ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської
науково-практичної конференції

27 листопада 2025 року

м. Львів

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ

ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ПРИВАТНИЙ ЗАКЛАД ВИЩОЇ ОСВІТИ «ІТ СТЕП УНІВЕРСИТЕТ»

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської науково-практичної конференції

27 листопада 2025 року

Львів – 2025

ББК 32.81+78.362

Інформаційна безпека та інформаційні технології: збірник тез доповідей VII Всеукраїнської науково-практичної конференції, м. Львів, 27 листопада 2025 року. Львів, ЛДУ БЖД, 2025, 493 с.

За точність наведених фактів, самостійність наукового аналізу та нормативність стилістики викладу, а також за використання відомостей, що не рекомендовані до відкритої публікації відповідальність несуть автори опублікованих матеріалів.

УДК 004.8:004.056:004.738.5

ІНТЕГРАЦІЯ SIEM, АВТОМАТИЗОВАНОГО МОНІТОРИНГУ ТА МОДЕЛЕЙ ПОВЕДІНКОВОГО АНАЛІЗУ ДЛЯ КОРПОРАТИВНОЇ БЕЗПЕКИ

Артем ІЩЕНКО[1], Ростислав ТКАЧУК[1,2], Валерія БАЛАЦЬКА[1]
[1] Львівський державний університет безпеки життєдіяльності,
[2]Національний університет «Львівська політехніка»

Проаналізовано систему захищеного віддаленого доступу в «Київстар», виявлено ключові вразливості та загрози. Розглянуто VPN, IPsec, SSL/TLS, Zero Trust, IAM, SIEM і MDM, оцінено ефективність їх впровадження. Наведено дворівневу архітектуру та результати тестування в Ubuntu Server із Wireshark, Nmap і Fail2ban. Запропоновано політику доступу з мінімізацією привілеїв. Дослідження підтверджує ефективність рішення для безпечного віддаленого доступу та підвищення кіберстійкості.

Ключові слова: *захищений віддалений доступ, VPN, Zero Trust, IPsec, SSL/TLS, SIEM, багатофакторна автентифікація, кібербезпека, MDM, корпоративна мережа, WireGuard, тестування безпеки, кіберзагрози.*

The secure remote access system at Kyivstar was analyzed, key vulnerabilities and threats were identified. VPN, IPsec, SSL/TLS, Zero Trust, IAM, SIEM and MDM were considered, and the effectiveness of their implementation was assessed. A two-tier architecture and testing results in Ubuntu Server with Wireshark, Nmap and Fail2ban were presented. An access policy with privilege minimization was proposed. The study confirms the effectiveness of the solution for secure remote access and increasing cyber resilience.

Keywords: *secure remote access, VPN, Zero Trust, IPsec, SSL/TLS, SIEM, multi-factor authentication, cybersecurity, MDM, corporate network, WireGuard, security testing, cyber threats.*

Аналіз системи захищеного віддаленого доступу в «Київстарі» засвідчив наявність низки критичних загроз та вразливостей, пов'язаних із використанням застарілого програмного забезпечення, слабкою сегментацією мережі, недостатнім рівнем захисту кінцевих пристроїв і відсутністю повноцінної багатофакторної автентифікації. Поширені ризики — фішингові атаки, brute-force, MITM, атаки на сесії — становлять особливу загрозу для корпоративного трафіку та персональних даних. Інциденти 2023–2024 років підтверджують необхідність глибокої модернізації інфраструктури безпеки та підвищення стійкості до складних кібератак.

Порівняльний аналіз технологій VPN, IPsec, SSL/TLS, Zero Trust та хмарних інтеграцій показав, що класичні VPN-рішення вже не забезпечують належного рівня захисту в умовах масштабності мережі та значної кількості мобільних пристроїв. Ефективним напрямом є впровадження Zero Trust-архітектури, централізованого управління доступом (IAM), систем моніторингу SIEM, пове-

дінкового аналізу та рішень MDM для контролю мобільних і BYOD-пристроїв. Ці засоби дозволяють мінімізувати ризики компрометації облікових записів та зменшити площу атаки в розподіленій інфраструктурі [1–3].

Для підвищення кіберстійкості великих ресурсів, таких до прикладу, як «Київстар» більш дієве комплексне оновлення системи безпеки: модернізацію протоколів шифрування, запровадження розширеного моніторингу подій, інтеграцію багатофакторної автентифікації, посилення контролю кінцевих точок та використання штучного інтелекту для виявлення аномалій у трафіку. Такий підхід забезпечить надійний захист критичних компонентів, зменшить імовірність несанкціонованого доступу та підвищить рівень готовності до сучасних кіберзагроз [4].

Модель захищеного віддаленого доступу, що використовується оператором «Київстар», ґрунтується на дворівневій архітектурі, яка поєднує шифрування трафіку та централізовану автентифікацію. На першому рівні застосовується захищений тунель, створений за протоколами IPSec або SSL/TLS, що забезпечує конфіденційність і цілісність переданих даних. Другий рівень передбачає автентифікацію користувачів через домен або Active Directory, застосування сертифікатів та контроль доступу відповідно до політик безпеки.

Основними компонентами архітектури є клієнтське програмне забезпечення на робочих станціях, VPN-шлюз, який виконує установлення та підтримку захищених сесій, а також сервер автентифікації, що перевіряє права доступу та керує обліковими записами. Усі події доступу логуються та можуть передаватися до системи моніторингу або SIEM для виявлення підозрілої активності й подальшого аналізу інцидентів.

Рішення забезпечує базовий захист корпоративного трафіку та дозволяє контролювати підключення співробітників до внутрішніх ресурсів із зовнішніх мереж. Водночас ефективність моделі значною мірою залежить від правильної конфігурації, регулярного оновлення компонентів безпеки та інтеграції з сучасними механізмами контролю доступу. Її подальша модернізація може бути спрямована на впровадження принципів Zero Trust, багатофакторної автентифікації та розширених засобів моніторингу для підвищення стійкості до актуальних кіберзагроз.

Для впровадження архітектури захищеного віддаленого доступу в компанії «Київстар» було створено тестове середовище у VirtualBox з установленим Ubuntu Server. Після розгортання ОС проведено налаштування мережі, SSH-доступу та основних сервісів безпеки. Це забезпечило можливість перевірити працездатність рішення до етапу інтеграції у виробниче середовище.

Практичне тестування проводилось за допомогою Wireshark, Nmap і Fail2ban. Wireshark дозволив оцінити затримки та ефективність трафіку, Nmap — перевірити доступність і конфігурацію сервісів, а Fail2ban — протестувати захист від brute-force атак. Тестові показники підтвердили очікувану різницю продуктивності між алгоритмами шифрування: ECDSA за-

Наукове видання

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської науково-практичної конференції

Відповідальні за випуск **Назарій БУРАК**
Олександр ХЛЕВНОЙ

Оригінал-макет **Юлія НАЗАР, Ольга СМОТР, Роман ГОЛОВАТИЙ, Діана РАЙТА, Віра ДОВБНЯК, Іван РОВЕЦЬКИЙ, Наталія ЖЕЗЛО-ХЛЕВНА**

Підписано до друку 12.11.2025 р.
Формат 60×84/16. Гарнітура Times New Roman.
Друк на різографі. Папір офсетний.
Ум. друк. арк. 30.

Друк ЛДУ БЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
тел./факс: (032) 233-32-40, 233-24-79.