**COMPUTER SYSTEMS AND NETWORKS**

**Vol. 7, No. 1, 2025**

DOI: https://doi.org/10.23939/csn2025.01.119

**УДК 004: 054**

# КОМПЛЕКСНА СИСТЕМА БЕЗПЕКИ РЕГІОНАЛЬНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ ЕТАЛОННОЇ МОДЕЛІ OSI ТА МОДЕЛІ "ГЛИБОКОГО ЗАХИСТУ"

**В. Б. Дудикевич, Г. В. Микитин, Т. Є. Мурак**

Національний університет "Львівська політехніка",
кафедра захисту інформації
*E-mail: valerii.b.dudykevych@lpnu.ua, halyna.v.mykytyn@lpnu.ua, taras.murak.mkbst.2024@lpnu.ua*



**Стратегія Агентства ЄС з питань кібербезпеки (ENISA) і Стратегія кібербезпеки України спрямовані на розвиток і практичну реалізацію нових підходів, методологій, технологій у просторі подолання кібербезпекових викликів предметних сфер інфраструктури суспільства, зокрема за вектором забезпечення конфіденційності даних в корпоративних мережах.**

**Проведено аналітичний огляд відомих методів і технологій безпеки корпоративних мереж у просторі: безпечного обміну даними і безпечного зберігання; вдосконалення моделей, засобів безпеки та систем захисту інформації; використання методів машинного навчання та нейромережевих технологій для виявлення аномалій в корпоративних мережах.**

**Наведено комплексну системи безпеки регіональної корпоративної мережі (РКМ) на основі семирівневої моделі OSI, моделі "глибокого захисту", концепції "загроза – технології безпеки", яка є універсальною для різних мережевих топологій та уможливлює проєктування систем захисту інформації на кожному рівні OSI відповідно до нормативного забезпечення.**

**Розроблено програмне забезпечення криптографічного захисту інформації транспортного мережевого рівня OSI на основі симетричного блокового алгоритму AES-256 засобами мови програмування Python, що практично реалізується на базі протоколу OpenVPN і технології транспортного рівня TLS та забезпечує високий рівень конфіденційності інформації в регіональних корпоративних мережах.**

**Ключові слова: корпоративна мережа, еталонна модель OSI, модель глибокого захисту, комплексна система безпеки, випадкові та цілеспрямовані загрози, транспортний рівень, шифрування даних.**

## Вступ

Ефективна співпраця України з Європейським союзом у просторі кібербезпеки на рівні взаємодії Держспецзв'язку, Національного координаційного центру кібербезпеки з Агенством кібербезпеки ENISA є фундаментом для розвитку кібердіалогів Україна – ЄС, зокрема у сегменті мережевої та інформаційної безпеки, які цілеспрямовані на комплексну протидію кіберзагрозам і забезпечення високого рівня кіберстійкості та кіберзахисту [1, 2]. Актуальним є розгортання векторів Директиви ЄС NIS 2 [3], яка належить до компаній критичної інфраструктури і систем, зокрема в

секторах енергетики, транспорту, цифрової інфраструктури, управління ІКТ-послугами, екології, медицини, космосу. Відповідність стандарту ДСТУ ISO/IEC 27001:2023 (Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги ISO/IEC 27001:2022, IDT), які розгортають структурований підхід до кібербезпеки, допоможуть українським компаніям, що співпрацюють на ринку ЄС, відповідати вимогам NIS 2 щодо сповіщення за інцидентами, створення політики компанії, розроблення плану безперервності та бізнесу; відповідальний вибір партнерства, багатофакторна аутентифікація; тренінги з кібербезпеки. Прогресивні тенденції Міжнародного кіберпростору є підґрунтям для розвитку кібердіалогів Україна – ЄС з метою створення універсальної платформи з кібербезпеки, орієнтованої на протидію загрозам в умовах гібридної війни, створенню механізмів реалізації захисту і новітніх технологій безпеки, зокрема нових підходів у сегменті безпеки регіональних корпоративних мереж.

**Огляд літературних джерел**

У праці [4] розглянуто комплексну систему безпеки інформаційних мереж, як одного з рівнів інформаційних технологій на основі концепції “об’єкт – загроза – захист”. У просторі комплексного захисту корпоративних мереж у праці [5] розглянуто механізми мережевої безпеки та відповідний інструментарій. У статті [6] проаналізовано відомі загрози та вразливості інформаційним мережам і методи протидії їм, а також запропоновано ефективні підходи до забезпечення безпеки інформаційно-телекомунікаційних мереж на основі ефективних методів виявлення вразливостей. Сегмент удосконалення систем захисту інформації в комп’ютерних мережах розвинуто на рівні застосування мережевих екранів “Fortigate” та “Cisco ASA” [7]. Напрацьовані тенденції мережевої безпеки на основі моделі OSI, зокрема у праці [8] досліджено основні атаки на канальний рівень комп’ютерних мереж та способи їх нейтралізації за допомогою програмних інструментів мережевого обладнання компанії Cisco; у працях [9, 10] розглянуто загрози комп’ютерним мережам на фізичному, канальному, мережевому, транспортному і прикладному рівнях та проведено аналіз методів і технологій їх захисту. У праці [11] наведено короткий аналіз використання методів машинного навчання та нейромережевих технологій для виявлення аномалій в корпоративних мережах і на цій основі запропоновано метод на основі нейромереж з LSTM та FFN-архітектурами та алгоритмічно-програмну реалізацію для виявлення програмно-технічних впливів на системи критичної інфраструктури в умовах кібервійни. Комплексний підхід до оптимального вибору систем мережевої безпеки підприємства на основі об’єктивного порівняння різних критеріїв з урахуванням впливу кожного з них зокрема на загальний рівень захищеності та надійність захисту наведено у праці [12]. Автори статті [13] охарактеризували найпоширеніші методи інтернет-атак та інших загроз в сучасних комп’ютерних мережах, а також висвітлено сучасні технології безпеки в інтернеті та системи виявлення вторгнень в мережу.

У просторі мережевої безпеки на основі моделі Zero Trust (*CISA, Агентство кібербезпеки та інфраструктурної безпеки*) запропоновано: метод цільової сегментації трафіку, який дає змогу аналізувати взаємодію між додатками, користувачами та інфраструктурою корпоративної мережі, що підвищує рівень виявлення складних загроз [14]; концепцію “ніколи не довіряти, завжди перевіряти”, яка спрямована на підтвердження користувачем достовірності своїх даних під час кожного запиту на доступ до всіх ресурсів як усередині мережевого периметра компанії, так і за її межами [15]. Ефективними є сегменти безпеки комп’ютерних систем та комп’ютерних мереж, які комплексно представляють безпеку апаратно-програмного забезпечення, безпечний обмін даними і безпеку зберігання даних на рівні технологій контролю доступу, шифрування даних, ізоляції мережі [16]. Цікавим є сегмент проєктування архітектури безпечної мережі виробничих компаній, для якого у праці [17] розглянуто застосування ефективних технологій безпеки, зокрема фаєрвол, IDS, що уможливлює підвищення стійкості систем захисту. Сучасний напрям мережевої безпеки представляють методи виявлення розподілених мережевих атак, програмовані мережі, техніки машинного навчання [18]. У розвитку систем виявлення вторгнень (IDS) є новий метод на основі нейронної

мережі довгострокової пам'яті (p-LSTM), який уможливлює зниження рівня хибних сповіщень та підвищення надійності виявлення вторгнень [19]. Триває розвиток підходів безпеки LAN і WAN мереж: розглянуто сценарії застосування VPN у корпоративних WAN-мережах [20]; запропоновано застосування міжмережевих екранів (фаєрволів), технологій маскування, переадресації портів і на цій основі побудови сильної політики безпеки [21]. Актуальним є новий підхід до оцінки ризику (RS) на основі ваги ризиків, що ґрунтується на стандартах NIST CSF і ISA/IEC 62443; у цьому підході RS модифіковано шляхом введення нових метрик ризику: ризик, зниження ризику, пріоритетизація ризику та пріоритетизація зниження ризику з метою створення спеціалізованої формули ймовірності оцінки ризиків широкосмугових WAN-мереж, що використовуються в інфраструктурі операційних технологій [22].

Розглянуті методи, засоби мережевої безпеки є основою для розвитку підходів безпеки РКМ, які на сьогодні є актуальними у просторі задач безпечної інтелектуалізації предметних сфер суспільства.

## Постановка задачі

На основі проведеного аналізу було встановлено завдання: 1) запропонувати структуру комплексної системи безпеки регіональних корпоративних мереж на основі багаторівневих моделей – еталонної моделі OSI та моделі "глибокого захисту"; 2) розробити програмну реалізацію криптографічного захисту даних на транспортному рівні OSI на основі симетричного блокового алгоритму шифрування AES-256 засобами мови програмування Python. Метою статті є створення комплексної системи безпеки регіональної корпоративної мережі та на цій основі розроблення програмної реалізації алгоритму шифрування даних AES-256 для протоколу OpenVPN і технології TLS, як одного з ефективних механізмів реалізації захисту інформації, що забезпечуватиме високий ступінь захисту даних на транспортному рівні.

## Базова еталонна модель OSI та модель"глибокого захисту" у просторі безпеки регіональних корпоративних мереж

***Регіональні корпоративні мережі у предметних сферах інфраструктури суспільства.*** Регіональним корпоративним мережам властиві: високий ступінь безпеки обміну даними за профілем конфіденційності, висока пропускна здатність та надійність, особливо для обробки великих обсягів даних, розгортання приватних віртуальних мереж. Серед усталених топологій на практиці в РКМ найбільше використовується гібридна, перевагами якої є гнучкість структури, підвищена надійність та відмовостійкість, масштабованість, сегментація та високий рівень безпеки, ефективність та висока швидкість обміну даними.

***Основні характеристики РКМ.***

*Обсяг покриття:* РКМ охоплюють велику географічну територію (міста чи навіть країни) з метою забезпечення зв'язку між віддаленими офісами та філіями.

*Розмір та комплексність:* під'єднання до мережі значної кількості офісів і складної інфраструктури для забезпечення надійності та продуктивності.

*Швидкість передачі даних:* врахування великих відстаней та використання технології зв'язку високої пропускної здатності для швидкого та ефективного обміну інформацією.

*Безпека:* необхідність в ефективних стратегіях безпеки, оскільки зв'язок по великій відстані є більш вразливим до кіберзагроз.

*Технології зв'язку:* застосування різноманітних технологій, зокрема інтернет-з'єднань великої швидкості, віртуальних приватних мереж (VPN), оптоволоконних ліній тощо з метою забезпечення надійного і безпечного з'єднання між регіональними підрозділами.

***Особливості застосування РКМ.***

*Керування великими обсягами даних:* здійснюють ефективний обмін великими обсягами даних між великою кількістю віддалених корпорацій.

*Глобальне управління:* реалізують глобальне управління обладнанням, програмним забезпеченням та політиками безпеки на всіх рівнях компанії.

*Оптимізація роботи мережі:* використовуються з метою оптимізації роботи мережі та забезпечення надійного та швидкого з'єднання між віддаленими офісами.

*Спільний доступ до ресурсів:* уможливлюють спільний доступ до централізованих ресурсів – баз даних, серверів тощо.

*Бізнес-контингентність:* дає змогу підприємствам впроваджувати стратегії бізнес-контингентності та на цій основі уможливлюють невідкладне відновлення роботи у випадку аварійних і кризових ситуацій.

*Глобальні комунікації:* забезпечують ефективний зв'язок на рівні глобальних комунікацій між різними філіями та дочірніми компаніями в межах корпорації.

***Базова еталонна модель OSI та модель "глибокого захисту".*** З метою створення комплексної системи безпеки регіональних корпоративних мереж розглянемо багаторівневий підхід, що передбачає застосування багаторівневої базової еталонної моделі OSI та багаторівневої моделі "глибокого захисту" і на цій основі забезпечення високого ступеня конфіденційності інформації.

*Базова еталонна модель OSI.* На рис. 1 наведено базову еталонну модель OSI (ДСТУ ISO/IEC 7498-1:2004 Інформаційні технології. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 1. Еталонна модель).

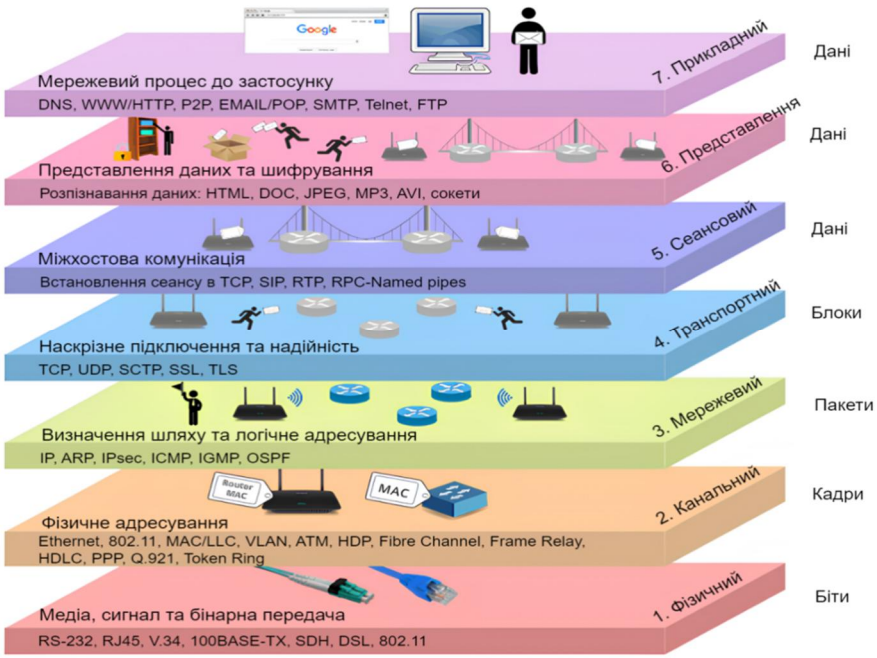


*Рис. 1. Базова еталонна модель OSI*

*Фізичний рівень* (Ethernet-кабель, оптоволокно, Wi-Fi, Bluetooth). Захист фізичного рівня спрямований на забезпечення безпечного фізичного доступу до обладнання, кабелів і каналів передавання даних. Найпоширенішими загрозами є крадіжка/ несанкціонований доступ до обладнання, пошкодження/ відключення кабелів, перехоплення сигналів. Заходами безпеки, спрямованими на протидію загроз, є контроль фізичного доступу (електронні замки, системи відеоспостереження), використання захищених кабелів (екранованих, волоконно-оптичних), застосування безперебійного живлення (UPS), захист від відмов електромережі.

*Канальний рівень* (протоколи: Ethernet, PPP (*Point-to-Point Protocol*), MAC-адреси). Забезпечує передавання даних між сусідніми вузлами; реалізує поділ бітів на пакети; уможливлює виявлення та корекцію помилок у середовищі передавання даних.

*Мережевий рівень* (протоколи: IPv4, IPv6, ICMP (*Internet Control Message Protocol*). Реалізує маршрутизацію пакетів від відправника до одержувача, використовує логічні адреси.

*Транспортний рівень* (протоколи: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), *TLS/SSL для шифрування*). Забезпечує надійність обміну даними між кінцевими точками мережі, контролює цілісність і порядок передавання, управління сегментацією, потоком з метою уникнення перевантаження, контроль помилок, повторне передавання інформації в разі її втрати.

*Сеансовий рівень* (протоколи: NetBIOS, PPTP (*Point-to-Point Tunneling Protocol*). Забезпечує встановлення, підтримку та завершення сеансів зв'язку між пристроями; здійснює управління синхронізацією та повторним підключенням у разі переривання; реалізує аутентифікацію користувачів.

*Рівень представлення* (формати: JPEG, MP3, GIF). Здійснює перетворення даних у формат, зрозумілий для отримувача; реалізує шифрування даних для безпечного передавання.

*Сеансовий рівень* (протоколи: HTTP (для вебдоступу), FTP (для передавання файлів), SMTP (для електронної пошти); додатки; веббраузери; поштові клієнти; файлові менеджери). Надання інтерфейсів та сервісів для взаємодії користувачів з мережевими додатками; реалізує обробку запитів користувачів та відповіді від серверів.

*Модель "глибокого захисту"*. На рис. 2 наведено структуру моделі "глибокого захисту" регіональних корпоративних мереж [23]. Модель "глибокого захисту" РКМ забезпечує стійкість до кіберзагроз на основі рівнів безпеки:

1. *План безпеки мережі* – 1.1 визначення каналів зв'язку всередині мережі системи управління, 1.2 виконання повного аудиту пристроїв в мережі, 1.3 запис параметрів безпеки кожного пристрою, 1.4 створення детальної схеми мережі.

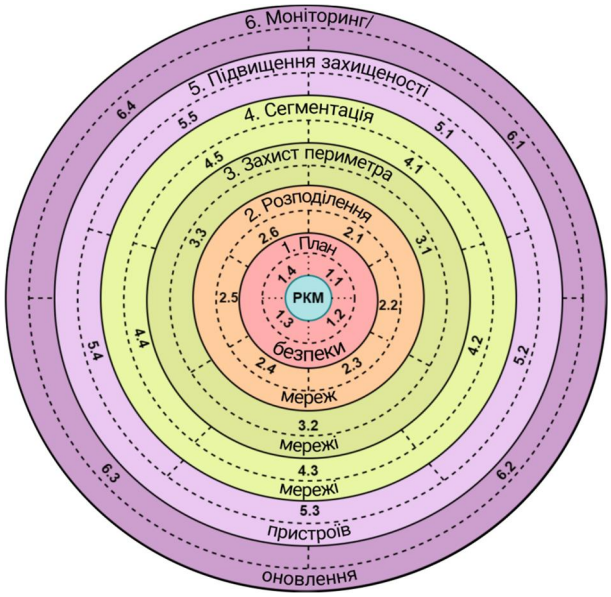


*Рис. 2. Багаторівнева модель "глибокого захисту" регіональних корпоративних мереж*

*2. Розподілення мереж* – 2.1 організація необхідного обладнання для безперешкодного мережевого передавання інформації (сервери, які збирають дані з систем управління і поширюють їх всередині), 2.2 управління оновленнями програмного забезпечення, 2.3 сервер антивірусного програмного забезпечення, 2.4 сервер вебдоступу, 2.5 точка безпровідного доступу, 2.6 віддалений доступ.

*3. Захист периметра мережі* – 3.1 застосування міжмережевих екранів (брандмауерів), які виконують функції фільтрації пакетів, 3.2 фільтрація трафіку, 3.3 застосування проксі-шлюзу

*4. Сегментація мережі*: *переваги* – 4.1 протидія проникненню шкідливого вмісту трафіку, яке можливе тільки в один сегмент однієї мережі, 4.2 ефективність безпеки, оскільки вузли є непомітними з несанкціонованих для доступу мереж, 4.3 протидія зловмисникам, які сканують мережі вглибину за ієрархією, перш ніж вибрати систему для атаки, 4.4 запобігання витоку інформації за умов порушення безпеки мережі, 4.5 підвищення продуктивності мережі та зменшення її навантаження.

*5. Підвищення захищеності пристроїв* – 5.1 управління паролями, зокрема шифрування, 5.2 відключення невикористовуваних служб, 5.3 контроль доступу, 5.4 мережева система виявлення вторгнень NIDS (*Network intrusion detection systems*), 5.5 сувора аутентифікація.

*6. Моніторинг/ оновлення* – 6.1 моніторинг пакетів реєстрації, 6.2 моніторинг журналу подій, 6.3 перехоплення аутентифікації, 6.4 використання системи виявлення вторгнень IDS (*Network Intruder Detection System*).

**4. Комплексна система безпеки регіональної корпоративної мережі у предметних сферах**

Комплексна система безпеки регіональної корпоративної мережі предметної сфери побудована на основі моделей OSI та "глибокого захисту" і розгорнута у просторі концепції "загрози – технології безпеки" (табл.).

**Комплексна система безпеки РКМ на основі моделі OSI та моделі "глибокого захисту"**

| РКМ: модель OSI, елементи "глибокого захисту" | | Концепція "загрози – технології безпеки" |
|---|---|---|
| Модель OSI: Фізичний | | |
| 1 | 2 | 3 |
| Загрози | Випадкові | 1. Природні катастрофи<br>2. Перебої в електропостачанні<br>3. Пожежі<br>4. Несправність в будівлях з обладнанням |
| | Ціле-спрямовані | 1. Навмисне пошкодження фізичного обладнання<br>2. Викрадення обладнання<br>3. Використання спеціальних засобів для незаконного отримання інформації<br>4. Фізичне вторгнення |
| Технології безпеки з елементами *глибокого захисту* | Апаратні | 1. *Biometric Access Control: Використання біометричних систем контролю доступу для обмеження фізичного доступу до серверних приміщень*<br>2. *CCTV Surveillance: Встановлення систем відеоспостереження для візуального контролю за фізичними об'єктами мережевої інфраструктури*<br>3. *Protected Cable Routing: Захищені маршрути кабелів для запобігання перехопленню інформації*<br>4. Hardware Locks and Cages: Використання апаратних засобів, таких як замки та клітки з метою фізичного захисту серверного обладнання |
| Модель OSI: Канальний | | |
| Загрози | Випадкові | 1. Електромагнітні/ радіочастотні перешкоди, спричинені зовнішніми факторами впливу<br>2. Перебої в передаванні даних, що можуть призвести до втрати пакетів<br>3. Випадкові помилки в конструкції/ специфікаціях каналів |
| | Ціле-спрямовані | 1. Маніпуляція кадрами<br>2. ARP Spoofing<br>3. MAC-Флуд<br>4. DNS Spoofing |

*Продовження табл.*

| 1 | 2 | 3 |
|---|---|---|
| Технології безпеки з елементами *глибокого захисту* | Апаратні | 1. Використання апаратних фільтрів MAC-адрес для обмеження доступу до фізичного рівня мережі<br>*2. Використання апаратного розділення мережі за допомогою VLAN для ізоляції різних груп користувачів*<br>3. Використання апаратного забезпечення для обмеження кількості підключених пристроїв до портів комутатора<br>4. Використання апаратних засобів, таких як замки та спеціальні шафи, для фізичного захисту комутаційного обладнання |
| | Програмні | 1. Використання протоколу 802.1X для програмної аутентифікації пристроїв на канальному рівні<br>2. Встановлення програмного забезпечення для моніторингу стану портів комутатора та виявлення аномальної активності<br>3. Network Access Control (NAC) Software: Використання програмного забезпечення контролю доступу до мережі для визначення статусу безпеки підключених пристроїв |
| Модель OSI: Мережевий | | |
| Загрози | Випадкові | 1. Проблеми функціонування мережевих протоколів<br>2. Переповнення буфера<br>3. Несправність мережевого обладнання |
| | Ціле-спрямовані | 1. Мережеве сканування<br>2. DDoS-атаки<br>3. Спроби перехоплення трафіку<br>4. Використання фальшивих IP-адрес<br>5. Заповнення ARP-таблиці |
| Технології безпеки з елементами *глибокого захисту* | Апаратні | 1. Використання апаратних брандмауерів для фільтрації мережевого трафіку та блокування небезпечних пакетів<br>2. Використання апаратних функцій безпеки на маршрутизаторах, таких як фільтрація пакетів та VPN-з'єднання<br>3. Intrusion Detection Systems (IDS): Встановлення апаратних систем виявлення вторгнень для моніторингу та виявлення небезпечної активності |
| | Програмні | *1. Використання програмного забезпечення VPN для шифрування та безпечного з'єднання через відкриті мережі*<br>2. Використання програмного забезпечення для безпечної реалізації протоколів маршрутизації (BGP, OSPF)<br>*3. Network Address Translation (NAT): Використання програмного забезпечення для здійснення NAT з метою захисту внутрішніх IP-адрес від прямого доступуі з зовнішньої мережі*<br>4. Packet Filtering Software: Встановлення програм для фільтрації пакетів на основі правил та політик безпеки |
| Модель OSI: Транспортний | | |
| Загрози | Випадкові | 1. Пошкодження даних внаслідок електромагнітних збоїв<br>2. Випадкові зміни маршрутів передавання пакетів, що можуть призвести до втрати з'єднання або затримок<br>3. Випадкові збої в роботі програмного забезпечення протоколів |
| | Ціле-спрямовані | 1.Man-in-the- Middle-атака<br>2. Session Hijacking<br>3. Атака на створення великої кількості неправильних TCP-з'єднань для перевантаження сервера та відмови в обслуговуванні<br>4. Атака на UDP, в якій зловмисники відправляють фальшиві або випадкові UDP-запити для перевантаження мережі |

*Закінчення табл.*

| 1 | 2 | 3 |
|---|---|---|
| Технології безпеки з елементами *глибокого захисту* | Апаратні | 1. Використання апаратних балансувальників навантаження для розподілу трафіку та запобігання DoS-атак<br>2. Використання апаратних прискорювачів SSL/TLS для оптимізації та безпеки шифрування<br>3. Network-Based Intrusion Prevention Systems (IPS): Встановлення апаратних систем запобігання вторгненням для виявлення та блокування аномальної активності на транспортному рівні |
| | Програмні | 1. Transport Layer Security (TLS) Protocols: Використання програмного забезпечення для імплементації протоколів TLS і реалізації шифрування транспортного рівня<br>*2. Secure Socket Layer (SSL) VPN Software: Використання програмного забезпечення для реалізації безпечних VPN з'єднань на транспортному рівні*<br>*3. Transport Layer Security (TLS) Inspection Software: Використання програм для інспекції трафіку TLS з метою виявлення загроз та атак* |
| Нормативне забезпечення | 1. ДСТУ ISO/IEC 27033:2013 – Інформаційні технології. Методи захисту. Безпечність мережі. Частина 3. Еталонні мережеві сценарії. Загрози, методи проектування та проблеми керування.<br>2. ДСТУ ISO/IEC 18033-1:2017 – Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 1. Загальні положення.<br>3. ДСТУ ISO/IEC 15408-1:2022 – Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінки для IT-безпеки.<br>4. ДСТУ ISO/IEC 27001:2023 – Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги.<br>5. ДСТУ ISO/IEC 27033-7:2023 – Інформаційні технології – Мережева безпека. Керівництво з безпеки віртуалізації мережі. | |

**Криптографічний захист даних на транспортному рівні OSI регіональної корпоративної мережі на основі: протоколу OpenVPN, технології TLS, алгоритму AES-256**

З метою реалізації запропонованої комплексної системи безпеки регіональних корпоративних мереж використовуємо елементи еталонної моделі OSI та моделі "глибокого захисту" у просторі застосування ефективного інструментарію: протоколу OpenVPN, технології транспортного рівня TLS, симетричного блокового алгоритму шифрування AES-256, що цілісно забезпечуватиме високий ступінь конфіденційності інформації, швидкість обміну даних, безпеку з'єднання. Серед відомих VPN–протоколів (OpenVPN, WireGuard, IKEv2/IPSec, L2TP/IPSec, PPTP), які управляють створенням і шифруванням VPN–з'єднань, протокол OpenVPN є універсальним, сумісним з усіма платформами і таким, що ефективно використовує AES-256 і на цій основі забезпечує високий ступінь криптостійкості у процесі передавання конфіденційних даних корпоративними мережами.

Технології TLS забезпечують безпеку на транспортному рівні OSI регіональної корпоративної мережі: аутентифікацію користувача, конфіденційність інформації, цілісність передавання даних. Перевагами використання симетричного блокового алгоритму AES-256 є: 1) *висока швидкість* – алгоритм ефективно працює як на апаратному, так і на програмному рівні; 2) *надійний захист* – його структура стійка до багатьох типів атак, він вважається одним із найбезпечніших алгоритмів шифрування; *гнучкість* – підтримка різної довжини ключа дає змогу налаштовувати рівень захисту залежно від потреб. Алгоритм шифрування ефективно використовується для безпечного обміну конфіденційними даними в корпоративних мережах; безпечного зберігання інформації; криптографічного захисту даних у хмарних середовищах та на мобільних пристроях.

Для програмної реалізації шифрування даних на транспортному рівні OSI регіональної корпоративної мережі використано мову програмування Python, якій властиві зрозумілий синтаксис, велика стандартна бібліотека модулів, велика кількість сторонніх бібліотек, що робить цю мову універсальною, а також такі бібліотеки, як "pycryptodome" і "cryptography", які надають готові інструменти для реалізації алгоритму шифрування AES-256.

Основна структура програмного коду містить такі елементи:

1. *Імпорт необхідних модулів:*

**Argparse** – для парсингу аргументів командного рядка

**Crypto.Cipher** – для роботи з шифрами AES

**Crypto.Random** – для генерації випадкових байтів

**Crypto.Util.Padding** – для додавання та видалення доповнень до блоків даних

**pyDH** – для реалізації протоколу Діффі-Хеллмана

**hashlib** – для використання хеш-функції SHA-256.

2. *Оголошення функцій*. У програмі використані 4 функції, які працюють з текстовим файлом:

**read_file(file_path)** – зчитує вміст файлу

**write_file(file_path, data)** – записує вміст у файл

**encrypt_file(input_file, output_file, key) –** шифрує файл за допомогою AES

**decrypt_file(input_file, output_file, key)** – дешифрує файл, зашифрований за допомогою AES.

3. *Розбір аргументів командного рядка за допомогою модуля* argparse. За допомогою даних аргументів можливо зашифрувати та розшифрувати текстовий файл. Аргументи включають:

**action** - вказує дію, яку треба виконати: шифрування або дешифрування

**input_file** - шлях до вхідного файлу

**output_file** - шлях до вихідного файлу

**--shared_key** - спільний ключ для шифрування або дешифрування (необов'язковий параметр).

4. *Генерація ключа за допомогою протоколу Діффі-Хеллмана*. Для генерації публічного ключа та обчислення спільного ключа використовується об'єкт **pyDH.DiffieHellman().**

5. *Хешування згенерованого ключа за допомогою хеш-функції SHA-256.* Оскільки згенерований ключ має довжину в 64 байт, а алгоритм AES підтримує ключі довжиною 16, 24 та 32 байт, то потрібно скорочувати отриманий ключ для можливості шифрування/дешифрування файлу.

6. *Шифрування/ дешифрування файлу.* Викликаються функції encrypt_file() або decrypt_file() з переданим вхідним файлом, вихідним файлом та спільним ключем.

Команда для шифрування текстового файлу має такий вигляд:

**python alice.py encrypt input_file.txt output_file.txt,**

де **input_file.txt** – шлях до вхідного файлу, **output_file.txt** – шлях, куди потрібно зберегти вихідний зашифрований файл. При цьому створюється новий унікальний ключ, за допомогою якого шифрується **input_file.txt**.

Якщо потрібно зашифрувати файл уже існуючим ключем, то для цього можна використати таку команду:

**python alice.py encrypt input.txt output.txt --shared_key ABCDEFG123456789**

Після аргументу **--shared_key** потрібно ввести існуючий ключ, який був згенерований раніше. Аналогічні команди використовуються для дешифрування зашифрованого файлу, тільки замість аргументу **encrypt** потрібно використати **decrypt.** На рис. 3–4 наведено скріни програмної реалізації, відповідно, шифрування та дешифрування даних.

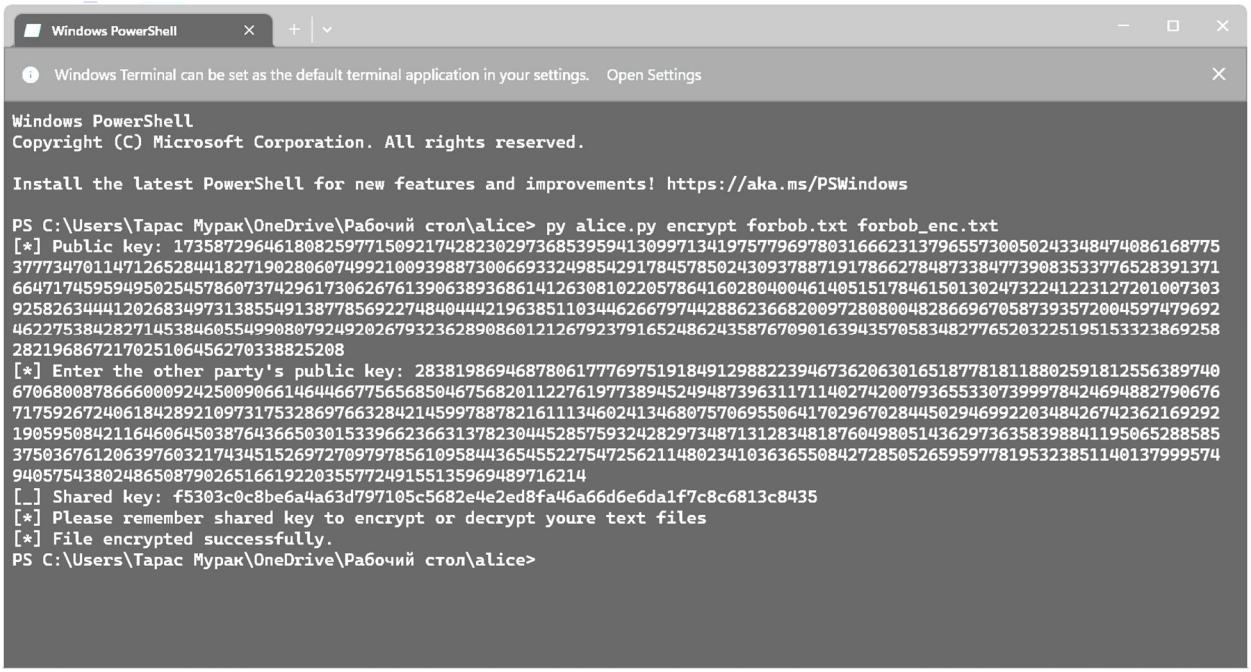


*Рис. 3. Створення секретного ключа та шифрування файлу*


*Рис. 4. Дешифрування отриманого файлу за допомогою секретного ключа*

## Результати дослідження

За результатами проведеного дослідження розглянуто відомі підходи до забезпечення безпеки корпоративних мереж, які представлені моделями, методами, технологіями та системами захисту інформації за профілем конфіденційності даних. Синтезовано семірівневу модель OSI та модель “глибокого захисту” регіональних корпоративних мереж у просторі побудови комплексної системи безпеки РКМ на основі концепції “загрози – технології безпеки”. Запропоновано комплексну систему безпеки регіональних корпоративних мереж, яка уможливлює забезпечення конфіденційності інформації на фізичному, канальному, мережевому, транспортному рівнях на основі апаратного і програмного інструментарію з елементами технологій “глибокого захисту” відповідно до випадкових і цілеспрямованих загроз. Наведено програмну реалізацію “глибокого захисту” РКМ засобами шифрування даних на транспортному рівні OSI на основі: протоколу OpenVPN, технології TLS, симетричного блокового алгоритму AES-256, мови програмування Python.

## Висновки

Запропонований підхід до забезпечення конфіденційності інформації в регіональних корпоративних мережах, який: 1) розгорнутий комплексною системою безпеки згідно з багаторівневою мережевою моделлю OSI та моделлю “глибокого захисту” та концепцією “загрози – технології безпеки” відповідно до випадкових і цілеспрямованих загроз; 2) практично реалізований механізмом захисту інформації транспортного рівня OSI на основі інструментарію – алгоритму AES-256 засобами мови Python, протоколу OpenVPN, технології TLS, що уможливлює забезпечення високого ступеня кіберстійкості та кіберзахисту.

## Список літератури


1. *International strategy of the EU agency for cybersecurity. 2021. URL: https://www.enisa.europa.eu/sites/default/files/all_files/2022-02-16%20ENISA%20International%20Strateg y.pdf (дата звернення: 10.01.2025).*
2. *Стратегія кібербезпеки України (2021- 2025). URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 10.01.2025).*
3. *NIS 2: Огляд Директиви ЄС про кібербезпеку. URL: https://gigacloud.ua/blog/navchannja/nis-2-ogljad-direktivi-es-pro-kiberbezpeku (дата звернення: 10.01.2025).*
4. *Bobalo Y., Dudykevych V., Mykytyn H. Information technologies for data collection: concept, methodological approaches, security = Інформаційні технології відбору даних: концепція, методологічні підходи, безпека : монографія. Lviv : Spolom, 2024. 148 с.*
5. *Чинчик Д. М., Коробейнікова Т. І., Захарченко С. М. Методи і засоби комплексного захисту корпоративної мережі. InterConf: with the Proceedings of the 5th International Scientific and Practical Conference "Theory and Practice of Science: Key Aspects". 2021. (84). С. 433- 450. DOI: https://doi.org/10.51582/interconf.7-8.11.2021.043.*
6. *Ільєнко А. В., Ільєнко С. С., Кваша Д. С., Мазур Я. С. Практичні підходи щодо виявлення вразливостей в інформаційно-телекомунікаційних мережах. Кібербезпека: освіта, наука, техніка. 2023. № 3(19). С. 96- 108. DOI: 10.28925/2663-4023.2023.19.96108.*
7. *Андрощук О., Коваленко О, Тітова В., Чешун В., Поляков А. Удосконалення систем захисту інформації в комп'ютерних мережах Державної прикордонної служби України. Військові науки. 2021. № 2, 3(85). С. 5- 21. DOI: https://doi.org/10.32453/3.v85i2-3.828.*
8. *Полотай О. І., Федінець Н. І., Кухарська Н. П. Дослідження загроз інформаційної безпеки та способів їх вирішення в комп'ютерних мережах на канальному рівні. Вісник ЛДУБЖД. 2024. № 29. С. 65- 71. DOI: https://doi.org/10.32447/20784643.29.2024.07.*
9. *Кучернюк П. В. Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні). Мікросистеми, Електроніка та Акустика. 2017. Т. 22, № 6(101). С. 64- 70. DOI: https://doi.org/10.20535/2523-4455.2017.22.6.113191.*
10. *Кучернюк П. В. Методи і технології захисту комп'ютерних мереж (мережний, транспортний та прикладний рівні). Мікросистеми, Електроніка та Акустика. 2018. Т. 23. № 1(102). С. 52- 58. DOI: https:// doi. org /10.20535/2523-4455.2018.23.1.113193.*
11. *Лебідь О. В., Кіпоренко С. С., Вовк В. Ю. Виявлення кібератак та підвищення інформаційної безпеки на основі технологій нейронних мереж в умовах кібервійни. Наука і техніка сьогодні. 2023. № 1(15). С. 238- 256. DOI: https://doi.org/10.52058/2786-6025-2023-1(15)-238-256.*
12. *Савченко В. А., Рибальченко О. Г. Побудова ефективної системи мережевої безпеки підприємства на основі методу аналізу ієрархій показників якості. Сучасний захист інформації. 2024. No 1(57). С. 6- 14. DOI: 10.31673/2409-7292.2024.010001.*
13. *Янко А. С., Вигівський Р. А. Система захисту комп'ютерної мережі. Системи управління, навігації та зв'язку. 2022. № 2. С. 91- 94. DOI: 10.26906/SUNZ.2022.2.091.*
14. *Tolkachov M., Dzheniuk N., Yevseiev S., Lysetskyi Y., Shulha V., Grod I., Faraon S., Ivanchenko I., Pasko I., Balagura D. Development of a method for protecting information resources in a corporate network by segmenting traffic. Eastern-European Journal of Enterprise Technologies. 2024. 5 (9 (131)). Pp. 63–78. DOI: https://doi.org/10.15587/1729-4061.2024.313158.*
15. *Habash R. M., Ibrahem M. K., Zero Trust Security Model for Enterprise Networks. Iraqi Journal of Information and Communication Technology. 2023. Vol. 6. No. 2. Pp. 68- 77. DOI: https://doi.org/ 10.31987/ ijict. 6.2.223.*
16. *Zhang G.-L. Analysing Computer System Security and Computer Network Security. Engineering Technology Trends. 2024. Vol. 2 Issue 4. Pp. 11- 15. DOI: 10.37155/2972-483X-0204-3.*
17. *Hosam O., Abousamra R., Hassouna M., Azzawi R. Security Analysis and Planning for Enterprise Networks. Industry 4.0 Key Technological Advances and Design Principles in Engineering, Education, Business, and Social Applications, 2024. Pp. 69- 100. DOI: 10.1201/9781003343332-5.*
18. *Lyu M., Gharakheili H. H., Sivaraman V. A Survey on Enterprise Network Security: Asset Behavioral Monitoring and Distributed Attack Detection. IEEE Access. 2024. Vol. 12. Pp. 89363- 89383. DOI: 10.48550/ arXiv.2306.16675.*

*19. Sudha M., Mahesh Kumar Reddy V., Deva Priya W., Rafi S. M., Subudhi S., Jayachitra S. Optimizing intrusion detection systems using parallel metric learning. Computers and Electrical Engineering. 2023. Vol. 110. Pp. 76- 91. DOI: https://doi.org/10.1016/j.compeleceng.2023.108869.*

*20. Bhagat N. MPLS vs. IPsec VPN: Choosing the Right Network Architecture for Enterprise WAN. International journal of scientific research in engineering and management. 2021. Vol. 05. Issue 12. DOI: 10.55041/ijsrem11326.*

*21. Taslim A., Uddin R, Evan N, Alam R. Enterprise Network: Security Enhancement and Policy Management Using Next-Generation Firewall (NGFW). Lecture Notes on Data Engineering and Communications Technologies. 2021. Vol. 66. Pp. 753–769. DOI: 10.1007/978-981-16-0965-7_59.*

*22. Abergos V. J., Medjek F. A Risk Assessment Analysis to Enhance the Security of OT WAN with SD-WAN. J. Cybersecur. 2024. Priv. 4(4). Pp. 910- 937. DOI: https://doi.org/10.3390/jcp4040042.*

*23. Onyagu C. L., Okonkwo O. R., Akawuku G., John J. Enhancing Security in Internet of Things (IoT) Architecture through Defense-in-Depth Mechanism: A Comprehensive Study. Newport international journal of engineering and physical sciences. 2024. Vol. 4(1). Pp. 17- 22. DOI: 10.59298/NIJEP/2024/411722.1.1100.*

## COMPLEX SECURITY SYSTEM OF A REGIONAL CORPORATE NETWORK BASED ON THE OSI MODEL AND THE “DEFENSE-IN-DEPTH” MODEL

**V. B. Dudykevych, H. V. Mykytyn, T. Y. Murak**

Lviv Polytechnic National University,
Department of Information Protection



**The strategy of the EU Agency for Cybersecurity (ENISA) and Ukraine’s Cybersecurity Strategy aims to develop and implement new approaches, methodologies, and technologies for addressing cybersecurity challenges in critical infrastructure sectors, particularly in ensuring data confidentiality within corporate networks.**

**An analytical review of well-known corporate network security methods and technologies has been conducted in secure data exchange and storage; enhancement of security models, tools, and information protection systems; and the application of machine learning methods and neural network technologies for anomaly detection in corporate networks.**

**A comprehensive security system for a regional corporate network is presented based on the seven-layer OSI model, the “defense-in-depth” model, and the “threat–security technologies” concept, which is universal for different network topologies and enables the design of information protection systems at each OSI layer by regulatory requirements.**

**Software for the cryptographic protection of information at the transport network layer of the OSI model has been developed using the symmetric block cipher AES-256, implemented in Python. This solution is practically realized through the OpenVPN protocol and TLS transport layer technology, ensuring a high level of data confidentiality in regional corporate networks.**

**Keywords: corporate network, OSI reference model, defense-in-depth model, comprehensive security system, random and targeted threats, transport layer, data encryption.**