УДК 004.056.53 DOI: https://doi.org/10.32631/pb.2023.1.17

СЕРГІЙ ВОЛОДИМИРОВИЧ КАЛЯКІН,
Харківський національний університет внутрішніх справ,
кафедра протидії кіберзлочинності;
https://orcid.org/0000-0001-5435-5921,
e-mail: svkalyakin@ukr.net;

ЮРІЙ МИКОЛАЙОВИЧ ОНИЩЕНКО,
кандидат наук з державного управління, доцент,
Харківський національний університет внутрішніх справ,
факультет № 4;
https://orcid.org/0000-0002-7755-3071,
e-mail: onischenko1980@gmail.com;

ВІТАЛІЙ ВІКТОРОВИЧ НОСОВ,
кандидат технічних наук, доцент,
Харківський національний університет внутрішніх справ,
кафедра протидії кіберзлочинності;
https://orcid.org/0000-0002-7848-6448,
e-mail: vitnos.g@gmail.com

КІБЕРБЕЗПЕКА МІСЬКОЇ ІНФРАСТРУКТУРИ

Статтю присвячено проблематиці захисту міської критичної інфраструктури від кіберзагроз у сучасних непростих умовах. Досліджено досвід інших країн у сфері захисту критичних об'єктів інфраструктури. Розглянуто особливості використання методик захисту інфраструктури в умовах ведення гібридної війни. Надано рекомендації щодо підвищення рівня захисту міської інфраструктури від кіберзагроз.

Ключові слова: *кібербезпека, критична міська інфраструктура, Інтернет речей (IoT), штучний інтелект, блокчейн.*

Оглядова стаття

ВСТУП. За прогнозами ООН, до 2050 р. 60 % населення планети проживатиме в містах. Можливості для отримання економічних і соціальних вигід можуть бути важливими причинами урбанізації та переміщення людей із внутрішніх районів у великі міста (Dwevedi, Krishna, Kumar, 2018). Сучасне місто – це складна система, яка потребує єдиного системного підходу до забезпечення громадської безпеки, правопорядку та безпеки довкілля в умовах високого рівня ризиків як техногенного, так і природного характеру (Degbelo et al., 2016).

Протидія природним і техногенним чинникам, актам незаконного втручання і терактам – одне з найважливіших завдань керівництва країни стосовно забезпечення соціальної стабільності міської спільноти. В умовах різкої активізації використання різних форм ведення війни існує висока ймовірність виникнення нових викликів та загроз, для яких об'єкти критичної інфраструктури в містах є цілями для нанесення ударів. Ризики та загрози безпеці для міст можуть бути більш критичними через загрозу використання зброї масового знищення.

Варто наголосити на тому, що інформаційні технології відіграють важливу роль у забезпеченні життєдіяльності сучасного міста. Автоматизовані системи управління все ширше використовуються для регулювання процесів життєдіяльності міста. Зростає кількість онлайн-сервісів, які впроваджено в міську інфраструктуру. Це стало причиною того, що останнім часом все частіше як кіберзлочинні угруповання, так і хакери-одинаки обирають інформаційні елементи міської інфраструктури як цілі своїх атак, що збільшує ризики для критичної міської інфраструктури в цілому (Ramos et al., 2018). Великі та маленькі міста дедалі частіше стикаються з усе більш серйозними викликами у сфері кібербезпеки, які суттєво впливають на життєздатність, конкурентоспроможність, психологічну стійкість і безпеку їхніх мешканців незалежно від площі міста та його розташування (Albino, Berardi, Dangelico, 2015).

Кібератака є делікатною проблемою у світі інтернет-безпеки. Уряди та бізнес-організації в усьому світі докладають величезних зусиль для захисту своїх даних. Вони використовують

різні типи інструментів і методів, щоб підтримувати бізнес, водночас зловмисники намагаються порушити безпеку та надсилати шкідливе програмне забезпечення, таке як ботнети, віруси, трояни тощо, для доступу до цінних даних. Щодня ситуація погіршується через появу нових типів зловмисного програмного забезпечення, яке атакує мережі (Al-Mohannadi et al., 2016).

Згідно зі звітом Міністерства внутрішньої безпеки США, кількість зареєстрованих кіберінцидентів проти критичної інфраструктури у Сполучених Штатах неухильно зростає протягом останніх кількох років. У 2020 р. було зареєстровано 295 інцидентів, порівняно зі 146 у 2018 р. Також згідно зі звітом «Cybersecurity Ventures» загальні збитки від кібератак по всьому світу сягнули6 трлн дол. у 2021 р., що є значним зростанням порівняно з попередніми роками. Проте з появою Інтернету речей (далі – IoT) продовжується розвиток розумних міст, а також посилюється необхідність вирішення проблем безпеки. Наприклад, у багатьох містах Європи впроваджують рішення IoT, спрямоване на моніторинг рівнів забруднення, за допомогою кількох пристроїв IoT і підключених датчиків (Toma et al., 2019). Через величезну кількість підключених пристроїв у середовищах IoT, таких як розумні міста, контроль доступу в цій сфері має забезпечувати високий ступінь масштабованості з урахуванням вимог безпеки (Buschsieweke, Gunes, 2017).

З огляду на збільшення кількості підключених до мережі Інтернет пристроїв і поширення використання хмарних технологій та Інтернету речей кібератаки на міську інфраструктуру можуть стати серйозною загрозою для безпеки жителів міст та економічного розвитку регіонів (Ainane, Ouzzif, Bouragba, 2018). Отже, важливо підвищувати свідомість про кібербезпеку та застосовувати ефективні заходи захисту, щоб запобігти можливим кібератакам на міську інфраструктуру.

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ. Кібербезпека міської інфраструктури є критичною проблемою в сучасному світі, оскільки міста у своєму розвитку все більше покладаються на цифрові технології. Міська інфраструктура включає в себе різні системи, такі як транспортні мережі, водопровідні й очисні споруди, енергетичні мережі та системи зв'язку. Кожна із цих систем є вразливою до кібератак. У розвинених країнах світу вже накопичено певний досвід щодо протидії таким атакам. *Мета* цієї статті полягає в аналізі, узагальненні та систематизації досвіду протидії кібератакам на критичну міську інфраструктуру країн світу, що є провідними в цій галузі.

Для досягнення поставленої мети потрібно виконати такі *завдання*:

– розглянути типи найпоширеніших у світі кібератак на міську інфраструктуру;

– проаналізувати й узагальнити досвід закордонних фахівців з кібербезпеки щодо протидії цим кібератакам в умовах сьогодення;

– спираючись на досвід закордонних колег, надати рекомендації щодо протидії кіберзагрозам в умовах розбудови сучасної міської інфраструктури.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ. У галузі кібербезпеки існує безліч методологій наукових досліджень, які допомагають дослідникам виконувати свої завдання. Наведемо декілька найбільш поширених із них.

Методологія аналізу загроз допомагає ідентифікувати загрози, що можуть виникнути в мережі або на конкретному комп'ютері. Вона використовується для виявлення потенційних вразливостей у системах кібербезпеки та визначення наслідків їхньої експлуатації.

Методологія побудови моделей загроз допомагає створити математичні моделі загроз та їх впливу на систему кібербезпеки. Вона дозволяє провести аналіз ризиків і визначити стратегії захисту від потенційних атак.

Методологія тестування вразливостей використовується для виявлення вразливостей у програмному забезпеченні та інших складових системи кібербезпеки. Вона полягає в тестуванні системи на наявність вразливостей і вжитті відповідних заходів щодо їх усунення.

Методологія аналізу випадків використання використовується для аналізу потенційних сценаріїв використання системи кібербезпеки, зокрема для виявлення можливих атак і викрадення даних. Вона дозволяє виявити слабкі місця в системі та вжити відповідних заходів щодо їх усунення.

Методологія управління ризиками допомагає оцінити рівень ризику і прийняти рішення щодо відповідних заходів із його зниження.

Відповідно до мети і завдань дослідження в роботі використано раціональну сукупність деяких з наведених методологій, здебільшого застосовувалися аналіз загроз та аналіз випадків використання.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТА ДИСКУСІЯ. Прогресивні досягнення в інформаційно-комунікаційних технологіях призвели до того, що сучасна критична інфраструктура стає дедалі складнішою, взаємопов'язаною та постійно розвивається. Збільшення складних

взаємозв'язків між такими критично важливими системами створює нові вразливості безпеки, якими можуть скористатися зловмисники для компрометації конфіденційних даних та інших систем, навіть таких, що знаходяться далеко від зони впливу (Ficco, Choraś, Kozik, 2017).

Важливо зазначити, що кібератаки на міську інфраструктуру, таку як транспортні системи, системи зв'язку, електромережі, системи водо- та газопостачання, очисні споруди, викликають дедалі більше занепокоєння в сучасному взаємопов'язаному світі. Відтак забезпечення кібербезпеки міської інфраструктури – важлива проблема, особливо для тих міст, що швидко розбудовуються і розвиваються. Зростання кількості підключених до мережі Інтернет пристроїв, які використовуються для контролю роботи електромережі, транспортних систем, газових та водопровідних мереж тощо, збільшує ризики злому систем та крадіжки або спотворення даних. Запобігання кібератакам на міську інфраструктуру стає необхідною умовою подальшого розвитку міста. Кібербезпека була головною проблемою для енергетичних компаній, які впроваджують інтелектуальні лічильники і технології розумних мереж. Незважаючи на добре відомі переваги технології інтелектуальних мереж і інтелектуальних лічильників, поки що не зовсім зрозуміло, як і якою мірою кібератаки можуть перешкоджати роботі інтелектуальних лічильників і віддаленому збору даних щодо споживання електроенергії клієнтом (Kumar, Gunnam, 2019).

Багато міських систем були розроблені десятиліття тому, коли вимоги до кібербезпеки були менш жорсткими і не були призначені для підключення до інтернету. Це означає, що багато систем мають застарілі протоколи та програмне забезпечення, які можуть бути легко піддані атакам. З іншого боку, енергоефективність мікропроцесорів зросла експоненціально за останнє десятиліття, водночас вартість найдешевших доступних на ринку процесорів суттєво знизилася. Було кілька проривних інновацій у нових дисциплінах, наприклад штучний інтелект (далі – AI), IoT, бездротові технології п'ятого покоління та повністю автономні транспортні засоби (далі – AV). Щоб автоматизувати процеси, штучний інтелект замінює людські здібності технологіями (наприклад, промисловими роботами) з метою підвищення продуктивності та зменшення ризиків для безпеки (Girdhar et al., 2022). Це призвело до виникнення нових сфер застосування вбудованих комп'ютерів, особливо в галузі автоматизації промислового контролю, медичного обслуговування та ведення домашнього господарства. Ці пристрої часто з'єднуються між собою за допомогою бездротових мереж архітектури Інтернету речей (IoT – Internet of Things), в якій будь-який пристрій може «спілкуватися» зі всіма іншими. Це робить IoT перспективним напрямом для сучасних міст. Однак ці процеси можуть зіткнутися з багатьма проблемами для свого успішного використання (Ivanova, 2017).

Вбудовані пристрої зазвичай використовують недороге обладнання і часто живляться від батареї, що призводить до жорстких обмежень на потужність споживання та потужність обробки. Крім цих технічних проблем, успішні IoT-протоколи також повинні забезпечувати безпеку даних, що в контексті IoT складається з цілісності, конфіденційності, актуальності даних, автентифікації та контролю доступу. Останній має особливе значення в розумних містах, оскільки несанкціонований доступ до критичної інфраструктури може спричинити величезні фінансові втрати і ставить під загрозу безпеку життєдіяльності мешканців міста.

Однією з найнебезпечніших загроз кібербезпеці міської інфраструктури є кібератаки на системи управління транспортом. Наприклад, у разі злому систем управління світлофорами можливе блокування дорожнього руху в багатьох частинах міста, що призведе до серйозних проблем із транспортним потоком та безпекою дорожнього руху. Система дорожнього руху для автомобілів не змінювала своїх фізичних, промислових і соціальних структур протягом більш ніж 100 років з моменту її появи в суспільстві. Вона була розгорнута у великих масштабах і відіграє важливу роль у мобільності. Елементи системи - водій, автомобіль і дорога - фізично контактують одне з одним, і системою керує лише людина. Удосконалення електричних та електронних технологій протягом понад 30 років покращило продуктивність автомобіля, але не покращило роботу водія та дороги (Miyata, 2018).

Сьогодні транспортні засоби все частіше підключаються до Інтернету речей, що дозволяє їм надавати постійний доступ до інформації водіям і пасажирам під час руху. Однак оскільки кількість підключених транспортних засобів продовжує зростати, з'являються нові вимоги (такі як безперервний, безпечний, надійний, масштабований обмін інформацією між транспортними засобами, людьми та придорожньою інфраструктурою) до автомобільних мереж (Contreras, Zeadally, Guerrero-Ibanez, 2018). Як

загальна тенденція розвитку автомобільної промисловості підключені й автономні транспортні засоби (далі – CAV) можна використовувати для підвищення безпеки транспортування, сприяння вибору мобільності, зниження витрат користувачів і створення нових робочих місць. Однак із підвищенням рівня підключення та автоматизації зловмисники можуть легко здійснювати різні види атак, які загрожують безпеці CAV (Sun, Yu, Zhang, 2021).

Також однією з тенденцій розвитку авторинку є збільшення кількості електромобілів. У 2020 р. спеціалісти з кібербезпеки виявили недоліки безпеки в додатку «ChargePoint Home» для зарядки електромобілів. Цей недолік дозволить віддаленому зловмиснику вторгнутися в зарядний пристрій і втрутитися в зарядку електромобіля через з'єднання Wi-Fi із зарядним пристроєм. Також були виявлені недоліки безпеки в зарядних пристроях «EVlink» виробництва Schneider Electric (Acharya et al., 2020).

Новим видом міського транспорту стали автономні літальні апарати (далі – AAV) – системи літальних апаратів, екіпаж яких замінено автономними комп'ютерними системами та радіолінією, що управляється дистанційно з наземної станції. Цей вид транспорту нещодавно був прийнятий як засіб пересування в рамках піонерської ініціативи Дубая. Очікується, що незабаром цей вид транспорту запровадять більше розумних міст, оскільки вважається, що він продемонструє потенціал трансформації міського транспорту та майбутньої мобільності. Однак занепокоєння викликає безпека цих систем та інфраструктури розумного міста, від якої вони залежать у своїй діяльності. Звичайно, впровадження AAV у транспортну інфраструктуру міста порушує багато нових питань кібербезпеки, які потребують дослідження та відповідей (Dawam, Feng, Li, 2018).

Захист від кібератак на системи управління транспортом повинен включати в себе розробку криптографічних протоколів, захист від дій зловмисників на мережному рівні й інші заходи, які в комплексі дозволять зробити транспортний рух більш безпечним.

Об'єднання тисяч пристроїв IoT під час спілкування один з одним через інтернет для створення розумної системи призводить до створення величезної кількості даних, які називаються «Big Data». Інтеграція послуг Інтернету речей для отримання даних про місто в режимі реального часу, а потім ефективна обробка такого великого обсягу даних, спрямована на створення розумного міста, є складним завданням (Rathore, Ahmad, Paul, 2016). Вочевидь зі збільшенням кількості підключених пристроїв, пов'язаних з мережею Інтернет, посилюється і ризик атак на них. Сучасні міста стають все більш залежними від технологій і відповідно більш чутливими до кібератак. Наприклад, міська інфраструктура може враховувати водозаборні системи, електростанції, транспортну інфраструктуру, лікарні тощо. Усі ці системи містять обладнання, яке може стати об'єктом атаки з боку хакерів, що може становити серйозну загрозу безпеці громади (Morales Lucas, de Mingo López, Gómez Blas, 2018). Одним з найбільш небезпечних видів кібератак є розповсюдження шкідливих програм, які можуть зашифрувати файли на комп'ютерах міської інфраструктури. Це може призвести до втрати важливої інформації та негативно позначитися на функціонуванні міських служб (Nagano, 2010).

Кібератаки є одними з головних ризиків, з якими стикаються органи місцевого самоврядування. Лише у 2019 р. було зареєстровано 162 атаки програм-вимагачів проти державних і місцевих органів влади Сполучених Штатів Америки (Preis, Susskind, 2020). Найбільш гучна атака сталася 7 травня у м. Балтімор, де спрацював криптолокер «RobbinHood». У той же день муніципалітет Балтімора повідомив ФБР і вимкнув частину своїх систем, вважаючи, що таким чином зможе зупинити поширення шкідливого програмного забезпечення, яке на той час вже встигло заразити голосову та електронну пошти, систему оплати штрафів, систему оплати рахунків за воду, систему відеоспостереження, а також систему оплати податків за нерухомість, через що більше 1500 угод з нерухомістю було призупинено. Зловмисники вимагали викуп у розмірі трьох біткоїнів за кожну з атакованих систем або 13 біткоїнів за повернення доступу до всіх систем відразу. На засіданні міського бюджетного комітету чиновники Балтімора підрахували, що напад коштував місту 18,2 млн дол.

Випадок у Балтиморі не є поодиноким. RobbinHood до Балтімора атакував ще одне американське місто – Гринвиль у Північній Каліфорнії. Місто Лейк-Сіті, штат Флорида, декілька днів відновлювалося після атаки іншого шифрувальника «TripleThreat», який вразив його електронну пошту та електронні платіжні системи 10 червня 2019 р. І це лише невеличка частина інцидентів такого роду.

На останньому Всесвітньому економічному форумі в Давосі обговорювалася можливість кібератаки такої потужності, що призведе до глобальної катастрофи. Хоча ще невідомо, чи виправдаються прогнози про катастрофічну за наслідками кібератаку, за останні кілька років

відбулася низка гучних зламів із достатнім імпульсом, щоб вважати їх катастрофічними. Одна з найвідоміших кібератак сталася у 2020 р. Атака на ланцюг поставок «SolarWinds» призвела до компрометації 100 компаній та 9 федеральних агентств. Також у наступному 2021 р. атака програми-здирника «Colonial Pipeline» змусила організацію перекрити 5500 миль трубопроводів.

Розвиток розумного міста з належним використанням новітніх технологій значно зменшує проблеми безпеки, витрати енергії, економить час і покращує безпеку людей у міських районах під час урбанізації. Наступним викликом для сучасного міста стає зростаюча складність кіберзагроз. Ситуація, яка зараз склалася, потребує детального прогнозування інцидентів. Для вирішення цієї проблеми потрібне формування ефективних систем безпеки критичних об'єктів із використанням управління якістю безпеки, що передбачає забезпечення нормативного рівня безпеки шляхом виконання функцій планування, контролю, інформаційного обслуговування, розробки, впровадження заходів та прийняття рішень щодо якості їх виконання (Nafrees, Sujah, Mansoor, 2021).

Щоб протистояти цим викликам, уряди та особи, які приймають рішення, впроваджують проєкти розумних міст, спрямовані на стале економічне зростання та покращення якості життя як для мешканців, так і для гостей. Щоб зменшити ризики кібербезпеки для міської інфраструктури, важливо мати комплексний інтегрований підхід, який враховує як технічні, так і нетехнічні рішення. Це може бути впровадження надійної автентифікації та контролю доступу, моніторинг мережного трафіку на наявність аномалій, використання шифрування та інших технологій безпеки, а також регулярне оновлення програмного та апаратного забезпечення для усунення відомих вразливостей (Osman, 2019).

Розглянемо зазначені вище заходи докладніше. Перш за все, міста повинні проводити регулярні огляди інфраструктури для виявлення можливих вразливостей. Крім того, міста повинні використовувати сучасні технології захисту, які здатні виявляти та блокувати кібератаки. Також потрібно забезпечити оновлення програмного забезпечення та встановлення необхідних патчів, які запобігають вразливості мережі перед зловмисниками. Це може бути забезпечено регулярними аудитами безпеки мережі та вчасним відповідним оновленням програмного забезпечення.

Навчання персоналу є надзвичайно важливим в аспекті кібербезпеки. Всі працівники, які мають доступ до мережі та важливої інформації, повинні знати про кібербезпеку та вміти розпізнавати загрози і поведінку, що може призвести до їхньої реалізації. Персонал повинен також знати процедуру зміни паролів і робити це регулярно.

Під час планування кібербезпеки міської інфраструктури необхідно пам'ятати про резервні копії даних. Це допоможе відновити доступ до важливих даних у разі їх втрати або пошкодження. Резервні копії повинні зберігатися в безпечному місці, що забезпечує їхню конфіденційність і доступність.

Наступним етапом удосконалення процесу забезпечення якості безпеки має бути структурний підхід до переведення інженерно-технічних систем, сил забезпечення безпеки та персоналу об'єкта, що захищається, з поточного стану в бажаний майбутній стан із вищим рівнем безпеки. Він передбачає проведення систематичного моніторингу для визначення змін якості безпеки, що впливають на небезпечні фактори та стратегії зменшення ризиків до того, як вони будуть реалізовані на практиці, що дозволяє оцінювати стратегії управління непрямими ризиками безпеки.

Управління змінами якості безпеки допомагає усунути прогалини і передбачає проведення систематичного моніторингу зовнішнього середовища об'єкта, аналіз змін об'єктів і територій, що прилягають до нього, дозволяє з високою достовірністю визначити, що та за яких умов може статися, а постійно коригований план дає можливість сформувати оптимальний сценарій дій, враховуючи способи та засоби протидії загрозам. Обов'язковою умовою прогнозування є необхідна аналітична робота, для якої потрібне чітке координування зусиль усіх задіяних сторін.

Використання даних у реальному часі покращує операційну ефективність, підключення, процес прийняття рішень і загальну продуктивність комп'ютерних мереж і комунікаційних платформ на основі IoT для збору даних, керування пристроями та хмарних рішень (Protic et al., 2022).

Підтримка безпечного міста передбачає створення інфраструктури для здійснення діяльності та надання технологій, яка включає в себе три основні види діяльності:

1) спільне усвідомлення ситуації, прийняття рішень і зворотній зв'язок. Оскільки фізичні та кібернетичні загрози виникають у багатьох сферах, у тому числі фінансованих державою, через злочинців, стихійні лиха і просто недбалість, то створення протоколів співпраці між державним і приватним секторами для

побудови безпечного міста є пріоритетом для планування та підзвітності;

2) використання комплексного оперативного управління для запобігання, пом'якшення наслідків інцидентів та відновлювання після них;

3) впровадження нових технологій, які будуть сприяти як фізичній, так і кібернетичній безпеці. Прикладами таких технологій є датчики, сканери, бар'єри, аудіо- та відеоспостереження, біометрія, розвідка й аналіз даних.

Наведені ключові елементи системи протидії загрозам не є незалежними один від одного і повинні бути об'єднані разом у певних рамках, щоб представити спеціалізовані варіанти реагування для кожної з безлічі загроз. Потрібне міцне та надійне державно-приватне партнерство як для створення, так і для захисту міської інфраструктури, особливо за сучасних умов, коли загрози безпеці не тільки зростають, але і стають дедалі більш витонченими.

Інший можливий метод забезпечення кібербезпеки міської інфраструктури – це застосування блокчейн-технології. Технологія блокчейн забезпечує безпеку та покращує комунікацію і торгівлю за рахунок підвищення прозорості транзакцій (Samuel et al., 2020). Блокчейн може бути використаний для забезпечення безпеки великої кількості пристроїв, підключених до IoT, що складають міську інфраструктуру. За допомогою блокчейну можна створити безпечну мережу, яка буде захищена від хакерських атак і зловмисного використання.

Блокчейн може бути використаний для забезпечення кібербезпеки на декількох рівнях. Наведемо декілька способів, якими блокчейн може допомогти у забезпеченні кібербезпеки:

1) захист конфіденційності та цілісності інформації. Блокчейн може бути використаний для захисту конфіденційної інформації, оскільки дані, які зберігаються в блокчейні, зашифровані та недоступні для змін. Через те, що кожна транзакція зберігається в окремих блоках, він забезпечує надійне збереження та перевірку даних. Отже, блокчейн забезпечує більшу безпеку, ніж стандартні централізовані системи зберігання даних;

2) автентифікація користувачів. Блокчейн може допомогти у забезпеченні автентифікації користувачів, що дозволяє встановлювати безпечний доступ до ресурсів. Так, наприклад, у фінансовому секторі можна використовувати блокчейн для автентифікації транзакцій і підтвердження правильності платежів;

3) захист від кібератак. Блокчейн може допомогти у забезпеченні захисту від кібератак, оскільки дані, які зберігаються в блокчейні, розподіляються між багатьма комп'ютерами. Це означає, що для того, щоб зламати систему, зловмисник повинен зламати кожен комп'ютер у мережі, що практично неможливо. Також блокчейн може бути використаний для захисту від DDoS-атак, які спрямовані на забруднення мережі. Блокчейн-платформа може використовувати різноманітні методи захисту від DDoS, такі як Proof-of-Work (PoW), Proof-of-Stake (PoS) та Proof-of-Activity (PoA);

4) відновлення даних. Блокчейн може бути використаний для відновлення даних у разі їх втрати або пошкодження. Це може бути корисно в тих випадках, коли дані необхідні для забезпечення безперебійної роботи системи.

Отже, блокчейн може бути корисним інструментом для забезпечення кібербезпеки, оскільки він забезпечує надійний захист даних, що в ньому зберігаються. Блокчейн також забезпечує автентифікацію та надійну ідентифікацію користувачів, що дозволяє уникнути відкриття доступу до інформації для шахраїв та інших зловмисників. Таким чином, блокчейн може забезпечити захист персональних даних мешканців міста, які використовують міські сервіси та послуги. За допомогою блокчейну можна створити безпечну і прозору систему, в якій персональні дані будуть захищені від несанкціонованого доступу.

Однак, на жаль, застосування блокчейну в міській інфраструктурі залишається поки що недостатньо дослідженим напрямом. Залишилося багато завдань і проблем, які потрібно вирішити, щоб впровадження блокчейну було успішним (Samuel et al., 2020).

Для підвищення інформаційної безпеки міської інфраструктури необхідно приділити увагу ще кільком аспектам.

1. Захист усіх напрямів

Інфраструктура будь-якої організації безпечна лише тоді, коли захищені всі її активи. Потрібно захистити всі критичні сфери корпоративного ризику: кінцеві точки, хмарні робочі місця, системи ідентифікації та сховища даних. Обрані рішення, повинні забезпечувати надточне виявлення й автоматичний захист і відновлення, пошук небезпечних загроз і пріоритетне спостереження за вразливими місцями. Необхідно встановити міцну IT-гігієну за допомогою інвентаризації активів і постійного контролю вразливостей. Важливо усвідомлювати, що неможливо захистити елементи системи, про які ви не знаєте.

2. Вивчення свого супротивника

За кожною кібератакою стоїть людина. Якщо ви знаєте особливості поведінки супротивників, то, орієнтуючись на галузь або особливості місцевості, в якій знаходиться ваша організація, можна підготуватися до організації ефективного захисту від інструментів і тактик, які використовують зловмисники.

3. Пильність і постійна готовність

Швидкість часто визначає успіх або невдачу. Особливо це стосується кібербезпеки. Приховані зломи можуть статися за лічені хвилини з руйнівними наслідками. Команди безпеки будь-якого розміру повинні інвестувати в швидкість і маневреність для щоденної роботи та прийняття тактичних рішень шляхом автоматизації профілактичних, розшукових, слідчих дій і процесів реагування з інтегрованою розвідкою про кіберзагрози, яка дозволить безпосередньо спостерігати «лінію фронту», коли кожна секунда на рахунку.

4. Сучасні системи протидії атакам

Майже 80 % кібератак використовують атаки на основі ідентифікаційної інформації для компрометації законних облікових даних та різні методи для уникнення виявлення. Сучасні системи протидії кібератакам забезпечують надточність виявлення загроз і запобігання атакам на основі ідентифікації даних у реальному часі, поєднуючи потужність передового штучного інтелекту, поведінкової аналітики та гнучкого механізму політики безпеки для виконання умовного доступу на основі оцінки ризиків.

5. Прийняття нульової довіри

Оскільки зловмисники хочуть монетизувати свою діяльність, вони націлюються на пошук даних своїх жертв, які дозволять отримати оплату за рахунок викупу та здирництва, і навіть виставити дані на аукціон, щоб отримати найвищий прибуток. Сучасна глобальна економіка вимагає доступу до даних будь-де та будь-коли, тому дуже важливо прийняти модель нульової довіри, тобто дані повинні бути максимально захищеними від несанкціонованого доступу, але при цьому завжди доступними для використання авторизованим користувачем.

6. Стеження за кримінальним підпіллям

Зловмисники збираються для співпраці, використовуючи приховані повідомлення на різних платформах і темних вебфорумах. Окрім моніторингу власного середовища, служби безпеки повинні бути пильними та стежити за діяльністю кримінального підпілля. Використання інструментів моніторингу цифрових ризиків, таких як, наприклад, Falcon X Recon, для відстеження можливих загроз для особистих даних громадян або даних юридичних осіб дозволяє отримати завчасні попередження про активні загрози та використати цю інформацію для запобігання випадкам витоку даних і фінансових або репутаційних втрат.

7. Своєчасне усунення помилок і недоліків

Найпоширенішими причинами хмарних вторгнень залишаються людські помилки, наприклад упущення під час спільної адміністративної діяльності. Важливо створити нову інфраструктуру з шаблонами за замовчуванням, які спрощують налаштування рівнів безпеки. Ця стратегія гарантує, що нові облікові записи створюються передбачуваним чином з усуненням поширених джерел людських помилок. Також потрібно обов'язково встановити налаштовані ролі та групи безпеки мережі, які не дозволяють розробникам і операторам будувати їхні власні профілі безпеки, оскільки вони випадково можуть зробити це з помилками.

8. Інвестування в сучасні технології захисту

Експерти з кібербезпеки помітили, що 62 % кібератак включають у себе нешкідливе програмне забезпечення, що відстежує діяльність клавіатури. Коли супротивники просувають своє програмне забезпечення таким чином, щоб обійти застарілі рішення безпеки, лише автономного машинного навчання недостатньо, щоб їх зупинити. Поєднання технологій з експертними мисливцями за загрозами є абсолютно обов'язковим, щоб побачити та зупинити найскладніші загрози. Найвищу якість захисту можуть надати лише найсучасніші рішення, які за допомогою експертного досвіду, ресурсів і покриття проблемної галузі, що базується на штучному інтелекті, гарантують більш високий рівень захисту.

9. Створення культури кібербезпеки

Незважаючи на те, що технологія має важливе значення для виявлення та припинення вторгнень, кінцевий користувач залишається вирішальною ланкою в ланцюжку запобігання порушенням. Щоб підвищити обізнаність користувачів, необхідно запровадити програми для боротьби з постійною загрозою фішингу та пов'язані з ним методи соціальної інженерії. Для команд служби безпеки необхідна постійна практика. Потрібно заохочувати середовище, яке регулярно виконує вправи за столом, і проводити тренінги для виявлення прогалин та усунення недоліків у кібербезпеці організації.

ВИСНОВКИ. Отже, забезпечення кібербезпеки міської інфраструктури є надзвичайно складним завданням та потребує багатогранного комплексного підходу, який має забезпечити належний рівень ефективного захисту

як окремих інфраструктурних об'єктів, так і мережі в цілому від можливих атак з боку зловмисників. Кібератаки на міську інфраструктуру можуть мати різні форми і наслідки. Наприклад, хакери можуть спробувати зламати системи керування транспортом або енергетичні мережі, щоб створити хаос або знизити ефективність роботи цих систем.

У світі все більше компаній, установ і організацій стають жертвами кібератак. Це може бути пов'язано з розширенням мережі Інтернету речей і збільшенням кількості підключених до неї пристроїв. Ціна кібератак може бути високою як для їх жертв, так і для суспільства в цілому. Кібератаки можуть призвести до викрадення чутливої інформації, знищення даних або розшифрування зашифрованих даних. Крім того, такі атаки можуть призвести до втрати робочого часу та призупинення роботи систем, що може мати серйозні наслідки для міської інфраструктури.

Щоб запобігти кібератакам, необхідно використовувати сучасні методи захисту даних, враховуючи захист мереж і комп'ютерів, а також використання шифрування та забезпечення безпеки в застосуваннях. Крім того, необхідно здійснювати регулярне оновлення програм. Навчання персоналу, регулярні аудити та своєчасне встановлення патчів є ключовими моментами у забезпеченні безпеки мережі. Резервні копії даних також є важливим елементом захисту мережі від втрати важливої інформації.

Забезпечення кібербезпеки міської інфраструктури є дуже важливим та актуальним завданням в сучасному світі, де міста стають все більш інформаційно залежними. Ми розглянули різні методи забезпечення кібербезпеки, такі як застосування штучного інтелекту, Інтернету речей та блокчейну. Кожен із цих методів має свої переваги і недоліки, але в комплексі вони можуть бути успішно використані для створення безпечної міської інфраструктури.

Підсумовуючи, зазначимо, що атаки на міську інфраструктуру будуть і далі поширюватися, відповідно потрібно бути заздалегідь готовими до них. Забезпечення інформаційної безпеки міста вимагає великих коштів, але витрати на відновлення втрачених даних можуть набагато перевищити витрати на інформаційну безпеку.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Acharya S., Dvorkin Yu., Pandzic H., Karri R. Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective. *IEEE Access*. 2020. Vol. 8. Pp. 214434–214453. DOI: https://doi.org/10.1109/access.2020.3041074.

2. Ainane N., Ouzzif M., Bouragba K. Data security of smart cities // SCA'18: Proceedings of the 3rd International Conference on Smart City Applications (New York, United States, 10 October 2018). DOI: https://doi.org/10.1145/3286606.3286866.

3. Albino V., Berardi U., Dangelico R. M. Smart Cities*:* Definitions, Dimensions, Performance, and Initiatives. *Journal of Urban Technology*. 2015. Vol. 22 (1). Pp. 3–21. DOI: https://doi.org/10.1080/10630732.2014.942092.

4. Al-Mohannadi H., Mirza Q., Namanya A., Awan I., Cullen A., Disso J. Cyber-Attack Modeling Analysis Techniques: An Overview // 4th International Conference on Future Internet of Things and Cloud Workshops (Vienna, Austria, 22–24 August 2016). DOI: https://doi.org/10.1109/w-ficloud.2016.29.

5. Buschsieweke M., Gunes M. Securing critical infrastructure in smart cities: Providing scalable access control for constrained devices // 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (Montreal, Canada, 8–13 October 2017). DOI: https://doi.org/10.1109/pimrc.2017.8292689.

6. Contreras J., Zeadally S., Guerrero-Ibanez J. A. Internet of Vehicles: Architecture, Protocols, and Security. *Internet of Things Journal*. 2018. Vol. 5, Iss. 5. DOI: https://doi.org/10.1109/jiot.2017.2690902.

7. Dawam E. S., Feng X., Li D. Autonomous Arial Vehicles in Smart Cities: Potential Cyber-Physical Threats // 20th International Conference on High Performance Computing and Communications (Exeter, UK, 28–30 June 2018). DOI: https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00247.

8. Degbelo A., Granell C., Trilles S., Bhattacharya D., Casteleyn S., Kray C. Opening up Smart Cities: Citizen-Centric Challenges and Opportunities from GIScience. *International Journal of Geo-Information.* 2016. Vol. 5, Iss. 2. DOI: https://doi.org/10.3390/ijgi5020016.

9. Dwevedi R., Krishna V., Kumar A. Environment and Big Data: Role in Smart Cities of India*. Resources.* 2018. Vol. 7, Iss. 4. DOI: https://doi.org/10.3390/resources7040064.

10. Ficco M., Choraś M., Kozik R. Simulation platform for cyber-security and vulnerability analysis of critical infrastructures. *Journal of Computational Science.* 2017. Vol. 22. Pp. 179–186. DOI: https://doi.org/10.1016/j.jocs.2017.03.025.

11. Girdhar M., You Yo., Song T.-J., Ghosh S., Hong J. Post-Accident Cyberattack Event Analysis for Connected and Automated Vehicles. *IEEE Access.* 2022. Vol. 10. DOI: https://doi.org/10.1109/ACCESS.2022.3196346.

12. Ivanova Yo. Modelling the impact of cyber attacks on the traffic control centre of an urban automobile transport system by means of enhanced cybersecurity // BulTrans-2017 – 9th International Scientific Conference on Aeronautics, Automotive and Railway Engineering and Technologies (Sozopol, Bulgaria, 7 November 2017). DOI: https://doi.org/10.1051/matecconf/201713307001.

13. Kumar S., Kumar H., Gunnam G. R. Security Integrity of Data Collection from Smart Electric Meter under a Cyber Attack // 2nd International Conference on Data Intelligence and Security (South Padre Island, USA, 28–30 June 2019). DOI: https://doi.org/10.1109/icdis.2019.00009.

14. Miyata H. Digital Transformation of Automobile and Mobility Service // International Conference on Field-Programmable Technology (Naha, Japan, 10–14 December 2018). DOI: https://doi.org/10.1109/fpt.2018.00012.

15. Morales Lucas C., de Mingo López L., Gómez Blas N. Natural Computing Applied to the Underground System: A Synergistic Approach for Smart Cities. *Sensors.* 2018. Vol. 18, Iss. 12. DOI: https://doi.org/10.3390/s18124094.

16. Nafrees A., Sujah A., Mansoor C. Smart Cities: Emerging technologies and Potential solutions to the Cyber security threads // 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (Mysuru, India, 10–11 December 2021). DOI: https://doi.org/10.1109/ICEECCOT52851.2021.9707994.

17. Nagano H. Development of ICT Infrastructure for Local Socio-Economic System in Japan Another Approach Toward Cybersecurity in the Non-urban Area // International Conference on Availability, Reliability and Security (Krakow, Poland, 15–18 February 2010). DOI: https://doi.org/10.1109/ares.2010.114.

18. Osman A. M. S. A novel big data analytics framework for smart cities. *Future Generation Computer Systems.* 2019. Vol. 91. Pp. 620–633. DOI: https://doi.org/10.1016/j.future.2018.06.046.

19. Preis B., Susskind L. Municipal Cybersecurity: More Work Needs to be Done. *Urban Affairs Review*. 2020. Vol. 58, Iss. 2. DOI: https://doi.org/10.1177/1078087420973760.

20. Protic D., Gaur L., Stankovich M., Rahman A. Cybersecurity in Smart Cities: Detection of Opposing Decisions on Anomalies in the Computer Network Behavior. *Electronics.* 2022. Vol. 11, Iss. 22. DOI: https://doi.org/10.3390/electronics11223718.

21. Ramos F., Trilles S., Torres-Sospedra J., Perales F. New Trends in Using Augmented Reality Apps for Smart City Contexts. *International Journal of Geo-Information.* 2018. Vol. 7, Iss. 12. DOI: https://doi.org/10.3390/ijgi7120478.

22. Rathore M. M., Ahmad A., Paul A. IoT-based smart city development using big data analytical approach // International Conference on Automatica (Curico, Chile, 19–21 October 2016). DOI: https://doi.org/10.1109/ica-acca.2016.7778510.

23. Samuel O., Almogren A., Javaid A., Zuair M., Ullah I., Javaid N. Leveraging Blockchain Technology for Secure Energy Trading and Least-Cost Evaluation of Decentralized Contributions to Electrification in Sub-Saharan Africa. *Entropy.* 2020. Vol. 22, Iss. 2. DOI: https://doi.org/10.3390/e22020226.

24. Sun X., Yu F. R., Zhang P. A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs). *Transactions on Intelligent Transportation Systems*. 2021. Vol. 23, Iss. 7. Pp. 6240–6259. DOI: https://doi.org/10.1109/tits.2021.3085297.

25. Toma C., Alexandru A., Popa M., Zamfiroiu A. IoT Solution for Smart Cities' Pollution Monitoring and the Security Challenges. *Sensors.* 2019. Vol. 19, Iss. 15. DOI: https://doi.org/10.3390/s19153401.

Надійшла до редакції: 27.02.2023

Прийнята до опублікування: 16.03.2023

REFERENCES

1. Acharya, S., Dvorkin, Yu., Pandzic, H., & Karri, R. (2020). Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective. *IEEE Access, 8*, 214434-214453. https://doi.org/10.1109/access.2020.3041074.

2. Ainane, N., Ouzzif, M., & Bouragba, K. (2018, October 10). *Data security of smart cities* [Conference presentation abstract]. SCA'18: Proceedings of the 3rd International Conference on Smart City Applications, New York, United States. https://doi.org/10.1145/3286606.3286866.

3. Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart Cities*:* Definitions, Dimensions, Performance, and Initiatives. *Journal of Urban Technology, 22*(1), 3-21. https://doi.org/10.1080/10630732.2014.942092.

4. Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., & Disso, J. (2016, August 22-24). *Cyber-Attack Modeling Analysis Techniques: An Overview* [Conference presentation abstract]. 4th International Conference on Future Internet of Things and Cloud Workshops, Vienna, Austria. https://doi.org/10.1109/w-ficloud.2016.29.

5. Buschsieweke, M., & Gunes, M. (2017, October 8-13). *Securing critical infrastructure in smart cities: Providing scalable access control for constrained devices* [Conference presentation abstract]. 28th Annual

International Symposium on Personal, Indoor, and Mobile Radio Communications, Montreal, Canada. https://doi.org/10.1109/pimrc.2017.8292689.

6. Contreras, J., Zeadally, S., & Guerrero-Ibanez, J. A. (2018). Internet of Vehicles: Architecture, Protocols, and Security. *Internet of Things Journal, 5*(5). https://doi.org/10.1109/jiot.2017.2690902.

7. Dawam, E. S., Feng, X., & Li, D. (2018, June 28-30). *Autonomous Arial Vehicles in Smart Cities: Potential Cyber-Physical Threats* [Conference presentation abstract]. 20th International Conference on High Performance Computing and Communications, Exeter, UK. https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00247.

8. Degbelo, A., Granell, C., Trilles, S., Bhattacharya, D., Casteleyn, S., & Kray, C. (2016). Opening up Smart Cities: Citizen-Centric Challenges and Opportunities from GIScience. *International Journal of Geo-Information, 5*(2). https://doi.org/10.3390/ijgi5020016.

9. Dwevedi, R., Krishna, V., & Kumar, A. (2018). Environment and Big Data: Role in Smart Cities of India. *Resources, 7*(4). https://doi.org/10.3390/resources7040064.

10. Ficco, M., Choraś, M., & Kozik, R. (2017). Simulation platform for cyber-security and vulnerability analysis of critical infrastructures. *Journal of Computational Science, 22*, 179-186. https://doi.org/10.1016/j.jocs.2017.03.025.

11. Girdhar, M., You, Yo., Song, T.-J., Ghosh, S., & Hong, J. (2022). Post-Accident Cyberattack Event Analysis for Connected and Automated Vehicles. *IEEE Access, 10*. https://doi.org/10.1109/ACCESS.2022.3196346.

12. Ivanova, Yo. (2017, November 7). *Modelling the impact of cyber attacks on the traffic control centre of an urban automobile transport system by means of enhanced cybersecurity* [Conference presentation abstract]. BulTrans-2017 – 9th International Scientific Conference on Aeronautics, Automotive and Railway Engineering and Technologies, Sozopol, Bulgaria. https://doi.org/10.1051/matecconf/201713307001.

13. Kumar, S., Kumar, H., & Gunnam, G. R. (2019, June 28-30). *Security Integrity of Data Collection from Smart Electric Meter under a Cyber Attack* [Conference presentation abstract]. 2nd International Conference on Data Intelligence and Security, South Padre Island, USA. https://doi.org/10.1109/icdis.2019.00009.

14. Miyata, H. (2018, December 10-14). *Digital Transformation of Automobile and Mobility Service* [Conference presentation abstract]. International Conference on Field-Programmable Technology, Naha, Japan. https://doi.org/10.1109/fpt.2018.00012.

15. Morales Lucas, C., de Mingo López, L., & Gómez Blas, N. (2018). Natural Computing Applied to the Underground System: A Synergistic Approach for Smart Cities. *Sensors, 18*(12). https://doi.org/10.3390/s18124094.

16. Nafrees, A., Sujah, A., & Mansoor, C. (2021, December 10-11). *Smart Cities: Emerging technologies and Potential solutions to the Cyber security threads* [Conference presentation abstract]. 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques, Mysuru, India. https://doi.org/10.1109/ICEECCOT52851.2021.9707994.

17. Nagano, H. (2010, February 15-18). *Development of ICT Infrastructure for Local Socio-Economic System in Japan Another Approach Toward Cybersecurity in the Non-urban Area* [Conference presentation abstract]. International Conference on Availability, Reliability and Security, Krakow, Poland. https://doi.org/10.1109/ares.2010.114.

18. Osman, A. M. S. (2019). A novel big data analytics framework for smart cities. *Future Generation Computer Systems, 91*, 620-633. https://doi.org/10.1016/j.future.2018.06.046.

19. Preis, B., & Susskind, L. (2020). Municipal Cybersecurity: More Work Needs to be Done. *Urban Affairs Review, 58*(2). https://doi.org/10.1177/1078087420973760.

20. Protic, D., Gaur, L., Stankovich, M., & Rahman, A. (2022). Cybersecurity in Smart Cities: Detection of Opposing Decisions on Anomalies in the Computer Network Behavior. *Electronics, 11*(22). https://doi.org/10.3390/electronics11223718.

21. Ramos, F., Trilles, S., Torres-Sospedra, J., & Perales, F. (2018). New Trends in Using Augmented Reality Apps for Smart City Contexts. *International Journal of Geo-Information, 7*(12). https://doi.org/10.3390/ijgi7120478.

22. Rathore, M. M., Ahmad, A., & Paul, A. (2016, October 19-210. *IoT-based smart city development using big data analytical approach* [Conference presentation abstract]. International Conference on Automatica, Curico, Chile). https://doi.org/10.1109/ica-acca.2016.7778510.

23. Samuel, O., Almogren, A., Javaid, A., Zuair, M., Ullah, I., & Javaid, N. (2020). Leveraging Blockchain Technology for Secure Energy Trading and Least-Cost Evaluation of Decentralized Contributions to Electrification in Sub-Saharan Africa. *Entropy, 22*(2). https://doi.org/10.3390/e22020226.

24. Sun, X., Yu, F. R., & Zhang, P. (2021). A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs). *Transactions on Intelligent Transportation Systems, 23*(7), 6240-6259. https://doi.org/10.1109/tits.2021.3085297.

25. Toma, C., Alexandru, A., Popa, M., & Zamfiroiu, A. (2019). IoT Solution for Smart Cities' Pollution Monitoring and the Security Challenges. *Sensors, 19*(15). https://doi.org/10.3390/s19153401.

Received the editorial office: 27 February 2023

Accepted for publication: 16 March 2023

СЕРГЕЙ ВЛАДИМИРОВИЧ КАЛЯКИН,
Харьковский национальный университет внутренних дел,
кафедра противодействия киберпреступности;
ORCID: https://orcid.org/0000-0001-5435-5921,
e-mail: svkalyakin@ukr.net;

ЮРИЙ НИКОЛАЕВИЧ ОНИЩЕНКО,
кандидат наук по государственному управлению, доцент,
Харьковский национальный университет внутренних дел,
факультет № 4;
ORCID: https://orcid.org/0000-0002-7755-3071,
e-mail: onischenko1980@gmail.com;

ВИТАЛИЙ ВИКТОРОВИЧ НОСОВ,
кандидат технических наук, доцент,
Харьковский национальный университет внутренних дел,
кафедра противодействия киберпреступности;
ORCID: https://orcid.org/0000-0002-7848-6448,
e-mail: vitnos.g@gmail.com

КИБЕРБЕЗОПАСНОСТЬ ГОРОДСКОЙ ИНФРАСТРУКТУРЫ

Статья посвящена проблематике защиты городской критической инфраструктуры от киберугроз в современных непростых условиях. Исследован опыт других стран в сфере защиты критических объектов инфраструктуры. Рассмотрены особенности использования методик защиты инфраструктуры в условиях ведения гибридной войны. Даны рекомендации по повышению уровня защиты городской инфраструктуры от киберугроз.

Ключевые слова: *кибербезопасность, критическая городская инфраструктура, Интернет вещей (IoT), искусственный интеллект, блокчейн.*

SERHII VOLODYMYROVYCH KALIAKIN,
Kharkiv National University of Internal Affairs,
Department of Combating Cybercrime;
ORCID: https://orcid.org/0000-0001-5435-5921,
e-mail: svkalyakin@ukr.net;

YURII MYKOLAIOVYCH ONISHCHENKO,
Candidate of Law, Associate Professor,
Kharkiv National University of Internal Affairs,
Faculty No. 4;
ORCID: https://orcid.org/0000-0002-7755-3071,
e-mail: onischenko1980@gmail.com;

VITALII VICTOROVICH NOSOV,
Candidate of Technical Sciences, Associate Professor,
Kharkiv National University of Internal Affairs,
Department of Combating Cybercrime;
ORCID: https://orcid.org/0000-0002-7848-6448,
e-mail: vitnos.g@gmail.com

CYBERSECURITY OF THE MUNICIPAL INFRASTRUCTURE

A modern city is a complex system that requires a unified systematic approach to ensuring public safety, law and order and environmental safety in the face of high levels of both man-made and natural risks. Due to the growing role of information technology in the functioning of a modern city, the threat of cyberattacks on critical municipal infrastructure has increased. The cost of such cyber-attacks can be very high, both for individual victims and for society as a whole. Cyberattacks can lead to the theft of sensitive information, data destruction or the disclosure of personal

data. In addition, such attacks can lead to loss of working time and suspension of systems, which can have serious consequences for the city's viability.
The experience of other countries in protecting critical municipal infrastructure from cyber threats has been studied, analysed and summarised. The impact of the latest information technologies (such as the Internet of Things, artificial intelligence, blockchain) on the development of municipal infrastructure, the use of these technologies to protect critical infrastructure from cyberattacks, their advantages and disadvantages compared to classical security technologies have been considered. Particular attention has been paid to the problems of safe automation of modern city management processes such as automation of traffic control systems, environmental monitoring systems, financial systems, power grids, water and gas supply systems, communication systems, and control systems for wastewater treatment plants. The features of cyber attacks and the use of methods for protecting critical infrastructure in the context of hybrid warfare have been examined. Recommendations for a comprehensive increase in the level of protection of municipal critical infrastructure from cyber threats have been provided, taking into account the latest global trends in cybersecurity.

Key words: *cybersecurity, critical municipal infrastructure, Internet of Things (IoT), artificial intelligence, blockchain.*

Цитування (ДСТУ 8302:2015): Калякін С. В., Онищенко Ю. М., Носов В. В. Кібербезпека міської інфраструктури. *Право і безпека*. 2023. № 1 (88). С. 190–201. DOI: https://doi.org/10.32631/pb.2023.1.17.

Citation (APA): Kaliakin, S. V., Onishchenko, Yu. M., & Nosov, V. V. (2023). Cybersecurity of the municipal infrastructure. *Law and Safety, 1*(88), 190–201. https://doi.org/10.32631/pb.2023.1.17.