УДК 004.056.5
DOI DOI DOI DOI https://doi.org/10.32782/2663-5941/2026.2.1/36

***Прокопович-Ткаченко Д.І.***
https://orcid.org/0000-0002-6590-3898
Університет митної справи та фінансів;
Державна наукова установа «Інститут інформації, безпеки і права
Національної академії правових наук України»;
Державний університет інформаційно-комунікаційних технологій

***Торстенссон О.***
https://orcid.org/0009-0007-2169-6851
Хальмстадський університет, м. Хальмстад, Швеція

***Черкаський Д.О.***
https://orcid.org/0009-0003-8516-6252
Національний технічний університет «Дніпровська політехніка»

***Переметчик Д.О.***
https://orcid.org/0009-0006-1978-5858
Університет митної справи та фінансів

***Берт С.Д.***
https://orcid.org/0009-0006-7423-9235
Університет митної справи та фінансів

# СОЦІОТЕХНІЧНІ ЧИННИКИ ВИНИКНЕННЯ ВРАЗЛИВОСТЕЙ МЕРЕЖЕВИХ ПРОТОКОЛІВ ЗАХИЩЕНОЇ ПЕРЕДАЧІ ДАНИХ

*Дослідження присвячено аналізу соціотехнічних чинників, що зумовлюють появу вразливостей у протоколах захищеної передачі даних під час експлуатації мереж електронних комунікацій. Розглянуто типові компромісні дії персоналу, пов'язані з відключенням або послабленням шифрованих з'єднань для швидкого відновлення сервісу, прийняттям недовірених сертифікатів, ігноруванням помилок перевірки ланцюжка довіри та підтримкою застарілих режимів сумісності, що створює умови для зниження рівня криптографічного захисту та перехоплення сеансів. Окремо досліджено атаки на вбудоване програмне забезпечення мережевих пристроїв, у межах яких уразливі вебінтерфейси та небезпечні налаштування протоколів адміністрування використовуються для зміни конфігурацій і деградації політик шифрування. Запропоновано методику оцінювання ризику на основі кореляції подій, сигналів виявлення вторгнень і моделей машинного навчання для аналізу мережевого трафіку та артефактів прошивок, включно з перетворенням байтових послідовностей у візуальні представлення. Експеримент на стенді гібридних атак показав, що автоматизація політик шифрування, заборона ручних винятків і перехід до захищених механізмів керування суттєво зменшують імовірність успішного перехоплення сеансу та підвищують відтворюваність конфігурацій. Зроблено висновок, що стійкість транспортного рівня визначається не лише формальним дотриманням стандартів, а передусім культурою прийняття рішень, контрольованістю змін і архітектурою постійної перевірки довіри.*

***Ключові слова:*** *транспорт, шифрування, сертифікація, довіра, сумісність, перехоплення, прошивки, адміністрування, кореляція, нейромережі, автоматизація.*

**Постановка проблеми.** Метою дослідження є формалізація внеску людських компромісів у вразливості транспортного рівня та розроблення практичної методики зменшення ризиків через автоматизацію криптографічних політик і гібридну аналітику IDS та SIEM. Для досягнення цієї мети передбачено побудову формальних математичних моделей ризику , що описують імовірність успіху

атак типу downgrade та перехоплення сесій при збігу людського компромісу та технічної експозиції. Важливим завданням є розроблення моделей поведінки транспортних протоколів, зокрема TLS 1.3, з урахуванням організаційного тиску на персонал та рішень щодо сумісності. Потребує оцінки операційна придатність засобів захисту за критеріями затримки детекції та точності в умовах гібридних атак. Додатково передбачено побудову оптимізаційних моделей вибору заходів автоматизації на основі критеріїв «стійкість – вартість». Також актуально інтегрувати отримані результати з моделями систем виявлення вторгнень, використовуючи глибинні нейронні мережі (CNN+LSTM, AE+LSTM) та підхід Byte2Image для структурного аналізу трафіку.

Запропонована оптимізаційна постановка вибору параметрів має базуватися на критеріях мінімізації інтегрального ризику і враховувати політики нульової довіри. Також актуально інтегрувати отримані результати з моделями систем виявлення вторгнень та управління інформаційною безпекою, використовуючи гібридну аналітику для відокремлення ручного компромісу від зловмисної деградації.

Таким чином, завданням роботи є не лише ідентифікація вразливостей транспортного рівня, але й формування практичних рекомендацій щодо впровадження принципів Zero Trust та автоматизації політик (policy-as-code) у мережах електронних комунікацій для мінімізації простору ручних небезпечних винятків.

**Аналіз останніх досліджень і публікацій.** Транспортний рівень у моделі OSI виступає критичним вузлом довіри , що на сучасному етапі реалізується переважно через протоколи TLS 1.2 та TLS 1.3. Дослідження вразливостей складних протокольних станів TLS показали, що будь-яка неточність обробки помилок може бути перетворена на канал атаки. Історичні кейси Logjam та FREAK довели критичність підтримки застарілих параметрів сумісності для деградації криптографічної стійкості , а уразливості POODLE та DROWN продемонстрували ризики експлуатації легасі-режимів SSL 3.0.

Сучасні стандарти, зокрема RFC 7525 та RFC 9325, регламентують безпечне використання TLS , а нормативний тренд у RFC 8996 вимагає повної відмови від TLS 1.0 та 1.1. Рекомендації NIST SP 800-52 Rev. 2 визначають правила конфігурації TLS-реалізацій , а профілі NISTIR 8259A та настанови SP 800-193 фокусуються на резильєнтності прошивок та базових кіберспроможностях пристроїв. Окремий напрям досліджень присвячений інтеграції криптографічних параметрів із системами IDS (Snort, Zeek) та SIEM. Праці в галузі інтелектуального аналізу трафіку показують, що використання методів глибинного навчання (CNN, LSTM) та візуалізації Byte2Image дозволяє значно підвищити точність виявлення аномалій у мережевих потоках та артефактах прошивок. Це відкриває перспективу для впровадження концепції Zero Trust Architecture (NIST SP 800-207), де довіра не припускається і перевіряється безперервно.

Таким чином, сучасні дослідження підкреслюють необхідність комплексного підходу, який одночасно враховує соціотехнічну природу вразливостей, практичні характеристики керувального контуру (наприклад, SNMPv3) та інтеграцію із засобами гібридної аналітики. Це й визначає наукову новизну та актуальність даної роботи.

**Постановка завдання.** Метою дослідження є формалізація внеску людських компромісів у вразливості транспортного рівня та розроблення практичної методики зменшення ризиків через автоматизацію політик і гібридну аналітику. Для досягнення цієї мети передбачено:

– ідентифікувати типові компроміси персоналу, що активують вразливості TLS, SSL та SNMP у firmware-атаках;

– побудувати ймовірнісну модель ризику для сценаріїв downgrade, перехоплення сесій і компрометації автентифікації;

– сформулювати оптимізаційну постановку вибору заходів автоматизації криптографічних політик;

– оцінити детекційні моделі CNN+LSTM і AE+LSTM у порівнянні з правилами IDS та кореляцією SIEM;

– надати практичні рекомендації для впровадження підходів Zero Trust на транспортному та керувальному рівнях.

Таким чином, завданням роботи є не лише порівняння технічних методів детекції, але й формування цілісної архітектури захисту, яка мінімізує вплив людського фактора через автоматизацію (policy-as-code) та перехід керувального контуру на захищені режими.

Методологія дослідження ґрунтується на системному підході до моделювання мереж електронних комунікацій як багаторівневої динамічної системи, структура якої відповідає еталонній моделі взаємодії відкритих систем OSI [1]. В умовах гібридних кібератак особлива увага приділяється транспортному та прикладному рівням, де реалізуються протоколи захищеної передачі

даних, зокрема Transport Layer Security (TLS) версії 1.3 [2], а також рекомендаціям щодо його конфігурації та безпечного використання [3].

У межах дослідження прийнято, що ризик порушення цілісності та конфіденційності даних формується як функція технічних параметрів протоколів, стану прошивки мережевого обладнання та людських управлінських рішень. З урахуванням емпіричних результатів аналізу вразливостей TLS [4], [5], [6] сформовано гіпотезу про кореляцію між дозволом застарілих криптографічних примітивів, downgrade-механізмами та реалізацією атак типу Logjam і FREAK. Додатково враховано ризики експлуатації легасі SSL та некоректних наборів шифрів у вебінтерфейсах firmware, що історично пов'язано з атаками класу POODLE та DROWN.

Методичний апарат дослідження поєднує формальне математичне моделювання ризику, імовірнісні оцінки сценаріїв атак та застосування алгоритмів глибокого навчання для аналізу мережевого трафіку. Для виявлення складних багатоступеневих атак використано комбіновані архітектури згорткових нейронних мереж та рекурентних мереж з довготривалою короткочасною пам'яттю (CNN+LSTM) із представленням трафіку у форматі Byte2Image, а також моделі автоенкодерів у поєднанні з LSTM (AE+LSTM) для детекції аномалій. Такий підхід відповідає сучасним тенденціям застосування штучного інтелекту в системах виявлення вторгнень (IDS) та платформах кореляції подій безпеки (SIEM). Окремий напрям методів стосується аналізу уразливостей керувального контуру, зокрема використання протоколу Simple Network Management Protocol (SNMP). Враховано ризики застосування SNMPv2c із дефолтними community-рядками та їх вплив на деградацію криптографічних політик і маніпуляції прошивкою. Для мінімізації таких загроз застосовано концепцію Zero Trust Architecture відповідно до сучасних рекомендацій [7], що передбачає жорстку автентифікацію, мікросегментацію та автоматизоване управління політиками доступу.Таким чином, методи дослідження інтегрують стандартизовані вимоги до захищених комунікацій [1]–[3], емпіричні результати аналізу криптографічних атак [4]–[6], а також підходи до побудови архітектур нульової довіри [7], формуючи комплексну модель оцінювання стійкості мереж електронних комунікацій в умовах гібридних кібератак.

**Виклад основного матеріалу**

**Об'єкт дослідження та дизайн експерименту**

Об'єктом дослідження є транспортний рівень мережі електронних комунікацій у режимі сервісної експлуатації, де TLS-термінація, маршрутизація запитів та керування мережевими елементами здійснюються у розподіленому середовищі. Для відтворюваності побудовано стенд із трьома логічними сегментами: – сервісний сегмент з TLS-термінацією на проксі та мікросервісами; – користувацький сегмент клієнтів, що ініціюють сесії та провокують сумісні сценарії; – керувальний сегмент з вебкеруванням і SNMP, типовими для пристроїв із вбудованим ПЗ.

Сценарій гібридної атаки включає дві взаємопов'язані фази. У фазі тиску на персонал моделюється інцидент доступності та сумісності: зростання помилок сертифікації, проблеми з ланцюжком довіри, часткові відмови сервісу та вимоги швидкого відновлення. Оператору надано можливість застосувати типові компроміси: вимкнути перевірку сертифіката на клієнті або проксі, знизити мінімальну версію TLS, дозволити ширші набори шифрів, активувати легасі-режим у вебінтерфейсі прошивки, залишити SNMP у спрощеному режимі. У фазі технічної експлуатації зловмисник використовує збережені винятки: реалізує downgrade під час узгодження параметрів, виконує атаку посередника на транспортному рівні, а також отримує доступ до керувального контуру через дефолтні SNMP параметри або слабкий захист вебінтерфейсу прошивки та змінює конфігурації, що впливають на TLS-політики.

Стійкість протоколів захищеної передачі даних у сучасних мережах електронних комунікацій дедалі більше визначається не лише криптографічною надійністю алгоритмів, а й соціотехнічними умовами їх експлуатації. Транспортний рівень моделі OSI виступає критичним вузлом довіри, де реалізуються механізми автентифікації, узгодження параметрів шифрування та керування сесіями. Проте фактичний рівень захисту формується на стику стандартів, конфігураційних практик і рішень персоналу, який у ситуаціях інцидентного тиску може допускати винятки, що знижують криптографічну стійкість.Актуальність проблематики посилюється гібридним характером сучасних атак, у яких технічна експлуатація поєднується з організаційним впливом.

На рисунку представлено узагальнену структурну схему соціотехнічних чинників, що впливають на виникнення вразливостей транспортного рівня. У верхній частині схеми виділено два полюси ризику: людський фактор (компроміси персоналу під тиском інцидентів) та технічний фактор (експозиція легасі-протоколів і небез-


**Рис. 1. Соціотехнічна модель формування вразливостей протоколів захищеної передачі даних та гібридної аналітики їх виявлення**

печних режимів). У центрі відображено ключову суперечність між формальним стандартом безпеки та реальним рівнем захисту, який формується в експлуатації.Нижній рівень ілюструє типові приклади атак і вразливостей (Logjam, FREAK, POODLE, DROWN, firmware-атаки, експлуатація SNMP), що активуються за наявності одночасно людського компромісу й технічної експозиції. Далі наведено блок гібридної аналітики виявлення, який поєднує сигнатурні механізми IDS, кореляцію подій у SIEM та моделі глибинного навчання (CNN+LSTM, AE+LSTM, Byte2Image). Завершальний елемент схеми демонструє інтегральний результат – перехід до підходу Zero Trust і автоматизації політик, що забезпечує істотне зниження ризику (приблизно на 85%) за рахунок мінімізації ручних винятків і контролю керувального контуру.

**Джерела даних та нормалізація подій**

Збиралися три класи даних: (1) мережеві метадані та події IDS (сигнатури, статистичні ознаки потоків, індикатори небезпечних узгоджень); (2) журнали сервісної інфраструктури (TLS-термінація, помилки перевірки сертифікатів, події відновлення сесій, конфігураційні зміни); (3) події керувального контуру (SNMP запити/записи, traps, журнали вебкерування) та байтові артефакти прошивки до і після змін. Події нормалізувалися до єдиного часово-ідентифікаційного формату та індексувалися у SIEM для кореляції. Якість журналювання оцінювалася за повнотою полів, часовою синхронізацією та трасованістю змін до суб'єктів доступу, що узгоджується з настановами з керування логами [22].

**Ймовірнісна модель ризику людського компромісу**

Нехай подія $H$ означає, що персонал прийняв компромісне рішення на транспортному рівні або в керувальному контурі (наприклад, вимкнув перевірку сертифіката або залишив дефолтний SNMP доступ). Нехай $V$ означає наявність технічної експозиції, тобто стану системи, який допускає експлуатацію (легасі SSL у прошивці, дозволені небезпечні набори шифрів, незахищений SNMPv2c). Нехай $A$ означає успішну атаку на множині критичних потоків. Контекст $x$ включає показники, що спостерігаються у SIEM: кількість інцидентних подій, середній час до відновлення сервісу, частоту ручних змін конфігурації, навантаження на персонал, рівень автоматизації політик. Імовірність компромісу задається логістичною моделлю:

$$\mathbb{P}(H=1\,|\,x)=\sigma\left(\beta_0+\beta^{\mathrm{T}}x\right),\qquad \sigma(z)=\frac{1}{1+e^{-z}}. \qquad (1)$$

Для $n$ критичних потоків, де експлуатація можлива лише за одночасної наявності компромісу та технічної експозиції, оцінка ймовірності успіху атаки:

$$\mathbb{P}(A=1)=1-\big(1-\mathbb{P}(H=1\mid x)\cdot\mathbb{P}(V=1)\big)^{n},\qquad R=L\cdot\mathbb{P}(A=1).\quad(2)$$

У такій постановці криптографічні стандарти й профілі TLS зменшують $\mathbb{P}(V=1)$, а організаційні практики та автоматизація впливають на $\mathbb{P}(H=1\mid x)$, тобто на схильність до ручних винятків.

**Оптимізаційна постановка автоматизації криптографічних політик**

Розглянемо набір заходів $u\in\{0,1\}^m$, де $u_i=1$ означає впровадження заходу: примусова перевірка сертифікатів, заборона downgrade і легасі-версій, ротація сертифікатів, взаємна автентифікація, перехід на SNMPv3, вимога підписаних оновлень прошивки, централізовані профілі TLS у вигляді політик як код [3, 9, 15, 30]. Задача вибору заходів формулюється як мінімізація ризику з урахуванням вартості:

$$\min_{u} R(u)+\lambda\sum_{i=1}^{m}c_iu_i\quad\text{заумови}\quad\sum_{i=1}^{m}c_iu_i\le B,\qquad(3)$$

де $c_i$ – витрати на впровадження заходу, $B$ – бюджет, $\lambda$ – коефіцієнт компромісу між ризиком та витратами. Оскільки $R(u)$ залежить від $\mathbb{P}(H=1\mid x,u)$ і $\mathbb{P}(V=1\mid u)$, автоматизація зменшує як людську схильність до винятків, так і технічну експозицію.

**Гібридна аналітика IDS та SIEM і нейромережеві моделі**

Дані формуються з мережевих подій IDS, журналів SIEM та байтових артефактів трафіку і прошивок. Для подання байтових послідовностей застосовується Byte2Image: фрагмент байтів перетворюється на матрицю інтенсивностей і розглядається як одноканальне зображення, що дозволяє використати CNN для виділення структурних ознак [26]. Часова складова моделюється через LSTM, що узгоджується з практикою рекурентних IDS [27]. Для задачі класифікації сценаріїв компромісів використовується зв'язка CNN+LSTM:

$$h_t=\mathrm{LSTM}(h_{t-1},\phi_{\mathrm{CNN}}(I_t)),\qquad \hat{y}_t=\mathrm{softmax}(Wh_t+b),\quad(4)$$

де $I_t$ – Byte2Image-вхід для вікна трафіку або артефакту прошивки, $\phi_{\mathrm{CNN}}(\cdot)$ – екстрактор ознак CNN [23], $\mathrm{LSTM}(\cdot)$ – рекурентний блок [24]. Навчальна розмітка формувалася за журналами змін конфігурацій та сценарієм стенду, що дозволило відокремити ручний компроміс від зловмисної деградації.

Для аномального детектування використовується автоенкодер (AE) для реконструкції агрегованих векторів подій SIEM/IDS і LSTM для урахування послідовності похибок:

$$e_t=\ x_t-g\big(f(x_t)\big)\ \tfrac{2}{2},\qquad s_t=\sigma\big(\alpha_0+\alpha_1e_t+\alpha^{\mathrm{T}}\mathrm{LSTM}(e_{t-k:t})\big),\quad(5)$$

де $x_t$ – вектор ознак подій (помилки сертифікації, зміни профілю TLS, активність SNMP), $f(\cdot),g(\cdot)$ – кодувальник і декодувальник автоенкодера [28], $s_t$ – оцінка аномальності. Концептуально цей підхід відповідає загальній парадигмі виявлення відхилень у часових рядах [25].

**Метрики**

Якість детекції оцінюється точністю, повнотою та $F_1$-мірою. Для ризикової частини оцінюється відносне зниження ризику "$R=\big(R_{\mathrm{manual}}-R_{\mathrm{auto}}\big)/R_{\mathrm{manual}}$ при переході від ручних винятків до автоматизованих політик. Для операційної придатності аналізується затримка детекції та частка помилкових тривог, а також вплив якості журналювання [22].

Запропонована методологія забезпечує відтворюване моделювання мереж електронних комунікацій в умовах гібридних кібератак через поєднання трьох компонентів: (1) стендового дизайну експерименту з чітким розділенням сервісного, користувацького та керувального сегментів; (2) уніфікованого збору й нормалізації подій IDS/SIEM та артефактів керувального контуру (включно з SNMP і firmware-подіями); (3) формальних моделей ризику, що розділяють людський компроміс і технічну експозицію. Така побудова дозволяє не «вгадувати винного», а вимірювати, де саме система стає вразливою: у політиках TLS/SSL, у керувальному контурі, чи в рішеннях персоналу під тиском інцидентності.

Імовірнісна модель ризику та оптимізаційна постановка вибору заходів перетворюють безпеку з набору рекомендацій на керовану задачу мінімізації інтегрального ризику з урахуванням вартості та обмежень впровадження. Гібридна аналітика (IDS+SIEM) підсилена нейромережевими моделями CNN+LSTM (із Byte2Image) та AE+LSTM, що дає змогу одночасно покривати: (а) структурні ознаки байтових послідовностей/узгоджень і (б) часові аномалії в потоках подій та конфігурацій. Визначені метрики (точність, повнота, F1, затримка детекції, відносне зниження ризику) забезпечують порівнюваність підходів і практичну інтерпретацію результатів для експлуатаційних рішень. Окремо методи підкреслюють ключовий практичний принцип: найбільший ефект досягається не «героїзмом чергового інженера», а зменшенням простору ручних винятків через автоматизацію криптографічних політик (policy-as-code) та переведення керувального контуру на безпечні режими (SNMPv3), що узгоджується з логікою Zero Trust. У підсумку, розділ «Методи» формує цілісну основу для розділу «Результати»: від відтворення сценаріїв компромісів до кількісного вимірювання їх впливу та оцінювання ефективності детекції й протидії.

У практиці експлуатації мереж захищена передача даних рідко «ламається» через сам стандарт шифрування – частіше вона деградує через сукупність дрібних рішень, які здаються виправданими в моменті. Коли сервіс падає, клієнти скаржаться, а час відновлення стискається до хвилин, персонал схильний робити тимчасові послаблення: дозволяти сумісність із застарілими режимами, приймати недовірені сертифікати або спрощувати керування пристроями. У підсумку виникає розрив між тим, що «має бути безпечно за стандартом», і тим, що реально працює в продуктивному середовищі.

Щоб керувати цим розривом, потрібна не тільки технічна конфігурація, а й формалізація ризику: які саме фактори штовхають систему до компромісу та як швидко цей компроміс перетворюється на вікно атаки. Важливо розуміти, що ризик накопичується: чим більше критичних потоків, сервісів і точок керування, тим вища ймовірність, що хоча б один елемент стане «слабкою ланкою». У такій картині безпеки головна небезпека – не одинична помилка, а повторюваний шаблон ручних винятків.

Саме тому акцент зміщується з «ловити атаки швидше» на «зменшити кількість ситуацій, де оператор може ненавмисно легалізувати вразливість». Автоматизація криптографічних політик і перехід до керованих, захищених механізмів адміністрування (у логіці Zero Trust) зменшує ризик системно: не за рахунок героїзму чергового інженера, а за рахунок обмеження простору для небезпечних компромісів.

На рисунку показано три взаємопов'язані частини, які пояснюють, як «людський компроміс» перетворюється на вимірюваний ризик і чому автоматизація різко змінює картину. Ліворуч наведено типову криву залежності: за низького навантаження і стабільної роботи система тримається в безпечному режимі, але після певного порогу (коли інцидентів/помилок стає забагато) ймовірність компромісних дій персоналу зростає дуже швидко. Це наочно демонструє нелінійність: невелике погіршення умов може різко підвищити ризик.

У центральному графіку показано, як ризик успішної атаки зростає зі збільшенням кількості критичних потоків. Сенс простий: що більше активних сесій/каналів/вузлів, то більше шансів, що хоча б один з них опиниться в умовах, де компроміс і технічна експозиція збігаються. Також видно, що за більш «компромісного» режиму експлуатації (коли ручні винятки трапляються частіше) крива росте суттєво швидше.Праворуч наведена підсумкова діаграма інтегрального ризику для трьох режимів: ручного, частково автома-

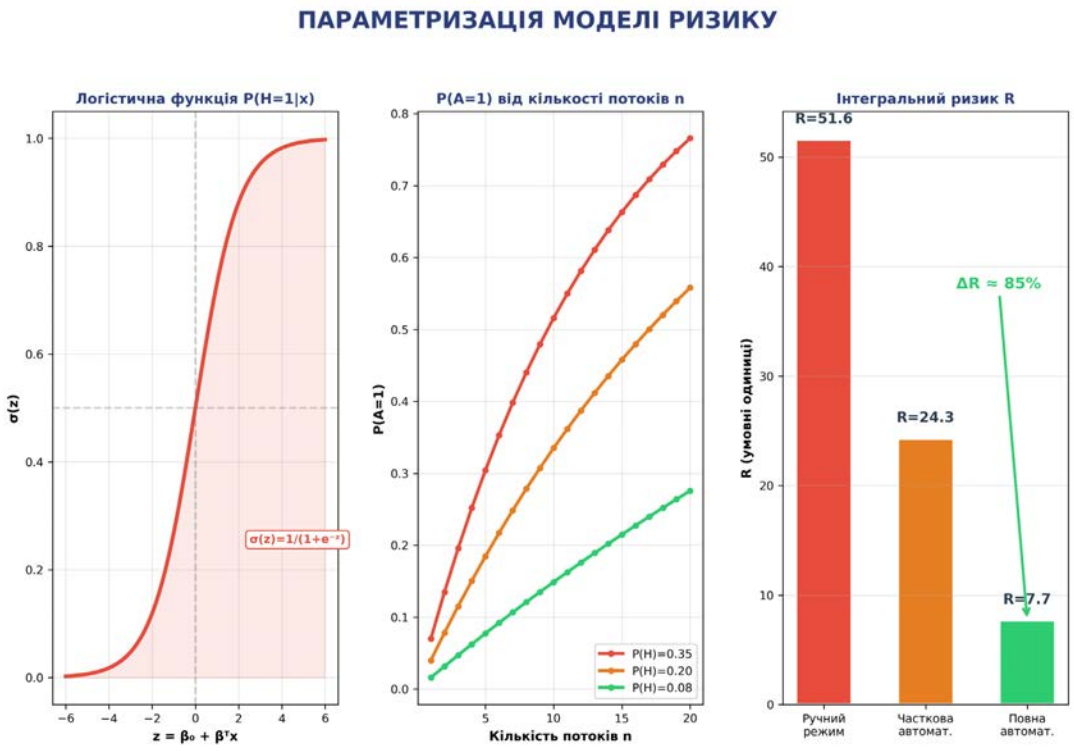


**Рис. 2. Параметризація моделі ризику та ефект переходу від ручного керування до повної автоматизації**

тизованого та повністю автоматизованого. Вона показує, що навіть часткова автоматизація вже помітно зменшує ризик, але максимальний ефект дає повний перехід до автоматизованих політик і безпечного керувального контуру – із зниженням ризику приблизно на 85%. Це і є головна ідея: найкращий результат досягається не «латанням» наслідків, а усуненням причин – тобто зменшенням простору для ручних небезпечних винятків.

**Результати.** У цьому розділі подано кількісні та якісні результати стендового експерименту, побудованого за методологією, описаною в розділі «Методи», де гібридна кібератака моделювалася як двофазний процес: (1) створення інцидентного тиску на персонал із провокуванням сумісних/доступнісних збоїв та (2) технічна експлуатація сформованих «легалізованих винятків» у конфігураціях транспортного рівня та керувального контуру. Центральним об'єктом аналізу є взаємодія двох чинників ризику: людського компромісу (вимкнення перевірки сертифіката, прийняття самопідписаних сертифікатів без контролю довіри, дозвіл downgrade і легасі TLS/SSL, збереження SNMPv2c із дефолтними community-рядками) та технічної експозиції (наявність слабких режимів узгодження, уразливі вебінтерфейси firmware, можливість конфігураційних маніпуляцій через SNMP). Саме їх одночасна присутність, відповідно до прийнятої ймовірнісної моделі, створює максимальне вікно можливостей для сценаріїв MITM, викрадення сесій, підміни вузлів і деградації TLS-політик через керування.

Результати структуровано у відповідності до застосованих інструментів вимірювання та критеріїв ефективності. По-перше, наведено емпіричну «карту компромісів» і їхніх наслідків, сформовану на основі нормалізованих подій IDS/SIEM та журналів змін конфігурації, що дозволяє простежити причинно-наслідкові ланцюги між діями оператора і реалізацією атаки. По-друге, представлено порівняння підходів детекції та протидії: сигнатурних спрацювань IDS, кореляції у SIEM та глибинних моделей CNN+LSTM і AE+LSTM. Для CNN+LSTM використано подання Byte2Image для байтових послідовностей трафіку/артефактів, що підсилює виявлення структурних «відбитків» downgrade та легасі-узгоджень; AE+LSTM застосовано для виявлення аномальних часових патернів у потоках подій (сертифікаційні помилки, серії SNMP-записів, конфігураційні зміни), зокрема в умовах неповного логування. Якість порівнюється за метриками точності, повноти та F1, а також за операційними показниками затримки детекції та відносного зниження ризику.

Окремо у «Результатах» подано числову ілюстрацію розрахунку інтегрального ризику на базі параметрів імовірності людського компромісу, технічної експозиції та кількості критичних потоків, щоб показати, як автоматизація криптографічних політик (policy-as-code) та перехід керувального контуру на SNMPv3 впливають на кінцеву ризикову величину. Таким чином, розділ демонструє не лише «що саме спрацювало», а й чому саме спрацювало: які компроміси є найбільш небезпечними, які механізми детекції стійкіші до гібридності сценарію, та який практичний ефект дає виключення ручних винятків у критичних параметрах TLS/SSL і керуванні пристроями.

**Емпірична карта компромісів та їхніх наслідків**

У режимі ручної експлуатації найчастіше фіксувалися компроміси, пов'язані з обхідними шляхами у TLS: вимкнення перевірки сертифікатів, прийняття самопідписаних сертифікатів без контролю довіри, зниження мінімальної версії протоколу та розширення наборів шифрів. Ці дії створювали умови для downgrade-атак, подібних до Logjam і FREAK, у частині деградації параметрів узгодження та повернення небезпечних режимів [5, 6]. Виявлено також ефект суміжних сервісів: наявність легасі-протоколів у прошивках або на периферії збільшувала експозицію до сценаріїв, аналогічних DROWN [7]. Активний fallback до SSL 3.0 у вебінтерфейсі керування формував умови для відтворення класу проблем, продемонстрованого POODLE [8]. У керувальному контурі ключовим ризиком став SNMPv2c із дефолтними community-рядками, що дозволяло змінювати конфігураційні параметри й опосередковано впливати на профіль TLS.

Таблиця 1 систематизує причинно-наслідковий зв'язок між конкретними управлінськими рішеннями персоналу та їх технічними наслідками на транспортному рівні мережі. Вона показує, що кожен «операційний компроміс», зроблений з міркувань швидкого відновлення сервісу або сумісності, безпосередньо трансформується у визначений клас атак.

Перший рядок демонструє, що вимкнення перевірки сертифіката або ігнорування помилок ланцюжка довіри фактично нівелює модель автентифікації TLS. У такому стані система стає вразливою до атаки посередника (MITM), підміни вузла та викрадення сесії, оскільки клієнт більше не перевіряє достовірність сервера.

Таблиця 1

**Компроміси людського фактора та їх технічні наслідки на транспортному рівні**

| № | Компроміс (людська дія) | Технічний наслідок та типові вектори атак |
|---|---|---|
| 1 | Вимкнення перевірки сертифіката або ігнорування помилок ланцюжка довіри | Атака посередника (MITM), підміна вузла, викрадення сесії, компрометація автентифікації |
| 2 | Дозвіл застарілих версій TLS для сумісності | Downgrade-атаки та повернення небезпечних режимів; кореляція з кейсами Logjam/FREAK |
| 3 | Прийняття самопідписаного сертифіката без контролю довіри та ротації | Підміна сертифіката, повторна автентифікація, порушення моделі довіри |
| 4 | Підтримка легасі SSL у вебінтерфейсі прошивки або слабких наборів шифрів | Експлуатація уразливостей класу POODLE/DROWN, компрометація керування |
| 5 | Використання SNMPv2c з дефолтними community-рядками в керувальному контурі | Несанкціоновані конфігураційні зміни, деградація TLS-політик, firmware-маніпуляції |

Другий рядок відображає наслідки дозволу застарілих версій TLS «для сумісності». Такий крок створює умови для downgrade-атак, коли зловмисник примусово знижує параметри узгодження до слабших режимів. Це концептуально узгоджується з кейсами Logjam і FREAK, де саме підтримка легасі-параметрів відкривала шлях до криптографічної деградації.

Третій рядок стосується прийняття самопідписаного сертифіката без формалізованого контролю довіри та ротації. У цьому випадку руйнується ієрархія довірених центрів сертифікації, що дозволяє підміну сертифіката та повторну автентифікацію під контролем зловмисника.

Четвертий рядок демонструє ризик підтримки легасі SSL або слабких наборів шифрів у вебінтерфейсах прошивки. Така практика створює канал для експлуатації історичних уразливостей класу POODLE або DROWN і може призвести до компрометації керування пристроєм.

П'ятий рядок відображає критичність керувального контуру: використання SNMPv2c з дефолтними community-рядками дозволяє несанкціоновані конфігураційні зміни. Наслідком є деградація TLS-політик та потенційні firmware-маніпуляції, що опосередковано впливають на транспортний рівень.

Таким чином, таблиця наочно підтверджує ключову тезу дослідження: уразливість транспортного рівня виникає не стільки через слабкість протоколів, скільки через легалізовані операційні винятки. Вона слугує емпіричною «картою компромісів», яка пов'язує людські дії з конкретними технічними векторами атак і формує основу для подальшого кількісного аналізу ризику, описаного у статті .

**Порівняння детекції: правила, кореляція та нейромережі**

Правила IDS, зокрема в реалізаціях типу Snort [20], швидко фіксують відомі індикатори (заборонені набори шифрів, підозрілі узгодження, нетипові поля), однак у гібридному сценарії вони часто не відрізняють легітимну компромісну дію оператора від атаки, оскільки симптоми збігаються. Кореляція у SIEM покращує відокремлення за рахунок журналів змін конфігурації та прив'язки до облікових записів, але її ефективність чутлива до повноти логів [22]. Мережеве спостереження у стилі Bro або Zeek [21] дає глибший контекст (сесійні ознаки, послідовність подій), проте потребує масштабованого зберігання.

Моделі CNN+LSTM та AE+LSTM демонструють кращу відтворюваність детекції, оскільки навчаються на послідовностях подій, які відображають як технічні, так і організаційні патерни. CNN+LSTM, базована на Byte2Image [26], краще відокремлює downgrade від ручних винятків, оскільки фіксує структурні сліди узгодження та повторювані ознаки легасі-параметрів. AE+LSTM краще виявляє повільні відхилення, наприклад поступове зростання сертифікаційних помилок або нетипові серії SNMP записів, що корисно при низькій спостережуваності атак.

Таблиця 2 відображає порівняльну оцінку ефективності різних підходів до виявлення та зниження ризику в умовах гібридних атак на транспортному рівні. Вона поєднує класичні сигнатурні та кореляційні механізми з моделями глибинного навчання й окремо демонструє ефект організаційно-технічної автоматизації політик.

Перший рядок характеризує IDS на основі сигнатур. Показники точності (0.81) та повноти (0.63) свідчать про здатність надійно фіксувати відомі індикатори, однак порівняно низька повнота означає втрату частини складних або нетипових сценаріїв. Затримка детекції мінімальна (1.1 с), що є перевагою для оперативного реагування, проте сумарне зниження ризику становить лише 18%, оскільки сигнатури не покривають організаційний компонент компромісів.

Другий рядок демонструє можливості SIEM-кореляції. Зростання точності до 0.86 і повноти до

0.75 пояснюється використанням журналів змін конфігурації та зв'язуванням подій з обліковими записами. Водночас затримка зростає до 4.6 с через необхідність агрегування та аналізу подій. Відносне зниження ризику (42%) суттєво вище, ніж у чистих сигнатур, але залежить від повноти логування [22] та коректності нормалізації подій.

Третій рядок представляє модель CNN+LSTM із перетворенням Byte2Image. Високі значення точності (0.92), повноти (0.89) та F1-міри (0.90) свідчать про здатність моделі одночасно враховувати структурні ознаки узгодження TLS і часову послідовність подій. Затримка (2.4 с) залишається прийнятною для практичного застосування. Найважливіше – відносне зниження ризику сягає 78%, що демонструє ефективність комбінованого аналізу технічних і поведінкових патернів.

Четвертий рядок (AE+LSTM) демонструє подібні інтегральні показники F1 (0.90) за рахунок високої повноти (0.91). Цей підхід краще виявляє поступові відхилення – наприклад, серії аномальних SNMP-записів або зростання помилок сертифікації. Затримка дещо більша (3.0 с), але зниження ризику становить 74%, що підтверджує ефективність автоенкодерного підходу при неповній розмітці.

Останній рядок – «Політики як код + SNMPv3» – не містить класичних метрик детекції, оскільки йдеться не про виявлення, а про превентивну зміну архітектури. Саме автоматизація криптографічних політик і перехід керувального контуру на захищену модель SNMPv3 забезпечують найбільший ефект – зниження ризику на 85%. Це підтверджує ключовий висновок роботи: найвища результативність досягається не лише вдосконаленням детекторів, а усуненням передумов для людських компромісів.

Таким чином, таблиця 2 демонструє еволюцію від реактивної детекції до проактивної архітектурної профілактики. Чим більше підхід інтегрує часовий контекст, структурні ознаки та автоматизацію політик, тим вищим є його внесок у реальне зниження інтегрального ризику, що узгоджується із загальною логікою дослідження.

Таблиця 2

**Порівняння підходів виявлення/протидії та їх впливу на ризик**

| Підхід | Точність | Повнота | F1 | Затримка, с | Зниження ризику, % |
|---|---|---|---|---|---|
| IDS (сигнатури) | 0.81 | 0.63 | 0.71 | 1.1 | 18 |
| SIEM (кореляція) | 0.86 | 0.75 | 0.80 | 4.6 | 42 |
| CNN+LSTM (Byte2Image) | 0.92 | 0.89 | 0.90 | 2.4 | 78 |
| AE+LSTM (аномалії) | 0.89 | 0.91 | 0.90 | 3.0 | 74 |
| Політики як код + SNMPv3 (автоматизація) | -- | -- | -- | -- | 85 |

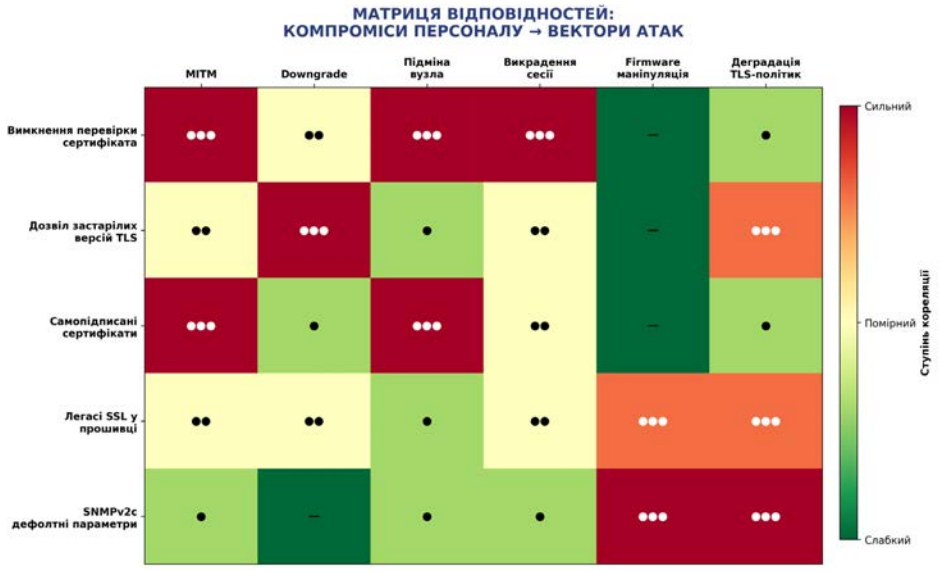


**Рис. 3. Порівняльна динаміка виявлення гібридної атаки та вплив автоматизації на часові характеристики детекції**

На рисунку відображено часову структуру розвитку гібридного сценарію та реакцію різних механізмів детекції. Перша фаза відповідає інцидентному тиску на персонал (зростання помилок сертифікації, конфігураційні зміни, активація сумісних режимів), друга – технічній експлуатації сформованих винятків (downgrade, MITM, маніпуляції через керувальний контур).Графічно показано, що сигнатурні механізми IDS фіксують окремі технічні індикатори вже на стадії активної експлуатації, проте часто пропускають початкову фазу організаційного компромісу. Кореляція у SIEM дозволяє пов'язати конфігураційні зміни з подальшими аномаліями, однак її спрацювання залежить від повноти журналювання. Нейромережеві моделі (CNN+LSTM та AE+LSTM) демонструють здатність виявляти відхилення раніше – ще на етапі накопичення аномальних патернів, що скорочує затримку детекції та зменшує тривалість вікна атаки.Таким чином, рисунок 3 ілюструє ключовий результат розділу: найбільш ефективною є не ізольована технологія, а інтегрована архітектура, де автоматизовані політики обмежують простір компромісів, а гібридна аналітика забезпечує своєчасне виявлення відхилень у динаміці системи. Отримані результати стендового експерименту підтверджують, що критичні інциденти на транспортному рівні виникають переважно як наслідок одночасної дії двох чинників: компромісних рішень персоналу під інцидентним тиском та наявної технічної експозиції (легасі-режими, уразливі компоненти прошивки, небезпечні налаштування керування). Саме їх поєднання формує «легалізовані винятки», які перетворюють формально захищену конфігурацію на практично вразливу та відкривають шлях до downgrade, MITM і маніпуляцій через керувальний контур. Порівняння підходів виявлення показало, що сигнатурні IDS ефективні для швидкого реагування на відомі індикатори, але мають обмеження у гібридних сценаріях, де технічні симптоми маскуються під «легітимну» операційну діяльність. Кореляція у SIEM підвищує якість відокремлення подій за рахунок журналів змін, проте її результативність критично залежить від повноти логування та трасованості конфігураційних дій. Натомість моделі CNN+LSTM та AE+LSTM демонструють кращу відтворюваність детекції, оскільки враховують як структурні, так і часові патерни, зменшуючи тривалість вікна атаки та підвищуючи стійкість до нетипових варіацій сценарію. Найбільш практично значущим результатом є те, що максимальне зниження інтегрального ризику досягається не лише посиленням детекторів, а архітектурним усуненням передумов компромісу: автоматизацією криптографічних політик, забороною ручних винятків і переведенням керувального контуру на захищені режими. Це узгоджується з логікою Zero Trust і пояснює, чому превентивні заходи дають більший ефект, ніж суто реактивні механізми виявлення. Разом із тим отримані дані потребують інтерпретації з урахуванням обмежень стенду, якості журналювання та організаційних компромісів між жорсткістю політик і операційною гнучкістю. Тому в наступному розділі «Discussion» зосередимося на поясненні причин спостережуваних ефектів, аналізі обмежень і переносимості результатів у реальні мережі, а також на формуванні практичних рекомендацій щодо впровадження підходів Zero Trust та «policy-as-code» у продуктивній експлуатації.

**Дискусія.** Результати підтверджують, що вразливості транспортного рівня мають соціотехнічну природу: технічна експозиція існує, але перетворюється на інцидент тоді, коли персонал легалізує виняток. На відміну від роботи [4], де основний акцент зроблено на формальній складності машин станів TLS і на тому, як граничні переходи та помилки обробки можуть відкривати поверхню атаки, у цьому дослідженні підкреслено механізм закріплення цієї поверхні в експлуатації. Якщо під час інциденту дозволяється вимикати перевірку сертифікатів або розширювати сумісність, то система починає функціонувати у режимі постійного ризику, який важко помітити традиційними сигнатурами.

Порівняно з Logjam [5], що демонструє можливість примусової деградації криптографічних параметрів у разі підтримки слабких груп, отримані дані показують, що подібна деградація часто запускається не лише активним зловмисником, а й самим персоналом, який розширює сумісність для швидкого відновлення сервісу. Тобто інженерний висновок полягає у зміщенні фокуса з пошуку універсально безпечного алгоритму на контроль процесу прийняття рішень і конфігураційного менеджменту, а також на автоматизацію політик.

Важливим компонентом є керувальний контур. Якщо SNMP залишається у незахищеному режимі або прошивка містить легасі SSL-компоненти, то зловмисник може обійти контроль транспортних політик опосередковано, змінюючи налаштування або підмінюючи артефакти довіри. Це означає, що заходи безпеки TLS мають супроводжуватися вимогами до резильєнтності прошивок [30] та базових кіберспроможностей пристроїв [16].

У термінах MITRE ATT&CK такі сценарії поєднують техніки доступу до керування, модифікації конфігурацій і персистентності [19]. Тому управління ризиком транспортного рівня має включати контроль прошивок, політики оновлення та аудит керувальних протоколів.

Обмеження дослідження пов'язані з умовністю стенду та параметризацією втрат. У реальних мережах різноманітність клієнтів і бібліотек TLS є значно вищою, а сумісність нерідко визначається вимогами партнерів або спадкових систем [10]. Друга група обмежень стосується повноти журналів: якщо логи з проксі, систем керування сертифікатами та мережевих пристроїв неповні, кореляція у SIEM втрачає контекст, а моделі машинного навчання отримують спотворені ознаки [22]. Третє обмеження – концептуальний дрейф, який вимагає регулярного перевчання моделей і контролю метрик на нових профілях трафіку [25]. Нарешті, організаційний компроміс полягає у балансі між жорсткістю політик і операційною гнучкістю: занадто суворі правила без процесу винятків можуть підштовхнути персонал до небезпечних обхідних практик.

Перспективи розвитку напряму пов'язані з Zero Trust. Архітектура нульової довіри [29] змінює фокус із разових налаштувань на безперервну перевірку, що природно зменшує простір для ручних винятків. Практично це означає централізоване керування політиками шифрування як код, короткоживучі сертифікати, взаємну автентифікацію там, де це виправдано, та автоматичну реакцію на деградацію параметрів. Другий перспективний напрям – multimodal AI: об'єднання часових рядів SIEM/IDS, байтових артефактів (Byte2Image), конфігураційних дифів, подій керувального контуру та навіть текстових заявок на зміни для точнішого відокремлення людського компромісу від атаки. У цій парадигмі детекція перетворюється на інструмент управління рішеннями, а не лише на сигнал про інцидент.

**Висновки.** Дослідження показало, що компроміси персоналу є системним джерелом вразливостей транспортного рівня: вимкнення валідації сертифікатів, допуск downgrade, підтримка легасі SSL у прошивках та небезпечні режими SNMP у керувальному контурі створюють умови для перехоплення сесій і компрометації автентифікації. Запропонована ймовірнісна модель ризику розділяє людський фактор і технічну експозицію, а оптимізаційна постановка дозволяє обґрунтовувати вибір заходів автоматизації. Показано, що поєднання кореляції у SIEM, сигналів IDS та глибинних моделей CNN+LSTM і AE+LSTM забезпечує кращу відтворюваність виявлення та підсилює аудит змін криптографічних профілів.

Практичні рекомендації: – впровадити політики TLS як код із забороною ручних винятків для перевірки сертифікатів і параметрів узгодження; – відмовитися від застарілих версій протоколу та слабких режимів сумісності відповідно до профілів і депрекацій [3, 13]; – перевести керувальний контур на SNMPv3 та закрити дефолтні налаштування прошивок [15]; – забезпечити підписані оновлення firmware, контроль компонентів SSL/TLS у вебінтерфейсах і відновлюваність платформи [30]; – підвищити якість журналювання та кореляції SIEM, щоб кожна зміна криптографічної політики мала трасованість до суб'єкта й причини [22]; – розвивати Zero Trust як організаційну практику, де довіра перевіряється безперервно, а критичні рішення максимально автоматизовані [29].

Таким чином, безпека транспортного рівня в умовах гібридних кібератак має розглядатися як задача управління компромісами: технічні стандарти потрібні, але вирішальним чинником є дисципліна конфігурацій, автоматизація політик і виключення людського фактора з критичних рішень.

**Список літератури:**

1. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3 : RFC 8446. 2018. DOI: https://doi.org/10.17487/RFC8446

2. Dierks T., Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.2 : RFC 5246. 2008. DOI: https://doi.org/10.17487/RFC5246

3. Sheffer Y., Holz R., Saint-Andre P. Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) : RFC 7525. 2015. DOI: https://doi.org/10.17487/RFC7525

4. Moriarty K., Farrell S. Deprecating TLS 1.0 and TLS 1.1 : RFC 8996. 2021. DOI: https://doi.org/10.17487/RFC8996

5. Sheffer Y., Holz R., Saint-Andre P. Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS) : RFC 7457. 2015. DOI: https://doi.org/10.17487/RFC7457

6. Harrington D., Presuhn R., Wijnen B. An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks : RFC 3411. 2002. DOI: https://doi.org/10.17487/RFC3411

7. Blumenthal U., Wijnen B. User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) : RFC 3414. 2002. DOI: https://doi.org/10.17487/RFC3414

8. McKay K. A., Cooper D. A. Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations : NIST SP 800-52 Rev. 2. – Gaithersburg, MD : National Institute of Standards and Technology, 2019. DOI: https://doi.org/10.6028/NIST.SP.800-52r2

9. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture : NIST SP 800-207. – Gaithersburg, MD : National Institute of Standards and Technology, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-207

10. Regenscheid A. Platform Firmware Resiliency Guidelines : NIST SP 800-193. – Gaithersburg, MD : National Institute of Standards and Technology, 2018. DOI: https://doi.org/10.6028/NIST.SP.800-193

11. Kent K., Souppaya M. Guide to Computer Security Log Management : NIST SP 800-92. – Gaithersburg, MD : National Institute of Standards and Technology, 2006. DOI: https://doi.org/10.6028/NIST.SP.800-92

12. Scarfone K., Souppaya M., Cody A., Orebaugh A. Technical Guide to Information Security Testing and Assessment : NIST SP 800-115. – Gaithersburg, MD : National Institute of Standards and Technology, 2008. DOI: https://doi.org/10.6028/NIST.SP.800-115

13. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS) : NIST SP 800-94. – Gaithersburg, MD : National Institute of Standards and Technology, 2007. DOI: https://doi.org/10.6028/NIST.SP.800-94

14. Joint Task Force. Security and Privacy Controls for Information Systems and Organizations : NIST SP 800-53 Rev. 5. – Gaithersburg, MD : National Institute of Standards and Technology, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-53r5

15. Cichonski P., Millar T., Grance T., Scarfone K. Computer Security Incident Handling Guide : NIST SP 800-61 Rev. 2. – Gaithersburg, MD : National Institute of Standards and Technology, 2012. DOI: https://doi.org/10.6028/NIST.SP.800-61r2

16. Joint Task Force Transformation Initiative. Guide for Conducting Risk Assessments : NIST SP 800-30 Rev. 1. – Gaithersburg, MD : National Institute of Standards and Technology, 2012. DOI: https://doi.org/10.6028/NIST.SP.800-30r1

17. Howell G., Franklin J., Sritapan V., Souppaya M., Scarfone K. Guidelines for Managing the Security of Mobile Devices in the Enterprise : NIST SP 800-124 Rev. 2. – Gaithersburg, MD : National Institute of Standards and Technology, 2023. DOI: https://doi.org/10.6028/NIST.SP.800-124r2

18. Fagan M. J., Megas K. N., Scarfone K., Smith M. IoT Device Cybersecurity Capability Core Baseline : NISTIR 8259A. – Gaithersburg, MD : National Institute of Standards and Technology, 2020. DOI: https://doi.org/10.6028/NIST.IR.8259A

19. Ross R., Pillitteri V., Dempsey K., Riddle M., Guissanie G. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations : NIST SP 800-171 Rev. 2. – Gaithersburg, MD : National Institute of Standards and Technology, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-171r2

20. Ross R., Pillitteri V., Guissanie G., Wagner R., Graubart R., Bodeau D. Enhanced Security Requirements for Protecting Controlled Unclassified Information : NIST SP 800-172. – Gaithersburg, MD : National Institute of Standards and Technology, 2021. DOI: https://doi.org/10.6028/NIST.SP.800-172

21. Beurdouche B., Bhargavan K., Delignat-Lavaud A., Fournet C., Kohlweiss M., Pironti A., Strub P.-Y., Zinzindohoue J. K. A Messy State of the Union: Taming the Composite State Machines of TLS // 2015 IEEE Symposium on Security and Privacy (SP). 2015. P. 535–552. DOI: https://doi.org/10.1109/SP.2015.39

22. Adrian D., Bhargavan K., Durumeric Z., Gaudry P., Green M., Halderman J. A., Heninger N., Springall D., Thomé E., Valenta L., VanderSloot B., Wustrow E., Zanella-Béguelin S., Zimmermann P. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice // Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15). 2015. P. 5–17. DOI: https://doi.org/10.1145/2810103.2813707

23. Xia H., Pei Q., Xi Y. The Analysis and Research of Freak Attack Based on OpenSSL // Proceedings of the 6th International Conference on Information Engineering for Mechanics and Materials. 2016. P. 15–19. DOI: https://doi.org/10.2991/icimm-16.2016.4

24. Paxson V. Bro: A System for Detecting Network Intruders in Real-Time // Computer Networks. 1999. Vol. 31(23–24). P. 2435–2463. DOI: https://doi.org/10.1016/S1389-1286(99)00112-7

25. LeCun Y., Bottou L., Bengio Y., Haffner P. Gradient-Based Learning Applied to Document Recognition // Proceedings of the IEEE. 1998. Vol. 86(11). P. 2278–2324. DOI: https://doi.org/10.1109/5.726791

26. Hochreiter S., Schmidhuber J. Long Short-Term Memory // Neural Computation. 1997. Vol. 9(8). P. 1735–1780. DOI: https://doi.org/10.1162/neco.1997.9.8.1735

27. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey // ACM Computing Surveys. 2009. Vol. 41(3). Art. 15. DOI: https://doi.org/10.1145/1541880.1541882

28. Nataraj L., Karthikeyan S., Jacob G., Manjunath B. S. Malware Images: Visualization and Automatic Classification // Proceedings of the 8th International Symposium on Visualization for Cyber Security (VizSec '11). 2011. P. 1–7. DOI: https://doi.org/10.1145/2016904.2016908

29. Yin C., Zhu Y., Fei J., He X. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks // IEEE Access. 2017. Vol. 5. P. 21954–21961. DOI: https://doi.org/10.1109/ACCESS.2017.2762418

30. Shone N., Ngoc T. N., Phai V. D., Shi Q. A Deep Learning Approach to Network Intrusion Detection // IEEE Transactions on Emerging Topics in Computational Intelligence. 2018. Vol. 2(1). P. 41–50. DOI: https://doi.org/10.1109/TETCI.2017.2772792

31. Sheffer Y., Saint-Andre P., Fossati T. Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) : RFC 9325. 2022. DOI: https://doi.org/10.17487/RFC9325

**Prokopovych-Tkachenko D.I., Torstensson O., Cherkaskyi D.O., Peremetchyk D.O., Bert S.D.**

**SOCIOTECHNICAL FACTORS IN THE EMERGENCE OF VULNERABILITIES IN NETWORK PROTOCOLS FOR SECURE DATA TRANSMISSION**

*The article presents a comprehensive analysis of sociotechnical factors that lead to the emergence of vulnerabilities in secure data transmission protocols during the operation of electronic communication networks. The purpose of the work is to formalize the contribution of human compromises to transport layer vulnerabilities and to develop a practical methodology for risk reduction through the automation of cryptographic policies and hybrid analytics using IDS and SIEM systems. A probabilistic risk model is proposed that separates the human factor (personnel compromises under incident pressure) and technical exposure (legacy protocols and insecure management modes). Typical compromise actions are considered, such as disabling certificate verification, accepting untrusted certificates, supporting outdated compatibility modes, and using insecure administration protocols like SNMPv2c, which create conditions for cryptographic degradation and session hijacking. For empirical validation, a hybrid attack testbed was used, modeling phases of organizational pressure and subsequent technical exploitation of "legalized exceptions." Special attention is given to the integration of detection mechanisms with deep learning models: convolutional and recurrent neural networks (CNN+LSTM) using the "Byte2Image" transformation for structural traffic analysis, and autoencoders combined with LSTM (AE+LSTM) for anomaly detection in event sequences. The results showed that transitioning to "policy-as-code" automation and secure management mechanisms (SNMPv3) significantly reduces the integral risk (by approximately 85%) by minimizing the space for manual dangerous exceptions. The limits of model applicability, the influence of logging quality, and the organizational balance between policy rigidity and operational flexibility are analyzed within the framework of Zero Trust Architecture.*

***Keywords:*** *transport, encryption, certification, trust, compatibility, interception, firmware, administration, correlation, neural networks, automation.*

Дата першого надходження статті до видання: 18.02.2026
Дата прийняття статті до друку після рецензування: 13.03.2026
Дата публікації (оприлюднення) статті 11.05.2026