Drive, AWS та Dropbox, які дозволяють уникнути виявлення; шифрування SSL/TLS для захисту трафіку C2; мережу Tor, яку часто використовують для анонімізації серверів C2. Представники обох категорій використовують однакові готові інструменти для пост-експлуатації та збору даних, зокрема інструменти Cobalt Strike, Metasploit, Mimikatz тощо [3].

Отже, конвергенція кіберсуб'єктів національних держав та організованих кібергруп є ознакою трансформаційного зсуву в ландшафті кіберзагроз. Ці суб'єкти, які ще недавно суттєво відрізнялися один від одного через відмінні мотиви та методи кібернападу, все частіше обмінюються інструментами, тактикою і навіть мають спільні цілі. Подібне використання ШІ, складних методів ухилення й векторів атак, які накладаються, ще більше ускладнює виявлення і притягнення до відповідальності держав-агресорів і кіберзлочинців.

Підсумовуючи, слід зазначити, що ймовірним є подальше поглиблення конвергенції цих суб'єктів внаслідок загострення геополітичної напруженості, застосування економічних санкцій і стрімкого розвитку технологій.

6. Cyber Operations Tracker. *Council on Foreign Relation USA*. URL: https://www.cfr.org/cyber-operations/#OurMethodology (дата звернення: 22.04.2026).
7. Shloman T. Blurring the Lines: How Nation-States and Organized Cybercriminals Are Becoming Alike. January 7, 2025. *Trellix*. URL: https://www.trellix.com/blogs/ research/blurring-the-lines-how-nation-states-and-cybercriminals-are-becoming-alike/ (дата звернення: 22.04.2026).
8. Proxy Wars in Cyberspace: Tracking Nation-State Influence Through Threat Actor Alliances. September 30, 2025. *Falconfeeds.* URL: https://falconfeeds.io/blogs/proxy-wars-cyberspace-nation-state-threat-actor-alliances/ (дата звернення: 22.04.2026).

Архітектура комплексу криптографічного захисту каналів зв'язку мережевої системи контролювання доступу

УДК 004.056

Ігор Муляр[1], Вікторія Дика[2]

Хмельницький національний університет,
[1]muliariv@khmnu.edu.ua, [2]dikaviktoria@khmnu.edu.ua

У рамках даного дослідження розроблювана система розглядається як клієнт-серверний додаток, де «Клієнт» виконує роль імітатора апаратного контролера системи контролювання доступу (СКД), а «Сервер» є вузлом централізованого прийняття рішень та управління криптографічними ключами. Відповідно до обраної гібридної моделі шифрування, функціональні вимоги до системи класифіковано за чотирма основними напрямками: вимоги до криптографічних примітивів, вимоги до серверної частини, вимоги до клієнтської частини та вимоги до обробки виняткових ситуацій [1].

Для реалізації сформульованих функціональних вимог розроблено логічну архітектуру програмного комплексу та формалізовано модель мережевої

взаємодії між вузлами системи. Архітектура розроблюваної системи криптографічного захисту будується на основі класичної клієнт-серверної топології з використанням стека протоколів TCP/IP як транспортного середовища.

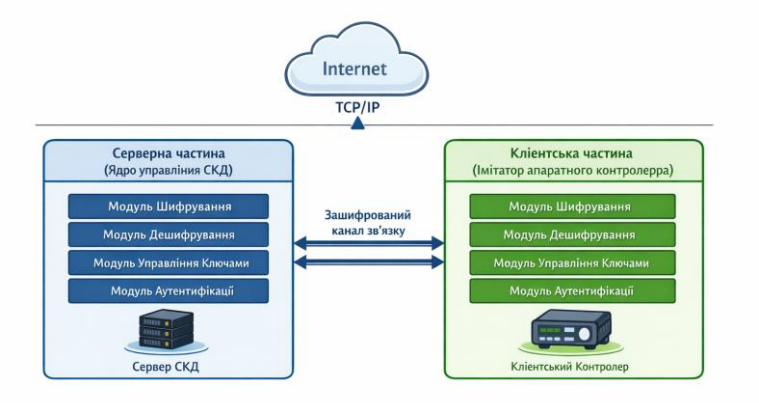

Рис.1. Узагальнена структурна схема архітектури системи криптографічного захисту

Запропонована архітектурна модель логічно розділяє систему на дві незалежні підсистеми: серверну частину (ядро управління СКД) та клієнтську частину (імітатор апаратного контролера). Кожна з підсистем містить власний набір криптографічних модулів для забезпечення повного циклу гібридного шифрування.

Серверна підсистема функціонує як багатопотоковий мережевий вузол, що очікує на вхідні з'єднання. До її внутрішньої архітектури входять такі базові компоненти.

Модуль управління асиметричними ключами відповідає за генерацію пари ключів зберігання приватного ключа в захищеній області пам'яті та серіалізацію публічного ключа для передачі клієнтам.

Модуль мережевої взаємодії забезпечує прослуховування заданого порту (наприклад, 65432), створення окремого потоку для кожного підключеного контролера та управління життєвим циклом сокет-з'єднання.

Криптографічний процесор виконує розшифрування сеансового ключа за допомогою алгоритму RSA-OAEP, а також потокове дешифрування та шифрування вхідних/вихідних пакетів за допомогою алгоритму AES-256 у режимі CBC.

Модуль верифікації цілісності обчислює та перевіряє хеш-код HMAC-SHA256 для кожного отриманого криптопакета.

Контролер логіки доступу імітує бізнес-логіку серверної частини СКД (звірка ідентифікаторів з локальною базою даних прав доступу).

Клієнтська підсистема імітує поведінку периферійного пристрою СКД. Її архітектура включає.

Генератор ентропії - модуль для створення криптографічно стійкого симетричного сеансового ключа та унікальних векторів ініціалізації.

Модуль інкапсуляції ключів відповідає за шифрування згенерованого сеансового ключа отриманим від сервера відкритим ключем RSA.

Емулятор подій СКД генерує тестові послідовності даних, що імітують зчитування RFID-карток (наприклад, UID картки у форматі HEX) або спрацьовування датчиків проходу.

Мережевий клієнт забезпечує встановлення з'єднання із сервером та двосторонню маршрутизацію пакетів.

Взаємодія між контролером та сервером відбувається за строго визначеним протоколом, який складається з фази встановлення захищеного з'єднання та фази захищеного обміну даними, контролер ініціює TCP-з'єднання з сервером. Сервер приймає з'єднання і виділяє для нього окремий сокет [2].

Формування чіткого переліку функціональних вимог дозволяє визначити архітектурні межі системи, необхідні програмні модулі та механізми забезпечення конфіденційності, цілісності та автентичності інформаційного обміну між апаратними контролерами та центральним сервером.

1. Yevseiev, S. Modeling of security systems for critical infrastructure facilities : monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych [et al.]. – Kharkiv : PC TECHNOLOGY CENTER, 2022. – 196 p
2. Rashid, N. N. A Comprehensive Framework for Harnessing IoT and 5G for Enhanced Disaster Response / N. N. Rashid, Z. Ghanim Ali, A. Hussein Ali, N. Adnan Taher, S. Khdhaer Mukhlif, I. V. Muliar, H. Muthanna Noori // Proceeding of the 36th Conference of FRUCT Association. – 2024. – P. 655–663. – ISSN 2305-7254.

Інтеграція приватного блокчейну та сліпих підписів Чаума для забезпечення анонімності й цілісності збору даних у платформі OwlView

УДК 004.056.55 (043.2)

Анастасія Начинка[1], Валерій Трушевський[2]

Львівський національний університет імені Івана Франка,
[1]anastasiia.nachynka@lnu.edu.ua, [2]valeriy.trushevskyy@lnu.edu.ua

Платформи онлайн-опитувань акумулюють дані спеціальних категорій (ст. 9 GDPR) [4]: політичні погляди, релігія, здоров'я. Провідні сервіси (Google Forms, SurveyMonkey, Typeform) не забезпечують ані шифрування на рівні полів (field-level encryption), ані криптографічної перевірки цілісності відповідей. Виникає суперечність між необхідністю ідентифікації респондента для запобігання повторному голосуванню та забезпеченням приватності.

Мета роботи — спроєктувати й реалізувати у складі OwlView підсистему збору відповідей, що одночасно гарантує: 1) анонімність респондента; 2) неможливість повторного голосування; 3) перевірену цілісність агрегату; 4) індивідуальну верифікацію голосу без розкриття його змісту.

Наукова новизна — поєднання приватного блокчейну з консенсусом Proof-of-Work і деревами Меркла з протоколом сліпих підписів Чаума у єдиному