управління життєвим циклом користувачів, застосування банів та модерацію підозрілого контенту.

Розроблена платформа демонструє ефективність застосування підходу Security-by-Design при побудові сучасних веб-застосунків на основі Node.js. Запропонована захищена архітектура із застосуванням RBAC, строгим контролем вхідних даних та ізоляцією медіа-контенту забезпечує стійкість системи до поширених веб-вразливостей і може бути масштабована для інших високонавантажених соціальних платформ.

1. Newzoo Global Games Market Report 2024. — Режим доступу: https://newzoo.com/resources/trend-reports/newzoos-global-games-market-report-2024-free-version
2. Cantelon M., Harter M. Node.js in Action. — Manning Publications, 2017. — 392 p.
3. RAWG Video Games Database API Documentation. — Режим доступу: https://rawg.io/apidocs
4. Martin R. C. Clean Architecture: A Craftsman's Guide to Software Structure and Design. — Prentice Hall, 2017. — 432 p.
5. Bryk O., Mudryk I., Holubovskyi M., Stoianov Y. Machine learning models and methods aspects of processing unstructured data. Proceedings of the 1st International Workshop on Bioinformatics and Applied Information Technologies (BAIT 2024), Zboriv, Ukraine, 2024. 2024. P. 64–74.

Конвергенція кіберсуб'єктів національних держав та організованої кіберзлочинності

УДК 004.056:355.4

Світлана Легомінова[1], Тетяна Капелюшна[2], Тетяна Мужанова[3]

Державний університет інформаційно-комунікаційних технологій,
[1]s.legominova@duikt.edu.ua, [2]t.kapeliushna@duikt.edu.ua,
[3]t.muzhanova@duikt.edu.ua

Як свідчать реалії, в сучасному швидкозмінному кіберландшафті відмінності між кіберсуб'єктами національних держав і організованими кіберзлочинцями стають дедалі більш розмитими. На попередніх етапах ці суб'єкти мали різні мотиви: національні держави прагнули досягти довгострокових геополітичних переваг за допомогою шпигунських і розвідувальних операцій, у той час як кіберзлочинці прагнули отримати фінансову вигоду, експлуатуючи вразливості ІКС для вимагання, крадіжок і шахрайства.

Однак упродовж кількох останніх років відзначено тривожну тенденцію щодо злиття тактик, методів і цілей цих суб'єктів, що ускладнює їх розмежування, можливості виявлення і притягнення винних до відповідальності (кібератрибуції), а також виносить на порядок денний критичні питання щодо стрімкої еволюції кіберзагроз та її критичних наслідків для глобальної безпеки.

Як відомо, домінуючими агресивними гравцями у кіберпросторі залишаються Китай, РФ, Іран та Північна Корея, які з великим відривом випереджають решту держав світу [1]. Їхні цілі історично передбачали нанесення шкоди геополітичним суперникам та отримання розвідувальних даних для підтримки або посилення власного глобального впливу.

Кожна з перелічених держав має у своєму арсеналі державні кібергрупи, чиї операції були зосереджені переважно на:

- технологічному шпигунстві, критично важливих секторах інфраструктури конкурентів, насамперед США (Китай);
- шпигунстві політичного характеру й ураженні критичної інфраструктури в США та Європі (РФ);
- розвідці, атаках на критично важливі галузі, такі як енергетика та фінанси, підриві регіональних суперників, втручання у виборчі процеси в США (Іран);
- поєднанні традиційного шпигунства з фінансовими крадіжками, використанні програм-вимагачів (Північна Корея) [2, 3].

Сьогодні співпраця між суб'єктами національних держав і кіберзлочинцями посилюється і, як наслідок, ще більше розмиває межі між діяльністю, спрямованою на державу, та злочинною діяльністю переважно з метою наживи.

Постійно зростає кількість кіберзлочинних організацій, які експлуатують вразливості ІКС для отримання прибутку. Програми-вимагачі та крадіжка даних швидко стали їхніми основними інструментами, що спричинило розширення діяльності таких груп до безпрецедентних масштабів. У то й же час, злиття зусиль кібергруп і суб'єктів, що спонсоруються державами, вказує на спільні ресурси та взаємну вигоду. Крім того, ШІ став потужним інструментом кіберзлочинів, який дозволяє проводити більш складні й ефективні операції, зокрема зі створенням хибного контенту з діпфейками, автоматизації фішингових кампаній і масштабної розвідки.

Державні кіберсуб'єкти запозичили тактику, яка колись асоціювалася переважно з криміналом, зокрема програми-вимагачі використовуються державами з метою акумуляції коштів для їхньої подальшої геополітичної діяльності. Водночас, організовані кіберзлочинці перейняли більш складні методи, традиційно пов'язані з державними суб'єктами (APT-атаки, приховані мережеві проникнення, атаки на ланцюги постачання, системи пост-експлуатації).

Спільні вектори атак (соціальна інженерія, атаки на ланцюги постачання, готові експлойти, DNS-тунелювання) ще більше звужують розрив між цими суб'єктами. Улюблена тактика фішингу використовується обома сторонами: державами - проти урядів конкуруючих країн і дисидентів, а організованими злочинними групами - для поширення програм-вимагачів. Представники обох категорій застосовують передові методи уникнення виявлення, зокрема безфайлове шкідливе ПЗ і легітимні системні інструменти для зловмисної діяльності.

Державні дійові особи та кіберзлочинці використовують подібні методи для встановлення і підтримки зв'язку зі своїм шкідливим ПЗ: спільну інфраструктуру командування та управління C2, зокрема хмарні сервіси Google

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