машин та сервісів між вузлами.

Деякі розділи Cisco Press, що присвячені мережевій архітектурі та проектуванню, систематизують найкращі практики класифікації корпоративних мереж за доменами й ролями, описують патерни побудови мульти-доменниї інфраструктур та підкреслюють важливість єдиної моделі політик для різних сегментів мережі. Тут розглядаються архітектури, де кампус, WAN, дата-центр і хмарні ресурси реалізовані як частини єдиного логічного домену, в якому сегментація мережі, політики доступу та пріоритезації трафіку визначаються централізовано. Такий підхід спрощує інтеграцію нових майданчиків і сервісів у вже існуючу мережу. [9]

Референс-архітектури Juniper для корпоративних WAN описують типові топології "hub-and-spoke", частково сітчасті та повністю сітчасті (full-mesh) рішення, а також сценарії використання SD-WAN поверх цих топологій. У схемі "hub-and-spoke" центральний сайт (hub) забезпечує доступ до спільних сервісів і вихід до Інтернету, тоді як філії (spoke) підключаються до нього через один або кілька каналів; у full-mesh-конфігураціях між ключовими сайтами існують прямі з’єднання, що підвищує відмовостійкість і зменшує затримки. Документи

наголошують, що вибір конкретної топології залежить від вимог до доступності, затримок і вартості каналів. [8]

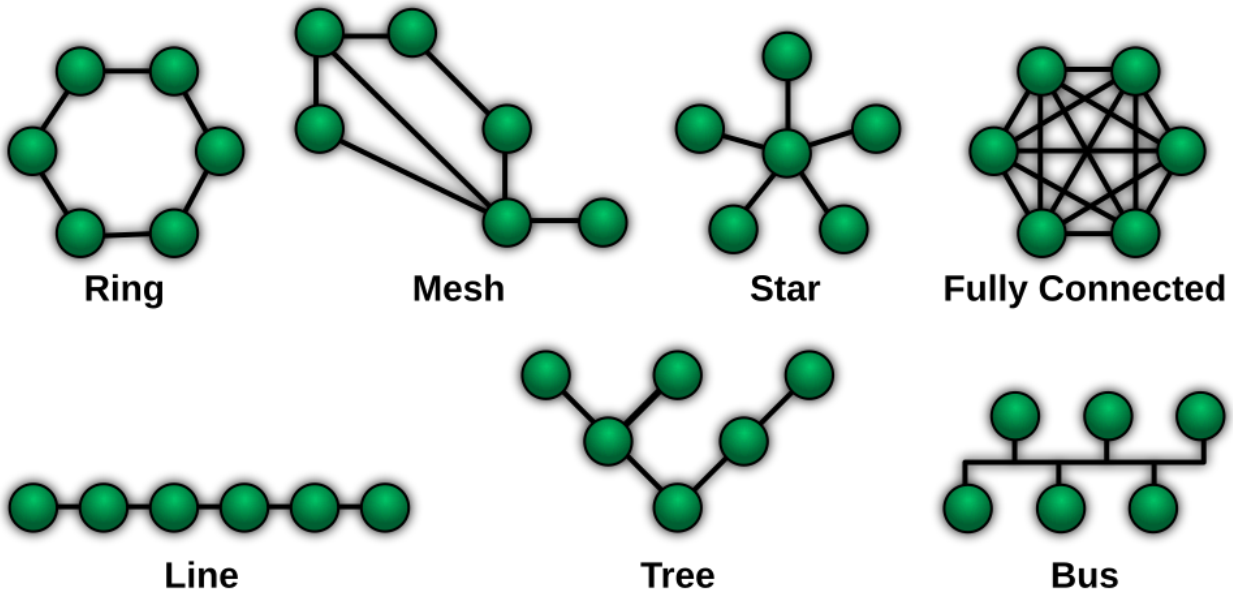

Рис. 1.3 Порівняння WAN-топологій

Доповненням до цих сценаріїв є розширені Enterprise WAN Reference Architecture, де описується інтеграція SD-WAN-фабрики, яка накладається поверх класичних топологій і забезпечує політично керований вибір транспортної мережі для різних класів трафіку. Центральні контролери аналізують стан каналів, характеристики додатків і визначені політики, після чого динамічно маршрутизують трафік між MPLS, широкосмуговим Інтернетом і мобільними мережами, водночас забезпечуючи наскрізне шифрування та контроль якості обслуговування. Це дозволяє класифікувати архітектури не лише за фізичною топологією, а й за характером логічного керування та рівнем автоматизації. [10]

У сценаріях SD-WAN поверх базових топологій формується накладена мережа тунелів між майданчиками, де рішення про вибір транспортного каналу приймається за політиками, що враховують тип застосунку, затримку, втрати та завантаження лінків. Це дозволяє розділяти трафік за класами і забезпечувати, наприклад, мінімальну затримку для голосу, стабільність для критичних бізнес-систем і використання більш доступних каналів для фонових передач даних. У поєднанні з наскрізним шифруванням і централізованим контролем це

формує окремий клас архітектур, де ключовими є не стільки фізичні з’єднання, скільки логічні політики й автоматизація керування.

1.4 Аналіз загроз інформаційній безпеці корпоративних мереж та особливості їх виявлення

Сучасні корпоративні мережі піддаються широкому спектру загроз, серед яких виділяють атаки типу відмови в обслуговуванні (DoS або DDoS), перехоплення та модифікацію трафіку (man-in-the-middle), сканування й експлуатацію вразливостей мережевих протоколів, несанкціонований доступ до внутрішніх ресурсів, розповсюдження шкідливого трафіку й здійснення складних багатоступеневих вторгнень. У фундаментальних оглядах мережевої безпеки ці загрози описуються через моделі атак, які включають етапи розвідки, експлуатації вразливостей, закріплення в системі та руху всередині мережі (переміщення всередині мережі), що дозволяє формувати відповідні стратегії виявлення й протидії. Особливу небезпеку становить той факт, що значна частина шкідливої активності може маскуватися під легітимний трафік або використовувати стандартні протоколи. [5]

До окремої групи загроз належать атаки на інфраструктурні механізми L2 та L3 рівнів, які можуть використовуватися для непомітного перехоплення трафіку або порушення доступності: підміна ARP-відповідей, нав’язування некоректних параметрів через підроблений DHCP, перевантаження таблиць MAC-адрес (MAC flooding), маніпуляції з протоколами резервування або спроби обходу сегментації. Для корпоративних мереж це особливо небезпечно, оскільки атакувальник, потрапивши в один сегмент (наприклад, гостьовий Wi-Fi), може намагатися вплинути на роботу шлюзів або отримати доступ до керівного контуру. Відповідно, захист має охоплювати не лише прикладні сервіси, а й мережеву інфраструктуру як об’єкт атак.

У працях, орієнтованих на корпоративні комп’ютерні мережі та їх безпеку, загрози розглядаються крізь призму бізнес-ризиків: вплив на конфіденційність,

цілісність і доступність інформаційних активів, а також на фінансові результати та репутацію організації. Тут наголошується важливість розмежування внутрішніх і зовнішніх загроз, випадкових помилок персоналу й навмисних дій зловмисників, а також необхідність розроблення політик безпеки, що враховують специфіку бізнес-процесів, регуляторні вимоги та прийнятний рівень ризику. На основі таких моделей будуються вимоги до сегментації мережі, контролю доступу, журналювання подій і використання багаторівневих засобів захисту. [4]

Моделювання загроз у корпоративній мережі варто проводити через виділення активів (критичні сервіси, облікові записи, дані клієнтів), меж довіри та шляхів доступу до них. На цій основі формуються зони безпеки (користувацька, серверна, гостьова, керівна), визначаються допустимі потоки між зонами та вибираються контрольні точки, де реалізуються фільтрація, автентифікація й журналювання. Такий підхід дозволяє обґрунтувати, чому саме сегментація VLAN/підмережами, правила міжсегментного доступу та централізовані журнали є не "додатковими", а базовими вимогами до корпоративної мережі навіть у невеликій організації.

Аналітичні звіти про сучасні кібератаки, зокрема кампанії типу ransomware, показують, що попри певне зменшення частки успішних виплат викупу останніми роками, активність таких атак залишається високою, а їхні сценарії стають дедалі складнішими. У публікаціях, які посилаються на дані Chainalysis, зазначається, що організації частіше відмовляються платити викуп завдяки кращій підготовці до інцидентів – резервному копіюванню, планам реагування та правовим обмеженням щодо взаємодії з кіберзлочинцями. Водночас зловмисники комбінують фішингові кампанії, експлуатацію вразливостей VPN-шлюзів та компрометацію внутрішніх облікових даних, щоб отримати глибокий доступ до корпоративної мережі перед шифруванням і викраденням даних. [11]

Особливість виявлення загроз у корпоративних мережах полягає в тому, що традиційні засоби захисту периметра, орієнтовані на просту фільтрацію за IP-адресами, портами та протоколами, вони вже не забезпечують достатнього

рівня виявлення загроз та дають достатньо функцій контролю. Своєю чергою сучасні концепції безпеки базуються на поєднанні класичних міжмережевих екранів із системами виявлення та запобігання вторгненням, які виконують глибоку інспекцію трафіку, аналіз поведінки та кореляцію подій із різних джерел.

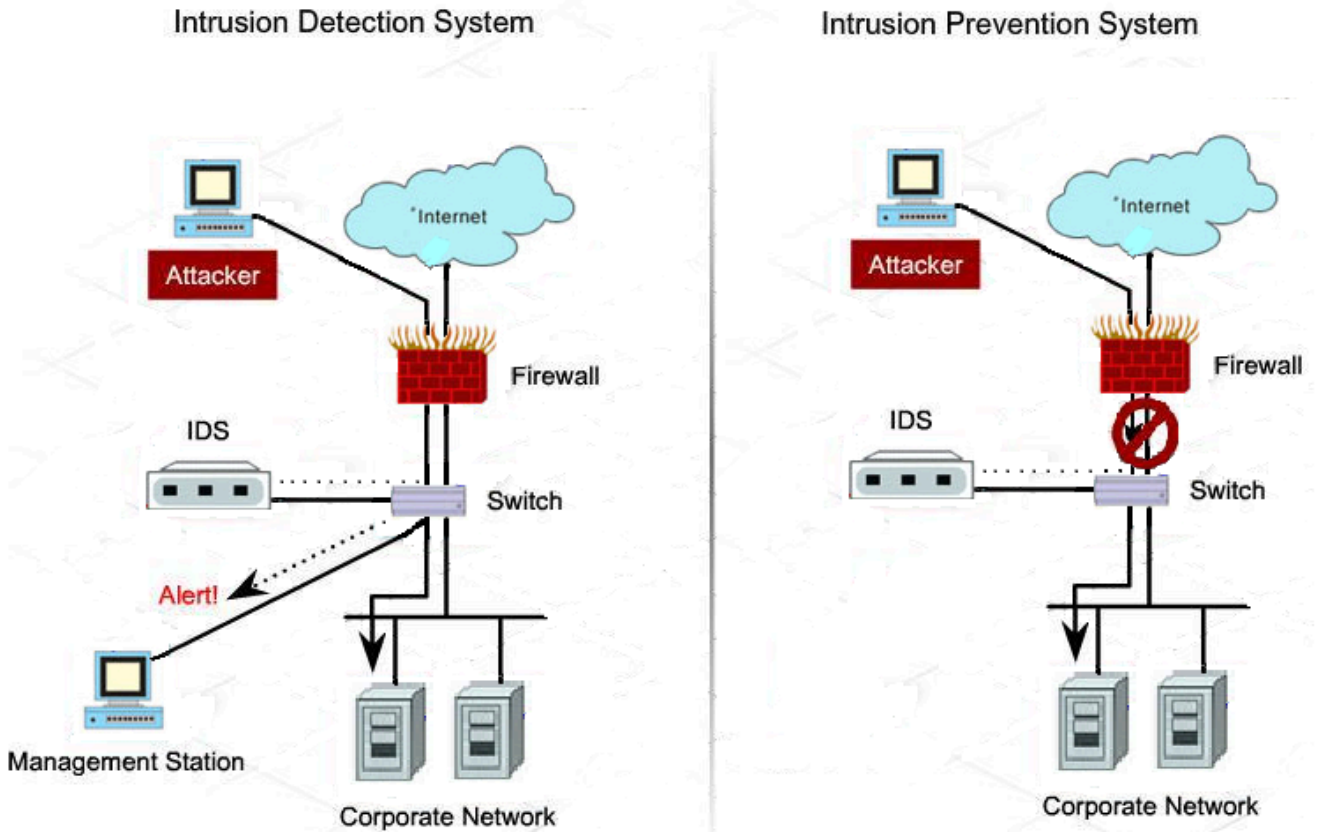

Рис. 1.4 Розміщення засобів контролю трафіку

Ефективне виявлення інцидентів у корпоративній мережі спирається на багатоджерельну телеметрію: журнали фаєрвола та VPN, події маршрутизації, системні логи серверів, а також мережеві події рівня IDS/IPS. Для коректної кореляції подій критичною є синхронізація часу (NTP), уніфікований формат логів та визначені процедури зберігання й ретенції. У технічному сенсі саме наявність структурованих подій (наприклад, у форматі JSON) забезпечує можливість автоматизованого аналізу, побудови правил реагування й подальшої інтеграції з системами управління подіями безпеки.

1.5 Основні етапи побудови мереж малого або середнього підприємства

Побудову будь-якої мережі варто розглядати як послідовність етапів: спочатку визначається фізична структура приміщення та кабельної інфраструктури, далі проектуються логічні сегменти мережі на рівні комутаторів і маршрутизатора, налаштовуються базові сервіси та механізми доступу до зовнішніх ресурсів, після чого формуються політики безпеки, бездротовий доступ і система моніторингу. Такий покроковий підхід дозволяє не пропустити критичні аспекти й забезпечити узгодженість між апаратною частиною, логічною архітектурою й вимогами бізнесу.

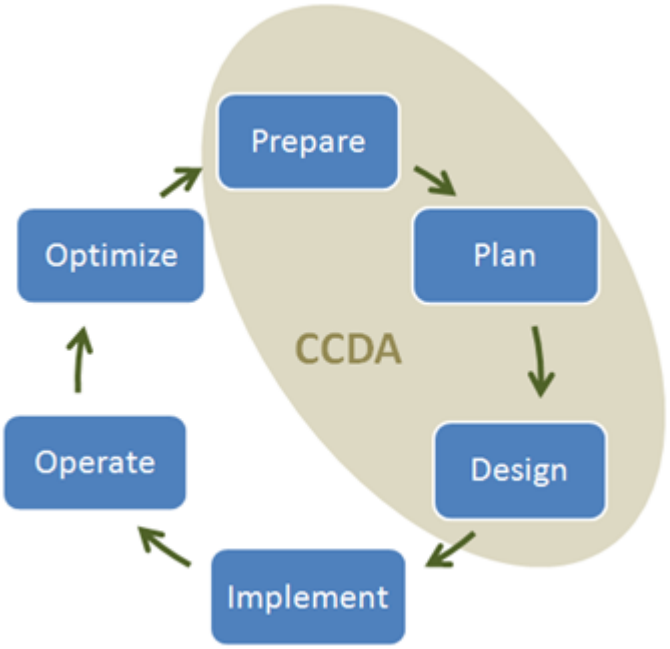

Рис. 1.5 Блок-схема етапів побудови SMB-мережі

Першим кроком варто сформувати технічні вимоги та сценарії використання: кількість робочих місць і типи пристроїв, потреба в гостьовому доступі, наявність касових терміналів або віддалених сервісів, вимоги до відеоспостереження, а також очікуваний ріст мережі на горизонті 1–3 років. На цьому етапі визначаються мінімально прийнятні показники доступності, пропускної здатності та затримки, а також обирається схема підключення до провайдера (основний і резервний канал), що безпосередньо впливає на архітектуру маршрутизації та політики безпеки.

На фізичному рівні проектування починається з аналізу планування приміщення: місця розташування робочих місць, касових терміналів, серверного

вузла, зон для Wi-Fi-доступу, IP-камер чи спеціалізованого обладнання. Класичні підручники рекомендують використовувати структуровану кабельну систему зі зіркоподібною топологією, коли всі робочі розетки зводяться до комутаційної шафи з патч-панеллю та комутатором, а кабелі виконуються на основі витої пари тому категорії або, за потреби, оптичного волокна для магістральних ліній. Це спрощує облік і обслуговування, а також забезпечує можливість подальшого масштабування без кардинальної перебудови всієї фізичної інфраструктури. [1]

Окремо слід врахувати живлення та фізичну безпеку мережевого вузла: застосування UPS для маршрутизатора й комутаторів, можливість подачі PoE для точок доступу та IP-камер, резервування блока живлення (за наявності), а також контроль доступу до комутаційної шафи. Практика показує, що маркування кабелів і портів, ведення схеми підключень і виділення місця під розширення (додаткові патч-панелі, запасні порти) суттєво знижують час відновлення при інцидентах і спрощують подальше обслуговування.

На канальному рівні для невеликого об’єкта, такого як аптека чи відділення пошти, зазвичай достатньо одного або кількох комутаторів рівня доступу, але навіть у цьому випадку варто одразу закладати логічну сегментацію. Підхід "згори донизу" передбачає, що мережа спочатку розбивається на окремі групи пристроїв і сервісів: касові термінали, робочі місця персоналу, гостьовий Wi-Fi, IP-камери, сервери, а потім кожній групі відповідає власна VLAN. Комутатори налаштовуються таким чином, щоб порти, до яких підключені кінцеві пристрої, були портами доступу для відповідних VLAN, а транкові порти використовувались для зв’язку з маршрутизатором або іншим комутатором, що забезпечує транспортування кількох віртуальних мереж одним фізичним лінком. [2]

Під час формування VLAN варто виходити з принципу мінімізації перетинів між різними типами трафіку та різними рівнями довіри. З технічної точки зору це означає: визначення транкових лінків між комутатором і маршрутизатором (або L3-комутатором), налаштування фільтрації VLAN на мостах/комутаторах, а також вибір точки маршрутизації між VLAN (частіше на

шлюзі). При цьому важливо одразу закласти механізми захисту L2-рівня: контроль широкомовних штормів, обмеження невідомих MAC-адрес, відключення невикористаних портів і фіксацію дозволених VLAN на транках.

Для типового об’єкта малого або середнього бізнесу практичними є такі сегменти:

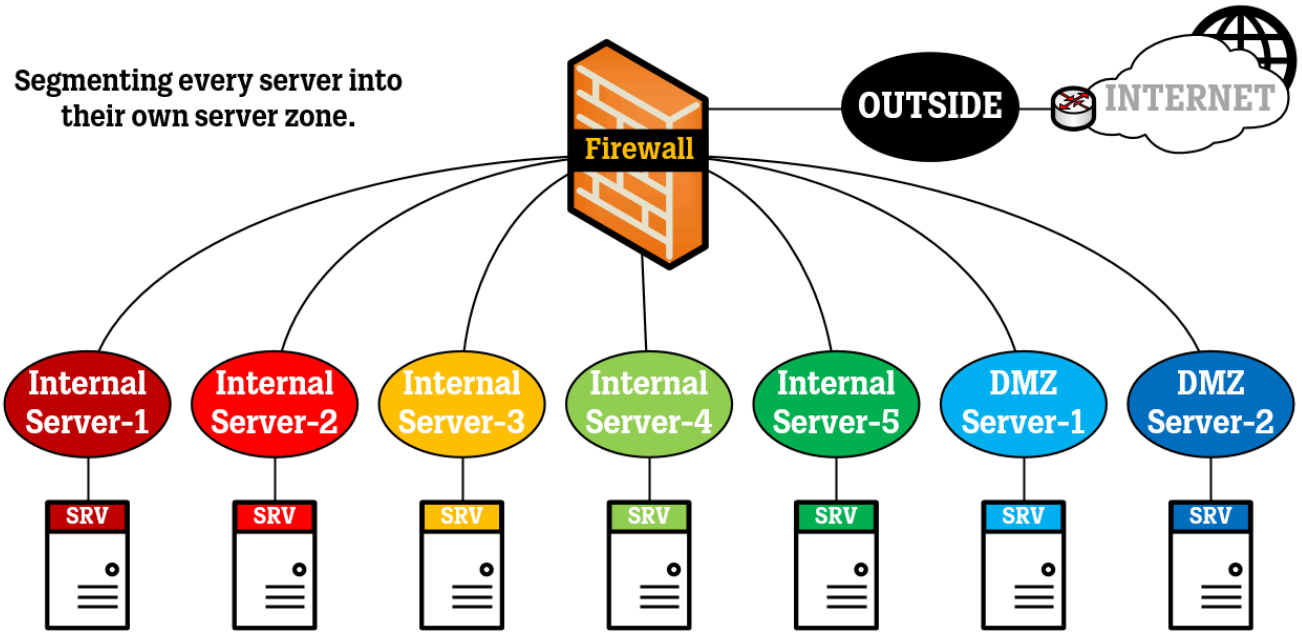

Рис. 1.6 Приклад сегментації

– офісні робочі місця персоналу (корпоративний доступ)
– касові термінали/платіжна інфраструктура (підвищений рівень ізоляції)
– гостьовий Wi-Fi (ізоляція клієнтів і обмеження доступу лише в Інтернет)
– відеоспостереження та IoT (обмеження доступу до керівних інтерфейсів)
– керування обладнанням (адміністративний сегмент для доступу до інтерфейсів керування)

На мережевому рівні проектуються підмережі й IP-адресація для кожної VLAN, визначається роль маршрутизатора як шлюзу за замовчуванням для внутрішніх сегментів і як вузла виходу в Інтернет або корпоративну WAN. Системний підхід до побудови мережі підкреслює необхідність чіткого планування діапазонів адрес, масок підмереж і маршрутів між сегментами, щоб у подальшому було легко додавати нові підсистеми (наприклад, окремий сегмент для відеоспостереження або службового адміністрування) без конфліктів. Для

малих об’єктів, як правило, достатньо статичної маршрутизації, однак у випадку підключення філії до головного офісу можуть застосовуватися протоколи динамічної маршрутизації та тунельні технології для побудови захищених міжмайданчикових з’єднань. [3]

План адресації має бути узгоджений із сегментацією: для кожного VLAN визначається підмережа, шлюз, пул DHCP і правила доступу. З практичного погляду варто резервувати окремі діапазони під статичні адреси серверів, мережевих пристроїв і систем моніторингу, а також застосовувати узагальнення маршрутів (summarization) для спрощення керування, якщо в майбутньому планується додавання філій. Для міжмайданчикових з’єднань (офіс–склад–філія) слід передбачати VPN-тунелі та маршрутизацію між підмережами, щоб забезпечити контрольований доступ до сервісів без відкриття внутрішньої адресації в Інтернет.

Практичні рекомендації щодо побудови кампусних і філійних мереж пропонують розглядати невелике відділення як спрощений варіант кампусної архітектури з одним рівнем доступу й "урізаним" рівнем розподілу. Комутатор доступу обслуговує всі локальні VLAN, тоді як маршрутизатор або багатофункціональний маршрутизатор-комутатор виконує роль точки маршрутизації між ними, шлюзу в Інтернет і, за потреби, вузла підключення до корпоративної WAN. У такій схемі важливо відразу відокремити касові термінали, робочі місця персоналу, гостьових користувачів та обладнання відеоспостереження, щоб у разі інциденту в одному сегменті мінімізувати вплив на інші частини мережі. [6]

Навіть у невеликій мережі варто передбачати мінімальний рівень резервування та керування трафіком: резервний інтернет-канал (наприклад, LTE/5G як backup), автоматичне перемикання за ознакою доступності (monitoring of gateway), а також пріоритезацію трафіку критичних сервісів (термінали, VPN у головний офіс, VoIP). Технічно це реалізується через політики маршрутизації та QoS на шлюзі, профілі для різних класів трафіку та контроль завантаження каналу, що дозволяє зменшити вплив "важких" потоків на роботу критичних сервісів.

З погляду безпеки корпоративні мережі навіть у невеликих організаціях мають розглядатися як носій бізнес-ризиків, оскільки збій або компрометація інформаційних сервісів може призвести до фінансових втрат або порушення регуляторних вимог. При побудові мережі малого/середнього підприємства варто вже на ранньому етапі визначити сегменти різного рівня довіри (касова система, внутрішні робочі місця, гостьовий доступ), ввести мінімально необхідні правила фільтрації на межах між ними та на периметрі, а також забезпечити базове журналювання подій на маршрутизаторі та ключових сервісах. Особливої уваги потребують вузли, які обробляють платіжні дані, персональні дані клієнтів чи медичну інформацію, якщо йдеться, наприклад, про медичний заклад. [4]

Важливою вимогою для малого та середнього бізнесу є безпечний віддалений доступ для адміністратора та, за потреби, для інтеграції з головним офісом. Рекомендованим підходом є використання VPN з чітко визначеними підмережами та правилами доступу, обмеження керівних інтерфейсів лише з адміністративного сегмента, а також застосування журналювання для всіх керівних дій. Окремо варто передбачити резервне копіювання конфігурацій обладнання та контроль змін (хто, коли і що змінював), щоб у випадку інциденту або помилки можна було швидко відновити працездатність.

Сучасні аналітичні звіти щодо кібератак нагадують, що навіть невеликі підприємства є цілями для шкідливих кампаній, зокрема атак типу ransomware, які поєднують шифрування даних з їх викраденням та вимаганням викупу. Статистика показує, що успішність таких атак багато в чому залежить від відсутності базових засобів захисту, сегментації та планів реагування, а не лише від розміру організації. Це означає, що при проектуванні мережі для невеликого відділення пошти або комп’ютерного клубу важливо передбачити механізми, які ускладнюють поширення атаки в мережі, дозволяють локалізувати інцидент у межах одного сегмента й відновити роботу сервісів без тривалого простою. [11]

З урахуванням сучасних сценаріїв ransomware варто планувати мережу так, щоб компрометація одного робочого місця не призводила до зупинки всієї організації. Практично це означає: мінімізацію доступів між сегментами,

розділення сервісів зберігання даних і робочих станцій, а також наявність резервних копій, ізольованих від основної доменної інфраструктури. У контексті мережевого проектування важливо також передбачити контроль вихідних з’єднань, оскільки зловмисники часто використовують канали керування та ексфільтрації даних перед шифруванням.

Завершальним етапом побудови мережі є підготовка до експлуатації: налаштування моніторингу доступності (ICMP/SNMP), централізованого збору логів (syslog), перевірка коректності часу на всіх вузлах, а також проведення приймальних тестів – перевірка доступу між сегментами, роботи VPN, правил фаєрвола та швидкості доступу до критичних сервісів. Документування схеми VLAN/адресації, списку обладнання, резервних каналів і процедур відновлення (backup/restore) підвищує керованість та істотно зменшує ризики простою при подальших змінах або інцидентах.

Узагальнюючи, процес побудови мережі для малого та середнього бізнесу можна розглядати як адаптацію загальних принципів проектування корпоративних мереж до обмеженого масштабу: обережне планування фізичної інфраструктури, логічна сегментація на рівні VLAN та підмереж, чітко визначені шлюзи й маршрути, базові політики безпеки на периметрі та між сегментами, а також мінімально необхідні засоби моніторингу й журналювання. Подальші розділи роботи детально розкриють, як ці етапи реалізуються на практиці із використанням обладнання MikroTik та програмного комплексу Suricata.

РОЗДІЛ 2 МЕТОДОЛОГІЯ ПОБУДОВИ КОРПОРАТИВНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ОБЛАДНАННЯ MIKROTIK ТА IDS/IPS SURICATA

2.1 Порівняльний аналіз мережевого обладнання для мереж малого та середнього бізнесу

Для побудови корпоративних мереж малих і середніх підприємств важливо поєднати достатню функціональність рівня L3/L4 (маршрутизація, VLAN, VPN, фаєрвол, QoS) з прийнятною вартістю та простотою адміністрування. У цьому сегменті присутні різні виробники SOHO/SMB-обладнання, але лінійка MikroTik приваблює тим, що навіть базові моделі оснащуються операційною системою RouterOS з широким набором функцій, які зазвичай доступні лише на дорожчих рішеннях інших провідних виробників.

У межах роботи доцільно зосередитися на чотирьох представниках лінійки MikroTik, які покривають типові сценарії для малого та середнього бізнесу: бюджетний Wi-Fi-маршрутизатор hAP lite (RB941-2nD), більш гнучкий RB2011UiAS-2HnD-IN, компактні точки доступу wAP ac (RBwAPG-5HacT2HnD) та cAP lite (RBcAPL-2nD), а також потужний маршрутизатор RB4011iGS+5HacQ2HnD-IN для середніх підприємств.

Порівняння бюджетних та продуктивних рішень різних виробників мережевого обладнання показує, що обладнання MikroTik забезпечує суттєво кращий баланс між функціональністю мережевого рівня та вартістю, особливо у сегменті малого та середнього бізнесу. У таблицях додатку А проведено зіставлення представників лінійки MikroTik з аналогами компаній TP-Link, Cisco та Ubiquiti, причому для порівняння взято саме моделі, що реально використовуються в SOHO/SMB-сегменті, а не тільки теоретично близькі за параметрами рішення. Це дозволяє оцінити не лише технічні характеристики, а й практичну доцільність вибору платформи для побудови корпоративної мережі.

Порівняння бюджетного маршрутизатора hAP lite (RB941-2nD) з типовим недорогим Wi-Fi-маршрутизатором TP-Link TL-WR841N демонструє ключову ідеологічну перевагу MikroTik: за близької апаратної платформи (одноядерний процесор і 32 МБ ОЗП) пристрій MikroTik працює під керуванням RouterOS із повноцінною підтримкою VLAN, тунельних протоколів та динамічної маршрутизації, тоді як аналогічне рішення TP-Link орієнтоване насамперед на домашнє використання і має істотно обмежений набір мережевих функцій. При цьому різниця у вартості між моделями є порівняно невеликою, що робить hAP lite більш доцільним вибором для офісу чи відділення, де потрібні VPN, сегментація та керований фаєрвол, а не лише базовий вихід до Інтернету (табл. А.1).

На рівні філійних маршрутизаторів, де важливими є кількість фізичних портів, підтримка оптичних інтерфейсів та гнучкість сценаріїв резервування каналів, порівняння RB2011UiAS-2HnD-IN із Cisco RV260W також схиляє вибір на користь MikroTik. RB2011 пропонує більше фізичних портів (комбінація Fast Ethernet, Gigabit Ethernet і окремий SFP-слот), підтримку живлення інших пристроїв через PoE out та значно ширші можливості налаштування завдяки RouterOS (скрипти, Netwatch, черги, гнучкі політики маршрутизації). Cisco RV260W має сучасніший радіомодуль Wi-Fi, однак істотно дорожчий, тоді як RB2011 залишається у кілька разів дешевшим при вищій гнучкості для побудови складніших схем підключення філій (табл. А.2). Для задач, де бездротова частина може бути винесена на окремі точки доступу, техніко-економічна перевага маршрутизатора MikroTik є очевидною.

У сегменті продуктивних маршрутизаторів для ядра мережі або центральних вузлів порівнюються RB4011iGS+5HacQ2HnD-IN та Ubiquiti UniFi Dream Machine Pro. Обидва пристрої розраховані на гігабітні та 10-гігабітні швидкості й велику кількість клієнтів, однак RB4011 поєднує потужний процесор, порт SFP+ 10 Гбіт/с, десять гігабітних портів та вбудований дводіапазонний Wi-Fi із 4×4 MIMO у діапазоні 5 ГГц. UDM-Pro, навпаки, не має вбудованого радіомодуля і передбачає використання окремих точок доступу, а разом із цим є

суттєво дорожчим. При цьому MikroTik покладається на інтеграцію з зовнішніми системами типу Suricata для IDS/IPS, що узгоджується з архітектурою цієї роботи, тоді як вбудований механізм загроз у UDM-Pro є менш гнучким з точки зору налаштувань та інтеграції (табл. А.3).

Аналіз точок доступу wAP ac та cAP lite у порівнянні з Ubiquiti UniFi AC Lite підтверджує, що MikroTik здатен закривати різні сценарії покриття бездротової мережі, зберігаючи економічну доцільність. Ubiquiti UniFi AC Lite є еталонним рішенням для офісного сегменту, однак вимагає окремого програмного або апаратного контролера. У випадку MikroTik роль контролера бере на себе CAPsMAN, інтегрований у будь-який маршрутизатор з RouterOS, без додаткових витрат на окремий пристрій керування. Модель wAP ac завдяки всепогодному корпусу дозволяє організувати покриття на фасаді будівлі або зовні приміщення, тоді як cAP lite виступає бюджетною внутрішньою точкою доступу для "сліпих зон" у приміщенні. При цьому сумарна вартість вирішення задачі покриття офісу або невеликого об’єкта за рахунок комбінації wAP ac і cAP lite є нижчою, ніж використання лише UniFi-точок (табл. А.4).

Таким чином, результати порівняння демонструють, що техніко-економічна ефективність використання обладнання MikroTik полягає у поєднанні: повнофункціональної мережевої операційної системи RouterOS на всіх класах пристроїв, широких можливостей налаштування й автоматизації, наявності моделей для різних сценаріїв (від мікробізнесу до центральних вузлів) та помітно нижчої вартості в порівнянних класах обладнання інших виробників. Це обґрунтовує вибір MikroTik як базової платформи для побудови корпоративної мережі в даній роботі та забезпечує одночасно технічну гнучкість і економічну доцільність. Базова модель hAP lite орієнтована на малі офіси, відділення чи філії з кількома робочими місцями. Пристрій має одноядерний процесор із частотою 650 МГц, 32 МБ ОЗП, чотири порти Fast Ethernet 10/100 Мбіт/с та дволанцюговий бездротовий інтерфейс 2,4 ГГц 802.11b/g/n з максимальною швидкістю до 300 Мбіт/с, працює під керуванням RouterOS з ліцензією рівня 4. Така конфігурація

робить hAP lite доречною точкою входу для невеликих мереж із базовими вимогами до продуктивності, але з потребою в повноцінному маршрутизаторі з фаєрволом і підтримкою VPN.

Маршрутизатор RB2011UiAS-2HnD-IN належить до вищого класу й позиціонується як універсальне рішення для філій або невеликих офісів, де одночасно потрібні дротові підключення, бездротовий доступ і можливість роботи з оптичними лінками. Пристрій оснащено процесором Atheros AR9344 із частотою 600 МГц, 128 МБ ОЗП, п’ятьма портами Fast Ethernet, п’ятьма портами Gigabit Ethernet та слотом SFP, а також дволанцюговою точкою доступу 2,4 ГГц 802.11b/g/n з підтримкою технології MIMO 2×2 та ліцензією RouterOS рівня 5. Додатково підтримується пасивне PoE-живлення на першому порту та PoE-вихід на десятому порту, що дозволяє живити інші пристрої без окремого блока живлення. Це рішення вже підходить для невеликих центрів обробки даних підприємства чи головних офісів з виділенням VLAN та маршрутизацією між сегментами.

Окремим класом є точки доступу wAP ac та cAP lite, які доцільно використовувати як складові Wi-Fi-інфраструктури поверх наявної дротової мережі. Модель wAP ac (RBwAPG-5HacT2HnD) побудована на процесорі QCA9556 з частотою 720 МГц і 64 МБ ОЗП, має один порт Gigabit Ethernet та підтримує одночасну роботу в діапазонах 2,4 ГГц (802.11b/g/n, до 300 Мбіт/с) і 5 ГГц (802.11a/n/ac, до 1300 Мбіт/с), при цьому корпус має ступінь захисту IP54 і розрахований на встановлення зовні будівлі. Точка доступу cAP lite (RBcAPL-2nD), навпаки, оптимізована для внутрішніх приміщень: вона оснащена процесором AR9533 650 МГц, 64 МБ ОЗП, одним портом Fast Ethernet 10/100 Мбіт/с та дволанцюговим інтерфейсом 2,4 ГГц 802.11b/g/n із максимальною сукупною швидкістю до 300 Мбіт/с, живиться через PoE та підтримує централізоване керування CAPsMAN.

Для мереж середнього бізнесу, де кількість користувачів може сягати сотні та існують вимоги до агрегації великої кількості гігабітних лінків, актуальним стає клас маршрутизаторів на кшталт RB4011iGS+5HacQ2HnD-IN. Пристрій використовує чотириядерний процесор AL21400 Cortex-A15 із частотою 1,4 ГГц, має 1 ГБ ОЗП, десять портів Gigabit Ethernet, один SFP+ із підтримкою швидкості до 10 Гбіт/с, дводіапазонну Wi-Fi-частину (2,4 ГГц 2×2 802.11b/g/n до 300 Мбіт/с і 5 ГГц 4×4 802.11a/n/ac до 1733 Мбіт/с) та RouterOS з ліцензією рівня 5. Наявність апаратного прискорення IPsec і PoE-виходу на десятому порту робить його доцільним вибором для побудови центрального вузла мережі або для офісів із високими вимогами до пропускної здатності та захищених VPN-каналів.

Підсумовуючи проведений порівняльний аналіз, можна зазначити, що всередині лінійки MikroTik є як надбюджетні рішення для простих філій, так і потужні маршрутизатори для середніх підприємств. Це дозволяє спроектувати корпоративну мережу з урахуванням техніко-економічної ефективності: використовувати найдешевші пристрої там, де цього достатньо за функціональністю, і поступово переходити до більш продуктивних моделей у вузлах, які потребують масштабування, не змінюючи при цьому платформу керування (RouterOS) та підхід до конфігурації.

Таблиця 2.1

Порівняння базових маршрутизаторів MikroTik

Параметр	**hAP lite (RB941-2nD)**	**RB2011UiAS-2HnD-IN**	**Коментар**
Клас пристрою	Бюджетний SOHO/малий офісний маршрутизатор з Wi-Fi	Маршрутизатор для філій/малих офісів з розширеною комутацією	RB2011 закриває потреби складніших сценаріїв
CPU	1 × 650 МГц	1 × 600 МГц Atheros 74K MIPS	Обчислювальна потужність вища у RB2011 за рахунок більшої ОЗП та додаткових інтерфейсів
Оперативна пам’ять	32 МБ	128 МБ	Важливо для кількості сесій, тунелів, правил фаєрвола
RouterOS ліцензія	Level 4	Level 5	L5 забезпечує розширені можливості для VPN та маршрутизації

Продовження таблиці 2.1

Ethernet-порти	4 × 10/100 Мбіт/с	5 × 10/100 Мбіт/с + 5 × 10/100/1000 Мбіт/с	RB2011 дозволяє розділяти доступ на Fast/Gigabit сегменти
SFP	Немає	1 × SFP (1 Гбіт/с)	Під’єднання до оптичних магістралей
Wi-Fi	2,4 ГГц 802.11b/g/n, до 300 Мбіт/с	2,4 ГГц 802.11b/g/n, MIMO 2×2, до 300 Мбіт/с	RB2011 підтримує технологію MIMO
PoE in / PoE out	Переважно живлення від адаптера, без PoE-виходу	Пасивне PoE-живлення на Ether1, пасивний PoE-вихід на Ether10	Дозволяє живити інші пристрої без окремого БЖ
Типові сценарії	Невеликий офіс, відділення з 3–5 робочими місцями, базовий VPN	Філія з декількома VLAN, під’єднанням камер, Wi-Fi-точок, оптики	RB2011 доречний як головний маршрутизатор філії

Таблиця 2.2

Порівняння точок доступу MikroTik для малого/середнього бізнесу

Параметр	**wAP ac (RBwAPG-5HacT2HnD)**	**cAP lite (RBcAPL-2nD)**	**Коментар**
Клас пристрою	Зовнішня дводіапазонна точка доступу (outdoor)	Внутрішня точка доступу для стелі/стіни (indoor)	Разні сценарії встановлення
CPU	1 × 720 МГц (QCA9556)	1 × 650 МГц (AR9533)	Обидві моделі достатні для ролі AP
Оперативна пам’ять	64 МБ	64 МБ	Для CAPsMAN/невеликих конфігурацій цього достатньо
Ethernet-порти	1 × Gigabit Ethernet	1 × Fast Ethernet 10/100 Мбіт/с	Gigabit-порт wAP ac краще підходить для високих швидкостей uplink

Продовження таблиці 2.2

Wi-Fi діапазони	2,4 ГГц 802.11b/g/n (до 300 Мбіт/с) + 5 ГГц 802.11a/n/ac (до 1300 Мбіт/с)	2,4 ГГц 802.11b/g/n, до 300 Мбіт/с	wAP ac забезпечує значно більшу пропускну здатність і підтримку 5 ГГц
Антени/корпус	Вбудовані антени, всепогодний корпус, IP54	Вбудована 2,4-ГГц антена, компактний пластиковий корпус	wAP ac підходить для вулиці, cAP lite – для інтер'єру
RouterOS ліцензія	Level 4	Level 4	Обидві моделі можна інтегрувати в централізовану систему CAPsMAN
Живлення	PoE in 802.3af/at, 11–57 В	PoE in 802.3af/at або DC, 5–60 В	Обидві легко живити по звитій парі
Типові сценарії	Вуличне покриття біля офісу, майданчик, зовнішні камери, гостьова мережа	Готельні номери, офісні open-space, торгові зали	Часто використовуються в одній мережі, з центральним контролером

Таблиця 2.3

Порівняння RB2011UiAS-2HnD-IN та RB4011iGS+5HacQ2HnD-IN

Параметр	**RB2011UiAS-2HnD-IN**	**RB4011iGS+5HacQ2HnD-IN**	**Коментар**
Клас пристрою	Маршрутизатор для малих офісів/філій	Потужний маршрутизатор для середнього бізнесу, центральних вузлів	RB4011 – наступний клас за продуктивністю
CPU	1 × 600 МГц Atheros 74K MIPS	4 × 1,4 ГГц AL21400 Cortex-A15	Чотириядерний CPU RB4011 суттєво підвищує пропускну здатність і можливості IPsec
Оперативна пам’ять	128 МБ	1 ГБ	Важливо для великої кількості з’єднань, VPN-тунелів, складних правил
Порти Ethernet	5 × Fast Ethernet + 5 × Gigabit Ethernet	10 × Gigabit Ethernet	RB4011 оптимізований для агрегації багатьох гігабітних лінків

Продовження таблиці 2.3

SFP / SFP+	1 × SFP (1 Гбіт/с)	1 × SFP+ (10 Гбіт/с)	RB4011 дозволяє підключення до 10-гігабітних магістралей
Wi-Fi	2,4 ГГц 802.11b/g/n, 2×2 MIMO, до 300 Мбіт/с	2,4 ГГц 2×2 802.11b/g/n до 300 Мбіт/с + 5 ГГц 4×4 802.11a/n/ac до 1733 Мбіт/с	RB4011 має значно вищу бездротову продуктивність у діапазоні 5 ГГц
RouterOS ліцензія	Level 5	Level 5	Розширені можливості маршрутизації та VPN
PoE in / PoE out	Пасивне PoE in (Порт №1), пасивний PoE out (Порт №10)	Пасивне PoE in (Порт №1), пасивний PoE out (Порт №10)	Обидва можуть живити підключене обладнання по останньому порту
Орієнтовний масштаб мережі	Малі офіси, філії до кількох десятків користувачів	Офіси й вузли з до ~200 користувачів, центральні маршрутизатори, VPN-шлюзи	RB4011 доречний як ядро мережі малого/середнього підприємства

У сегменті бюджетних керованих комутаторів для SMB логічно порівнювати MikroTik CSS326-24G-2S+RM та TP-Link TL-SG3428, оскільки обидві моделі вирішують типові задачі рівня доступу/агрегації (сегментація VLAN, контроль L2-трафіку, дзеркалювання для діагностики), але мають різний підхід до адміністрування і різний запас для побудови магістралей. CSS326 працює під керуванням SwOS – це спеціалізована ОС для комутаторів MikroTik, орієнтована на web-конфігурацію і базові функції керованої L2-комунікації (VLAN, port-to-port forwarding, ACL/фільтрація за MAC/IP/портами, storm control, mirroring, обмеження пропускної здатності). Важливо, що SwOS не передбачає керування через CLI чи API, тому модель більше підходить для сценаріїв, де достатньо веб-інтерфейсу та не планується важка інтеграція з централізованими системами керування.

TP-Link TL-SG3428 належить до лінійки JetStream/Omada і позиціонується виробником як L2+ керований комутатор із 4 SFP-слотами, який може інтегруватися в Omada SDN для централізованого віддаленого керування. Для експлуатації в мережах підприємств це корисно тим, що TL-SG3428 підтримує не лише web-інтерфейс, а й CLI, а також стандартизовані механізми моніторингу та інтеграції з NMS – SNMP (v1/v2c/v3) і RMON. Тобто, якщо в мережі вже використовується централізований моніторинг або потрібне керування через уніфіковані протоколи, TL-SG3428 зазвичай буде зручнішим в обслуговуванні.

Ключова апаратна відмінність між моделями – аплінки. MikroTik CSS326 має 24×1GbE RJ45 та 2×SFP+, причому SFP-клітка підтримує модулі 1.25Gb SFP і 10Gb SFP+, що дозволяє будувати 10-гігабітні магістральні підключення до маршрутизатора/ядра або до комутатора агрегації навіть у бюджетному сегменті. Натомість TP-Link TL-SG3428 має 24×1GbE RJ45 та 4×SFP (1GbE): оптичних портів більше за кількістю, але без 10GbE у межах цієї моделі, тому пропускна здатність магістралей буде обмежена рівнем 1GbE. На практиці це означає, що CSS326 доцільніше використовувати там, де важливий запас під майбутнє (наприклад, серверна/відеоспостереження/агрегація трафіку з кількох комутаторів

доступу), а TL-SG3428 – коли пріоритетом є централізоване керування, типове для інфраструктур Omada, і достатньо 1GbE-аплінків.

З техніко-економічного погляду обидва рішення залишаються в близькому ціновому діапазоні, однак CSS326 часто виглядає привабливішим, коли потрібні 10GbE аплінки за мінімальну вартість, а TL-SG3428 – коли важлива зручність експлуатації через стандартні засоби керування і централізація (Omada SDN) навіть при 1GbE-магістралях.

2.2 Засоби маршрутизації, сегментації та фільтрації трафіку в MikroTik (VLAN, VPN, Firewall, NAT)

Однією з ключових передумов побудови захищеної корпоративної мережі є правильна маршрутизація та сегментація трафіку. MikroTik підтримує створення віртуальних локальних мереж на базі стандарту IEEE 802.1Q, роботу з trunk- та access-портами, а також VLAN-фільтрацію в програмному мосту. Це дає змогу логічно відокремлювати користувацькі, серверні, гостьові й службові сегменти, обмежуючи взаємодію між ними за допомогою чітко регламентованих політик доступу.

Функція Firewall у RouterOS реалізує станову фільтрацію з розподілом правил на ланцюги обробки вхідного, вихідного й транзитного трафіку, а також містить засоби маркування пакетів і з’єднань. У поєднанні з механізмами NAT це дозволяє організувати трансляцію адрес, приховати внутрішню структуру мережі та мінімізувати поверхню атаки. Підтримка різних типів VPN-тунелів забезпечує захищений доступ віддалених користувачів і філій до ресурсів підприємства, а журнали подій створюють основу для подальшого аналізу інцидентів і взаємодії з системою Suricata.

2.3 Архітектура та принципи функціонування програмного комплексу Suricata

Suricata є відкритим програмним комплексом для виявлення та запобігання мережевим вторгненням (IDS/IPS) і одночасно платформою мережевого моніторингу (NSM). На відміну від класичних однониткових IDS, Suricata спочатку трактувалися як багатопотоковий рушій, що здатний ефективно використовувати багатоядерні процесори та масштабуватися разом зі зростанням пропускної здатності мережі [28]. Завдяки цьому комплекс може застосовуватися як у невеликих локальних мережах, так і на магістральних ділянках з високим навантаженням.

Архітектура Suricata складається з кількох логічних рівнів: підсистеми захоплення трафіку, модулів декодування протоколів, механізмів відстеження потоків (flow/stream engine), підсистеми застосування правил (rule engine) та підсистеми виводу результатів (output). На етапі захоплення пакети надходять із мережевих інтерфейсів або з файлів дампів (pcap), після чого декодуються відповідно до стеку протоколів (Ethernet, VLAN, IPv4/IPv6, TCP/UDP, HTTP, TLS тощо). Далі механізм відстеження потоків агрегує окремі пакети в логічні сесії, що дозволяє аналізувати контекст з’єднання, а не тільки ізольовані пакети.

Багатопотоковість реалізується через концепцію "worker-потоків", які паралельно обробляють різні потоки трафіку. В офіційному керівництві користувача описано кілька режимів запуску (runmodes), серед яких af-packet, pcap, netmap, nfqueue та інші [28]. Це дозволяє адаптувати Suricata до різних сценаріїв розгортання: пасивного аналізу через дзеркальні порти комутаторів, роботи "в розриві" в режимі IPS або інтеграції з міжмережевими екранами через черги nfqueue.

З погляду принципів функціонування Suricata може працювати у трьох основних режимах: як система виявлення вторгнень (IDS), система запобігання вторгненням (IPS) та система мережевого моніторингу (NSM), [29]. У режимі IDS комплекс отримує копію трафіку й генерує оповіщення без втручання в процес маршрутизації. У режимі IPS Suricata інтегрується з маршрутизатором або брандмауером і має можливість блокувати небажані пакети чи з’єднання в режимі

реального часу. Як NSM-рішення Suricata забезпечує детальне журналювання подій, статистику сесій і метадані, які можуть використовуватися системами SIEM та платформами аналізу безпеки.

Конфігурація Suricata зберігається в основному файлі suricata.yaml, де задаються параметри мережевих інтерфейсів, джерела правил, режими роботи, обсяги буферів, параметри потоків і формати журналів. У посібнику Manualzz детально розглядається структура цього файлу, включно з окремими секціями для налаштування декодерів протоколів, TCP-реверсної збірки, HTTP-аналізу, TLS-модулів та механізмів виявлення аномалій [20]. Правильне налаштування цих параметрів є критично важливим для досягнення балансу між точністю виявлення атак і продуктивністю системи.

Функціонування Suricata визначається набором правил, що описують ознаки атак, небажаних протоколів або підозрілих шаблонів поведінки. Кожне правило складається з заголовка (rule header) та набору опцій (rule options) [28]. У заголовку зазначається дія (alert, drop, reject, pass тощо), протокол (tcp, udp, icmp, http, tls і т. д.), адреси та порти джерела й призначення, а також напрямок трафіку. В опціях задаються умови аналізу корисного навантаження (content, http_uri, file_data), обмеження за потоком (flow, flowbits), додаткові метадані (msg, classtype, priority, reference), а також службові параметри (sid, rev).

Стаття b4y.dev[32] окремо акцентує увагу на правильному задання ідентифікаторів правил (sid), системі класифікації загроз (classtype) та використанні механізмів порогів (threshold), які дають змогу зменшити кількість дублюючих сповіщень і налаштувати чутливість до певних типів подій. Завдяки цьому адміністратор може адаптувати набір правил до особливостей конкретної корпоративної мережі, уникнувши надмірної кількості хибних спрацьовувань.

Основними джерелами правил для Suricata є відкриті набори Emerging Threats (ET Open/Pro), а також офіційні й кастомні правила організації. У вступному посібнику Luo C. наголошується, що регулярне оновлення бази правил є ключовою передумовою актуальності системи захисту, оскільки більшість сучасних атак швидко еволюціонують [21]. Крім того, Suricata підтримує

розділення правил на окремі файли й категорії, що спрощує їх вибіркове ввімкнення та тестування в межах пілотних розгортань.

Suricata має розвинені можливості аналізу протоколів прикладного рівня. Для HTTP-трафіку підтримується декодування заголовків, URL-адрес, методів запитів, статус-кодів і тіло повідомлень; для TLS – збирання метаданих сертифікатів, версій протоколу, наборів шифрів; для DNS – аналіз запитів і відповідей з виявленням підозрілих доменів. Окремі модулі дозволяють зберігати передані файли або їх хеш-значення для подальшого аналізу антивірусними й пісочничними системами. У практичних гайдах з конфігурації підкреслюється, що активація аналізу файлів і протоколів потребує додаткових ресурсів і повинна супроводжуватися відповідним налаштуванням потоків і черг [29], [31].

Забезпечення високої продуктивності Suricata досягається за рахунок оптимізації кількості робочих потоків, використання режимів zero-copy для захоплення трафіку та правильного розподілу черг між ядрами процесора [28]. Практичні матеріали Markaicode демонструють підхід, коли для кожного інтерфейсу створюються окремі черги, а Suricata запускається з відповідною кількістю worker-процесів, що дозволяє уникнути вузьких місць і реалізувати обробку трафіку на швидкостях, близьких до лінійних [31].

Важливою складовою архітектури Suricata є гнучка система логування. Комплекс підтримує різні формати вихідних даних: традиційний unified2, XML, а також формат eve.json, що є де-факто стандартом інтеграції з платформами ELK/SELKS, Graylog та іншими системами збирання логів [27]. Через EVE JSON можуть експортуватися як сповіщення IDS/IPS, так і статистика потоків, HTTP-журнали, TLS-метадані та інформація про файли. Це створює основу для централізованого моніторингу та подальшого кореляційного аналізу інцидентів [28]. Suricata у даній роботі розглядається як рушій IDS/IPS/NSM, що виконує аналіз мережевого трафіку, застосовує правила детектування та формує події безпеки (зокрема у форматі eve.json) для подальшої обробки. Натомість SELKS є інтегрованою платформою мережевого моніторингу безпеки, яка включає Suricata та доповнює її компонентами збору, зберігання й візуалізації подій (як правило, на

базі ELK-стеку), забезпечуючи готове середовище для аналізу інцидентів і побудови дашбордів. Таким чином, Suricata відповідає за виявлення та генерацію телеметрії, тоді як SELKS – за організацію централізованого журналювання й зручного аналізу результатів детектування [24].

Таким чином, архітектура Suricata поєднує багатопотоковий механізм обробки трафіку, гнучку систему правил та потужні можливості логування. У поєднанні з правильною конфігурацією й актуальними наборами правил це дозволяє реалізувати надійний рівень виявлення загроз у корпоративній мережі. У наступних підрозділах роботи ці особливості будуть використані для побудови схеми взаємодії Suricata з маршрутизатором MikroTik та організації процесів моніторингу й реагування на інциденти.

2.4 Методики інтеграції систем виявлення та запобігання вторгненням у корпоративну мережу

Інтеграція систем виявлення та запобігання вторгненням у корпоративну мережу може бути реалізована кількома методами, що відрізняються ступенем впливу на мережеву інфраструктуру та рівнем захисту. Найпростіший підхід передбачає пасивний моніторинг трафіку через порти дзеркалювання або мережеві TAP-пристрої, коли IDS отримує копію трафіку й формує журнал подій без прямого втручання в процес передачі даних. Цей варіант мінімально впливає на конфігурацію мережі, але обмежує можливості автоматичного блокування загроз.

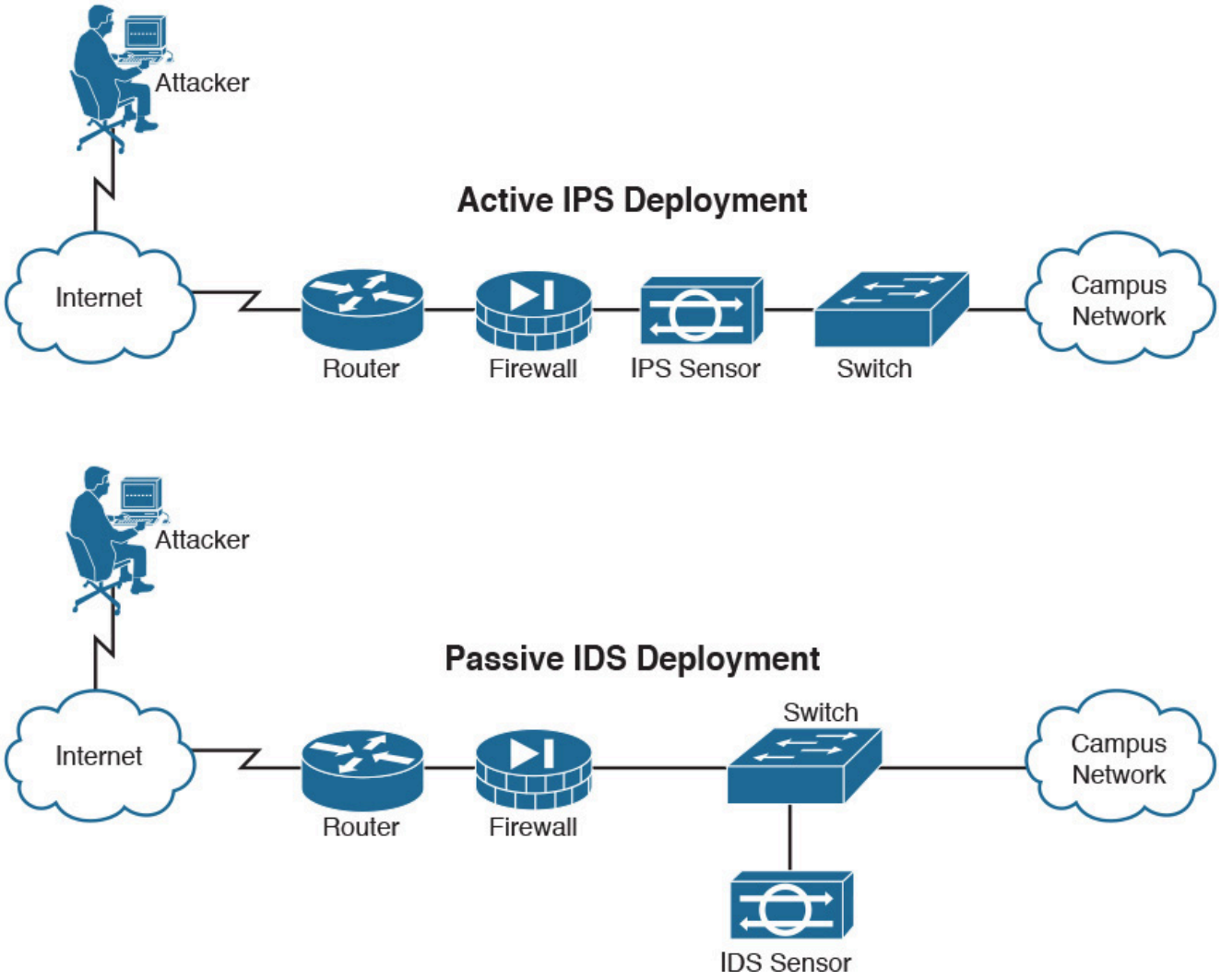

Рис. 2.1 Порівняння розміщення IDS/IPS у мережі

Більш просунута методика передбачає використання IPS у розриві або в режимі інтерактивної взаємодії з мережевим обладнанням. У першому випадку трафік фізично проходить через вузол із Suricata, де відбувається аналіз і, за потреби, блокування пакетів. У другому випадку IDS працює в пасивному режимі, але при спрацюванні критичних правил ініціює зміну політик фільтрації на маршрутизаторі через API чи інші механізми керування. Така схема, особливо в поєднанні з обладнанням MikroTik, дозволяє поєднати гнучкість архітектури з можливістю автоматизованого реагування на інциденти.

2.5 Обґрунтування методу побудови корпоративної мережі із застосуванням MikroTik та Suricata

Запропонований у роботі метод побудови корпоративної мережі зосереджений на розподілі ролей між обладнанням MikroTik і програмним комплексом Suricata. MikroTik використовується як граничний шлюз, основний маршрутизатор між VLAN-сегментами та платформа для реалізації базових політик фільтрації, NAT і VPN. Suricata, у свою чергу, відповідає за глибокий аналіз трафіку, виявлення складних атак і формування подій безпеки, які далі використовуються для автоматизованого або ручного реагування. Такий розподіл дозволяє максимально ефективно використати сильні сторони обох рішень.

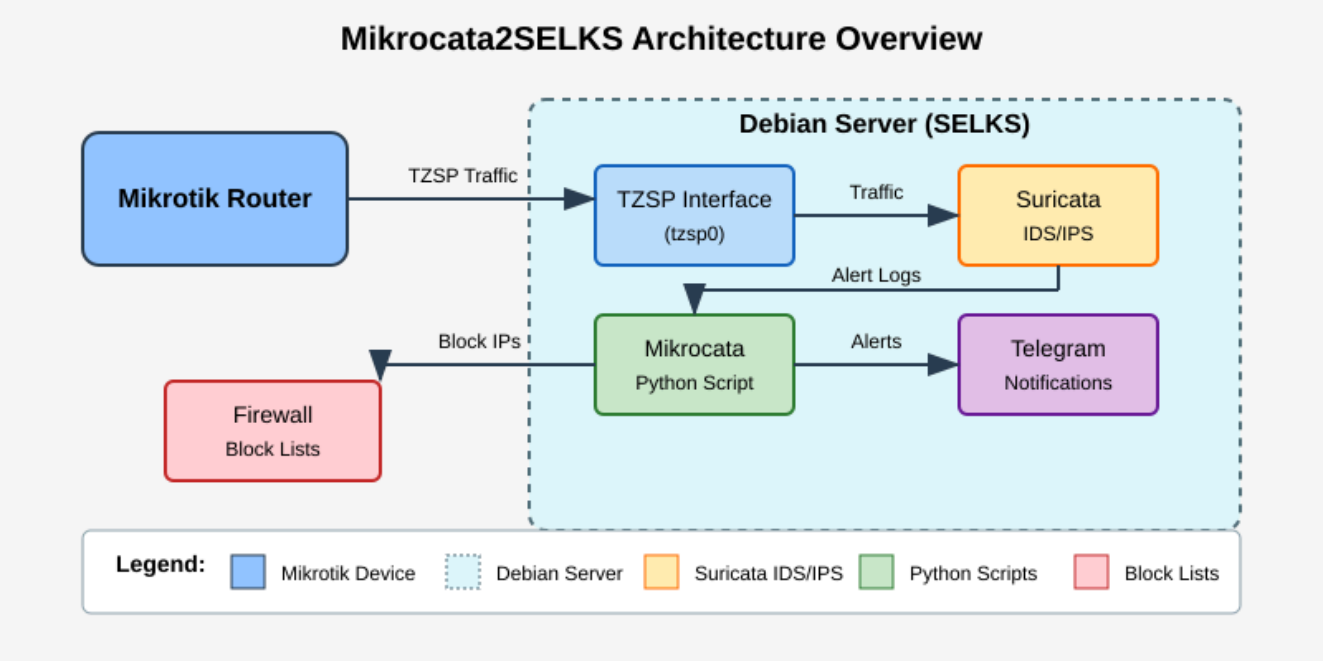

Рис. 2.2 Інтеграція Suricata у мережу на базі MikroTik

Архітектура Mikrocata2SELKS ілюструє розподіл функцій між мережевим периметром та сенсором IDS/IPS: маршрутизатор MikroTik виконує роль граничного вузла (маршрутизація, NAT, фільтрація, сегментація), тоді як копія трафіку з ключових інтерфейсів передається на окремий сервер із Suricata/SELKS

через механізм дзеркалювання або протокол TZSP. Suricata здійснює аналіз потоків і пакетів та формує події у форматі EVE JSON, які далі агрегуються в SELKS для зберігання й візуалізації (дашборди, пошук інцидентів). Принципово важливим елементом схеми є канал зворотного зв’язку: за результатами спрацювань правил автоматизований компонент звертається до RouterOS API і додає джерела підозрілого трафіку до address-list, після чого попередньо визначені правила фаєрвола блокують з’єднання на периметрі. У підсумку детектування та аналітика виконуються поза трактом передавання даних, а блокування реалізується на периметрі мережі, що підвищує керованість, масштабованість і практичну придатність рішення для SMB-сценаріїв [33].

Перевагою методу є поєднання доступної вартості обладнання з високим рівнем гнучкості налаштувань і відкритістю програмного забезпечення. На відміну від монолітних комерційних рішень, зв’язка MikroTik + Suricata дає змогу адаптувати архітектуру до специфіки конкретного підприємства, самостійно обирати джерела правил IDS/IPS і реалізовувати власні сценарії реагування. Це робить запропонований метод доцільним для малих і середніх організацій, які потребують балансу між рівнем захисту, вартістю та прозорістю функціонування системи.

2.6 Опис запропонованої методики організації моніторингу та виявлення атак у корпоративній мережі

Запропонована методика моніторингу безпеки базується на поєднанні журналів подій маршрутизатора MikroTik і детальних логів Suricata. На першому рівні фіксуються події, пов’язані зі спрацюванням правил міжмережевого екрана, змінами стану інтерфейсів, встановленням та розривом VPN-з’єднань. На другому рівні Suricata реєструє спроби експлуатації вразливостей, аномалії в поведінці користувачів, підозрілі з’єднання та інші індикатори компрометації. Об’єднання цих джерел даних забезпечує повніший контекст для аналізу інцидентів.

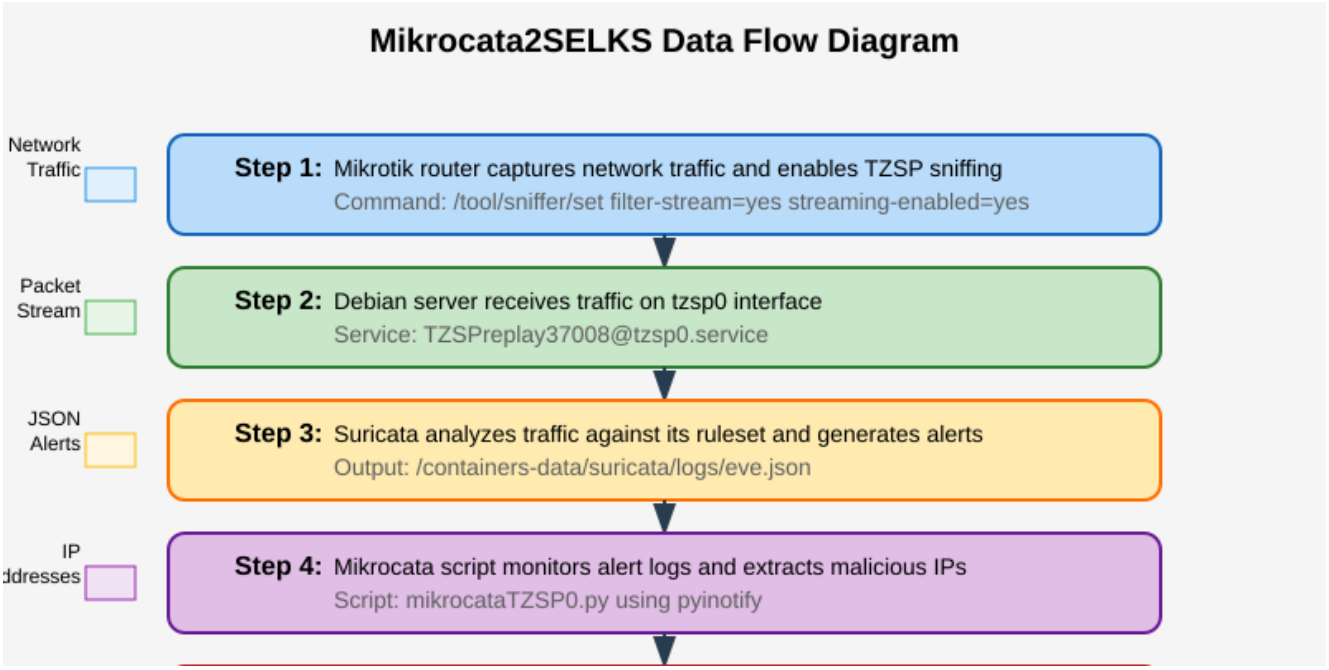

Рис. 2.3 Методика моніторингу та автоматизованого блокування адрес

Методика передбачає використання інструментів агрегації та візуалізації логів, а також сценаріїв автоматизації реагування. При спрацюванні критичних правил Suricata відповідні події передаються сервісу, який за допомогою API MikroTik додає IP-адреси до списків блокування, змінює правила фільтрації чи формує сповіщення для адміністратора. Таким чином скорочується час між виявленням атаки та вжиттям контрзаходів, а система захисту переходить від пасивного сповіщення до активного керування ризиками.

РОЗДІЛ 3 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ПІДПРИЄМСТВА НА ОСНОВІ ЗАПРОПОНОВАНОГО МЕТОДУ

3.1 Постановка задачі та вихідні вимоги до мережі підприємства

З метою демонстрації та аналізу розробленого методу було сформовано перелік вимог до мережі підприємства малого та середнього бізнесу з кількістю 10–40 кінцевих пристроїв на філію. У межах заданого профілю експлуатації передбачається функціонування внутрішніх критичних сервісів у головній філії (файловий та поштовий сервіси), а також доступ користувачів до зовнішнього хмарного CRM-сервісу через мережу Інтернет. Додатково встановлюється потреба організації віддаленого підключення співробітників і розділення бездротового доступу на корпоративний та гостьовий сегменти.

Вихідні умови та обмеження проекту:

а) склад сервісів та їх розміщення:

1) внутрішні сервіси у головній філії:

– файловий сервіс для зберігання робочих даних;

– поштовий сервіс для корпоративної комунікації;

2) зовнішні сервіси через мережу Інтернет:

– CRM як хмарний сервіс із доступом за захищеним протоколом прикладного рівня;

3) веб-сервіси підприємства:

– передбачено варіант розміщення веб-сервісів із виділенням демілітаризованої зони для публічного доступу;

б) мережеве обладнання та інфраструктура доступу:

1) центральний мережевий вузол:

– один маршрутизатор, який виконує функції маршрутизації між сегментами, міжмережевого екранування, трансляції адрес і забезпечення VPN-доступу;

2) бездротовий доступ:

– одна точка доступу для співробітників;

– одна точка доступу для гостей;

3) комутація та сегментація:

– керований комутатор для підтримки VLAN і організації дзеркалювання трафіку на сенсор безпеки;

в) засоби моніторингу та виявлення інцидентів:

1) сенсор безпеки:

– віртуальна машина для розгортання Suricata як системи мережевого моніторингу та виявлення атак;

2) підхід до інтеграції:

– базова інтеграція передбачає пасивний аналіз трафіку (IDS) з можливістю автоматизованого блокування джерел атак через адресні списки та правила фільтрації на маршрутизаторі;

Узагальнена модель загроз. Для підприємств малого–середнього бізнесу типовими є змішані загрози: зовнішні атаки з мережі Інтернет по периметру, компрометація робочих станцій через соціальну інженерію та наслідки поширення шкідливого програмного забезпечення у внутрішньому середовищі. У межах даної роботи модель загроз подано у вигляді сценаріїв, які визначають вимоги до сегментації, політик доступу та механізмів моніторингу.

а) зовнішній порушник (інтернет-сегмент):

1) розвідка та сканування периметра з метою визначення відкритих сервісів і помилково опублікованих портів;

2) підбір облікових даних (brute force) до служб віддаленого доступу, поштових сервісів та адміністративних інтерфейсів;

3) експлуатація вразливостей веб-сервісів у разі їх публічного розміщення;

б) компрометація робочої станції користувача:

1) наслідки фішингу, зокрема викрадення облікових даних та виконання шкідливого коду;

2) встановлення каналу керування (зовнішні комунікації з командними серверами) та спроби закріплення у середовищі;

3) спроби доступу до внутрішніх ресурсів і серверів із подальшим розширенням впливу;

в) ransomware-інцидент як критичний ризик для даних:

1) шифрування файлових ресурсів і службових каталогів;

2) розповсюдження у межах мережі через спільні ресурси та скомпрометовані облікові записи;

3) порушення доступності ключових сервісів для підрозділів;

г) внутрішній порушник або помилки налаштувань:

1) несанкціонований доступ до серверів і даних через надлишкові мережеві дозволи;

2) помилкова конфігурація правил, що відкриває внутрішні сервіси у зовнішній сегмент;

3) неконтрольоване підключення пристроїв у мережу гостей або у мережу співробітників;

Вихідні вимоги до мережі підприємства:

а) забезпечити роботу 10–40 кінцевих пристроїв із поділом дротового та бездротового доступу на корпоративний і гостьовий;

б) забезпечити доступ користувачів до внутрішніх сервісів головної філії, зокрема:

1) файлового сервісу;

2) поштового сервісу;

в) забезпечити керований доступ до зовнішнього CRM-сервісу через мережу Інтернет із пріоритетом на контроль вихідних з’єднань та мінімізацію небажаних напрямів трафіку;

г) забезпечити можливість віддаленого підключення співробітників до внутрішніх ресурсів через VPN із визначенням прав доступу відповідно до ролей;

ґ) реалізувати мережеве зонування з виділенням щонайменше таких логічних сегментів:

1) сегмента керування;

2) користувацького сегмента;

3) серверного сегмента;

4) гостьового сегмента;

5) демілітаризованої зони для веб-сервісів підприємства;

д) забезпечити моніторинг мережевих подій і виявлення атак класів scan, brute force, наслідків фішингу та ознак ransomware через сенсор Suricata з подальшим використанням подій для реагування на мережевому рівні.

Вимоги до резервного копіювання. Відновлюваність розглядається як обов'язкова складова стійкості до ransomware та операційних інцидентів. Політика резервного копіювання встановлюється у вигляді регламенту, який має бути реалізований у робочому середовищі.

а) виконувати резервування критично важливих файлів щодобово, зокрема:

1) даних файлового сервера:

– робочих каталогів підрозділів;

– спільних папок і проектних даних;

2) даних поштового сервісу:

– поштових скриньок або архівів (відповідно до реалізованої платформи);

3) даних, пов'язаних із CRM:

– експортів або звітів, що зберігаються у внутрішньому середовищі підприємства;

б) виконувати повне резервування всіх даних щотижня, включаючи:

1) повний вміст файлового сервера;

2) повні дані поштового сервісу;

3) конфігурації інфраструктури та засобів безпеки:

– конфігурацію маршрутизатора;

– конфігурації комутації та точок доступу;

– конфігурацію Suricata (налаштування, локальні правила, параметри логування);

Сформульовані вимоги використовуються як вихідна база для проектування VLAN-сегментації та зон безпеки, вибору фізичної схеми підключення сенсора Suricata, розроблення матриці доступу між сегментами та реалізації правил фільтрації і трансляції адрес на маршрутизаторі.

3.2 Побудова корпоративної мережі

3.2.1 Логічна сегментація та зони безпеки

Логічна сегментація корпоративної мережі застосовується як базовий механізм зменшення ризиків, пов’язаних із несанкціонованим доступом, переміщенням порушника всередині мережі ("lateral movement") та компрометацією критичних сервісів. Для підприємства малого та середнього бізнесу сегментація має бути достатньо деталізованою для реалізації політик доступу, але водночас – керованою в експлуатації та придатною до подальшого масштабування.

У межах запропонованого рішення сегментація реалізується через виділення зон безпеки, для яких визначаються окремі правила міжсегментної взаємодії. Такий підхід забезпечує скорочення площі атаки ("attack surface") за рахунок обмеження зайвих мережевих зв’язків, а також спрощує контроль і аудит доступу до серверів, мережевих пристроїв та публічних сервісів.

Принципи зонування та сегментації:

а) інфраструктура поділяється на зони відповідно до функціонального призначення вузлів і рівня довіри;

б) взаємодія між зонами здійснюється через маршрутизацію на центральному маршрутизаторі із застосуванням правил firewall, що виключає неконтрольовані міжсегментні з’єднання;

в) гостьовий доступ ізолюється від внутрішніх ресурсів підприємства з наданням виходу лише в мережу Інтернет;

г) адміністративний контур керування виділяється в окремий сегмент з обмеженням доступу за джерелами та сервісами;

ґ) публічні веб-сервіси (за наявності) розміщуються в DMZ із мінімально необхідними зв’язками до внутрішніх сервісів;

д) віддалений доступ користувачів через VPN логічно відокремлюється від користувацького сегмента для застосування додаткових обмежень і моніторингу.

Як технологічну основу сегментації використано технологію VLAN. Для кожної зони безпеки визначено окремий VLAN і окремий IP-підмережевий простір. З метою спрощення адміністрування та наочності проектного рішення в межах даної роботи для всіх сегментів використано підмережі формату /24.

Прийнята VLAN-структура корпоративної мережі:

а) сегмент керування MGMT:

1) призначення – адміністративний доступ до маршрутизатора, комутатора, точок доступу та сервісних компонентів;

2) параметри сегмента:

– VLAN ID 10;

– адресний простір 192.168.10.0/24;

б) користувацький сегмент USERS:

1) призначення: – робочі станції співробітників і корпоративні мобільні пристрої;

2) параметри сегмента:

– VLAN ID 20;

– адресний простір 192.168.20.0/24;

3) підключення бездротового доступу:

– точка доступу для співробітників функціонує в даному сегменті;

в) серверний сегмент SERVERS:

1) призначення – розміщення внутрішніх критичних сервісів головної філії;

2) параметри сегмента:

– VLAN ID 30;

– адресний простір 192.168.30.0/24;

3) типові вузли:

– файловий сервер;

– поштовий сервер;

г) гостьовий сегмент GUEST:

1) призначення – гостьовий доступ із виходом в Інтернет;

2) параметри сегмента:

– VLAN ID 40;

– адресний простір 192.168.40.0/24;

3) підключення бездротового доступу:

– гостьова точка доступу функціонує в даному сегменті;

ґ) демілітаризована зона DMZ:

1) призначення – розміщення публічних веб-сервісів підприємства (за наявності);

2) параметри сегмента:

– VLAN ID 50;

– адресний простір 192.168.50.0/24;

д) сегмент віддаленого доступу VPN:

1) призначення – адресний простір для VPN-користувачів із окремими політиками доступу;

2) параметри сегмента:

– VLAN ID 60;

– адресний простір 192.168.60.0/24;

Таблиця 3.1

Характеристика логічних сегментів і зон безпеки

Сегмент	VLAN id	Адресний простір	Призначення	Типові сервіси/трафік	Рівень довіри
MGMT	10	192.168.10.0/24	керування інфраструктурою	адміністрування мережевих пристроїв, доступ до консолей і сервісних компонентів	високий
USERS	20	192.168.20.0/24	робочі місця співробітників	доступ до файлового і поштового сервісів, вихід в Інтернет, доступ до CRM	середній
SERVERS	30	192.168.30.0/24	внутрішні критичні сервіси	файловий та поштовий сервіси, службові компоненти	підвищений
GUEST	40	192.168.40.0/24	гостьовий доступ	вихід в Інтернет без доступу до внутрішніх ресурсів	низький
DMZ	50	192.168.50.0/24	публічні веб-сервіси	веб-сервіси підприємства, обмежені з’єднання до SERVERS за потреби	низький
VPN	60	192.168.60.0/24	віддалені користувачі	контрольований доступ до USERS/SERVERS відповідно до ролей	середній

Запропонована структура зон безпеки забезпечує технічну основу для реалізації політик доступу. Ізоляція гостьового сегмента знижує ризик доступу сторонніх пристроїв до внутрішніх ресурсів. Виділення серверного сегмента дозволяє централізовано обмежити доступ до критичних сервісів і зменшити

ризик їх компрометації у разі зараження робочої станції. DMZ локалізує ризики публічних веб-сервісів і дозволяє застосовувати окремі правила публікації та контролю вхідного трафіку.

Окремий сегмент керування використовується для розмежування адміністративного доступу від користувацького трафіку, а сегмент VPN – для застосування додаткових обмежень до віддалених користувачів. Для інтеграції з Suricata пріоритетними напрямами моніторингу визначаються потоки до серверного сегмента та DMZ, а також трафік від VPN-користувачів, що дозволяє фокусувати виявлення мережевих атак на найбільш ризикових зонах і зменшувати кількість нерелевантних подій.

3.2.2 Фізична схема та розміщення обладнання MikroTik/Suricata

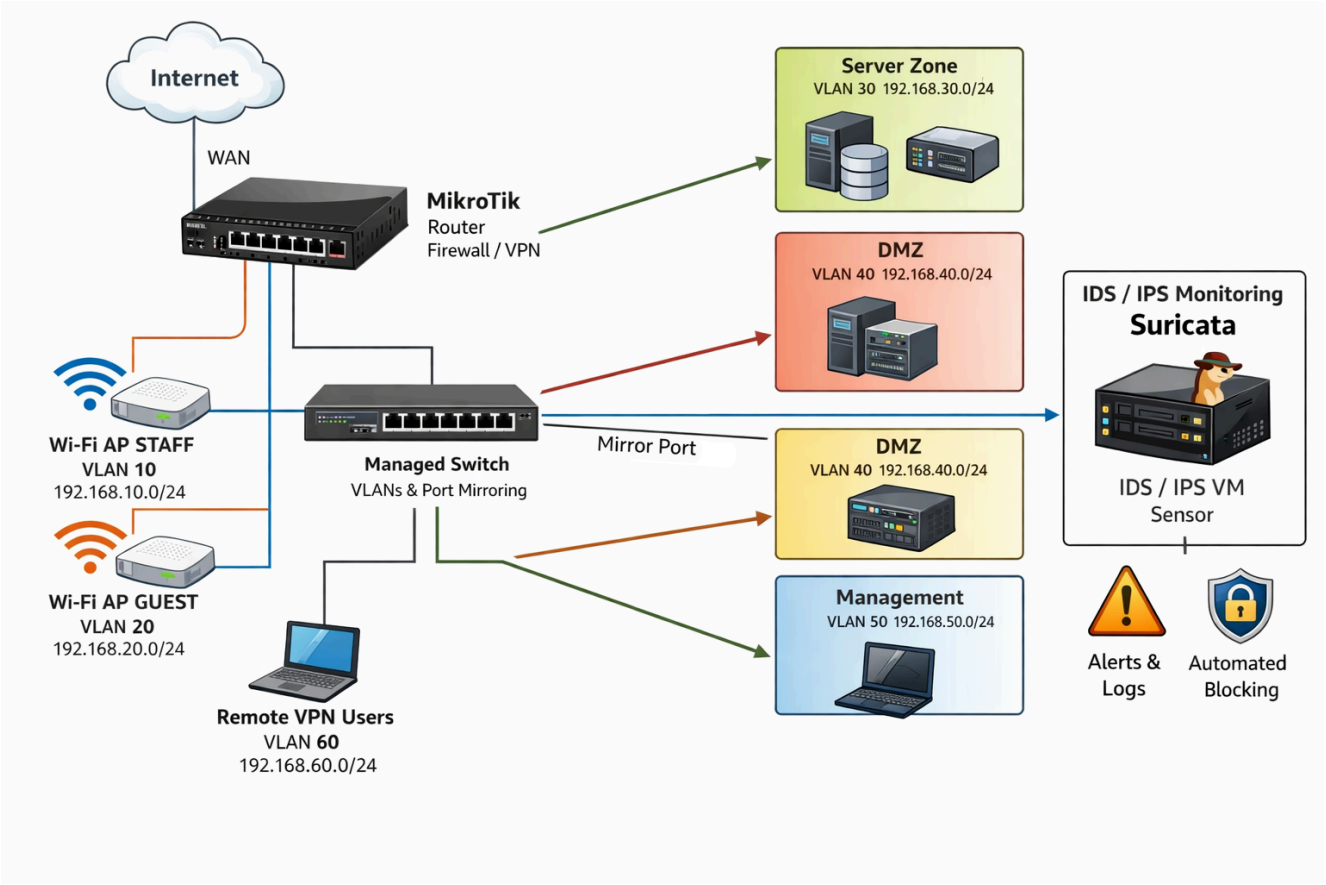

Рис. 3.1 Схема спроектованої корпоративної мережі

Фізична топологія мережі будується за принципом централізованого периметру з маршрутизацією між логічними сегментами на маршрутизаторі та

комутацією на керованому комутаторі. На рисунку 3.1 наведено узагальнену фізичну схему взаємодії мережевих пристроїв, серверної інфраструктури та IDS/IPS сенсора Suricata.

Загальна схема розміщення обладнання та підключень:

а) периметр корпоративної мережі реалізовано на маршрутизаторі MikroTik RB4011iGS+5HacQ2HnD-IN, який виконує функції:

1. підключення до провайдера через WAN-інтерфейс;
2. маршрутизації між VLAN-сегментами корпоративної мережі;
3. фільтрації трафіку (firewall), трансляції мережевих адрес (NAT);
4. організації віддаленого доступу через VPN для користувачів поза офісом;

б) рівень комутації та сегментації реалізовано на керованому комутаторі MikroTik CSS326-24G-2S+RM, який забезпечує:

1. підключення кінцевих пристроїв та серверів через порти доступу (access) відповідних VLAN;
2. uplink-з’єднання з маршрутизатором через trunk, що передає трафік кількох VLAN одним фізичним каналом;
3. дзеркалювання трафіку на виділений порт для підключення сенсора Suricata (портове дзеркалювання, mirror);

в) бездротовий доступ організовано через дві точки доступу:

1. точка доступу для співробітників підключається до корпоративного сегмента користувачів;
2. гостьова точка доступу підключається до гостьового сегмента з ізоляцією від внутрішніх ресурсів і дозволом виходу лише в Інтернет;

г) сервери головного офісу розміщуються у виділеному серверному сегменті та підключаються до комутатора через порти доступу;

ґ) за наявності публічних веб-сервісів передбачається їх розміщення в DMZ-сегменті, який фізично підключається до комутатора, а логічно контролюється правилами доступу на маршрутизаторі;

д) Suricata розгортається як віртуальна машина на окремому хості в головному офісі та підключається до порту комутатора, на який подається дзеркальована копія трафіку.

Окрім базового варіанта пасивного підключення Suricata через port mirroring на керованому комутаторі, у запропонованій архітектурі можуть бути корисними й інші способи інтеграції, які розширюють функціональні можливості моніторингу та підвищують керованість захисту залежно від експлуатаційних обмежень. Зокрема, застосування апаратного TAP дає змогу отримати більш стабільну та повну копію трафіку на критичних лініях (наприклад, на периметрі), зменшуючи ризик втрати пакетів порівняно зі port mirror, що важливо для коректного аналізу подій і відтворюваності експериментів. Включення Suricata в режимі IPS (inline) або через механізм NFQUEUE на вузлі обробки трафіку дозволяє перейти від суто детекційної моделі до превентивної, тобто блокувати частину шкідливих з'єднань у реальному часі, що потенційно зменшує наслідки атак типу підбору облікових даних (brute force) та атаки шифрувальника (ransomware) за рахунок раннього припинення небезпечних сесій. Додатково, дзеркалювання трафіку на рівні віртуалізації (vSwitch) може бути доцільним у разі розміщення частини сервісів у віртуальному середовищі, оскільки забезпечує видимість внутрішньохостового обміну між віртуальними машинами, який не завжди повністю відображається у фізичному port mirror; таким чином, альтернативні методи інтеграції можуть бути використані як інструменти підвищення повноти спостереження та переходу до керованого запобігання інцидентам без зміни загальної логіки сегментації мережі.

З огляду на розроблену схему мережі було обрано інтеграцію сенсора Suricata через port mirror на комутаторі як найбільш доцільний варіант:

а) простота впровадження: дзеркалювання реалізується засобами комутатора без зміни логіки маршрутизації та без перебудови топології;

б) надійність: відмова сенсора Suricata або помилки в його конфігурації не блокують робочий трафік, оскільки сенсор працює пасивно та отримує лише копію трафіку;

в) продуктивність та масштабування: ресурси аналізу трафіку переносяться на окремий хост (віртуальну машину), що дозволяє збільшувати обчислювальні ресурси сенсора без модернізації маршрутизатора.

3.2.3 Маршрутизація та VPN-доступ

Маршрутизація в межах запропонованої архітектури розглядається як механізм керованої взаємодії між логічними сегментами, а VPN-доступ, як інструмент надання віддаленим користувачам контрольованого доступу до внутрішніх ресурсів без розкриття сервісів у мережу Інтернет. З огляду на те, що мережа підприємства реалізована в одному майданчику та має один центральний маршрутизатор, пріоритетом є простота конфігурації, відтворюваність налаштувань і однозначність правил доступу.

Маршрутизація між VLAN-сегментами та вихід у мережу Інтернет:

а) для кожного VLAN-сегмента на маршрутизаторі створюється відповідний інтерфейс (VLAN або логічний інтерфейс у складі bridge) та задається адреса шлюзу в межах підмережі /24;

б) маршрутизація між сегментами реалізується через "безпосередньо підключені" маршрути (connected routes), що формуються автоматично після призначення IP-адрес інтерфейсам VLAN;

в) доступ у мережу Інтернет забезпечується статичним маршрутом за замовчуванням (default route) у напрямку провайдера;

г) застосування динамічної маршрутизації (OSPF) у даній топології не є обов’язковим, оскільки відсутні альтернативні маршрутизатори та розгалужені міжмайданчикові з’єднання; разом із тим OSPF може бути доцільним у випадку подальшого масштабування (друга філія, резервний маршрутизатор, декілька L3-вузлів);

ґ) policy routing у базовій конфігурації не використовується, однак може бути корисним за наявності двох каналів доступу до Інтернету

(балансування/резервування) або для примусового спрямування окремих класів трафіку (наприклад, гостьовий сегмент) у визначений канал.

Організація VPN-доступу. VPN-доступ призначений для співробітників, які підключаються поза межами офісу (віддалена робота, відрядження) та потребують доступу до внутрішніх ресурсів підприємства. У межах запропонованого проекту VPN реалізується на маршрутизаторі як окремий логічний сегмент із власним адресним простором, що відповідає прийнятому VPN-сегменту у загальній структурі мережі (192.168.60.0/24). При підключенні користувач отримує адресу з цього діапазону та розглядається як окремий клас джерел трафіку, для якого встановлюються спеціальні правила доступу.

а) тип VPN-підключення обирається з урахуванням вимог безпеки та сумісності клієнтських пристроїв; у контексті практичної реалізації доцільно застосовувати сучасний протокол із криптографічно стійкими алгоритмами та мінімальною складністю супроводження;

б) логіка доступу віддалених користувачів визначається матрицею доступу між сегментами: VPN-користувачі отримують доступ лише до тих сервісів і підмереж, які необхідні для виконання службових функцій (наприклад, файловий та поштовий сервіси), при цьому доступ до адміністративного сегмента керування обмежується;

в) режим маршрутизації трафіку VPN-клієнтів може бути реалізовано як split-tunnel (маршрутизується лише трафік до внутрішніх підмереж підприємства) або як full-tunnel (увесь трафік проходить через периметр підприємства); у межах малого–середнього бізнесу практично доцільним є split-tunnel, оскільки він знижує навантаження на периметр і не ускладнює доступ до зовнішніх сервісів (зокрема CRM), залишаючи при цьому контроль доступу до внутрішніх ресурсів;

г) для забезпечення керованості доступу VPN-підмережа та правила її взаємодії з іншими сегментами фіксуються в конфігурації маршрутизатора і надалі використовуються в правилах фільтрації та журналах подій, що спрощує аудит підключень та аналіз інцидентів.

3.3 Схема взаємодії MikroTik і Suricata

Взаємодія маршрутизатора MikroTik RB4011iGS+5HacQ2HnD-IN та сенсора Suricata в запропонованій архітектурі реалізується за моделлю пасивного контролю, за якої сенсор не впливає на проходження робочого трафіку, а аналізує його копію. Фізичні зв’язки компонентів визначені розробленою схемою мережі (рисунок 3.1): RB4011 виконує функції периметру та міжсегментної маршрутизації, а MikroTik CSS326-24G-2S+RM забезпечує комутацію VLAN і відбір трафіку для IDS/IPS за допомогою port mirroring.

Контур передавання робочого трафіку охоплює потоки між VLAN-сегментами та вихід у мережу Інтернет. На рівні RB4011 здійснюється маршрутизація між підмережами VLAN (/24 для кожного сегмента), застосовуються правила firewall і NAT, а також завершується VPN-тунель для віддалених користувачів. У результаті основні бізнес-потоки (доступ користувачів до файлового та поштового сервісів у VLAN SERVERS, вихід у Інтернет і доступ до зовнішньої CRM, доступ до ресурсів через VPN) проходять через RB4011 як центральний контрольний вузол периметра.

Контур відбору трафіку для аналізу реалізується на CSS326-24G-2S+RM. Завдяки налаштуванню конфігурації port mirror формується дзеркальна копія обраних потоків на виділений порт (mirror-target), до якого підключено мережевий інтерфейс хоста віртуалізації з Suricata (VM/SELKS). Такий підхід забезпечує отримання сенсором репрезентативного набору пакетів для детекції типових атак. Практично доцільним є відбір напрямів, що мають найбільшу безпекову цінність, зокрема трафіку до VLAN SERVERS, трафіку до VLAN DMZ (за наявності публічних сервісів) та трафіку, ініційованого VPN-користувачами.

Контур подій і логів формується безпосередньо на Suricata. Після захоплення дзеркальованого трафіку Suricata виконує декодування протоколів і застосовує набір правил детекції, формуючи події в структурованому вигляді. Основним вихідним артефактом є журнал подій у форматі EVE JSON, який містить записи спрацювань (alert) та допоміжні дані для розслідування (метадані

потоків, DNS/HTTP/TLS атрибути та службову статистику). Для забезпечення подальшого використання результатів аналізу EVE JSON обробляється двома каналами:

а) передавання подій у систему моніторингу (зокрема стек на базі SELKS/ELK або інший журналювальний компонент) для централізованого перегляду, фільтрації та кореляції;

б) передавання подій у модуль автоматизованого реагування, який виконує парсинг EVE JSON у режимі, наближеному до реального часу, нормалізує атрибути події та приймає рішення щодо керувального впливу.

Контур автоматизованого реагування замикається керувальними діями на RB4011. Після підтвердження релевантності події (тип активності, джерело, порогові значення) скрипт реагування ініціює додавання IP-адреси джерела до address-list на маршрутизаторі через керувальний інтерфейс (наприклад, MikroTik API або SSH). Далі правила firewall на RB4011, прив’язані до відповідного address-list, застосовують блокування або обмеження з’єднань. Для забезпечення простежуваності та можливості аудиту доцільним є журналювання як подій Suricata, так і факту застосування блокування на RB4011 (зокрема з фіксацією часу, адреси джерела та підстави дії).

Сформована схема потоків трафіку та подій узагальнена в таблиці Б.1, де деталізовано: джерела і призначення ключових потоків, точку дзеркалювання на CSS326, формати вихідних подій Suricata (EVE JSON), а також логіку доставлення подій у систему моніторингу й модуль реагування з подальшим застосуванням керувальних дій на RB4011. Для коректної кореляції подій у часі обов’язковою умовою є синхронізація часу на мережевих пристроях і сенсорі (NTP), оскільки часові розбіжності безпосередньо спотворюють інтерпретацію інцидентів і результати експериментального оцінювання.

3.4 Налаштування Suricata та власні правила виявлення

3.4.1 Базові правила ET Open

Налаштування сенсора Suricata у запропонованій архітектурі орієнтоване на пасивний режим виявлення мережевих загроз (IDS) з отриманням копії трафіку через port mirror на комутаторі. Такий підхід забезпечує повноцінне спостереження за ключовими потоками без впливу на доступність сервісів і без зміни логіки маршрутизації та сегментації. Suricata розгортається у вигляді віртуальної машини в головній філії, а її мережевий інтерфейс підключається до порту комутатора, на який подається дзеркальований трафік (mirror-target). На рівні гіпервізора мережевий адаптер сенсора налаштовується для приймання кадрів у проміскуїтетному режимі, що є обов’язковим для коректного аналізу копійованого трафіку.

Базовим сигнатурним набором прийнято ET Open – безкоштовний rule-set для IDS/IPS. Він використовується як загальний шар виявлення, тоді як локальні правила застосовуються для адаптації детекції під сегментацію мережі, критичні сервіси та прийняті політики доступу.

1) Прийняті змінні мережі (netvars) для правил і кореляції.

На основі підмереж, визначених у розділі 3 (CIDR /24), у конфігурації Suricata та файлі local.rules фіксуються такі змінні:

- MGMT_NET = 192.168.10.0/24
- USERS_NET = 192.168.20.0/24
- SERVERS_NET = 192.168.30.0/24
- GUEST_NET = 192.168.40.0/24
- DMZ_NET = 192.168.50.0/24
- VPN_NET = 192.168.60.0/24
- HOME_NET = [$MGMT_NET, $USERS_NET, $SERVERS_NET, $DMZ_NET, $VPN_NET]

Це забезпечує коректну інтерпретацію подій у логіці "внутрішній/зовнішній", з пріоритетом моніторингу потоків до серверного сегмента, до DMZ та трафіку від VPN-користувачів. GUEST_NET свідомо не

включено до HOME_NET, щоб не збільшувати обсяг нерелевантних спрацювань від гостьового доступу; за потреби цей сегмент доцільно покривати окремим профілем або вузькими локальними правилами. EXTERNAL_NET задається як: EXTERNAL_NET = !$HOME_NET.

2) Параметри захоплення трафіку з mirror-порту (IDS у пасивному режимі). Сенсор отримує L2-копію кадрів із mirror-target порту CSS326 та не виконує блокування на лінії. Прийнята схема мережевих інтерфейсів VM/SELKS:

- eth0 (MGMT) – керування, доступ до моніторингу та оновлень;
- eth1 (SNIFF) – підключений до mirror-target, без IP-адреси, PROMISC=on.

Для зниження ризику втрат на інтерфейсі eth1 прийнято базові системні налаштування:

- вимкнення offloading-функцій NIC (gro/lro/gso/tso = off);
- MTU = 1500 (якщо в trunk не використовується jumbo frames);
- тип захоплення: af-packet на eth1 як практичний варіант для високошвидкісного приймання mirror-трафіку в Linux VM.

Профіль af-packet прийнято як профіль що розрахований з запасом на пікові навантаження для мережі 10–40 хостів:

- threads: auto
- cluster-type: cluster_flow
- cluster-id: 99
- use-mmap: yes
- tpacket-v3: yes
- block-size: 1048576
- ring-size: 2048
- checksum-checks: auto.

3) Параметри журналювання Suricata (EVE JSON) під контур "monitoring + response".

Основним артефактом роботи сенсора визначено EVE JSON, який одночасно використовується для моніторингу та для подієвого парсингу у скрипті

реагування. Мінімальний набір типів подій EVE, достатній для детекції, кореляції та автоматизації:

- alert (обов’язково);
- flow і stats (контекст і контроль навантаження);
- dns, http, tls (метадані для ознак C2/фішингу/ексфільтрації);
- smtp (доцільно, якщо поштовий сервіс використовується в серверному сегменті);
- fileinfo (опційно; корисно для частини malware-сигнатур, але збільшує I/O);
- drop (потрібно лише для IPS-режиму; в базовому IDS може бути вимкнено).

Додаткові опції EVE, що спрощують кореляцію:

- community-id: true (стабільний ключ кореляції потоків);
- metadata: true (стандартизовані поля для нормалізації в скрипті реагування).

4) Rule-set’и та менеджмент правил (ET Open + локальні).

Базовий набір правил – ET Open. Оновлення та збирання правил виконується через suricata-update. Для адаптації під топологію та політики доступу використовуються локальні правила local.rules (asset-based детекція для критичних сервісів і сценарні правила). Для керованості профілю правил доцільно розділяти конфігураційні файли:

- enable.conf – увімкнення потрібних категорій/сигнатур;
- disable.conf – вимкнення шумних/нерелевантних;
- threshold.config – пороги для запобігання "alert storm";
- local.rules – локальні правила під конкретні сегменти та сервіси.

5) Сегментне профілювання (узгодження правил із сегментацією).

Оскільки сенсор фізично один і отримує mirror-трафік, сегментна специфіка реалізується через: загальні ET Open категорії як базовий шар та контекстні netvars з локальними правилами та умовами src/dst для $USERS_NET, $SERVERS_NET, $DMZ_NET, $VPN_NET. Прийняті акценти для категорій детекції:

- SERVERS (VLAN 30) – профіль "висока точність": scan/recon; brute force/auth; exploit/vulnerability attempts; SMB/RPC (як індикатор руху порушника всередині мережі); mail (за фактом використання); malware/C2; DNS/TLS.
- DMZ (VLAN 50) – профіль "периметр до публічних сервісів": web_server + exploit + scan; protocol anomalies / DoS (за наявності публічних HTTP(S)); malware/C2 (включно з вихідними з DMZ).
- VPN (VLAN 60) – "підсилений контроль входу": scan/recon і brute force; контроль доступу до SMB/RDP/SSH відповідно до дозволених сервісів; локальні правила для перевірки політик сегментації.
- USERS (VLAN 20) – "ознаки компрометації робочих станцій": malware/C2; DNS/TLS; web_client; внутрішній scan як маркер пост-компрометаційної активності; SMB як індикатор спроб доступу до серверних ресурсів.

3.4.2 Власні правила

Правило для виявлення індикатора brute force

```
alert tcp $HOME_NET any -> $SERVERS_NET [22,25,587,993,995,3389] (
  msg:"LOCAL Evidence trigger -- brute force to authentication services";
  flags:S;
  detection_filter:track by_src, count 20, seconds 60;
  classtype:attempted-user;
  sid:101001; rev:1;
)
```

Правило для

```
alert dns $HOME_NET any -> $EXTERNAL_NET any (
  msg:"LOCAL Evidence trigger -- DNS tunneling indicator (repeated long subdomain)";
  dns.query;
  pcre:"/^[A-Za-z0-9\-]{45,}\./";
```

```
  detection_filter:track by_src, count 10, seconds 120;
  classtype:policy-violation;
  sid:101002; rev:1;
)
```

Нижче запропоновано правила для реалізації керованого механізму збору доказів, який доповнює IDS-контур і формує матеріал для подальшої аналітики та вдосконалення сигнатур.

Запроваджується окремий контур "evidence capture" для випадків, коли фіксується агресивний шкідливий трафік. Під агресивним шкідливим трафіком (події з високою інтенсивністю або явними ознаками активної фази атаки) наприклад:

а) масове сканування критичних портів серверного сегмента (recon перед проникненням)

б) спроби експлуатації веб-сервісів у DMZ (шаблони traversal, доступ до чутливих шляхів, автоматизовані exploit-запити)

в) worm-подібне поширення в локальній мережі (наприклад інтенсивні звернення до SMB/RPC)

г) інтенсивні DNS-запити з ознаками тунелювання (DNS tunneling) як можливий канал керування або ексфільтрації

Мета контуру: у момент інциденту автоматично зафіксувати обмежений за часом фрагмент трафіку у форматі PCAP для подальшої детальної аналітики та уточнення правил.

Варіант 1 – кероване збереження PCAP засобами Suricata.

Цей варіант не потребує окремого "запуску сніфера", оскільки Suricata вже бачить трафік з mirror-інтерфейсу. Реалізація базується на тому, що правило при спрацюванні "тегує" сесію або хост, а вихід pcap-log зберігає лише помічені пакети.

Тригер-правило (експлуатація DMZ з тегуванням сесії):

```
alert http $EXTERNAL_NET any -> $DMZ_NET [80,443] (
  msg:"LOCAL Evidence trigger – DMZ exploit attempt, tag session for PCAP";
```

```
  flow:to_server,established;
  http.uri;
  pcre:"/(\.\.\/){2,}|\/(etc\/passwd|wp-admin|phpmyadmin|\.git\/|\.env)(\/|$)/Ui";
  tag:session,120,seconds;
  classtype:web-application-attack;
  sid:101003; rev:1;
)
```

Базова логіка налаштування збереження:

а) вмикається pcap-log у режимі "тільки умовно" (тільки те, що позначено тегом правила)

б) задається ротація файлів та обмеження дискового простору

в) у результаті PCAP формується лише тоді, коли спрацював тригер, і лише протягом заданого часу (наприклад 120 секунд)

Варіант 2 – правило у якості тригера для скрипту, який запускає tcpdump і зберігає PCAP

У цьому варіанті вихідні дані тригера обробляються віртуальною машиною реалізується через стандартний шлях подій: Suricata записує alert у EVE JSON, а скрипт на VM читає EVE JSON і, за потреби, запускає короткочасний сніфер.

Тригер-правило (приклад: агресивне сканування до SERVERS)

```
alert tcp $HOME_NET any -> $SERVERS_NET [22,135,139,445,3389] (
  msg:"LOCAL Evidence trigger – aggressive scan to server services";
  flags:S;
  detection_filter:track by_src, count 40, seconds 60;
  classtype:attempted-recon;
  sid:101004; rev:1;
)
```

Логіка запуску скрипта і сніфера:

а) скрипт працює як сервіс systemd на Linux VM (та сама VM, де Suricata або SELKS)

б) скрипт прослуховує потік подій через tail файлу eve.json

в) якщо event_type=alert і alert.signature_id дорівнює одному з "evidence SID" (наприклад 101001-101004) тоді:

1. витягується src_ip, timestamp, за потреби dest_ip і dest_port
2. застосовуються запобіжники (white-list, дедуплікація, обмеження частоти запусків)
3. запускається tcpdump на інтерфейсі eth1 (mirror), з фільтром host src_ip, на заданий час (наприклад 60-180 секунд)
4. PCAP зберігається з іменем, що містить час і джерело, та з ротацією за розміром/кількістю файлів

Критичні запобіжники для проекту:

а) rate limit – заборона запуску нового захоплення від того ж src_ip частіше, ніж 1 раз на X хвилин

б) ліміт диску – квота на каталог PCAP і автоматичне видалення найстаріших файлів

в) white-list – виключення довірених джерел та службових адрес

г) політика збереження – фіксований термін ретенції та контроль доступу до PCAP, оскільки PCAP може містити чутливі дані

Перевага ж першого підходу – мінімальна затримка та менший ризик деградації продуктивності, оскільки немає паралельного знімання трафіку окремим процесом.

Узгодження з реагуванням на MikroTik

Даний контур збору PCAP не замінює блокування, а доповнює його:

а) при спрацюванні агресивного тригера виконується захоплення трафіку для аналітики

б) паралельно або після виконання критеріїв блокування скрипт додає src_ip до suricata-block з timeout

в) блокування реалізується статичним правилом firewall, а скрипт керує лише вмістом address-list

Таблиця 3.2

Тригерні правила та дії збору доказів і реагування

SID	Ознака загрози	Дія PCAP	Дія MikroTik	Параметри
101001	експлуатація DMZ (HTTP traversal, доступ до чутливих шляхів)	зберегти PCAP з mirror-інтерфейсу для сесії, 120 с	додати src_ip в suricata-block	block timeout 60 хв, дедуплікація 10 хв
101002	агресивне сканування портів SERVERS	запустити tcpdump на eth1 з фільтром host src_ip, 120 с	додати src_ip в suricata-block	block timeout 15 хв, ескалація до 60 хв
101003	brute force до сервісів автентифікації	запустити tcpdump на eth1 з фільтром host src_ip, 180 с	додати src_ip в suricata-block	block timeout 30 хв, ескалація до 120 хв
101004	DNS tunneling (довгі піддомени, повторюваність)	зберегти PCAP тільки DNS трафіку host src_ip, 180 с	додати src_ip в suricata-watch або quarantine	watch 2 год або quarantine 4 год, блокування при повторі
ET Open malware/C2	malware/C2 (botcc, trojan, compromised)	запустити tcpdump на eth1 з фільтром host src_ip, 300 с	додати src_ip в suricata-quarantine	quarantine 4 год, ескалація до block 24 год при повторі

3.4.3 Ефективний сценарій протидії malware/C2

Для протидії malware/C2 доцільно застосувати обережну багатоступеневу модель реагування, оскільки одиничні сигнатурні спрацювання можуть відповідати як реальній компрометації, так і легітимним, але нетиповим

з'єднанням. Запропонований сценарій поєднує три компоненти: виявлення і кореляцію подій Suricata, керовану локалізацію інциденту на MikroTik через quarantine, а також автоматизований збір доказів для подальшого уточнення правил.

Виявлення та критерії тригера

Підставою для запуску сценарію є події Suricata типу alert, які відносяться до категорій malware, trojan, botnet, C2 або compromised, або мають підвищений рівень критичності. Щоб зменшити ризик хибних блокувань, тригер формалізується як одна з умов:

а) прямий тригер:

1. спрацювання сигнатури malware/C2 з високою критичністю або пріоритетом, що відповідає активній фазі шкідливої взаємодії

б) кореляційний тригер:

1. malware/C2 alert у поєднанні з додатковою ознакою, наприклад підозрілим DNS патерном, нетиповим SNI у TLS або повторюваними короткими сесіями до зовнішнього вузла
2. як мінімальна кореляція приймається правило "дві релевантні події протягом одного часового вікна" для одного src_ip

За результатом виконання умов src_ip визначається як ймовірно скомпрометований хост, для якого застосовується режим локалізації, а не негайне повне блокування.

Первинна дія "quarantine"

Первинна реакція реалізується як переведення джерела подій у режим quarantine шляхом додавання src_ip у address-list suricata-quarantine на MikroTik RB4011 з параметром timeout 2-4 години. Тайм-аут визначається як компроміс між необхідністю швидко припинити потенційно шкідливі зовнішні комунікації та потребою зберегти мінімальну працездатність робочого місця для виконання базових завдань і діагностики.

Мета quarantine полягає у тому, щоб зупинити або обмежити можливий канал керування C2 та ексфільтрацію, мінімізувати вплив на внутрішні сервіси,

необхідні для роботи і розслідування та не створити відмову доступу через одиничне або сумнівне спрацювання.

Політика quarantine на MikroTik

Політика quarantine реалізується статичними правилами firewall, які активуються для джерел з address-list suricata-quarantine. У проекті доцільно застосувати модель "deny by default" для зовнішніх з'єднань з дозволом мінімально необхідних сервісів. Приклад логіки політики:

а) обмеження виходу в Інтернет:

1. блокування всіх вихідних з'єднань з quarantine хоста до EXTERNAL_NET
2. за потреби окремий дозвіл лише на доступ до визначених адрес оновлень або корпоративних хмарних сервісів, якщо це погоджено політикою

б) мінімально необхідні дозволи:

1. дозвіл DNS тільки до корпоративного резолвера, щоб уникнути обходу через сторонні DNS
2. дозвіл доступу до внутрішніх ресурсів, необхідних для роботи або усунення інциденту, наприклад файлового сервера, доменних служб, системи оновлення, інструментів адміністрування
3. заборона прямого доступу до сегмента керування MGMT, якщо це не потрібно для роботи

в) обмеження бічного поширення:

1. заборона або суттєве обмеження доступу quarantine хоста до критичних сервісів серверного сегмента, окрім мінімально необхідних
2. за потреби окремі правила для блокування SMB або інших протоколів, що можуть використовуватися для розповсюдження шкідника всередині мережі

У такий спосіб quarantine виконує роль контрольованої локалізації, не відключаючи фізично порт і не змінюючи динамічно набір правил на маршрутизаторі, а використовуючи статичні правила і динамічні списки.

Ескалація до повного блокування

Якщо протягом інтервалу quarantine спостерігається повторення malware/C2 подій або збільшується їх інтенсивність, виконується ескалація. Критерій ескалації задається як повторювані спрацювання для того ж src_ip у межах заданого вікна, або поява додаткових підтверджуючих ознак. У випадку ескалації src_ip переноситься або дублюється у suricata-block з довшим timeout, наприклад 12-24 години. При цьому політика блокування застосовується як повне відкидання трафіку до зовнішніх і, за потреби, частини внутрішніх напрямів, що повністю припиняє можливу шкідливу активність.

Ескалація має два ефекти:

а) припинення будь-яких комунікацій, що можуть підтримувати керування або ексфільтрацію;

б) фіксація інциденту у керованому стані для подальшого реагування адміністратора;

Evidence capture для уточнення сигнатур

Паралельно із переведенням у quarantine запускається контур збору доказів у вигляді короткочасного захоплення трафіку у форматі PCAP. Захоплення виконується на віртуальній машині, яка приймає mirror трафік, і прив'язується до src_ip, що ініціював подію. Збір трафіку обмежується у часі (наприклад 180-300 секунд) та має обмеження за частотою запуску, щоб уникнути надмірного споживання дискового ресурсу. Отриманий PCAP використовується для поглибленої аналітики, відбору стійких індикаторів компрометації та подальшого уточнення локальних правил виявлення, що підвищує якість детекції для конкретної топології та профілю трафіку підприємства.

Узагальнений алгоритм сценарію malware/C2

а) Suricata формує alert подію, що відповідає malware/C2 або кореляції ознак

б) скрипт реагування відбирає подію, перевіряє white-list, виконує дедуплікацію і порогові умови

в) src_ip додається до suricata-quarantine з timeout 2-4 години

г) одночасно запускається захоплення PCAP для src_ip на mirror інтерфейсі на заданий час

ґ) у разі повторних або підсилених ознак malware/C2 протягом quarantine виконується ескалація до suricata-block з timeout 12-24 години

д) факт дій і параметри фіксуються у журналі скрипта та, за потреби, у журналі RouterOS для аудиту і подальшого розслідування.

ВИСНОВКИ

У кваліфікаційній роботі розглянуто та вирішено практично важливе та актуальне завдання побудови захищеної корпоративної мережі для підприємства малого та середнього бізнесу з використанням обладнання MikroTik та програмного комплексу Suricata. За результатами проведеного дослідження можна зробити такі висновки:

1. Проаналізовано сучасний стан і тенденції розвитку корпоративних комп'ютерних мереж. Встановлено, що для стабільної та безпечної роботи мережі дедалі більшого значення набувають сегментація, централізоване керування та засоби мережевого виявлення загроз. Також в ході дослідження показано, що лише периметрового захисту зазвичай недостатньо для протидії сучасним атакам.

2. Узагальнено основні загрози інформаційній безпеці в мережах малого та середнього бізнесу, зокрема scan-атаки, brute force, наслідки фішингу та інциденти типу ransomware. Зроблено висновок, що ефективний захист потребує не тільки фільтрації на периметрі, а й контролю трафіку всередині мережі та розділення її на логічні сегменти.

3. Виконано порівняльний аналіз обладнання для SMB-сегмента. Обґрунтовано доцільність вибору платформи MikroTik як технічно і економічно вигідного рішення, яке дає широкий набір мережевих функцій навіть у базових моделях (маршрутизація, VLAN, VPN, firewall, керування трафіком).

4. Пояснено доцільність використання Suricata як інструмента IDS/IPS у корпоративній мережі. Визначено, що Suricata забезпечує глибокий аналіз мережевого трафіку та формує події безпеки, які неможливо отримати лише вбудованими засобами RouterOS на рівні стандартного фаєрвола.

5. Розроблено метод побудови захищеної мережі на основі поєднання MikroTik та Suricata. Метод включає логічну сегментацію через VLAN, організацію маршрутизації між сегментами, налаштування VPN-доступу та пасивне підключення IDS за допомогою дзеркалювання трафіку. Такий підхід підвищує керованість і рівень безпеки без надмірного ускладнення мережевої

схеми.

6. Спроектовано логічну і фізичну архітектуру корпоративної мережі підприємства: визначено зони безпеки, розміщення обладнання та взаємодію між компонентами. Запропоновано правила виявлення атак і сценарії автоматизованого реагування, що дає можливість зменшити час між виявленням інциденту та застосуванням контрзаходів.

Отримані результати мають практичну цінність і можуть застосовуватися під час проектування, модернізації та експлуатації корпоративних мереж малого та середнього бізнесу. Запропонований метод є доцільним для впровадження в реальних умовах, оскільки поєднує сучасні підходи до захисту з техніко-економічною ефективністю та не потребує дорогих спеціалізованих рішень.

Подальші дослідження можна спрямувати на розширення механізмів автоматизованого реагування, інтеграцію з системами централізованого аналізу подій (SIEM), а також на практичну перевірку ефективності методу в багатофілійних мережах.

ПЕРЕЛІК ПОСИЛАНЬ

1. Tanenbaum A., Feamster N., Wetherall D. Computer Networks. 6th ed. Pearson, 2020.
2. Kurose J., Ross K. Computer Networking: A Top-Down Approach. 8th ed. Pearson, 2021.
3. Peterson L., Davie B. Computer Networks: A Systems Approach. Open Textbook Library, 2019.
4. Panko R. Corporate Computer and Network Security. 5th ed. Pearson, 2021.
5. Kizza J. M. Guide to Computer Network Security. 6th ed. Springer, 2024.
6. Cisco. Enterprise Campus Design (BRKENS-2031). Cisco Live, 2023.
7. Al-shawi M., Laurent A. Designing for Cisco Network Service Architectures (ARCH) Foundation Learning Guide: CCDP ARCH 300-320. 4th ed. Cisco Press, 2016.
8. Enterprise WAN Reference Architecture. Juniper Networks, 2023. URL: https://www.juniper.net/documentation/us/en/software/nce/enterprise-wan-ref-architecture/enterprise-wan-ref-architecture.pdf (date of access: 08.10.2025).
9. Prajapati D., Bowman J., Suvarna N. Designing Real-World Multi-Domain Networks. Hoboken, NJ : Cisco Press, 2024. 496 p.
10. Kizza J. M. Guide to Computer Network Security. 6th ed. Springer, 2024. 672 p.
11. Panko R. Corporate Computer and Network Security. 5th ed. Pearson, 2021. 775 p.
12. Milmo D. *Global ransomware payments plunge by a third amid crackdown.* The Guardian. 2025. URL: https://www.theguardian.com/technology/2025/feb/05/global-ransomware-payments-plunge-by-a-third-amid-crackdown (date of access: 16.10.2025).
13. Налаштування обладнання MikroTik — як настроїти різні параметри та функціонал обладнання MikroTik. *DEPS.* URL: https://deps.ua/ua/knowegable-base/samples-of-the-technical-solutions/9145.html (дата звернення: 16.10.2025).

14. VLAN. *MikroTik Help.* URL: https://help.mikrotik.com/docs/spaces/ROS/pages/88014957/VLAN (дата звернення: 16.10.2025).
15. Firewall. *MikroTik Help.* URL: https://help.mikrotik.com/docs/spaces/ROS/pages/250708066/Firewall (дата звернення: 16.10.2025).
16. Building Advanced Firewall. *MikroTik Help.* URL: https://help.mikrotik.com/docs/spaces/ROS/pages/328513/Building%2BAdvanced%2BFirewall (дата звернення: 23.10.2025).
17. Frolov A. Router Firewall Configuration: Step-by-Step Guide. *HackMag.* 09.06.2024. URL: https://hackmag.com/devops/mikrotik-firewall (дата звернення: 23.10.2025).
18. Open Information Security Foundation. Suricata Documentation. URL: https://docs.suricata.io/ (дата звернення: 23.10.2025).
19. Manualzz team. Suricata User Guide: Command Line Options. *Manualzz.* URL: https://manualzz.com/doc/o/n57fo/suricata-user-guide-command-line-options (дата звернення: 23.10.2025).
20. Luo C. Open Source IDS/IPS Suricata for Beginners. *DEV Community.* URL: https://dev.to/carrie_luo1/open-source-idsips-suricata-for-beginners-5d42 (дата звернення: 23.10.2025).
21. Suricata IDS Configuration: How to Detect Network Intrusions and Malware. *Markaicode.* URL: https://markaicode.com/suricata-ids-configuration-network-intrusion-detection/ (дата звернення: 23.10.2025).
22. SEC TTL. Understanding and Writing Suricata IDS Rules. *b4y.dev.* URL: https://b4y.dev/posts/ids-suricata-rules/ (дата звернення: 23.10.2025).
23. Mikrocata2SELKS: Integrating Mikrotik with Suricata for Network Security. *Sec-TTL.* URL: https://www.sec-ttl.com/mikrocata2selks-integrating-mikrotik-with-suricata-for-network-security/ (дата звернення: 23.10.2025).

24. elmaxid. ips-mikrotik-suricata. GitHub. URL: https://github.com/elmaxid/ips-mikrotik-suricata (дата звернення: 23.10.2025).
25. Suricata IDS/IPS integration with Mikrotik (now with OSSEC). *MikroTik Forum.* URL: https://forum.mikrotik.com/t/suricata-ids-ips-integration-with-mikrotik-now-with-ossec/101160 (дата звернення: 06.11.2025).
26. SIA "Mikrotīkls". IPS/IDS with SELK. *MikroTik Forum.* URL: https://forum.mikrotik.com/t/ips-ids-with-selk/164268 (дата звернення: 06.11.2025).
27. Cisco. Enterprise Campus Design (BRKENS-2031). Cisco Live, 2023. URL: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2023/pdf/BRKENS-2031.pdf (дата звернення: 06.11.2025).
28. Enterprise WAN Reference Architecture. Juniper Networks, Inc., 2023. URL: https://www.juniper.net/documentation/us/en/software/nce/enterprise-wan-ref-architecture/ (дата звернення: 06.11.2025).
29. SIA "Mikrotīkls". VLAN. *MikroTik Help.* URL: https://help.mikrotik.com/docs/spaces/ROS/pages/88014957/VLAN (дата звернення: 12.11.2025).
30. Ghazi D. S., Hamid H. S., Zaiter M. J., Behadili A. S. G. *Performance and efficacy of Snort versus Suricata in intrusion detection: A benchmark analysis.* 2024. URL: https://pubs.aip.org/aip/acp/article/3232/1/020024/3316611/Performance-and-efficacy-of-Snort-versus-Suricata (дата звернення: 12.11.2025).
31. Open Information Security Foundation. Public Data Sets. *Suricata Users Guide*. URL: https://docs.suricata.io/en/latest/public-data-sets.html (date of access: 12.11.2025).

Додаток А

Порівняння мережевого обладнання MikroTik та конкуруючих рішень

Таблиця А.1

Порівняння бюджетного маршрутизатора hAP lite з аналогом TP-Link

Параметр	MikroTik hAP lite (RB941-2nD)	TP-Link TL-WR841N	Коментар
Клас пристрою	Початковий SOHO маршрутизатор з функціями L3	Бюджетний домашній Wi-Fi маршрутизатор	TP-Link орієнтований на домашнього користувача, MikroTik – на SOHO/SMB
Операційна система	RouterOS (Level 4)	Пропрієтарна прошивка виробника	RouterOS надає корпоративний функціонал (VLAN, тунелі, OSPF) навіть на бюджетному пристрої
CPU / ОЗП	650 МГц / 32 МБ	~500-650 МГц / 32 МБ (залежить від ревізії)	Апаратна платформа схожа, але ефективність використання ресурсів різна

Продовження таблиці А.1

Ethernet-порти	4 × 10/100 Мбіт/с	4 × 10/100 Мбіт/с LAN + 1 × 10/100 WAN	Фізичні інтерфейси ідентичні за швидкістю
Wi-Fi	2,4 ГГц 802.11b/g/n (MIMO 2×2)	2,4 ГГц 802.11b/g/n (MIMO 2×2)	Обидва пристрої забезпечують базове покриття зі швидкістю до 300 Мбіт/с
Можливості VPN	IPsec, OpenVPN, L2TP, PPTP, WireGuard	Обмежені (Pass-through або прості тунелі)	hAP lite дозволяє організувати повноцінний захищений канал для віддаленого працівника
Орієнтовна ціна	~1 100 грн	~750 грн	Різниця в ціні незначна, але функціональний розрив колосальний на користь MikroTik

Таблиця А.2

Порівняння філійного маршрутизатора RB2011UiAS з аналогом Cisco

Параметр	**MikroTik RB2011UiAS-2HnD-IN**	**Cisco RV260W**	**Коментар**
Клас пристрою	Багатопортовий маршрутизатор для філій	VPN-маршрутизатор для малого бізнесу	Cisco RV серія є прямим конкурентом у ніші SMB
Кількість портів	5 × Fast Ethernet + 5 × Gigabit Ethernet + 1 × SFP	4 × Gigabit Ethernet LAN + 1 × Gigabit WAN + 1 × SFP (Combo)	RB2011 пропонує більше фізичних портів для прямого підключення робочих місць
Wi-Fi	2,4 ГГц 802.11b/g/n	802.11ac Wave 2 (2,4 + 5 ГГц)	Cisco має сучасніший радіомодуль, RB2011 обмежений стандартом 802.11n
Гнучкість налаштування	Висока (RouterOS L5: скрипти, Netwatch, черги)	Середня (Web-інтерфейс, фіксовані сценарії)	RouterOS дозволяє реалізувати нестандартні схеми резервування каналів
SFP інтерфейс	Окремий слот SFP (1 Гбіт/с)	SFP/RJ-45 Combo порт	Наявність SFP у MikroTik спрощує підключення до оптоволокна провайдера

Продовження таблиці А.2

PoE можливості	PoE in (Ether1) / PoE out (Ether10)	Зазвичай відсутнє PoE out	MikroTik дозволяє живити зовнішню антену або камеру без додаткового адаптера
Орієнтовна ціна	~5 000 грн	~17 000 грн	MikroTik утричі дешевший, пропонуючи більшу кількість портів і гнучкість

Таблиця А.3

Порівняння продуктивного маршрутизатора RB4011 з аналогом Ubiquiti

Параметр	**MikroTik RB4011iGS+5HacQ2HnD-IN**	**Ubiquiti UniFi Dream Machine Pro (UDM-Pro)**	**Коментар**
Клас пристрою	Потужний маршрутизатор ядра мережі	Універсальний шлюз безпеки з контролером (SDN)	Обидва пристрої розраховані на гігабітні швидкості та десятки/сотні клієнтів
Процесор	4 ядра × 1.4 ГГц (Cortex-A15)	4 ядра × 1.7 ГГц (Cortex-A57)	Обидва процесори забезпечують високу продуктивність маршрутизації та VPN

Продовження таблиці А.3

Керування	Локальне (WinBox/CLI) або централізоване (DUDE)	Централізоване (UniFi Controller), хмарне	Ubiquiti робить ставку на візуалізацію (GUI), MikroTik – на детальний контроль параметрів
Вбудований Wi-Fi	Є (Дводіапазонний AC, 4×4 MIMO у 5 ГГц)	Відсутній (потрібні зовнішні точки доступу)	RB4011 є самодостатнім пристроєм, UDM-Pro вимагає докупівлі точок доступу
Порти uplink	1 × SFP+ (10 Гбіт/с)	2 × SFP+ (10 Гбіт/с) LAN/WAN	MikroTik підтримує 10G підключення до ядра або сервера
Безпека (IDS/IPS)	Реалізується зовнішніми засобами (наприклад, Suricata)	Вбудована система (Threat Management)	Вбудована IPS у Ubiquiti простіша, але схема "MikroTik + Suricata" гнучкіша
Орієнтовна ціна	~12 000 грн	~20 000 грн	Рішення на MikroTik значно дешевше, враховуючи наявність вбудованого Wi-Fi модуля

Таблиця А.4

Порівняння точок доступу wAP ac / cAP lite з аналогом Ubiquiti

Параметр	**MikroTik wAP ac / cAP lite**	**Ubiquiti UniFi AC Lite (UAP-AC-LITE)**	**Коментар**
Позиціювання	wAP ac: Універсальна/Вулична; cAP lite: Бюджетна офісна	Стандартна стельова точка доступу для офісу	Ubiquiti є еталоном у цьому сегменті, MikroTik пропонує вузькоспеціалізовані рішення
Контролер Wi-Fi	CAPsMAN (вбудований у будь-який RouterOS)	UniFi Controller (потрібен ПК, сервер або Cloud Key)	MikroTik не вимагає додаткових витрат на апаратний контролер
Захист корпусу	wAP ac: IP54 (всепогодний); cAP lite: пластик	Тільки для приміщень (Indoor)	wAP ac можна встановлювати на фасаді будівлі без додаткового захисту
Швидкість Wi-Fi	wAP ac: AC1200; cAP lite: N300	AC1200 (867+300 Мбіт/с)	wAP ac є ідентичним по швидкості; cAP lite – бюджетна альтернатива
Живлення	PoE (Passive / 802.3af/at)	PoE (Passive 24V або 802.3af у нових ревізіях)	Обидва бренди легко інтегруються в мережу PoE-комутаторів
Орієнтовна ціна	wAP ac: ~3 500 грн cAP lite: ~1 150 грн	~4 000 грн	MikroTik дозволяє зекономити, при використанні бюджетних cAP lite для "сліпих зон"

Додаток Б

Схема потоків трафіку та подій

Таблиця Б.1

Схема потоків трафіку та логів (Mirror – Suricata – моніторинг/реагування)

Ідентифікатор потоку	Джерело -> призначення	Що передається	Де реалізовано	Інтерфейс/канал	Формат/протокол	Умови/частота	Результат/призначення
F1	VLAN USERS <-> VLAN SERVERS	робочий трафік до файлового/поштового сервісів	RB4011 (між-VLAN маршрутизація)	trunk RB4011 <-> CSS326 + access-порти	L3/L4, прикладні протоколи	постійно	основний бізнес-трафік; контроль доступу визначається політиками
F2	VLAN USERS/VLAN GUEST -> Інтернет	вихідні з'єднання (у т.ч. до зовнішньої CRM)	RB4011	WAN	NAT (masquerade) + маршрутизація	постійно	доступ до Інтернету; окремі обмеження для GUEST
F3	Інтернет – VLAN DMZ	вхідні/вихідні з'єднання до публічних сервісів	RB4011	WAN – DMZ через CSS326	dst-nat + filter	за потреби	контрольована публікація сервісів; мінімізація доступу до внутрішніх сегментів
F4	Віддалені користувачі -> RB4011	VPN-тунель (встановлення сесії)	RB4011	WAN	VPN-протокол (обраний у 3.2.3)	за потреби	захищений канал; автентифікація та авторизація користувачів
F5	VPN-сегмент -> внутрішні VLAN	доступ віддалених користувачів до ресурсів	RB4011 (між-VLAN)	логічний інтерфейс VPN + VLAN-інтерфейси	L3/L4	за потреби	рольовий доступ; окремі політики для VPN-клієнтів
M1	CSS326 -> порт сенсора	копія (дзеркало) трафіку вибраних портів/напрямів	CSS326 (mirror)	mirror-target порт -> NIC хоста Suricata	L2 копія кадрів	постійно під час mirror	видимість трафіку для Suricata без включення в розрив
M2	mirror-target порт -> Suricata	дзеркальований трафік на аналіз	Suricata VM/SELKS	NIC (promiscuous)	захоплення пакетів	постійно	декодування протоколів, відновлення потоків, первинна класифікація
L1	Suricata -> локальне сховище логів	події детекції та метадані потоків	Suricata VM/SELKS	локальний диск VM	EVE JSON + службові логи	постійно	формування записів alert/flow/dns/http/tls та статистики

Продовження таблиці Б.1

L2	Suricata -> система моніторингу	доставка подій для візуалізації та кореляції	SELKS/ELK або інший стек	локально або через агент	filebeat/syslog/Logstash (залежно від реалізації)	постійно	централізований перегляд, фільтрація, ретенція та звітність
L3	Suricata -> скрипт реагування	потік подій для прийняття рішень	вузол Suricata або окремий сервіс	читання EVE JSON (tail) / socket	JSON-парсинг	постійно/майже realtime	нормалізація подій, пороги, правила запуску реагування
R1	скрипт реагування -> RB4011	керувальна команда блокування джерела	RB4011	керувальний канал	MikroTik API / SSH (обраний спосіб)	подієво	додавання IP до address-list з таймаутом
R2	RB4011 firewall -> мережевий трафік	фактичне блокування/обмеження	RB4011	filter/input/forward	правила firewall з address-list	постійно	відсікання сканування, brute force та спроб експлуатації; локалізація інциденту
A1	RB4011 -> моніторинг/логи	аудит застосованих дій	RB4011	syslog/журнал RouterOS	текстові записи	подієво	підтвердження застосування блокування; основа для аналізу хибних спрацювань
T1	усі компоненти -> часовий сервіс	синхронізація часу	RB4011, CSS326, Suricata VM	NTP	NTP	постійно	коректна кореляція подій у часі та відтворюваність вимірювань

ПРЕЗЕНТАЦІЯ

ВИСНОВКИ

У кваліфікаційній роботі розглянуто та вирішено практично важливе та актуальне завдання побудови захищеної корпоративної мережі для підприємства малого та середнього бізнесу з використанням обладнання MikroTik та програмного комплексу Suricata. За результатами проведеного дослідження можна зробити такі висновки:

1. Проаналізовано сучасний стан і тенденції розвитку корпоративних комп'ютерних мереж. Встановлено, що для стабільної та безпечної роботи мережі дедалі більшого значення набувають сегментація, централізоване керування та засоби мережевого виявлення загроз. Також в ході дослідження показано, що лише периметрового захисту зазвичай недостатньо для протидії сучасним атакам.

2. Узагальнено основні загрози інформаційній безпеці в мережах малого та середнього бізнесу, зокрема scan-атаки, brute force, наслідки фішингу та інциденти типу ransomware. Зроблено висновок, що ефективний захист потребує не тільки фільтрації на периметрі, а й контролю трафіку всередині мережі та розділення її на логічні сегменти.

3. Виконано порівняльний аналіз обладнання для SMB-сегмента. Обґрунтовано доцільність вибору платформи MikroTik як технічно і економічно вигідного рішення, яке дає широкий набір мережевих функцій навіть у базових моделях (маршрутизація, VLAN, VPN, firewall, керування трафіком).

4. Пояснено доцільність використання Suricata як інструмента IDS/IPS у корпоративній мережі. Визначено, що Suricata забезпечує глибокий аналіз мережевого трафіку та формує події безпеки, які неможливо отримати лише вбудованими засобами RouterOS на рівні стандартного фаєрвола.

5. Розроблено метод побудови захищеної мережі на основі поєднання MikroTik та Suricata. Метод включає логічну сегментацію через VLAN, організацію маршрутизації між сегментами, налаштування VPN-доступу та пасивне підключення IDS за допомогою дзеркалювання трафіку. Такий підхід підвищує керованість і рівень безпеки без надмірного ускладнення мережевої

схеми.

6. Спроектовано логічну і фізичну архітектуру корпоративної мережі підприємства: визначено зони безпеки, розміщення обладнання та взаємодію між компонентами. Запропоновано правила виявлення атак і сценарії автоматизованого реагування, що дає можливість зменшити час між виявленням інциденту та застосуванням контрзаходів.

Отримані результати мають практичну цінність і можуть застосовуватися під час проектування, модернізації та експлуатації корпоративних мереж малого та середнього бізнесу. Запропонований метод є доцільним для впровадження в реальних умовах, оскільки поєднує сучасні підходи до захисту з техніко-економічною ефективністю та не потребує дорогих спеціалізованих рішень.

Подальші дослідження можна спрямувати на розширення механізмів автоматизованого реагування, інтеграцію з системами централізованого аналізу подій (SIEM), а також на практичну перевірку ефективності методу в багатофілійних мережах.