КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1111
УДК 004.056.55:004.75

Костюк Юлія Володимирівна
PhD in Computer Science,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0001-5423-0985
y.kostiuk@kubg.edu.ua

Складанний Павло Миколайович
кандидат технічних наук, доцент
завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Мазур Наталія Петрівна
кандидат педагогічних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0001-7671-8287
n.mazur@kubg.edu.ua

Рзаєва Світлана Леонідівна
кандидат технічних наук, доцент,
доцент кафедри кафедри комп'ютерних наук
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-7589-2045
s.rzaieva@kubg.edu.ua

Гнатченко Дмитро Дмитрович
PhD in Computer Science,
старший викладач кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, м. Київ, Україна
ORCID: 0000-0002-6584-4525
hnatchenko@knute.edu.ua

Гончаренко Ігор Станіславович
кандидат технічних наук,
старший викладач кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, м. Київ, Україна
ORCID: 0000-0002-9022-6083
okjraa@gmail.com

ФОРМАЛЬНА МОДЕЛЬ АДАПТИВНОГО ВИБОРУ КРИПТОГРАФІЧНИХ ПАРАМЕТРІВ ЗАХИСТУ КАНАЛІВ У КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ НА ОСНОВІ ДИНАМІЧНОЇ ОЦІНКИ ДОВІРИ

Анотація. У статті запропоновано формальну модель адаптивного вибору криптографічних параметрів захисту каналів зв'язку в корпоративних комп'ютерних мережах на основі динамічної оцінки довіри та інтегрованого ризику. Актуальність зумовлена тим, що поширені практики статичного налаштування алгоритмів шифрування, режимів роботи та параметрів криптостійкості не враховують змін контексту доступу й поведінки суб'єктів взаємодії, що спричиняє або надмірні обчислювальні витрати, або виникнення вікон уразливостей під час ескалації загроз. Наукова новизна полягає у трактуванні криптографічного профілю як керованого динамічного стану системи безпеки, де довіра виступає безпосереднім керуючим

параметром криптографічної конфігурації, а не лише чинником рішення щодо доступу. Захищений канал формалізовано кортежем стану, який поєднує суб'єкта, ресурс, контекст, рівень довіри, ризик і криптографічний профіль, а адаптивний вибір параметрів описано відображенням, що встановлює відповідність між (критичністю ресурсу, контекстом) та набором криптографічних характеристик (алгоритм, режим, параметр стійкості, час життя сесії). Розроблено оптимізаційну постановку вибору профілю з урахуванням компромісу між криптографічною стійкістю та експлуатаційними витратами, а також подієво-орієнтований механізм оновлення криптографічного стану (Rekey/Upgrade/Revoke) у відповідь на деградацію довіри, зростання ризику або критичні події безпеки. Сценарний аналіз (нормальний режим, контекстна/поведінкова аномалія, критична подія) демонструє здатність моделі узгоджено підвищувати стійкість і скорочувати час життя криптографічних сесій у ризикових ситуаціях, зменшуючи потенційне вікно атаки та зберігаючи прийнятну продуктивність у низькоризикових умовах. Отримані результати формують теоретичну основу для впровадження адаптивних криптографічних профілів у TLS/VPN та Zero Trust-орієнтованих корпоративних середовищах.

Ключові слова: динамічна довіра; інтегрований ризик; криптографічний профіль каналу; подієво-орієнтоване оновлення; криптостійкість; Zero Trust; корпоративні комп'ютерні мережі.

ВСТУП

Стрімка еволюція корпоративних комп'ютерних мереж, зумовлена зростанням кількості розподілених сервісів, віддаленого доступу та інтеграції хмарних і локальних компонентів, істотно ускладнює завдання забезпечення конфіденційності та цілісності передавання даних. У сучасних умовах криптографічний захист каналів зв'язку залишається базовим механізмом інформаційної безпеки, проте у переважній більшості практичних реалізацій він ґрунтується на статичному виборі алгоритмів, режимів роботи та параметрів криптостійкості, що не враховують поточний стан безпеки мережі, зміну контексту доступу або поведінкові особливості суб'єктів взаємодії [1-2, 8-9, 11]. Такий підхід призводить до дисбалансу між рівнем захисту та експлуатаційною ефективністю, створюючи або надмірні обчислювальні витрати, або, навпаки, потенційні вікна уразливостей у разі зростання ризику.

Парадигми Zero Trust та ризик-орієнтованого управління доступом суттєво розширили уявлення про динамічну оцінку довіри в корпоративних мережах, проте у наявних дослідженнях криптографічні механізми розглядаються переважно як фіксований інфраструктурний шар, параметри якого не залежать від результатів оцінювання довіри чи ризику [6, 9-10]. Відсутність формалізованого зв'язку між рівнем довіри, контекстними та поведінковими факторами і параметрами криптографічного захисту каналів обмежує можливості адаптивного реагування системи безпеки на динамічні загрози та ускладнює побудову цілісних моделей захисту корпоративних мереж.

У зв'язку з цим актуальною є наукова проблема формалізації механізмів адаптивного вибору криптографічних параметрів захисту каналів зв'язку як функції поточного стану довіри та ризику в корпоративній комп'ютерній мережі [2-4, 6, 8]. Розв'язання цієї проблеми потребує переходу від статичних криптографічних конфігурацій до керованої моделі, у якій алгоритм шифрування, режим роботи, рівень криптографічної стійкості та час життя криптографічної сесії визначаються динамічно на основі формалізованої оцінки безпекового контексту.

Наукова новизна дослідження полягає у формалізації принципово нового підходу до забезпечення криптографічного захисту каналів зв'язку в корпоративних комп'ютерних мережах, у межах якого криптографічні параметри розглядаються не як статичні конфігураційні налаштування, а як динамічний керований стан системи безпеки [8, 11]. Запропонований підхід ґрунтується на інтеграції механізмів динамічної оцінки довіри та ризику з процесом вибору алгоритмів шифрування, режимів їх роботи, параметрів криптографічної стійкості та часу життя криптографічних сесій, що раніше у наукових працях розглядалися ізольовано або на концептуальному рівні.

Уперше криптографічний захист каналу формалізується як багатовимірний стан, параметри якого змінюються у часі під впливом контекстних, поведінкових та подієвих факторів безпеки [6, 9]. На відміну від існуючих моделей, у яких рівень довіри використовується виключно для прийняття рішень щодо доступу, у даній роботі довіра виступає безпосереднім керуючим параметром криптографічного профілю захищеного каналу [10-11, 19]. Це забезпечує формальний зв'язок між результатами оцінювання безпеки та рівнем криптографічного захисту передавання даних, що дозволяє адаптувати криптографічні механізми до поточного стану мережі.

Подальший розвиток наукової новизни полягає у введенні подієво-орієнтованого механізму еволюції криптографічного стану, за якого параметри захисту каналів коригуються не лише за часовими інтервалами, а у відповідь на виявлені події безпеки, зміни поведінки суб'єктів або зростання ризику [15, 21, 24]. Такий підхід дозволяє мінімізувати періоди використання потенційно скомпрометованих криптографічних параметрів та зменшити вікно можливих атак без необхідності повного розриву мережевих з'єднань.

Важливим елементом наукової новизни є також формалізований опис залежності між критичністю інформаційних ресурсів, рівнем довіри та криптографічною стійкістю каналів зв'язку [9, 16]. Запропонована модель забезпечує узгоджене поєднання вимог безпеки та експлуатаційної ефективності, що дозволяє уникнути як надмірного ускладнення криптографічних механізмів у низькоризикових сценаріях, так і недостатнього рівня захисту в умовах підвищеної загрози. Таким чином, наукова новизна роботи полягає не лише у запропонуванні окремої моделі адаптивного вибору криптографічних параметрів, а й у формуванні нової концепції керування криптографічним захистом каналів у корпоративних мережах, яка поєднує формальні методи оцінювання довіри, ризику та криптографічної стійкості в єдину динамічну систему безпеки.

Теоретична цінність отриманих результатів полягає у розвитку формальних моделей захисту інформації в комп'ютерних мережах шляхом інтеграції криптографічних параметрів у загальну модель довіри та ризику [14]. Запропонована модель розширює існуючі підходи до оцінювання безпеки мережевих з'єднань, створюючи математичну основу для аналізу взаємозв'язку між довірою, ризиком та криптографічною стійкістю каналів зв'язку.

Практична цінність роботи полягає у можливості використання запропонованої моделі під час проєктування та модернізації систем захисту корпоративних комп'ютерних мереж, зокрема в архітектурах Zero Trust, системах управління доступом та захищених комунікаційних платформах [12, 18-19]. Результати дослідження можуть бути використані для реалізації механізмів адаптивного вибору криптографічних параметрів у реальних мережевих середовищах, що дозволяє підвищити рівень безпеки передавання даних без істотного погіршення продуктивності та керованості системи.

У роботі запропоновано підхід, у якому криптографічний профіль захищеного каналу розглядається не як фіксована конфігурація, а як керований динамічний стан, що узгоджено змінюється відповідно до довіри та інтегрованого ризику [9-11]. Це дозволяє перейти від статичних практик налаштування TLS/VPN до ризик-орієнтованого керування криптографічними параметрами з подієвим реагуванням. Основні науково-практичні результати полягають у такому: формалізовано стан захищеного каналу S_t із включенням криптографічного профілю K_t як керованої змінної; визначено відображення $\Phi(\cdot)$ та оптимізаційну постановку вибору профілю з компромісом між криптографічною стійкістю і експлуатаційними витратами; запропоновано подієво-орієнтований механізм еволюції криптографічного стану Rekey/Upgrade/Revoke, що мінімізує період використання потенційно скомпрометованих параметрів; введено метрики оцінювання ефективності (вікно атаки, частота оновлень, накладні витрати) та базові моделі для порівняння, що забезпечує відтворюваність результатів. Подальший виклад структуровано так, щоб послідовно перейти від постановки проблеми й аналізу джерел до формалізації стану каналу, постановки оптимізаційної задачі, механізму подієвого оновлення та сценарного аналізу з інтерпретацією практичних наслідків для TLS/VPN і Zero Trust-орієнтованих корпоративних середовищ.

Постановка проблеми. Забезпечення криптографічного захисту каналів зв’язку є одним із ключових завдань інформаційної безпеки корпоративних комп’ютерних мереж, особливо в умовах їх динамічного розвитку, зростання кількості розподілених сервісів та підвищення складності мережевих взаємодій [8-9]. У сучасних мережах криптографічні механізми шифрування трафіку, як правило, реалізуються на основі статично визначених алгоритмів, режимів роботи та параметрів криптостійкості, вибір яких здійснюється на етапі проєктування або первинного налаштування системи [2, 10, 22]. Такий підхід не враховує змінюваність контексту доступу, динаміку поведінки користувачів і сервісів, а також еволюцію загроз, що виникають у процесі експлуатації корпоративної мережі.

Одночасно з цим у межах сучасних архітектур інформаційної безпеки все ширше застосовуються механізми динамічної оцінки довіри та ризику, які використовуються для прийняття рішень щодо доступу до ресурсів, багатофакторної автентифікації або обмеження прав користувачів [9-10, 19]. Проте результати такої оцінки, як правило, не впливають на параметри криптографічного захисту каналів зв’язку, що залишаються незмінними незалежно від поточного стану безпеки [2, 8, 11, 16]. Відсутність інтеграції між механізмами оцінювання довіри та процесом керування криптографічними параметрами призводить до ситуації, коли рівень захисту передавання даних не відповідає актуальним загрозам або, навпаки, створює надмірне навантаження на мережеву інфраструктуру.

Таким чином, у сучасних корпоративних комп’ютерних мережах наявне протиріччя між необхідністю гнучкого, ризик-орієнтованого керування безпекою та використанням статичних криптографічних конфігурацій, що не адаптуються до змін стану мережі [2, 8-11]. Це протиріччя зумовлює виникнення потенційних вікон уразливостей у разі підвищення ризику, а також ускладнює досягнення оптимального балансу між криптографічною стійкістю та експлуатаційною ефективністю системи.

Наукова проблема, що розглядається у даній роботі, полягає у відсутності формалізованої моделі, яка дозволяла б пов’язати результати динамічної оцінки довіри та ризику з процесом вибору криптографічних параметрів захисту каналів зв’язку в корпоративних комп’ютерних мережах. Існуючі підходи не забезпечують математично обґрунтованого механізму адаптації алгоритмів шифрування, режимів їх роботи, рівня

криптографічної стійкості та часу життя криптографічних сесій відповідно до поточного стану безпеки мережі.

У зв'язку з цим актуальним є формулювання та розв'язання наукової задачі розроблення формальної моделі адаптивного вибору криптографічних параметрів захисту каналів зв'язку, яка б враховувала динамічний характер довіри, контексту доступу та ризику, а також забезпечувала узгоджене керування рівнем криптографічного захисту у часі. Розв'язання цієї задачі створює передумови для переходу від статичних криптографічних механізмів до адаптивних систем захисту каналів зв'язку, здатних ефективно реагувати на зміну безпекового середовища корпоративної мережі.

Для коректної інтерпретації запропонованої моделі необхідно явно визначити модель загроз і припущення щодо довіреної бази. У межах дослідження під захистом розглядаються: конфіденційність і цілісність даних у каналі зв'язку, ключовий матеріал та параметри криптографічної сесії (алгоритм, режим, параметр стійкості й час життя), а також контекстні атрибути, на основі яких формується динамічна оцінка довіри та ризику [2, 9, 14-15]. Супротивник моделюється як пасивний або активний: він може здійснювати прослуховування трафіку, спроби MITM, ініціювати компрометацію сесійних параметрів, провокувати деградацію безпекового контексту (наприклад, через підміну частини атрибутів контексту або імітацію аномальної поведінки), а також прагнути збільшити потенційне вікно атаки за рахунок утримання слабшого криптографічного профілю чи надто довгого часу життя сесії.

Водночас у межах даної роботи приймається, що криптографічні примітиви є стійкими у межах обраних параметрів, а компоненти довіреної бази (керування ключами/політиками, контроль доступу, механізми застосування політики на кінцевих вузлах) функціонують коректно та мають базові засоби забезпечення цілісності телеметрії [9, 11, 14]. Така постановка узгоджує подальшу формалізацію: адаптація криптографічних параметрів розглядається як реакція системи на зміну довіри та ризику за умов, що джерела сигналів можуть бути неповними або затриманими, а отже потребують порогів, гістерезису та політик стримування надмірно частих оновлень.

Аналіз останніх досліджень і публікацій. Останні дослідження у сфері захисту інформації в комп'ютерних мережах демонструють зростаючий інтерес до адаптивних криптографічних механізмів, однак реалізація цієї адаптивності має фрагментарний характер і рідко формалізується на рівні керування захищеними каналами корпоративних мереж. Зокрема, у роботі Zhang, Yang, Chen та ін. запропоновано метод адаптивного шифрування чутливих даних у середовищі дата-центрів на основі алгоритмів аналізу великих даних [1]. Незважаючи на практичну значущість такого підходу для захисту даних у сховищах, він не розглядає криптографічний захист мережевого каналу як динамічний об'єкт керування, а також не пов'язує вибір криптографічних параметрів із довірою чи ризиком у мережевому контексті.

Схожий напрямок представлений у роботі Kumar та Goel, де використано машинне навчання для адаптивного шифрування даних у fog-обчисленнях [3]. Автори показують можливість балансування між рівнем захисту та продуктивністю залежно від умов виконання, проте основна увага зосереджена на захисті даних і сервісів, а не на формалізованому керуванні криптографічними параметрами каналів зв'язку в корпоративних мережах. Аналогічно, Alanazi, Alhoweiti, Alhwaity та Alharbi пропонують гібридну адаптивну криптографічну архітектуру для ресурсно-обмежених IoT-пристроїв [4], у якій адаптація визначається апаратними та енергетичними обмеженнями, але не інтегрується з механізмами оцінки довіри та ризику на рівні мережевих з'єднань.

Більш близьким до задачі керування захищеними каналами є підхід, запропонований Pastor-Galindo, López-Millán, Marín-López та ін., які розробили фреймворк динамічної конфігурації TLS-з'єднань на основі стандартів [2]. Автори демонструють можливість зміни параметрів TLS-з'єднання, однак питання формального визначення правил такої адаптації залишається відкритим: у роботі не запропоновано математичної моделі, яка б пов'язувала вибір криптографічних параметрів із рівнем довіри, ризику або критичністю ресурсу в корпоративній мережі.

Фундаментальні властивості сучасних тунельних протоколів досліджуються у роботі Ruhault, Lafourcade та Mahmoud, де виконано уніфікований символьний аналіз безпеки протоколу WireGuard [7]. Отримані результати підтверджують криптографічну коректність протоколу, однак автори не ставлять за мету розгляд адаптивного керування параметрами криптографічної сесії залежно від динамічного стану мережі або довіри до суб'єктів взаємодії.

Питання криптоагільності систематизовано в оглядовій роботі Marchesi, Marchesi та Tonelli, де проаналізовано здатність сучасних систем безпеки до зміни криптографічних алгоритмів і параметрів у відповідь на еволюцію загроз, зокрема в контексті постквантової криптографії [8]. Автори наголошують на необхідності гнучкого керування криптографічними механізмами, проте криптоагільність розглядається переважно як інженерна властивість систем, без формалізації функцій вибору криптографічного профілю на основі довіри чи ризику.

Ризик-орієнтований підхід до адаптації механізмів безпеки розвивається у роботі Calvo та Beltrán, де запропоновано модель адаптивних контролів безпеки на основі оцінки ризику [9]. Подібний контекстно-ризиковий підхід для fog-IoT середовищ запропоновано Selvan та Mahinderjit Singh, які розглядають адаптивну модель протидії атакам на конфіденційність [10]. Водночас у зазначених роботах ризик використовується для керування політиками доступу або безпековими контролями загального рівня, без переходу до формалізованого вибору конкретних криптографічних параметрів захисту каналів зв'язку.

Окремий напрямок досліджень пов'язаний із протоколами узгодження ключів та аутентифікації. Так, Li, Ju, Zhao, Wei та Lan запропонували легковагову безсертифікатну схему автентифікованого узгодження ключів для спеціалізованих мереж (Internet of Drones) [5], що підвищує ефективність захищеної взаємодії. Проте ця робота зосереджена на властивостях окремої криптографічної схеми і не розглядає системне керування криптографічним профілем каналу у корпоративній мережі. Аналогічно, Pokhrel, Ghimire, Dawadi та Manzoni застосовують машинне навчання й гібридне шифрування для захисту повідомлень у середовищі програмно-керованих мереж SDN [6], однак адаптація здійснюється на рівні обміну повідомленнями, а не як формальна модель керування параметрами захищених каналів.

Таким чином, аналіз робіт Zhang et al. [1], Pastor-Galindo et al. [2], Kumar та Goel [3], Alanazi et al. [4], Li et al. [5], Pokhrel et al. [6], Ruhault et al. [7], Marchesi et al. [8], Calvo та Beltrán [9], Selvan та Mahinderjit Singh [10] свідчить, що сучасні дослідження або фокусуються на адаптивному шифруванні даних і сервісів, або розглядають криптографічну коректність протоколів і схем, або застосовують ризик-орієнтовані підходи без формального зв'язку з вибором параметрів криптографічного захисту каналів. Водночас відсутня цілісна формальна модель, у якій криптографічний профіль каналу зв'язку (алгоритм, режим, параметр криптографічної стійкості та час життя сесії) визначався б як функція динамічної оцінки довіри, інтегрованого ризику, контексту

доступу та критичності ресурсу з подієво-орієнтованим механізмом його оновлення. Усунення цієї прогалини і становить основний науковий фокус даного дослідження.

Мета статті. Метою даного дослідження є розроблення, формалізація та теоретичне обґрунтування адаптивної моделі вибору криптографічних параметрів захисту каналів зв'язку в корпоративних комп'ютерних мережах на основі динамічної оцінки довіри та ризику [2, 8-11]. Запропонована модель спрямована на забезпечення керованого та узгодженого вибору алгоритмів шифрування, режимів їх роботи, рівня криптографічної стійкості та часу життя криптографічних сесій відповідно до поточного стану безпеки мережі, контексту доступу та критичності інформаційних ресурсів.

Досягнення поставленої мети передбачає формалізований опис криптографічного захисту каналу як динамічного стану системи безпеки, параметри якого змінюються у часі під впливом подій безпеки, поведінкових та контекстних факторів [9-10]. У межах дослідження передбачається розроблення механізмів подієво-орієнтованої адаптації криптографічних параметрів, що дозволяє мінімізувати потенційні вікна уразливостей, підвищити стійкість каналів зв'язку до компрометації та водночас забезпечити прийнятний рівень експлуатаційної ефективності корпоративної мережі [11, 19]. Реалізація сформульованої мети також орієнтована на створення теоретичної основи для подальшого впровадження адаптивних механізмів керування криптографічним захистом у практичних системах корпоративних мереж, зокрема в архітектурах Zero Trust, системах управління доступом та захищених комунікаційних платформах.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Проведений аналіз наукових досліджень і сформульована постановка проблеми свідчать, що існуючі підходи до захисту каналів зв'язку в корпоративних комп'ютерних мережах не забезпечують формалізованого зв'язку між динамічною оцінкою довіри, рівнем ризику та параметрами криптографічного захисту [9-11]. Це унеможливлює побудову узгоджених механізмів адаптації криптографічних параметрів у відповідь на зміну безпекового стану мережі та обмежує ефективність ризик-орієнтованих архітектур безпеки.

З метою усунення зазначеної прогалини у подальшому викладі пропонується формальний опис захищеного каналу зв'язку як динамічного стану системи безпеки, параметри якого визначаються поточними значеннями довіри, ризику та контексту доступу. Такий підхід дозволяє розглядати криптографічні параметри не як фіксовані конфігураційні елементи, а як керовані змінні, що еволюціонують у часі відповідно до подій безпеки та зміни характеристик взаємодії.

У наступному підрозділі виконується формалізація стану захищеного каналу, що слугує базисом для подальшого визначення функцій адаптивного вибору криптографічних параметрів і подієво-орієнтованого механізму їх оновлення.

Формалізація стану захищеного каналу. У межах даного дослідження захищений канал зв'язку в корпоративній комп'ютерній мережі розглядається як динамічний об'єкт керування, стан якого визначається сукупністю параметрів безпеки, контексту доступу та криптографічних характеристик. На відміну від традиційних підходів, у яких криптографічні параметри фіксуються на етапі налаштування, запропонована модель трактує їх як змінні, що еволюціонують у часі відповідно до змін довіри та ризику [10-11]. Стан захищеного каналу зв'язку в момент часу t визначається кортежем:

$$S_t = \langle u, r, c_t, T_t, R_t, K_t \rangle, \quad (1)$$

де u – суб'єкт взаємодії (користувач, сервіс або процес), r – інформаційний ресурс або сервіс, до якого здійснюється доступ, c_t – контекст доступу в момент часу t, $T_t \in [0,1]$ – рівень довіри до суб'єкта, $R_t \in [0,1]$ – інтегрований рівень ризику, K_t – криптографічний профіль захищеного каналу.

Контекст доступу c_t подається у вигляді множини параметрів [10, 18]:

$$c_t = \left\{c_t^{(1)}, c_t^{(2)}, \dots, c_t^{(m)}\right\}, \quad (2)$$

де $c_t^{(i)}$ можуть відповідати мережевому сегменту, типу пристрою, часовим обмеженням, географічному розташуванню або характеристикам середовища виконання.

Криптографічний профіль захищеного каналу в момент часу t задається як [11]:

$$K_t = \langle A_t, M_t, L_t, \delta_t \rangle, \quad (3)$$

де A_t – клас або тип криптографічного алгоритму шифрування, M_t – режим його роботи, L_t – параметр криптографічної стійкості (наприклад, довжина ключа), δ_t – час життя криптографічної сесії. Таким чином, криптографічний захист каналу описується не одним параметром, а вектором характеристик, що дозволяє здійснювати гнучке керування рівнем безпеки.

Рівень довіри T_t визначається як агрегована оцінка поведінкових, контекстних і подієвих факторів:

$$T_t = f_T(c_t, b_t, e_t), \quad (4)$$

де b_t – поведінкові характеристики суб'єкта, e_t – множина подій безпеки, зафіксованих у момент часу t.

Інтегрований ризик визначається з урахуванням рівня довіри та критичності ресурсу [10, 19]:

$$R_t = f_R(T_t, c_t, Sens(r)), \quad (5)$$

$$R_t = clip\big(0, 1, \alpha(1 - T_t) + b \cdot RiskContext(c_t) + c \cdot Sens(r)\big),\ a, b, c \geq 0, \quad (6)$$

де $Sens(r) \in [0,1]$ – показник критичності інформаційного ресурсу, $RiskContext(c_t) \in [0,1]$ – нормована оцінка ризику контексту.

На рис. 1 наведено концептуальну схему моделі стану захищеного каналу. Захищений канал розглядається як динамічний стан S_t, що включає параметри доступу, довіри, ризику та криптографічного профілю. Рівень довіри формується на основі контекстних, поведінкових і подієвих факторів, тоді як інтегрований ризик визначається з урахуванням довіри, контексту та критичності ресурсу. Криптографічний профіль K_t виступає керованою складовою стану каналу.

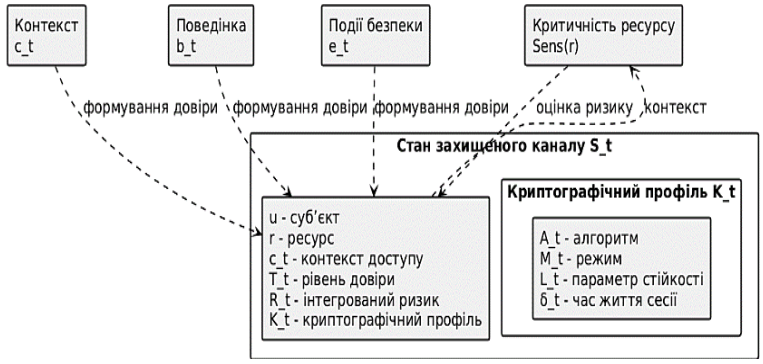

Рис. 1. Концептуальна схема моделі стану захищеного каналу

Оскільки в моделі довіра та ризик виступають керуючими змінними, важливо задати відтворюваний спосіб їх обчислення з нормованих факторів. Нехай кожен фактор контексту/поведінки/подій подається нормованою величиною $x_{i,t} \in [0,1]$, що характеризує безпековий стан (наприклад, відповідність пристрою політиці, стабільність геолокації, відповідність часовому вікну доступу, оцінка UEBA, ознаки підозрілої активності) [10, 19]. Тоді рівень довіри T_t може бути визначений як агрегована функція, що забезпечує монотонне зниження довіри за погіршення факторів, наприклад через логістичну агрегацію: $T_t = \sigma\left(\beta_0 + \sum_i \beta_i x_{i,t}\right)$, де $\sigma(\cdot)$ – логістична функція, а коефіцієнти β_i відображають вагомість факторів у конкретному корпоративному середовищі.

Інтегрований ризик R_t доцільно пов'язати з недовірою $(1 - T_t)$, критичністю ресурсу $Sens(r)$ та ризиком контексту $RiskContext(c_t)$, що дозволяє узгоджено підсилювати захист для критичних ресурсів навіть за помірних відхилень контексту. У такому разі R_t визначається як нормована композиція з обмеженням на інтервал $[0,1]$, що забезпечує коректність подальших порогових правил і оптимізаційної постановки, а також дозволяє інтерпретувати R_t як керуючий сигнал для скорочення часу життя криптографічних сесій та ініціювання подієвого оновлення профілю.

Еволюція стану захищеного каналу описується рівнянням переходу:

$$S_{t+1} = \Psi(S_t, e_t), \tag{7}$$

де e_t – подія безпеки, що може спричинити зміну рівня довіри, ризику або криптографічного профілю каналу. Таким чином, захищений канал розглядається як динамічна система зі станом, у якій криптографічні параметри є керованими змінними, що оновлюються у відповідь на зміну безпекового контексту.

Адаптивний вибір криптографічного профілю формалізується у вигляді відображення:

$$K_t = \Phi(T_t, R_t, Sens(r), c_t), \tag{8}$$

що встановлює відповідність між поточним станом довіри та ризику і параметрами захисту каналу.

Для параметра криптографічної стійкості справедливо:

$$p_t = clip(0, 1, w_R R_t + w_T(1 - T_t)), \tag{9}$$

$$L_t = clip(L_{min}, L_{max}, L_{min} + (L_{max} - L_{min})p_t), \tag{10}$$

що означає, чим менша довіра і більший ризик, тим більша стійкість.

Дискретно (реалістично для TLS/VPN):

$$L_t \in \{128, 192, 256\},\ L_t = \begin{cases} 128, & p_t < \theta_1 \\ 192, & \theta_1 \le p_t < \theta_2, \\ 256, & p_t \ge \theta_2 \end{cases} \quad (11)$$

Час життя криптографічної сесії визначається як:

$$\delta_t = cli\,p\big(\delta_{min}, \delta_{max}, \delta_{max}(T_t - \lambda R_t)\big), (\lambda \in [0,1]), \quad (12)$$

де λ – коефіцієнт чутливості до ризику.

Подієве оновлення криптографічного профілю ініціюється у разі виконання умови:

$$R_t \ge R_{crit} \ \vee \ T_t \le T_{crit}, \quad (13)$$

що відповідає сценаріям зростання загрози або деградації довіри.

Щоб керування криптографічним профілем відповідало інтуїції ризик-орієнтованого підходу, параметр криптографічної стійкості та час життя сесії мають змінюватися монотонно: зі зростанням ризику або зниженням довіри стійкість повинна підвищуватися, а час життя сесії – скорочуватися [9-11]. Тому залежності для L_t та δ_t доцільно визначати з явними межами та операцією обмеження, щоб уникнути некоректних значень (наприклад, від'ємного часу життя).

Параметр стійкості L_t задається як керована величина в межах $[L_{min}, L_{max}]$ із зростанням при збільшенні R_t та/або зменшенні T_t, тоді як час життя криптографічної сесії δ_t обмежується інтервалом $[\delta_{min}, \delta_{max}]$ і зменшується в ризикових режимах. У межах такої логіки подієве оновлення криптографічного профілю ініціюється, якщо ризик перевищує критичний поріг або довіра знижується нижче допустимого рівня, тобто за умов типу $R_t \ge R_{crit} \ \vee \ T_t \le T_{crit}$. Це забезпечує узгодженість моделі: у підвищено ризикових ситуаціях система переходить до більш стійких, але короткоживучих сесій, мінімізуючи потенційне вікно атаки, тоді як у низькоризикових умовах зберігається продуктивність завдяки помірним параметрам і довшим сесіям.

Адаптивний вибір криптографічних параметрів. На основі формалізованого опису стану захищеного каналу криптографічні параметри розглядаються як керовані змінні, вибір яких здійснюється адаптивно залежно від поточного рівня довіри, інтегрованого ризику, контексту доступу та критичності інформаційного ресурсу. Такий підхід дозволяє перейти від статичних криптографічних конфігурацій до динамічного керування рівнем захисту каналів зв'язку в корпоративній комп'ютерній мережі.

Нехай множина допустимих криптографічних профілів визначається як:

$$\mathcal{K} = \{K^{(1)}, K^{(2)}, \dots, K^{(n)}\}, \quad (14)$$

де кожен профіль $K^{(i)}$ описується кортежем:

$$K^{(i)} = \langle A^{(i)}, M^{(i)}, L^{(i)}, \delta^{(i)} \rangle, \quad (15)$$

Оптимізаційний вибір профілю має враховувати не лише критерій "безпека/вартість", а й політики допустимості, сумісність і мінімальні вимоги для критичних ресурсів. Тому множину кандидатів доцільно звузити до дозволених профілів $K_{allow}(r, c_t)$, які відповідають політикам безпеки підприємства, регуляторним

обмеженням і технічній сумісності кінцевих вузлів. Зокрема, для ресурсів із високою критичністю задається мінімально допустимий рівень криптографічної стійкості та/або обмеження на використання слабких режимів, а для певних контекстів (наприклад, зовнішній сегмент або невідомий пристрій) – заборона на профілі, що не забезпечують необхідного рівня захисту [10, 19]. У такій постановці оптимізація набуває практичного сенсу, оскільки рішення формується в межах політик, а не лише математичного максимуму, і може бути безпосередньо застосоване до TLS/VPN конфігурацій.

Для переходу від абстрактної множини допустимих криптографічних профілів K до практично реалізовної процедури оптимізаційного вибору введемо каталог типових криптографічних профілів $K^{(i)}$, що визначають допустимі комбінації алгоритмів, режимів роботи, параметрів криптографічної стійкості та часу життя сесій у корпоративній мережі (табл.1).

Таблиця 1

Каталог криптографічних профілів $K^{(i)}$ та їх параметри

ID профілю $K^{(i)}$	**$A^{(i)}$ (алгоритм / клас)**	**$M^{(i)}$ (режим)**	**$L^{(i)}$ (параметр стійкості)**	**$\delta^{(i)}$ (номінальний час життя)**	**Примітка / умови допустимості**
$K^{(1)}$	Симетричне шифрування (AES)	GCM	128	δ_{max}	Низькоризиковий контекст, внутрішній сегмент
$K^{(2)}$	Симетричне шифрування (AES)	GCM	192	$0{,}7\delta_{max}$	Стандартний корпоративний доступ
$K^{(3)}$	Симетричне шифрування (AES)	GCM	256	$0{,}5\delta_{max}$	Підвищена критичність ресурсу
$K^{(4)}$	Симетричне шифрування (ChaCha20)	Poly1305	256	$0{,}5\delta_{max}$	Мобільні / ресурсно-обмежені клієнти
$K^{(5)}$	Гібридний профіль (ECC + AES)	AEAD	256	$0{,}3\delta_{max}$	Зовнішній сегмент, нестабільний контекст
$K^{(6)}$	Посилений профіль	AEAD + частий Rekey	256	δ_{min}	Критичні ресурси, високий ризик
$K^{(7)}$	Максимальний захист	AEAD + примусовий Rekey	≥256	δ_{min}	Критичні події безпеки, деградація довіри

Таким чином, множина криптографічних профілів $K = \{K^{(1)}, \dots, K^{(n)}\}$ задає дискретний простір допустимих конфігурацій захисту каналу, у межах якого здійснюється оптимізаційний вибір відповідно до (16)–(22) [16, 23]. Кожен профіль характеризується узгодженим набором параметрів $\langle A^{(i)}, M^{(i)}, L^{(i)}, \delta^{(i)} \rangle$ та обмеженнями застосовності, що забезпечує практичну реалізовність адаптивного керування криптографічним станом каналу.

Задача адаптивного вибору криптографічних параметрів полягає у визначенні такого профілю $K_t^* \in \mathcal{K}$, який максимізує узгоджений критерій безпеки та ефективності за поточного стану каналу [23]:

$$K_t^* = \arg\max_{K^{(i)} \in \mathcal{K}} \mathcal{F}\left(K^{(i)}, T_t, R_t, Sens(r), c_t\right), \tag{16}$$

Цільова функція $\mathcal{F}(\cdot)$ визначається як зважена комбінація показників криптографічної стійкості та експлуатаційних витрат [16, 23]:

$$\mathcal{F} = \alpha \cdot S_{sec}\left(K^{(i)}, Sens(r)\right) - \beta \cdot C_{perf}\left(K^{(i)}, c_t\right), \quad (17)$$

де $\alpha, \beta \geq 0$ – коефіцієнти пріоритетності, S_{sec} – оцінка рівня криптографічного захисту, C_{perf} – оцінка обчислювальних та мережевих витрат. Максимізація цільової функції $\mathcal{F}$ забезпечує вибір такого криптографічного профілю, який є оптимальним з точки зору узгодженого впливу безпекових і продуктивнісних чинників у поточному контексті доступу. За рахунок параметрів α і β модель дозволяє формалізувати політику керування криптографічними ресурсами та гнучко адаптувати її до змін вимог безпеки або обмежень мережевого середовища.

Оцінка криптографічної стійкості визначається як [16]:

$$S_{sec} = w_1 \cdot \frac{L^{(i)}}{L_{max}} + w_2 \cdot \left(1 - \frac{\delta^{(i)}}{\delta_{max}}\right), \quad (18)$$

де $w_1 + w_2 = 1$.

Витрати експлуатації визначаються як:

$$C_{perf} = g\left(A^{(i)}, M^{(i)}, c_t\right), \quad (19)$$

де функція $g(\cdot)$ відображає обчислювальне навантаження та затримки, пов'язані з використанням відповідного криптографічного профілю в заданому контексті.

Для забезпечення адаптивності вводиться корекція параметрів криптографічного профілю залежно від поточного стану безпеки:

$$L_t^{(i)} = clip(L_{min}, L_{max}, L^{(i)} \cdot \left(1 + \gamma(R_t - T_t)\right)), \quad (20)$$

$$\delta_t^{(i)} = clip(\delta_{min}, \delta_{max}, \delta^{(i)} T_t (1 - R_t), \quad (21)$$

де γ – коефіцієнт чутливості до змін довіри та ризику [24]. Таким чином, за зростання ризику або зниження довіри система автоматично переходить до більш стійких, але короткоживучих криптографічних сесій. Використання оператора $clip$ $(\cdot)$ забезпечує дотримання допустимих меж параметрів та запобігає надмірному посиленню або ослабленню криптографічного захисту внаслідок флуктуацій показників довіри та ризику. Така форма корекції дозволяє плавно адаптувати рівень криптографічної стійкості до поточного безпекового стану, зберігаючи баланс між вимогами захисту та експлуатаційною ефективністю каналу.

На основі наведених співвідношень алгоритм адаптивного вибору криптографічних параметрів може бути подано у такому вигляді [23]:

Алгоритм 1. Адаптивний вибір криптографічного профілю каналу

1. Отримати поточний стан каналу $S_t = \langle u, r, c_t, T_t, R_t, K_t \rangle$.
2. Визначити множину допустимих криптографічних профілів $\mathcal{K}$ з урахуванням політик безпеки.

3. Для кожного $K^{(i)} \in \mathcal{K}$ обчислити скориговані параметри $L_t^{(i)}$ та $\delta_t^{(i)}$.
4. Обчислити значення цільової функції $\mathcal{F}\left(K^{(i)}, T_t, R_t, Sens(r), c_t\right)$.
5. Вибрати оптимальний профіль:

$$K_t^* = \arg\max_{K^{(i)} \in \mathcal{K}} \mathcal{F}, \tag{22}$$

6. Застосувати обраний криптографічний профіль K_t^* для захищеного каналу та ініціювати його подієве оновлення за потреби.

Запропонований алгоритм забезпечує формалізований і відтворюваний механізм вибору криптографічних параметрів з урахуванням поточного безпекового стану каналу та контексту доступу. Його структура дозволяє узгоджено інтегрувати оцінки довіри, ризику й критичності ресурсу в єдину оптимізаційну процедуру без жорсткої прив'язки до конкретних криптографічних алгоритмів. Використання цільової функції забезпечує баланс між рівнем захисту та експлуатаційними витратами у різних сценаріях функціонування мережі. Подієва ініціація оновлення криптографічного профілю дозволяє своєчасно реагувати на деградацію безпекового середовища, мінімізуючи потенційні вікна атак без порушення безперервності захищеного з'єднання.

На рис. 2 наведено формалізований псевдокод алгоритму адаптивного вибору криптографічного профілю захищеного каналу, який розглядає криптографічні параметри як керовані змінні динамічної системи. Алгоритм здійснює відбір допустимих криптографічних профілів з урахуванням політик безпеки, контексту доступу та критичності ресурсу, після чого оптимізує вибір за узгодженим критерієм «рівень захисту – експлуатаційні витрати». Подієва корекція параметрів дозволяє скорочувати потенційне вікно атаки в умовах зростання ризику та деградації довіри, зберігаючи ефективність у нормальних режимах функціонування мережі.

Algorithm 1. Adaptive Selection of the Channel Cryptographic Profile

```
Input:
  S_t = (u, r, c_t, T_t, R_t, K_t)          // current channel state
  K = {K^(1), K^(2), …, K^(n)}              // candidate profiles
  Policies, Constraints                     // security rules & compatibility
  Sens(r) ∈ [0,1]                           // asset criticality
  Parameters: α, β ≥ 0; w1, w2 (w1+w2=1); γ; bounds L_min,L_max, δ_min,δ_max

Output:
  K*_t                                      // selected cryptographic profile

Procedure:
1:  K_allow ← FilterAllowed(K, r, c_t, Policies, Constraints)
2:  if K_allow = ∅ then
3:      K_allow ← FallbackSecureSet(K, r, c_t)      // fail-safe set
4:  end if
5:  bestScore ← −∞
6:  K*_t ← null
7:  for each K^(i) ∈ K_allow do
8:      // K^(i) = (A^(i), M^(i), L^(i), δ^(i))
9:      L_i ← clip(L_min, L_max, L^(i) · (1 + γ · (R_t − T_t)))
10:     δ_i ← clip(δ_min, δ_max, δ^(i) · T_t · (1 − R_t))
11:     S_sec ← w1 · (L_i / L_max) + w2 · (1 − δ_i / δ_max)
12:     C_perf ← g(A^(i), M^(i), c_t)
13:     F_i ← α · S_sec − β · C_perf
14:     if F_i > bestScore then
15:         bestScore ← F_i
16:         K*_t ← (A^(i), M^(i), L_i, δ_i)
17:     end if
18: end for
19: ApplyProfileTLSVPN(K*_t, r, c_t)
20: return K*_t
```

Рис. 2. Псевдокод алгоритму адаптивного вибору криптографічного профілю каналу

Запропонований алгоритм забезпечує формалізований і відтворюваний механізм вибору криптографічних параметрів, у якому рівень захисту каналу безпосередньо залежить від динамічної оцінки довіри та ризику [24]. На відміну від статичних підходів, така модель дозволяє зменшити потенційні вікна уразливостей у разі деградації безпекового стану та оптимізувати використання криптографічних ресурсів у низькоризикових сценаріях [12, 16]. Це створює основу для практичного впровадження адаптивних криптографічних механізмів у корпоративних комп'ютерних мережах.

Подієво-орієнтований механізм оновлення криптографічного стану. Адаптивний вибір криптографічних параметрів набуває практичної цінності лише за умови своєчасного оновлення криптографічного стану у відповідь на зміну безпекового середовища [12, 23]. У межах запропонованої моделі оновлення параметрів захищеного каналу реалізується за подієво-орієнтованим принципом, який доповнює періодичні механізми ротації ключів і дозволяє реагувати на критичні зміни стану довіри та ризику в реальному часі.

Подієво-орієнтований підхід передбачає ініціювання оновлення криптографічного профілю не за фіксованим часовим інтервалом, а у відповідь на виявлення значущих змін контексту доступу, поведінкових аномалій або зростання інтегрованого ризику. Це дозволяє суттєво скоротити часовий проміжок між моментом виникнення загрози та застосуванням посилених криптографічних параметрів. На відміну від суто таймерних схем ротації ключів, подієва адаптація зменшує ймовірність тривалого використання потенційно скомпрометованого ключового матеріалу. Водночас у сценаріях помірної деградації безпекового стану зберігається безперервність захищеного з'єднання, що позитивно впливає на експлуатаційну ефективність корпоративної мережі.

Подією безпеки e_t називається зафіксована зміна стану системи, що може впливати на рівень довіри, ризику або криптографічну стійкість каналу, та описується кортежем [15, 23]:

$$e_t = \langle type, sev, src, \tau \rangle, \tag{23}$$

де $type$ – тип події (поведінкова аномалія, зміна контексту, порушення політики), $sev \in [0,1]$ – рівень критичності події, src – джерело події, τ – час виникнення події. Такий формалізований опис події безпеки дозволяє уніфікувати обробку різнорідних сигналів, що надходять із систем моніторингу, виявлення вторгнень та контролю доступу. Параметр sev відображає інтенсивність впливу події на безпековий стан каналу та використовується як тригер для ініціювання адаптивних дій на криптографічному рівні. Атрибут src забезпечує можливість кореляції подій з конкретними компонентами інфраструктури та підвищує достовірність оцінки ризику. Урахування часової мітки τ дозволяє аналізувати динаміку розвитку інцидентів і коректно реагувати на швидкі або накопичувальні зміни безпекового контексту.

Подієве оновлення криптографічного стану ініціюється за виконання хоча б однієї з умов [11-12]:

$$(T_{t+1} < T_{crit}) \vee (R_{t+1} > R_{crit}) \vee sev(e_t) \geq (sev_{crit}) \vee (\Delta T_t > \varepsilon_T) \vee (\Delta R_t > \varepsilon_R), \tag{24}$$

де T_{crit}, R_{crit} – порогові значення довіри та ризику, $\varepsilon_T, \varepsilon_R$ – допустимі швидкості зміни відповідних показників. Виконання наведених умов відображає настання критичних змін безпекового контексту, які потребують негайної адаптації криптографічного профілю з метою мінімізації потенційного вікна атаки. Такий подієво-орієнтований механізм

дозволяє системі реагувати не лише на абсолютні значення довіри та ризику, але й на їх динаміку, забезпечуючи більш чутливе й своєчасне оновлення параметрів захищеного каналу.

Оновлення криптографічного стану здійснюється шляхом переходу:

$$K_{t+1} = \begin{cases} Rekey(K_t). & sev(e_t) \geq (sev_{crit}) \\ Upgrade(K_t). & (R_{t+1} \geq R_{crit} \vee T_{t+1} \leq T_{crit} \\ Revoke(K_t), & \Delta T_t > \varepsilon_T \ \vee \Delta R_t > \varepsilon_R \\ K_t & \text{інакше} \end{cases}, \quad (25)$$

Операція Rekey передбачає зміну ключового матеріалу без зміни алгоритму, Upgrade – перехід до більш стійкого алгоритму або режиму роботи, Revoke – негайне завершення криптографічної сесії та ініціацію повторного встановлення захищеного каналу. Такий механізм переходів забезпечує градуйовану реакцію системи безпеки залежно від рівня критичності події та динаміки зміни довіри й ризику. Це дозволяє мінімізувати експлуатаційні втрати в умовах помірних загроз і водночас гарантувати негайну ізоляцію каналу у разі виявлення критичних або швидко ескалуючих атак. У результаті криптографічний стан каналу розглядається як керована динамічна величина, що адаптується до поточного безпекового контексту без порушення цілісності загальної архітектури захисту.

На рис. 3. представлено подієвий цикл адаптації криптографічного профілю захищеного каналу. Телеметрія та події безпеки використовуються для оцінки рівня довіри й інтегрованого ризику [12-13]. У разі виконання тригерних умов ініціюється рішення щодо оновлення криптографічного профілю (Rekey, Upgrade або Revoke), після чого оновлений профіль застосовується до каналу та цикл моніторингу повторюється.

Рис. 3. Подієвий цикл адаптації криптографічного профілю захищеного каналу

Для демонстрації впроваджуваності запропонованого підходу доцільно показати архітектурне розміщення механізму в корпоративній мережі. На рис. 4 наведено інтеграцію PDP/PEP із модулем вибору криптографічного профілю Ф (оптимізація) та Crypto-engine, який застосовує рішення до каналу TLS/VPN. Телеметрія з IdP, SIEM-UEBA, EDR/NAC і мережевих сенсорів формує керуючі сигнали для подієвого циклу Rekey/Upgrade/Revoke.

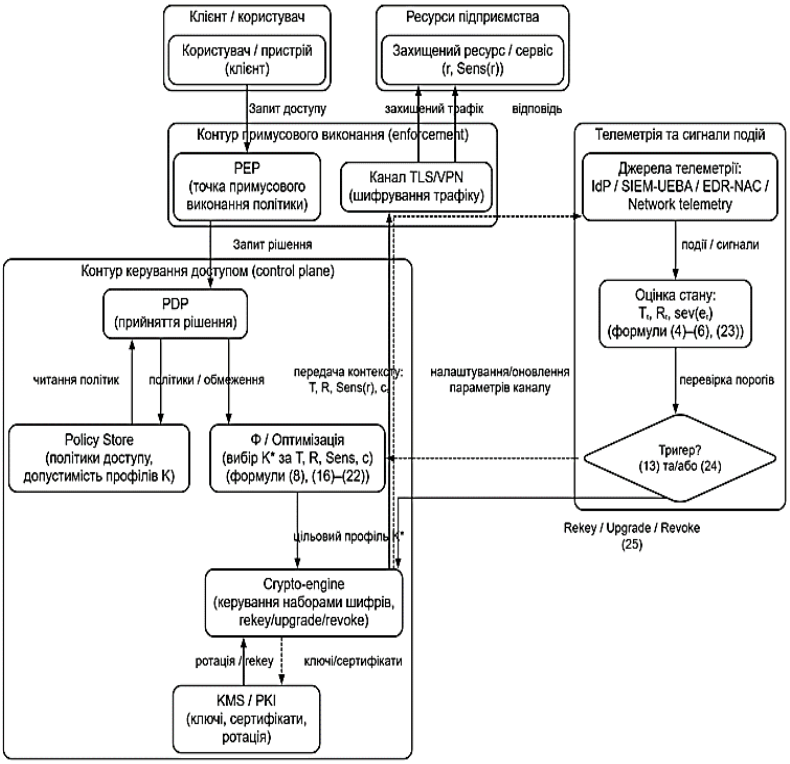

Рис. 4. Архітектурне розміщення механізму адаптації криптопрофілю в корпоративній мережі

Як видно з рис. 4, функція Ф/оптимізація працює в контурі керування (control plane) поруч із PDP і Policy Store, а виконання змін криптографічного стану здійснюється через Crypto-engine на рівні каналу TLS/VPN. Така декомпозиція дозволяє узгоджено адаптувати параметри профілю K_t без порушення логіки доступу та з контрольованими накладними витратами. Далі розглянемо сценарії, які ілюструють поведінку системи в нормальному режимі, за аномалій і за критичних подій.

Таким чином, криптографічний захист каналу реалізується як реактивна система, здатна обмежувати період використання потенційно скомпрометованих параметрів і зменшувати вікно атаки без повного розриву комунікації.

Сценарний приклад застосування моделі. Для ілюстрації роботи запропонованої формальної моделі розглянемо три типові сценарії функціонування захищеного каналу в корпоративній комп'ютерній мережі.

Сценарій 1. Нормальний режим функціонування

За відсутності аномалій рівень довіри залишається стабільно високим $T_t \approx 1$, а інтегрований ризик – низьким $R_t \approx 0$. У цьому випадку алгоритм адаптивного вибору визначає криптографічний профіль з оптимальним співвідношенням безпеки та продуктивності [17]:

$$K_t = \langle A_{base}, M_{base}, L_{optr}, \delta_{max} \rangle, \quad (26)$$

Криптографічні параметри оновлюються лише за регламентним таймером, що мінімізує обчислювальні витрати.

Сценарій 2. Контекстна або поведінкова аномалія

У разі виявлення нетипової поведінки або зміни контексту доступу рівень довіри знижується $T_t \downarrow$, а ризик зростає $R_t \uparrow$. Подія безпеки e_t ініціює подієве оновлення:

$$K_{t+1} = Upgrade(K_t) \tag{27}$$

що призводить до зменшення часу життя криптографічної сесії та збільшення параметра криптографічної стійкості [12, 15]. Передавання даних продовжується без розриву з'єднання, але за підвищеного рівня захисту.

Сценарій 3. Критична подія або компрометація

У разі фіксації критичної події ($sev \geq sev_{crit}$) або різкого зростання ризику ініціюється негайне припинення поточної криптографічної сесії:

$$K_{t+1} = Revoke(K_t) \tag{28}$$

після чого встановлюється новий захищений канал із максимальним рівнем криптографічного захисту [15, 20]. Такий сценарій мінімізує вікно можливих атак і забезпечує ізоляцію потенційно скомпрометованого каналу.

Розглянуті сценарії демонструють, що запропонована модель дозволяє адаптивно узгоджувати рівень криптографічного захисту з поточним станом довіри та ризику, забезпечуючи як ефективність у нормальних умовах, так і підвищену стійкість у разі виникнення загроз [12, 24]. Це підтверджує доцільність використання подієво-орієнтованого механізму оновлення криптографічного стану в корпоративних комп'ютерних мережах.

Для того щоб оцінювання запропонованої моделі було відтворюваним і порівнюваним із поширеними практиками, доцільно ввести набір метрик та базові моделі (baseline) [12, 15]. Ключовою безпековою метрикою є потенційне "вікно атаки" криптографічної сесії W, яке інтерпретується як інтервал від моменту компрометації поточних параметрів до моменту їх оновлення або відкликання (Rekey/Upgrade/Revoke); зменшення W є прямим показником підвищення стійкості до сесійної компрометації.

Для узгодженого порівняння запропонованого адаптивного підходу з поширеними практиками керування криптографічними параметрами доцільно розглянути типові сценарії функціонування захищеного каналу та відповідні реакції системи безпеки [12, 24]. У табл. 2 наведено зіставлення сценаріїв роботи каналу, умов ініціювання оновлення криптографічного стану та очікуваних змін параметрів захисту разом із ключовими метриками ефективності, що забезпечує відтворюваність і доказовість проведеного аналізу.

Таблиця 2

Сценарії функціонування захищеного каналу, базові моделі та метрики оцінювання

Сценарій / режим	Тип тригера (умови)	Очікувана дія	Зміна δ_t	Змін а L_t	Вікно атаки W	Частота оновлень	Накладні витрати
Нормальни й режим	Тригер відсутній	— (без змін)	—	—	високе	низька	мінімальні
Контекстна /	$T_t < T_{crit}$ або $\Delta T_t > \varepsilon_T$	Upgrade	↓	↑	↓	середня	помірні

поведінкова аномалія							
Критична подія безпеки	$R_t \geq R_{crit}$ або $sev(e_t) \geq sev_{crit}$	Revoke	↓↓	↑↑	мінімальне	висока	високі
Static (baseline)	Фіксований профіль	—	—	—	високе	мінімальна	мінімальні
Timer Rekey (baseline)	Періодичний таймер	Rekey	↓	—	середнє	фіксована	помірні
Only-(\delta) (baseline)	Зміна часу життя	Rekey	↓	—	середнє	середня	помірні
Proposed (запропонована модель)	Подієві умови (13), (24)	Rekey / Upgrade / Revoke	↓ / ↓↓	↑ / ↑↑	мінімальне	адаптивна	контрольовані

Позначення: ↓ — зменшення; ↑ — збільшення; — — відсутність змін.

Наведене порівняння показує, що статичні та таймерні базові моделі не забезпечують своєчасної реакції на деградацію довіри або зростання ризику, унаслідок чого потенційне вікно атаки W залишається значним. Часткова адаптація, обмежена лише скороченням часу життя сесії, зменшує W, однак не дозволяє адекватно підвищувати криптографічну стійкість каналу у разі критичних подій.

Запропонована подієво-орієнтована модель забезпечує узгоджену адаптацію як часу життя криптографічних сесій, так і параметрів криптографічної стійкості, що дозволяє мінімізувати W у ризикових сценаріях за рахунок контрольованого зростання накладних витрат. Це підтверджує доцільність використання адаптивних криптографічних профілів у корпоративних мережах та обґрунтовує практичну перевагу запропонованого підходу порівняно з поширеними базовими рішеннями.

На рис. 5 показано зміну потенційного «вікна атаки» для різних сценаріїв функціонування системи. Запропонована модель демонструє мінімальне значення W, особливо у сценаріях аномалій та критичних подій, що підтверджує ефективність подієво-орієнтованої адаптації криптографічного профілю.

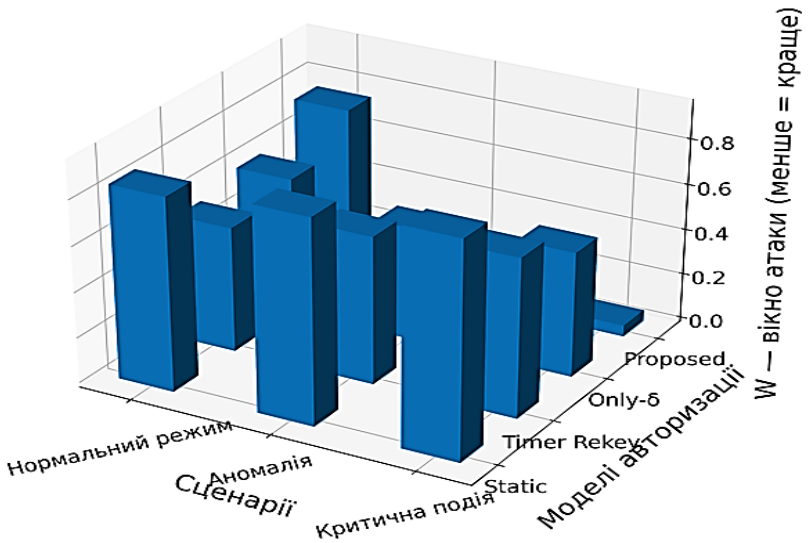

Рис. 5. Порівняння базових і запропонованої моделей авторизації за метрикою

Додатково оцінюються експлуатаційні наслідки адаптації: частота подієвих оновлень (скільки разів за інтервал спостереження виконується Rekey/Upgrade/Revoke),

а також накладні витрати, що проявляються у затримках повторного узгодження, обчислювальному навантаженні та деградації пропускної здатності в режимах підвищеного захисту [12]. Як базові моделі для порівняння розглядаються: статичний профіль, коли K фіксований на всю сесію; таймерна ротація, коли Rekey виконується з фіксованим періодом без урахування подій; часткова адаптація, коли змінюється лише час життя сесії без адаптації алгоритму/режиму [15]. На основі цих метрик і baseline можна узгоджено показати, що запропонована модель скорочує W у сценаріях аномалій і критичних подій, зберігаючи прийнятні експлуатаційні витрати у нормальному режимі, що є необхідною умовою для практичного впровадження в корпоративних мережах.

Обговорення. Отримані результати свідчать, що запропонована формальна модель адаптивного вибору криптографічних параметрів забезпечує принципово інший рівень узгодженості між оцінкою безпекового стану корпоративної комп'ютерної мережі та механізмами криптографічного захисту каналів зв'язку [24]. На відміну від традиційних підходів, у яких криптографічні параметри є статичними та не залежать від динаміки загроз, розроблена модель дозволяє розглядати криптографічний профіль каналу як керований стан, що еволюціонує у часі відповідно до змін довіри, ризику та контексту доступу.

Інтерпретація формалізованих співвідношень показує, що включення рівня довіри як безпосереднього керуючого параметра криптографічного профілю забезпечує більш адекватну реакцію системи на деградацію безпекового середовища. Зокрема, скорочення часу життя криптографічних сесій та підвищення параметрів криптографічної стійкості у разі зростання ризику дозволяє обмежити період використання потенційно скомпрометованих ключів без необхідності повного розриву мережевих з'єднань [15]. Це відрізняє запропонований підхід від моделей, у яких адаптація зводиться лише до зміни політик доступу або рівня автентифікації.

Порівняння з існуючими дослідженнями у сфері адаптивного шифрування та криптоагільності показує, що більшість відомих рішень зосереджуються на виборі алгоритмів або параметрів шифрування на основі заздалегідь визначених правил або ресурсних обмежень. Натомість запропонована модель вводить формальний зв'язок між оцінкою довіри, ризику та критичністю ресурсу, що дозволяє здійснювати адаптацію криптографічних параметрів у рамках єдиного математичного апарату. Це створює передумови для інтеграції моделі з архітектурами Zero Trust та системами управління доступом, де динамічна оцінка довіри вже використовується як ключовий механізм прийняття рішень.

Важливим результатом є демонстрація ефективності подієво-орієнтованого механізму оновлення криптографічного стану. На відміну від періодичних схем ротації ключів, подієва адаптація дозволяє реагувати на критичні зміни безпекового контексту практично миттєво, що зменшує потенційні вікна атак і підвищує стійкість каналів зв'язку до компрометації [15, 20]. При цьому збереження безперервності з'єднань у сценаріях помірної деградації довіри позитивно впливає на експлуатаційну ефективність корпоративних мереж.

З практичної точки зору запропонована модель може бути реалізована як політико-криптографічний адаптер у складі Zero Trust-орієнтованого контуру керування доступом і телеметрією. Джерела сигналів (IdP, UEBA/SIEM, EDR/NAC, мережеві сенсори) формують подієвий потік, на основі якого обчислюються T_t та R_t, після чого механізм $\Phi(\cdot)$ або оптимізаційна процедура вибору визначає цільовий профіль K_t^*. Далі рішення застосовується на рівні каналів TLS/VPN через керування наборами шифрів, параметрами узгодження ключів, політиками rekey і лімітами життя сесії, а подієві

переходи Rekey/Upgrade/Revoke реалізуються як контрольовані процедури оновлення криптографічного стану [12, 17, 24]. У результаті криптографічний шар перестає бути "незмінним інфраструктурним рівнем" і стає частиною керованої системи безпеки, яка узгоджено реагує на деградацію довіри та зростання ризику.

Разом з тим результати дослідження вказують на низку обмежень запропонованої моделі. Зокрема, ефективність адаптивного вибору криптографічних параметрів безпосередньо залежить від якості та достовірності механізмів оцінки довіри й ризику. Невірна або затримана ідентифікація подій безпеки може призвести як до надмірної жорсткості криптографічних параметрів, так і до недостатнього рівня захисту [15]. Крім того, визначення порогових значень і коефіцієнтів чутливості моделі потребує калібрування з урахуванням специфіки корпоративної мережі, типів ресурсів і допустимого рівня експлуатаційних витрат.

Обговорюючи практичну значущість отриманих результатів, слід зазначити, що запропонована модель не прив'язана до конкретного криптографічного алгоритму, протоколу або платформи реалізації. Це забезпечує її універсальність та можливість застосування у різних мережевих архітектурах, зокрема у VPN-системах, TLS-з'єднаннях, захищених міжсегментних каналах і хмарних комунікаційних середовищах [12, 20]. Водночас практичне впровадження моделі потребує інтеграції з системами моніторингу подій безпеки, механізмами оцінки поведінки користувачів та інструментами керування ключами.

Узагальнюючи результати, можна стверджувати, що запропонований підхід формує нову парадигму керування криптографічним захистом каналів у корпоративних комп'ютерних мережах, у якій криптографічна стійкість, довіра та ризик розглядаються як взаємопов'язані динамічні величини [24]. Це відкриває перспективи для подальших досліджень, спрямованих на експериментальну валідацію моделі, оптимізацію алгоритмів адаптації та розширення підходу на постквантові криптографічні механізми.

Разом з тим слід зазначити, що ефективність адаптивного вибору криптографічних параметрів безпосередньо залежить від якості оцінювання T_t та R_t і достовірності подій безпеки. Затримки або похибки у виявленні аномалій можуть призводити до несвоєчасного оновлення профілю або до надмірної "жорсткості" параметрів, що підвищує експлуатаційні витрати [15, 20]. Окремим ризиком є можливість коливань (oscillation) при частих змінах контексту, тому на практиці доцільно застосовувати пороги, гістерезис і обмеження частоти Upgrade/Rekey. Також модель не замінює захист кінцевих точок: компрометація клієнтського середовища або крадіжка ключового матеріалу на endpoint потребує додаткових механізмів (EDR, secure enclave, апаратний захист ключів), а запропонований підхід розглядається як узгоджене керування параметрами каналу в рамках загальної архітектури безпеки.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі розв'язано актуальну наукову задачу формалізації адаптивного вибору криптографічних параметрів захисту каналів зв'язку в корпоративних комп'ютерних мережах на основі динамічної оцінки довіри та ризику. Запропонований підхід дозволяє перейти від статичних криптографічних конфігурацій до керованої моделі, у якій криптографічний профіль каналу розглядається як динамічний стан системи безпеки.

У ході дослідження вперше формалізовано стан захищеного каналу у вигляді багатовимірного кортежу, що поєднує суб'єкт доступу, ресурс, контекст, рівень довіри, інтегрований ризик і криптографічні параметри. Така формалізація створює

математичну основу для узгодженого аналізу взаємозв'язку між безпековим станом мережі та рівнем криптографічного захисту передавання даних.

Розроблено модель адаптивного вибору криптографічних параметрів, у якій алгоритм шифрування, режим його роботи, параметр криптографічної стійкості та час життя криптографічної сесії визначаються як функція поточної оцінки довіри, ризику, контексту доступу та критичності інформаційного ресурсу. Запропонований алгоритм забезпечує формалізований і відтворюваний механізм прийняття рішень, орієнтований на досягнення балансу між криптографічною стійкістю та експлуатаційною ефективністю.

Запропоновано подієво-орієнтований механізм оновлення криптографічного стану, який дозволяє адаптувати параметри захисту каналів зв'язку у відповідь на виявлені події безпеки, деградацію довіри або зростання ризику. Такий підхід мінімізує потенційні вікна уразливостей і підвищує стійкість корпоративних мереж до динамічних загроз без порушення безперервності комунікацій у некритичних сценаріях.

Сценарний аналіз застосування моделі підтвердив її здатність коректно адаптувати криптографічні параметри у нормальних умовах експлуатації, за наявності поведінкових або контекстних аномалій та у випадках критичних подій безпеки. Це свідчить про універсальність запропонованої моделі та можливість її використання у різних архітектурах корпоративних комп'ютерних мереж, зокрема в системах захищених тунелів, TLS-з'єднаннях і середовищах Zero Trust.

Перспективи подальших досліджень пов'язані з експериментальною валідацією запропонованої моделі в реальних або імітаційних корпоративних мережах, оцінюванням впливу адаптивного вибору криптографічних параметрів на продуктивність та стійкість каналів зв'язку, а також оптимізацією коефіцієнтів чутливості та порогових значень моделі. Окремим напрямом є розширення підходу на постквантові криптографічні алгоритми та дослідження криптоагільності адаптивних каналів зв'язку в умовах еволюції загроз. Отримані результати можуть слугувати теоретичною та методологічною основою для розроблення інтелектуальних систем керування криптографічним захистом у корпоративних комп'ютерних мережах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Zhang, D., Yang, S., Chen, M., et al. (2025). Adaptive encryption method of sensitive data in data center database based on big data cross-mapping fusion algorithm. *Discover Applied Sciences, 7*, 924. https://doi.org/10.1007/s42452-025-07581-2
2. Pastor-Galindo, J., López-Millán, G., & Marín-López, R. (2022). A framework for dynamic configuration of TLS connections based on standards. *Journal of Network and Systems Management, 30*, 24. https://doi.org/10.1007/s10922-021-09640-6
3. Kumar, P. R., & Goel, S. (2025). A secure and efficient encryption system based on adaptive and machine learning for securing data in fog computing. *Scientific Reports, 15*, 11654. https://doi.org/10.1038/s41598-025-92245-9
4. Alanazi, M. J., Alhoweiti, R. A., Alhwaity, G. A., & Alharbi, A. R. (2025). An adaptive hybrid cryptographic framework for resource-constrained IoT devices. *Electronics, 14*(23), 4666. https://doi.org/10.3390/electronics14234666
5. Li, Z., Ju, Z., Zhao, H., Wei, Z., & Lan, G. (2025). A lightweight certificateless authenticated key agreement scheme based on Chebyshev polynomials for the Internet of Drones. *Sensors, 25*(14), 4286. https://doi.org/10.3390/s25144286
6. Pokhrel, C., Ghimire, R., Dawadi, B. R., & Manzoni, P. (2025). A machine learning-based hybrid encryption approach for securing messages in software-defined networking. *Network, 5*(1), 8. https://doi.org/10.3390/network5010008

7. Ruhault, S., Lafourcade, P., & Mahmoud, D. (2024). A unified symbolic analysis of WireGuard. In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2024)*. https://doi.org/10.14722/ndss.2024.24364
8. Marchesi, L., Marchesi, M., & Tonelli, R. (2024). A survey on cryptoagility and agile practices in the light of quantum resistance. *Information and Software Technology, 178*, 107604. https://doi.org/10.1016/j.infsof.2024.107604
9. Calvo, M., & Beltrán, M. (2022). A model for risk-based adaptive security controls. *Computers & Security, 115*, 102612. https://doi.org/10.1016/j.cose.2022.102612
10. Selvan, S., & Singh, M. M. (2022). Adaptive contextual risk-based model to tackle confidentiality-based attacks in fog-IoT paradigm. *Computers, 11*(2), 16. https://doi.org/10.3390/computers11020016
11. Cho, J., Lee, C., Kim, E., Lee, J., & Cho, B. (2024). Software-defined cryptography: A design feature of cryptographic agility. *arXiv preprint arXiv:2404.01808*.
12. Sokolov, V., Kostiuk, Y., Skladannyi, P., & Korshun, N. (2025). Adaptation of network traffic routing policy to information security and network protection requirements. In *Proceedings of the 13th International Scientific and Practical Conference "Information Control Systems and Technologies" (ICST 2025)* (pp. 397–411). CEUR-WS.org.
13. Dovzhenko, N., Ivanichenko, Y., Skladannyi, P., & Ausheva, N. (2024). Integration of security and fault tolerance in sensor networks based on the analysis of energy consumption and traffic. *Cybersecurity: Education, Science, Technique*, 1, 390–400. https://doi.org/10.28925/2663-4023.2024.25.390400
14. Zhdanova, Y., Spasiteleva, S., Shevchenko, S., & Kravchuk, K. (2020). Applied and methodological aspects of hash function usage in information security. *Cybersecurity: Education, Science, Technique, 4*(8), 85–96. https://doi.org/10.28925/2663-4023.2020.8.8596
15. Kostiuk, Y., Skladannyi, P., Rzayeva, S., Mazur, N., Cherevyk, V., & Anosov, A. (2025). Features of network attack implementation via TCP/IP protocols. *Cybersecurity: Education, Science, Technique, 1*(29), 571–597. https://doi.org/10.28925/2663-4023.2025.29.915
16. Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024). Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices. *Sensors, 24*(12), 4008. https://doi.org/10.3390/s24124008
17. Zhdanova, Y., Spasiteleva, S., & Shevchenko, S. (2019). Application of the security.cryptography class library for cybersecurity specialist training. *Cybersecurity: Education, Science, Technique, 4*(4), 44–53. https://doi.org/10.28925/2663-4023.2019.4.4453
18. Kostiuk, Y., Skladannyi, P., Rzayeva, S., Samoilenko, Y., & Korshun, N. (2025). Intelligent control and protection systems in cyber-physical and cloud-based smart grid environments. *Cybersecurity: Education, Science, Technique, 2*(30), 125–156. https://doi.org/10.28925/2663-4023.2025.30.956
19. Alharbe, N., Aljohani, A., Rakrouki, M. A., & Khayyat, M. (2023). An access control model based on system security risk for dynamic sensitive data storage in the cloud. *Applied Sciences, 13*(5), 3187. https://doi.org/10.3390/app13053187
20. Skladannyi, P., Kostiuk, Y., Zhyltsov O., Savchenko, Y., Antypin, Ye. (2025) Intelligent modeling of personalized learning in cybersecurity training. Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2025), October 26, 2025, Kyiv, Ukraine, Vol-4145, P. 95-119. ISSN 1613-0073.
21. Shevchenko, S., Zhdanova, Y., Dreis, Y., Kyrychok, R., & Tsyrkaniuk, D. (2023). Protection of information in telecommunication medical systems based on a risk-oriented approach. In *Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2023)*. CEUR Workshop Proceedings.
22. Skladannyi, P., Kostiuk, Y., Rzayeva, S., & Mazur, N. (2025). Parallel data processing in extensible hash structures and performance evaluation. *Cybersecurity: Education, Science, Technique, 3*(31), 242–269. https://doi.org/10.28925/2663-4023.2025.31.1015
23. Gour, A., Malhi, S., Singh, G., & Kaur, G. (2024). Hybrid cryptographic approach for secure data communication using block cipher techniques. *E3S Web of Conferences, 556*, 01048. https://doi.org/10.1051/e3sconf/202455601048
24. Siyal, R., Long, J., Khan, S. U., et al. (2025). Secure big data sharing with hybrid encryption and deep learning. *Journal of King Saud University – Computer and Information Sciences, 37*, 216. https://doi.org/10.1007/s44443-025-00093-4
25. Skladannyi, P. M., Hulak, H. M., & Kostiuk, Y. V. (2025). Generator of chaotic numbers with fuzzy control for cryptographic systems with dynamic trust. *Telecommunications and Information Technologies*, 4(89), 137–147. https://doi.org/10.31673/2412-4338.2025.048916

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Yuliia Kostiuk
PhD in Computer Science
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0001-5423-0985
y.kostiuk@kubg.edu.ua

Pavlo Skladannyi
PhD, Associate Professor, Head of the Department of Information and
Cyber Security named after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Nataliia Mazur
PhD, Associate Professor
Associate Professor of the Department of Information and
Cyber Securitynamed after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0001-7671-8287
n.mazur@kubg.edu.ua

Rzaeva Svitlana
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Computer Science
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-7589-2045
s.rzaieva@kubg.edu.ua

Dmytro Hnatchenko
PhD in Computer Science,
Senior Lecturer at the Department of Software Engineering and Cybersecurity
State University of Trade and Economic, Kyiv, Ukraine
ORCID: 0000-0002-6584-4525
hnatchenko@knute.edu.ua

Ihor Honcharenko
Candidate of Technical Sciences,
Senior Lecturer at the Department of Software Engineering and Cybersecurity
State University of Trade and Economic, Kyiv, Ukraine
ORCID: 0000-0002-9022-6083
okjraa@gmail.com

FORMAL MODEL OF ADAPTIVE SELECTION OF CRYPTOGRAPHIC PARAMETERS FOR CHANNEL PROTECTION IN CORPORATE COMPUTER NETWORKS BASED ON DYNAMIC TRUST ASSESSMENT

Abstract. The paper proposes a formal model for the adaptive selection of cryptographic parameters for protecting communication channels in corporate computer networks based on dynamic trust assessment and integrated risk. The relevance of the study stems from the fact that common practices of static configuration of encryption algorithms, modes of operation, and cryptographic strength parameters do not account for changes in access context and the behavior of interacting entities, which leads either to excessive computational overhead or to the emergence of vulnerability windows during threat escalation. The scientific novelty lies in interpreting the cryptographic profile as a controllable dynamic state of the security system, where trust acts as a direct control parameter

of the cryptographic configuration rather than merely a factor in access decision-making. A protected channel is formalized as a state tuple combining the subject, resource, context, trust level, risk, and cryptographic profile, while adaptive parameter selection is described by a mapping that establishes a correspondence between (resource criticality, context) and a set of cryptographic characteristics (algorithm, mode, strength parameter, session lifetime). An optimization formulation for profile selection is developed that accounts for the trade-off between cryptographic strength and operational costs, along with an event-driven mechanism for updating the cryptographic state (Rekey/Upgrade/Revoke) in response to trust degradation, risk increase, or critical security events. Scenario analysis (normal operation, contextual/behavioral anomaly, critical event) demonstrates the model's ability to coherently enhance strength and reduce cryptographic session lifetimes in high-risk situations, thereby reducing the potential attack window while maintaining acceptable performance under low-risk conditions. The obtained results provide a theoretical foundation for deploying adaptive cryptographic profiles in TLS/VPN and Zero Trust–oriented corporate environments.

Keywords: dynamic trust; integrated risk; channel cryptographic profile; event-driven update; crypto-agility; Zero Trust; corporate computer networks.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Zhang, D., Yang, S., Chen, M., et al. (2025). Adaptive encryption method of sensitive data in data center database based on big data cross-mapping fusion algorithm. *Discover Applied Sciences, 7*, 924. https://doi.org/10.1007/s42452-025-07581-2
2. Pastor-Galindo, J., López-Millán, G., & Marín-López, R. (2022). A framework for dynamic configuration of TLS connections based on standards. *Journal of Network and Systems Management, 30*, 24. https://doi.org/10.1007/s10922-021-09640-6
3. Kumar, P. R., & Goel, S. (2025). A secure and efficient encryption system based on adaptive and machine learning for securing data in fog computing. *Scientific Reports, 15*, 11654. https://doi.org/10.1038/s41598-025-92245-9
4. Alanazi, M. J., Alhoweiti, R. A., Alhwaity, G. A., & Alharbi, A. R. (2025). An adaptive hybrid cryptographic framework for resource-constrained IoT devices. *Electronics, 14*(23), 4666. https://doi.org/10.3390/electronics14234666
5. Li, Z., Ju, Z., Zhao, H., Wei, Z., & Lan, G. (2025). A lightweight certificateless authenticated key agreement scheme based on Chebyshev polynomials for the Internet of Drones. *Sensors, 25*(14), 4286. https://doi.org/10.3390/s25144286
6. Pokhrel, C., Ghimire, R., Dawadi, B. R., & Manzoni, P. (2025). A machine learning-based hybrid encryption approach for securing messages in software-defined networking. *Network, 5*(1), 8. https://doi.org/10.3390/network5010008
7. Ruhault, S., Lafourcade, P., & Mahmoud, D. (2024). A unified symbolic analysis of WireGuard. In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2024)*. https://doi.org/10.14722/ndss.2024.24364
8. Marchesi, L., Marchesi, M., & Tonelli, R. (2024). A survey on cryptoagility and agile practices in the light of quantum resistance. *Information and Software Technology, 178*, 107604. https://doi.org/10.1016/j.infsof.2024.107604
9. Calvo, M., & Beltrán, M. (2022). A model for risk-based adaptive security controls. *Computers & Security, 115*, 102612. https://doi.org/10.1016/j.cose.2022.102612
10. Selvan, S., & Singh, M. M. (2022). Adaptive contextual risk-based model to tackle confidentiality-based attacks in fog-IoT paradigm. *Computers, 11*(2), 16. https://doi.org/10.3390/computers11020016
11. Cho, J., Lee, C., Kim, E., Lee, J., & Cho, B. (2024). Software-defined cryptography: A design feature of cryptographic agility. *arXiv preprint arXiv:2404.01808*.
12. Sokolov, V., Kostiuk, Y., Skladannyi, P., & Korshun, N. (2025). Adaptation of network traffic routing policy to information security and network protection requirements. In *Proceedings of the 13th International Scientific and Practical Conference "Information Control Systems and Technologies" (ICST 2025)* (pp. 397–411). CEUR-WS.org.

13. Dovzhenko, N., Ivanichenko, Y., Skladannyi, P., & Ausheva, N. (2024). Integration of security and fault tolerance in sensor networks based on the analysis of energy consumption and traffic. *Cybersecurity: Education, Science, Technique*, 1, 390–400. https://doi.org/10.28925/2663-4023.2024.25.390400
14. Zhdanova, Y., Spasiteleva, S., Shevchenko, S., & Kravchuk, K. (2020). Applied and methodological aspects of hash function usage in information security. *Cybersecurity: Education, Science, Technique, 4*(8), 85–96. https://doi.org/10.28925/2663-4023.2020.8.8596
15. Kostiuk, Y., Skladannyi, P., Rzayeva, S., Mazur, N., Cherevyk, V., & Anosov, A. (2025). Features of network attack implementation via TCP/IP protocols. *Cybersecurity: Education, Science, Technique, 1*(29), 571–597. https://doi.org/10.28925/2663-4023.2025.29.915
16. Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024). Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices. *Sensors, 24*(12), 4008. https://doi.org/10.3390/s24124008
17. Zhdanova, Y., Spasiteleva, S., & Shevchenko, S. (2019). Application of the security.cryptography class library for cybersecurity specialist training. *Cybersecurity: Education, Science, Technique, 4*(4), 44–53. https://doi.org/10.28925/2663-4023.2019.4.4453
18. Kostiuk, Y., Skladannyi, P., Rzayeva, S., Samoilenko, Y., & Korshun, N. (2025). Intelligent control and protection systems in cyber-physical and cloud-based smart grid environments. *Cybersecurity: Education, Science, Technique, 2*(30), 125–156. https://doi.org/10.28925/2663-4023.2025.30.956
19. Alharbe, N., Aljohani, A., Rakrouki, M. A., & Khayyat, M. (2023). An access control model based on system security risk for dynamic sensitive data storage in the cloud. *Applied Sciences, 13*(5), 3187. https://doi.org/10.3390/app13053187
20. Skladannyi, P., Kostiuk, Y., Zhyltsov O., Savchenko, Y., Antypin, Ye. (2025) Intelligent modeling of personalized learning in cybersecurity training. Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2025), October 26, 2025, Kyiv, Ukraine, Vol-4145, P. 95-119. ISSN 1613-0073.
21. Shevchenko, S., Zhdanova, Y., Dreis, Y., Kyrychok, R., & Tsyrkaniuk, D. (2023). Protection of information in telecommunication medical systems based on a risk-oriented approach. In *Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2023)*. CEUR Workshop Proceedings.
22. Skladannyi, P., Kostiuk, Y., Rzayeva, S., & Mazur, N. (2025). Parallel data processing in extensible hash structures and performance evaluation. *Cybersecurity: Education, Science, Technique, 3*(31), 242–269. https://doi.org/10.28925/2663-4023.2025.31.1015
23. Gour, A., Malhi, S., Singh, G., & Kaur, G. (2024). Hybrid cryptographic approach for secure data communication using block cipher techniques. *E3S Web of Conferences, 556*, 01048. https://doi.org/10.1051/e3sconf/202455601048
24. Siyal, R., Long, J., Khan, S. U., et al. (2025). Secure big data sharing with hybrid encryption and deep learning. *Journal of King Saud University – Computer and Information Sciences, 37*, 216. https://doi.org/10.1007/s44443-025-00093-4
25. Skladannyi, P. M., Hulak, H. M., & Kostiuk, Y. V. (2025). Generator of chaotic numbers with fuzzy control for cryptographic systems with dynamic trust. *Telecommunications and Information Technologies*, 4(89), 137–147. https://doi.org/10.31673/2412-4338.2025.048916

Отримано редакцією журналу / Received:14.12.25
Прорецензовано / Revised: 06.01.26
Схвалено до друку / Accepted: 26.03.26