хто саме зайшов у систему. Це дає можливість прив'язувати сесію до конкретної особи, а також застосовувати розмежування доступу залежно від ролі. Концепція працює так: під час реєстрації для користувача створюється локальний профіль з ідентифікатором та роллю, а під час входу здійснюється біометричне розпізнавання, яке визначає належність до одного із зареєстрованих профілів. Після успішної ідентифікації система може надавати різні рівні доступу до функцій і даних. Таким чином, біометрія перетворюється на основу керування правами, а не лише на зручний «замок» для входу.

Логічним продовженням розвитку застосунку є поглиблення цього механізму: розширення системи ролей і політик доступу, додавання сценаріїв «підвищеного підтвердження» для критичних дій (повторна ідентифікація), а також гнучке налаштування правил приватності під конкретного користувача. Перспективними є й режими спільного використання одного пристрою кількома людьми, ведення безпечного локального журналу подій (без фінансових деталей, але з фіксацією фактів входу/виходу) та посилення захисту локального зберігання і резервних копій, щоб навіть у разі компрометації середовища дані залишалися недоступними без ключів і підтвердження особи.

У підсумку багаторівневий підхід дозволяє зробити офлайновий фінансовий застосунок не лише зручним, а й стійким до типових реальних загроз. Він поєднує механізми операційної системи, продуману логіку доступу та приватність інтерфейсу користувача (UI), формуючи просте правило: навіть якщо один бар'єр не спрацює, інші шари все одно зменшать ризик витоку та несанкціонованого доступу.

Безпека транспортної інфраструктури України в умовах повномасштабної війни як пріоритетне завдання Державної спеціальної служби транспорту

УДК 656.078:351.862 (477)

Володимир Будз[1], Сергій Костиря[2], Станіслав Шумлянський[3]

Науково-дослідний центр Державної спеціальної служби транспорту,
[1]budzwolodymyr@gmail.com, [2]kostyrya81@gmail.com,
[3]s.shumlianskyi@dsst.gov.ua

Критична інфраструктура (КІ) забезпечує повноцінне функціонування суспільства. До неї належать енергетичні мережі, транспортні вузли, зв'язок, системи водопостачання, охорона здоров'я, банківська система, оборонна промисловість, а також інформаційні технології, в умовах війни вона стає головною мішенню для ворога [1, с. 75]. Руйнування транспортної інфраструктури разом з іншими діями ворога створили безпрецедентні труднощі для національної економіки [2, с. 167], а безпека транспортних маршрутів є одним із ключових викликів для логістичної діяльності в умовах війни [2, с. 168]. Зокрема, за даними СБУ, на кінець січня 2026 року було нейтралізовано понад 14 тисяч масштабних кібератак на Україну за час повномасштабного вторгнення [3]. В умовах повномасштабної російсько-української війни захист КІ України набуває стратегічного значення, оскільки

захищена КІ зможе забезпечити стабільне функціонування української держави та не допустити зростання соціальної напруги в умовах повномасштабної війни.

Одним із найбільш важливих елементів КІ України є транспортна інфраструктура (ТІ). У цьому ракурсі *мета дослідження* – виявити заходи підвищення безпеки ТІ України, яка перебуває у сфері безпекової відповідальності Державної спеціальної служби транспорту (далі – Держспецтрансслужби), яка виконує функцію підтримки безпеки ТІ через її охорону, оборону, технічне прикриття, відновлення пошкоджених об'єктів та будівництво нових, а також проводить розмінування вибухонебезпечних предметів на об'єктах ТІ. Безперебійне функціонування ТІ України створює підґрунтя для ефективної логістики у сфері оборони та економіки, зокрема через військові та гуманітарні вантажні перевезення, забезпечує соціальну стабільність та соціальну захищеність українського населення.

ТІ України, яка перебуває у сфері безпекової відповідальності Держспецтрансслужби охоплює: автомобільні та залізничні мости, мережу шляхів (дороги, автомагістралі, залізниці, річкові, морські, повітряні), транспортні вузли (порти, вокзали, аеропорти), тунелі, а також розмаїті інженерні споруди, які забезпечують функціонування ТІ. В умовах повномасштабної російсько-української війни зазначені об'єкти ТІ стають одними із пріоритетних цілей для нанесення ракетних ударів, диверсійних дій, кібератак та інформаційно-психологічного впливу через явну чи фейкову загрозу їх замінування та можливих терористичних актів. У цьому ракурсі ключовим викликом щодо безпечного функціонування ТІ України є її стійкість до комбінованих загроз, які можуть включати фізичне руйнування/знищення об'єктів ТІ через ракетні удари та диверсійні дії разом із кібератаками на цифрові системи управління транспортними потоками та пасажирськими перевезеннями.

Для створення безпечних умов використання ТІ Держспецтрансслужба на міжвідомчому рівні забезпечує резервування транспортних маршрутів, приймає участь у створенні моделей альтернативних логістичних шляхів, комплектує мобільні інженерні підрозділи, які здатні швидкими темпами відновлювати пошкоджені об'єкти ТІ, розробляє та впроваджує сучасні інженерні технології швидкого відновлення об'єктів ТІ, у тому числі – через наукові розробки.

Сучасна ТІ України функціонує на основі цифрових технологій, автоматизованих систем управління транспортним рухом, які є вразливими для кібератак ворога. Особливо небезпечними є кібератаки на автоматизовані системи керування залізничним рухом, інформаційні мережі логістичних центрів, цифрові канали координації військових і гуманітарних перевезень. Кібератаки на ТІ у першу чергу спрямовані на її дестабілізацію, порушення логістики, блокування управлінських процесів та створення умов для транспортної кризи. На цій основі Держспецтрансслужбі слід зосередити увагу також на кібербезпеці ТІ, оскільки автоматизовані системи управління рухом транспорту та цифрові диспетчерські мережі можуть бути об'єктами кібератак.

Безпека ТІ повинна включати постійний моніторинг кіберзагроз, резервне копіювання даних, підготовку спеціалістів з кібербезпеки, створення багаторівневої системи кіберзахисту через сегментацію цифрових мереж,

створення рівнів доступу до інформаційних ресурсів, багатофакторну автентифікацію персоналу, ізоляцію критично важливих систем управління від відкритих мереж передачі даних, дублювання серверної інфраструктури, використання захищених мобільних центрів управління та створення альтернативних каналів передачі інформації, підвищення рівня знань із кібербезпеки персоналу ТІ, використання систем штучного інтелекту для аналізу ризиків щодо можливих кіберзагроз.

Концепцію безпеки ТІ України слід будувати на основі системного підходу як багаторівневу модель організаційних, міжвідомчих, технічних, наукових, інформаційних та кібербезпекових заходів, які створюють надійні умови використання ТІ України.

1. Ковальов К. Є. Сучасні виклики та загрози для критичної інфраструктури України під час воєнного стану. *Приватне та публічне право*. – 2025. – № 1. – С.75-80. DOI: https://doi.org/10.32782/2663-5666.2025.1.12
2. Коваль К. П., Тєлєгін О. О. Логістика в умовах війни: ключові виклики та шляхи протидії загрозам. *Проблеми і перспективи економіки та управління*. – 2025. – № 1 (41). – С. 167-178. DOI: https://doi.org/10.25140/2411-5215-2025-1(41)-167-178
3. СБУ нейтралізувала понад 14 тисяч масштабних кібератак на Україну за час повномасштабного вторгнення. URL: https://ssu.gov.ua/novyny/sbu-neitralizuvala-ponad-14-tysiach-masshtabnykh-kiberatak-na-ukrainu-za-chas-povnomasshtabnoho-vtorhnennia (дата звернення: 01.05.2026).

Graph-Based Model for Risk Assessment of Access to Corporate Databases in Network Infrastructure

UDK 004.056.5:004.7

Oleksandr Budzynskyi[1], Yurii Shchavinsky[2]

State University of Information and Communication,
[1]oleksandr.email@gmail.com, [2]y.shchavinskyi@duikt.edu.ua

Modern corporate databases are characterized by a large number of interconnected nodes, services and data exchange channels. Under such conditions, ensuring cybersecurity becomes one of the key tasks. Traditional security mechanisms are focused mainly on the analysis of individual events or network traffic, and cannot fully assess the risks of multi-stage attacks implemented by sequentially compromising network nodes. In this regard, the use of graph models becomes promising, since they allow formalizing the structure of the network infrastructure and assessing risks at the level of possible access paths to the database.

The relevance of the topic of using graph models to improve the effectiveness of corporate database protection is substantiated in many studies. In work [1], the authors showed the need to use structural graph attack models to detect complex lateral movement scenarios. In paper [2], a model for assessing the cyber-physical security