КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.21.156167
УДК 004.77

Машталяр Яна Русланівна
здобувач освіти спеціальності 125 Кібербезпека
кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID 0009-0004-9116-2538
yrpuzik.fitm22@kubg.edu.ua

Козачок Валерій Анатолійович
кандидат технічних наук, доцент
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0003-0072-2567
v.kozachok@kubg.edu.ua

Бржевська Зореслава Михайлівна
доктор філософії
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0002-7029-9525
z.brzhevska@kubg.edu.ua

Богданов Олександр Михайлович
доктор технічних наук, професор
професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID 0009-0005-2605-6189
o.bohdanov@kubg.edu.ua

Оксанич Ірина Миколаївна
кандидат технічних наук, с.н.с.
Інститут проблем математичних машин та систем НАН України, Київ, Україна
ORCID 0000-0002-1208-3427
inokc2018@gmail.com

Литвинов Валерій Андроникович
доктор технічних наук, професор
Інститут проблем математичних машин та систем НАН України, Київ, Україна
ORCID 0000-0001-5568-7629
litval@dr.com

ДОСЛІДЖЕННЯ РОЗВИТКУ ТА ІННОВАЦІЇ КІБЕРЗАХИСТУ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Об'єкти критичної інфраструктури — об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам. Віднесення об'єктів до критичної інфраструктури здійснюється в порядку, встановленому Кабінетом Міністрів України. Віднесення банків, інших об'єктів, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, платіжних організацій, учасників платіжних систем, операторів послуг платіжної інфраструктури здійснюється в порядку, встановленому Національним банком України. Віднесення об'єктів до критичної інфраструктури, що здійснюють діяльність на ринках послуг, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, здійснюється в порядку, встановленому такими державними органами. Зважаючи на значущість кібербезпеки в

сучасному світі, об'єкти критичної інфраструктури стають особливою мішенню для кіберзлочинців та кіберзагроз. Ці об'єкти включають енергетичні системи, транспорт, комунікаційні мережі, медичні установи та інші важливі сектори, які забезпечують необхідність функціонування суспільства. Ця стаття спрямована на аналіз та огляд сучасних підходів, що використовуються для забезпечення кібербезпеки на об'єктах критичної інфраструктури. Дослідження та впровадження новітніх стратегій та підходів у цій області може сприяти підвищенню рівня захисту важливих систем, а також виявленню та реагуванню на нові кіберзагрози, зберігаючи надійність та функціонування суспільства в цілому. Основні аспекти, які слід розглядати при розробці інноваційних підходів до захисту об'єктів критичної інфраструктури від кіберзагроз:

- прогностичний аналіз загроз: Розуміння потенційних кіберзагроз та їхніх впливів на об'єкти критичної інфраструктури. Виявлення нових векторів атак та вразливостей;
- розвиток та впровадження новітніх технологій: Використання штучного інтелекту, машинного навчання, блокчейну та інших інноваційних технологій у сфері кіберзахисту для запобігання атак та виявлення порушень безпеки;
- створення інтегрованих стратегій захисту, розробка гнучких та комплексних стратегій кіберзахисту, які враховують специфіку кожного сектору об'єктів критичної інфраструктури та його потреби;
- запровадження міжнародних стандартів та регулювань, співпраця на міжнародному рівні для встановлення єдиної системи стандартів та правил кіберзахисту для об'єктів критичної інфраструктури.

Кіберзахист постійно еволюціонує, враховуючи постійне зростання кількості та складності кіберзагроз. Для підвищення захищеності об'єктів критичної інфраструктури важливо розглянути низку сучасних технологічних тенденцій у кіберзахисті, а саме:

- штучний інтелект та машинне навчання;
- блокчейн та криптографія;
- Інтернет речей (IoT) та захист вбудованих систем;
- аналітика загроз та виявлення атак;
- автоматизовані засоби захисту;
- захист на рівні обробки даних.

Вивчення та впровадження цих технологічних тенденцій у секторі критичної інфраструктури дозволяє реагувати на складність сучасних кіберзагроз та забезпечує підвищення захищеності систем у реальному часі.

Ключові слова: об'єкт критичної інфраструктури; кібербезпека; шифрування даних; аутентифікація; управління доступом; аудит; соціальний інженірінг; фішинг.

ВСТУП

Об'єкти критичної інфраструктури — об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам.

Віднесення об'єктів до критичної інфраструктури здійснюється в порядку, встановленому Кабінетом Міністрів України [1].

Віднесення банків, інших об'єктів, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, платіжних організацій, учасників платіжних систем, операторів послуг платіжної інфраструктури здійснюється в порядку, встановленому Національним банком України [2].

Віднесення об'єктів до критичної інфраструктури, що здійснюють діяльність на ринках послуг, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, здійснюється в порядку, встановленому такими державними органами [3].

Віднесення об'єктів до критичної інфраструктури здійснюється за сукупністю критеріїв, що визначають їх соціальну, політичну, економічну, екологічну значущість для

забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, зокрема для реалізації життєво важливих функцій та надання життєво важливих послуг [3].

Захист критичної інфраструктури є складовою частиною забезпечення національної безпеки України [3].

Кіберзахист об'єкта критичної інфраструктури забезпечується шляхом впровадження на об'єкті критичної інформаційної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю [4].

Кіберзахист об'єкта критичної інфраструктури є складовою частиною робіт із створення та експлуатації об'єкта критичної інформаційної інфраструктури. Заходи з кіберзахисту передбачаються та впроваджуються на всіх стадіях життєвого циклу об'єкта критичної інформаційної інфраструктури [4].

Зважаючи на значущість кібербезпеки в сучасному світі, об'єкти критичної інфраструктури стають особливою мішенню для кіберзлочинців та кіберзагроз. Ці об'єкти включають енергетичні системи, транспорт, комунікаційні мережі, медичні установи та інші важливі сектори, які забезпечують необхідність функціонування суспільства.

Напади на критичну інфраструктуру можуть мати серйозні наслідки, зокрема призвести до перерв у постачанні послуг, втрати конфіденційності даних або навіть загрожувати життю людей. У зв'язку з постійним розвитком технологій та зростанням кількості кіберзагроз, захист критичної інфраструктури стає надзвичайно важливим завданням.

Дослідження методів підвищення кіберзахисту на об'єктах критичної інфраструктури стає запорукою розвитку стратегій та технологій, які спрямовані на запобігання та захист від кібератак.

Постановка проблеми. В наш час активно зростають загрози кібербезпеці об'єктам критичної інфраструктури та виникає потреба в інноваційних підходах до захису.

Об'єкти Критичної Інфраструктури (ОКІ) є ключовими компонентами суспільства, такими як енергетика, транспорт, медичні установи, телекомунікації тощо. Ці сектори є особливо вразливими перед кіберзагрозами через залежність суспільства від їхньої неперервної роботи.

Небезпека зловживання кібератаками на ОКІ постійно зростає через швидкі темпи цифровізації та підключення до мереж Інтернету. Технічні прогреси у кіберзлочинності стають все більш складними та виразними, і це вимагає надзвичайно інноваційних підходів до кіберзахисту.

Основні аспекти, які слід розглядати при розробці інноваційних підходів до захисту ОКІ від кіберзагроз:

- прогностичний аналіз загроз: Розуміння потенційних кіберзагроз та їхніх впливів на ОКІ. Виявлення нових векторів атак та вразливостей;
- розвиток та впровадження новітніх технологій: Використання штучного інтелекту, машинного навчання, блокчейну та інших інноваційних технологій у сфері кіберзахисту для запобігання атак та виявлення порушень безпеки;
- створення інтегрованих стратегій захисту, розробка гнучких та комплексних стратегій кіберзахисту, які враховують специфіку кожного сектору ОКІ та його потреби;
- запровадження міжнародних стандартів та регулювань, співпраця на міжнародному рівні для встановлення єдиної системи стандартів та правил кіберзахисту для ОКІ.

Аналіз останніх досліджень і публікацій. Проаналізуємо роботи у яких започатковано розв'язання даної проблеми.

В авторській колективній роботі [5] розглянута діяльність спрямована на зниження ризиків кібербезпеки і включає циклічний процес управління, що складається з п’яти функцій: ідентифікації ризиків, кіберзахисту, виявлення кіберінцидентів, реагування та відновлення стану кібербезпеки. Описано, як кожна функція сприяє ефективному управлінню ризиками та забезпечує надійність та безпеку об’єкта критичної інформації. Також в роботі запропоновані методи часткових показників ефективності.

В авторській колективній роботі [6] розглянуто моделі захисту критичної інформаційної інфраструктури, етапи і методи збору даних при виборі моделі захисту, розглянуті рівні забезпечення інформаційної інфраструктури та їх взаємодія, визначена структура моделювання процесу формування загроз та їх життєвий цикл. Автори статті зазначають, що безпека, базована на використанні формалізованих моделей, дозволяє уникнути помилок у розробці. Однак, вони також наголошують на необхідності періодичного перегляду моделей для максимальної адаптації до змін у завданнях та умовах, що виникають з часом.

В роботі [7] розроблені засади створення та функціонування центру кібербезпеки інформаційної інфраструктури об’єктів ядерної енергетики та його основні завдання.

Відсутність в українських наукових фахових виданнях обговорення результатів зарубіжних наукових досліджень, а також нормативно-правової бази з питань протидії кібертакам на об’єкти критичної інфраструктури є підставою для проведення власних досліджень.

Загалом, робота підкреслює комплексність проблеми захисту інформації та важливість поєднання традиційних та інноваційних підходів для ефективного управління інформаційною безпекою.

Мета статті. Мета статті полягає у аналізі та огляді інновацій та сучасних підходів, що використовуються для забезпечення кібербезпеки в контексті критичної інфраструктури.

Дослідження і впровадження новітніх стратегій та підходів у цій області може сприяти реагуванню на нові кіберзагрози, зберігаючи надійність та функціонування суспільства в цілому підвищенню рівня захисту важливих інформаційних систем.

РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

Технологічні тенденції у кіберзахисті

Кіберзахист постійно еволюціонує, враховуючи постійне зростання кількості та складності кіберзагроз. Для підвищення захищеності ОКІ важливо розглянути низку сучасних технологічних тенденцій у кіберзахисті, а саме:

- штучний інтелект та машинне Навчання: штучний інтелект та машинне навчання використовуються для аналізу величезних обсягів даних, що допомагає виявляти аномалії та прогнозувати потенційні загрози. Алгоритми навчаються розпізнавати відхилення від звичайної поведінки мережі та реагувати на них [8];
- аналіз біг даних та розпізнавання загроз: використання технологій аналізу великих обсягів даних допомагає в ідентифікації та розпізнаванні підозрілих паттернів у мережі, що можуть свідчити про потенційні загрози [9];
- блокчейн та криптографія: застосування технологій блокчейну та криптографії допомагає у створенні безпечних та непідробних систем збереження даних, а також у впровадженні безпечних методів ідентифікації та автентифікації [10];
- Інтернет речей (IoT) та захист вбудованих систем: ОКІ можуть використовувати безліч підключених до Інтернету пристроїв. Це потребує

розробки та впровадження надійних методів захисту вбудованих систем, щоб запобігти можливим кібератакам через ці пристрої [11];

- аналітика загроз та виявлення атак: використання спеціалізованих платформ для аналізу загроз дозволяє відстежувати, реагувати та виявляти атаки в реальному часі [12];
- автоматизовані засоби захисту: розвиток автоматизованих засобів захисту, які виявляють, аналізують та реагують на загрози без значного втручання людини, дозволяє забезпечити швидкий реакційний час та мінімізувати вплив кібератак [12];
- захист на рівні обробки даних: розвиток методів шифрування, механізмів захисту від утечок даних та контролю доступу до інформації на рівні обробки даних сприяє підвищенню загального рівня кіберзахисту [12].

Вивчення та впровадження цих технологічних тенденцій у секторі критичної інфраструктури дозволяє реагувати на складність сучасних кіберзагроз та забезпечує підвищення захищеності систем у реальному часі.

Шифрування та захист даних в кіберзахисті ОКІ.

Захист даних у сфері критичної інфраструктури стає дедалі важливішим, оскільки технології стають більш складними та загрози кібербезпеки зростають. Один з найважливіших методів захисту цих даних — шифрування.

Шифрування даних — це процес перетворення інформації у незрозумілу форму (шифр) з метою збереження конфіденційності та цілісності даних. В контексті критичної інфраструктури це означає застосування шифрування для захисту даних, що передаються по мережі та зберігаються на серверах та інших пристроях.

Використання шифрування даних у транспортних мережах, таких як застосування протоколів HTTPS для веб-трафіку, та використання шифрування даних на рівні файлів, папок та дисків допомагають у забезпеченні безпеки від зловмисних атак, включаючи перехоплення даних.

Додатково, шифрування може використовуватися для захисту даних від несанкціонованого доступу. Шифрування даних на підставному рівні важливо, оскільки воно надає додатковий шар захисту навіть у випадку, якщо зловмисник отримає фізичний доступ до обладнання чи файлів.

Шифрування також включає в себе застосування шифрувальних алгоритмів та ключів для забезпечення доступу тільки авторизованим користувачам. Використання сильних алгоритмів шифрування та безпечних ключів є важливими елементами для запобігання розшифруванню даних зловмисниками.

Застосування шифрування та захист даних важливі не лише для веб-переглядачів, але й для всіх пристроїв та систем у критичній інфраструктурі, що обробляють конфіденційну інформацію. Це включає сервери, мережеве обладнання, сховища даних, мобільні пристрої та багато іншого.

Шифрування та захист даних — це важливі складові кіберзахисту критичної інфраструктури, які сприяють у запобіганні витоку конфіденційної інформації та збереженні цілісності даних в умовах зростаючих кіберзагроз [13].

Управління ризиками та аналіз уразливостей в кібербезпеці

Управління ризиками та аналіз уразливостей є ключовими компонентами кібербезпеки, оскільки вони дозволяють ідентифікувати, оцінювати та зменшувати ризики та вразливості, які можуть призвести до кібератак та порушень безпеки. Ось детальний огляд цих процесів:

Управління ризиками:

- ідентифікація ризиків. Першим кроком управління ризиками є ідентифікація потенційних загроз та визначення можливих уразливостей у системах;
- оцінка ризиків. Після ідентифікації ризиків проводиться їх оцінка за ймовірністю та потенційним впливом на систему. Це допомагає визначити, які ризики потребують найбільшої уваги та заходів захисту;
- управління ризиками. Після оцінки ризиків визначаються стратегії зменшення чи управління ризиками. Це може включати уникнення ризиків, їх прийняття, зменшення, перенесення чи управління ризиками через захисні заходи;

Аналіз уразливостей:

- систематичний огляд систем. Аналіз уразливостей включає детальний огляд системи для виявлення потенційних уразливостей та слабких місць, що можуть стати точками входу для потенційних атак;
- визначення й категоризація уразливостей. Цей процес визначає, які системи, програми чи процеси мають уразливості, а також їхні можливі наслідки. Уразливості розглядаються за потенційним впливом на безпеку систем;
- план заходів з усунення уразливостей. Після виявлення уразливостей розробляються стратегії для виправлення та усунення цих проблем, щоб зменшити можливість експлуатації цих ділянок системи;
- перевірка та оновлення. По завершенні усунення уразливостей системи регулярно перевіряються та оновлюються, щоб упевнитися у їхній безпеці та відсутності нових уразливостей.

Управління ризиками та аналіз уразливостей є невід'ємною частиною стратегії кібербезпеки. Вони дозволяють вчасно виявляти та усувати потенційні проблеми, зменшуючи загрози та покращуючи загальний рівень захисту систем [14].

Управління доступом та аутентифікацією в кіберзахисті ОКІ

Управління доступом та аутентифікація грають критичну роль у забезпеченні безпеки ОКІ. Вони становлять важливі складові у проведенні контролю, хто має доступ до систем та даних, і як цей доступ здійснюється.

Управління доступом включає в себе створення та регулювання політик доступу до різних частин системи. Це означає встановлення правил та обмежень для користувачів, що мають доступ до певних даних та ресурсів. Важливо точно визначити рівні доступу та обмеження, щоб зменшити ризик витоку інформації чи несанкціонованого втручання.

Аутентифікація включає в себе перевірку та підтвердження ідентичності користувачів перед наданням доступу до системи. Сучасні методи аутентифікації використовують не лише паролі, але й біометричні дані, двофакторну аутентифікацію та мультифакторні методи для забезпечення безпеки.

Одним з методів управління доступом є **принцип найменших привілеїв (Least Privilege)**, що означає, що користувачеві надаються лише ті права, які необхідні для виконання його обов'язків. Це допомагає обмежити можливості зловмисників у разі компрометації облікових даних.

Технології одноразових паролів та біометричні методи, такі як сканування відбитків пальців чи розпізнавання обличчя, забезпечують високий рівень аутентифікації, оскільки вони ґрунтуються на унікальних фізичних характеристиках користувачів.

Ці методи сприяють ускладненню процесу несанкціонованого доступу до систем, проте їх ефективність вимагає постійного оновлення та вдосконалення. Наприклад,

застосування шифрування даних під час передачі та збереження, а також регулярне оновлення програмного забезпечення допомагають підвищити рівень безпеки.

Всі ці заходи спрямовані на забезпечення високого рівня захисту критичних систем та даних. Правильне управління доступом та ефективна аутентифікація є важливими компонентами для попередження несанкціонованого доступу та збереження інформації в безпеці [15].

Реагування та захист від DDOS-атак в ОКІ

Дистрибьовані атаки на відмову обслуговування (DDOS-атаки) представляють серйозну загрозу для критичних систем, оскільки вони можуть спричинити перебої в роботі та величезні фінансові збитки.

Реагування та захист від DDOS-атак вимагають ефективних стратегій та технічних рішень. Одним із ключових методів є розробка систем виявлення та миттєвої реакції на аномалії в мережі. Це дозволяє вчасно виявляти атаки та приймати заходи для їх локалізації.

Використання технологій, таких як «масштабне маршрутизоване вимкнення» (BGP blackholing) або «чистка трафіку» (traffic scrubbing), дозволяє розподілення шкідливого трафіку від легітимного, запобігаючи перебоям в роботі систем.

Паралельно із цим, важливо мати гнучкість в мережевих системах, щоб вони могли витримати значне збільшення трафіку в разі атаки та продовжувати надавати послуги без важливих перебоїв.

Планування та тренування персоналу стають важливими умовами для ефективного реагування на DDOS-атаки. Це включає у себе розробку планів дій у випадку атаки, тренування персоналу для швидкого реагування та вдосконалення засобів виявлення атак.

Багато компаній також використовують послуги сторонніх провайдерів безпеки, які спеціалізуються на мінімізації наслідків DDOS-атак. Ці провайдери можуть надавати сервіси захисту, які виявляють та фільтрують шкідливий трафік, що направляється на системи клієнта.

У підсумку, реагування та захист від DDOS-атак в критичній інфраструктурі потребує комплексного підходу, включаючи технічні заходи, планування, навчання персоналу та співпрацю зі спеціалізованими провайдерами безпеки [16].

Аудит та постійне вдосконалення кіберзахисту ОКІ.

Аудит та постійне вдосконалення кіберзахисту є ключовими процесами у забезпеченні ефективності та стійкості критичної інфраструктури перед кіберзагрозами.

Аудит включає в себе ретельний огляд систем, мереж та процедур, щоб виявити потенційні слабкі місця та вразливості. Це допомагає ідентифікувати можливі ризики та забезпечити прозорість стану кібербезпеки.

Постійне вдосконалення полягає в удосконаленні заходів безпеки на основі результатів аудиту та новітніх підходів до кіберзахисту. Це включає удосконалення процедур, оновлення технологій та впровадження нових стратегій з метою запобігання потенційним загрозам.

Ключовою частиною аудиту є оцінка поточних систем безпеки та їх відповідності стандартам безпеки, а також розробка планів для виправлення виявлених недоліків та вразливостей.

Постійне вдосконалення вимагає постійного оновлення знань персоналу та усвідомлення нових загроз. Це може включати проведення навчань, воркшопів та підвищення обізнаності персоналу зі стратегіями та технологіями кіберзахисту.

Важливою частиною цього процесу є також визначення ключових показників ефективності, які дозволяють оцінити успішність заходів кіберзахисту та ефективність планів вдосконалення.

У кінцевому результаті, аудит та постійне вдосконалення допомагають підтримувати високий рівень кібербезпеки в критичній інфраструктурі шляхом постійного аналізу, виявлення слабкі місця та удосконалення стратегій з метою попередження кіберзагроз [17].

ВИСНОВКИ

Стає очевидним, що кібербезпека вимагає постійного еволюційного підходу для ефективного протидії сучасним та майбутнім кіберзагрозам. Отримані результати наголошують на кількох ключових аспектах:

Постійне підвищення загроз. Сучасна кіберзагроза постійно зростає за своєю складністю та обсягом. Виявлення та протидія таким загрозам вимагає не тільки технічних інновацій, але й стратегічного перегляду підходів до кіберзахисту.

Інновації як ключовий фактор. Впровадження інновацій, таких як штучний інтелект, блокчейн та машинне навчання, має великий потенціал для підвищення ефективності заходів кіберзахисту. Розвиток та удосконалення таких технологій є важливим завданням для майбутнього.

Комплексний підхід та співпраця. Справжній успіх у кіберзахисті досягається лише через комплексний підхід, який враховує технічні, організаційні та людські аспекти. Співпраця між усіма сторонами, включаючи урядові органи, приватний сектор та громадянське суспільство, визначається як ключовий елемент успішної стратегії.

Свідомість та освіта. Освіта та навчання в галузі кібербезпеки мають вирішальне значення. Збільшення рівня свідомості та навичок у сфері кіберзахисту серед всіх працівників, від технічних експертів до керівного персоналу, сприятиме загальному підвищенню рівня кібербезпеки.

Узагальнюючи, лише поглиблений аналіз, постійне вдосконалення технологій та взаємодія всіх сторін можуть забезпечити ефективний та стійкий кіберзахист об’єктів критичної інфраструктури в умовах сучасної кіберзагрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 «Деякі питання об’єктів критичної інформаційної інфраструктури», Постанова Кабінету Міністрів України № 943 (2020) (Україна).
2 «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об’єктів критичної інфраструктури в банківській системі України», Постанова Правління Національного банку України № 178 (2022) (Україна).
3 «Про критичну інфраструктуру» Закон України № 1882-IX (2021) (Україна).
4 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» Постанова Кабінету Міністрів України № 518 (2019) (Україна).
5 Хлапонінб, Ю., Козубцова, Л., Козубцов, І., & Штонда, Р. (2022). Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури. *Кібербезпека: освіта, наука, техніка, 3(15)*, 124–134.
6 Кожедуб, Ю., Василенко, С., Максимець, А., & Гирда, В. (2021). Концептуальна модель захисту інформації об’єктів критичної Інформаційної інфраструктури України. Information Technology and Security, 9(2(17)), 151–164.
7 Гулак, Г,. Скітер, І., & Гулак, Є. (2021). Методологічні засади створення та функціонування центру кібербезпеки інформаційної інфраструктури об’єктів ядерної енергетики. *Кібербезпека: освіта, наука, техніка, 4(12)*, 172–186.

8 Бигаса, Ю., Бєлов, Д., & Заборовський, В. (2023). Штучний інтелект та авторські і суміжні права. *Науковий вісник Ужгородського Національного університету*. https://doi.org/10.24144/2307-3322.2022.76.2.47

9 Кагарлицький, Р. (2023). Біометрична автентифікація користувача смартфона за допомогою даних акселерометра. https://ela.kpi.ua/bitstream/123456789/60442/1/Kaharlytskyi_bakalavr.pdf

10 Поліщук, В. (2023). Аналіз технології блокчейн у сфері кібербезпеки та захисту інформації. https://openarchive.nure.ua/items/388e8be9-5443-46e2-bcd1-a381751127e4

11 Журило, О., Ляшенко, О., & Аветісова, К. (2023). Огляд рішень з апаратної безпеки кінцевих пристроїв туманних обчислень у Інтернеті речей. *Сучасний стан наукових досліджень та технологій в промисловості, 1(23)*, 57–71. https://doi.org/10.30837/ITSSI.2023.23.057

12 Загорняк, В. (2023). Дослідження механізмів захисту від соціально-інженерних атак та розробка методів їх виявлення. https://elartu.tntu.edu.ua/bitstream/lib/41860/2/Dyplom_Zahornyak_V_Y_2023.pdf

13 Давидюк, А. (2023). Система обміну знаннями та досвідом між фахівцями з кібербезпеки критичної інфраструктури. *Науково-практична конференція «Кібербезпека енергетики». Матеріали,* 67–73. https://www.researchgate.net/profile/Andrii_Davydiuk/publication/372401612_Sistema_obminu_znannami_ta_dosvidom_miz_fahivcami_z_kiberbezpeki_kriticnoi_infrastrukturi/links/64b4604dc41fb852dd7b7020/Sistema-obminu-znannami-ta-dosvidom-miz-fahivcami-z-kiberbezpeki-kriticnoi-infrastrukturi.pdf#page=6

14 Гнатюк, С., Бердибаєв, Р., Сидоренко, В., Жигаревич, О., & Смірнова, Т. (2023). Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури. *Кібербезпека: освіта, наука, техніка, 3(19),* 176–196.

15 Kozubtsova, L., et al. (2022). Performance indicators of the functioning of the information security system and cybersecurity of critical information infrastructure objects. *Computer-integrated technologies: education, science, production, 48*, 64–69. https://doi.org/10.36910/6775-2524-0560-2022-48-10

16 Лиштва, Є. (2023). Захист мультимедійної мережі від DDoS-атак на основі технології DPI. https://dspace.nau.edu.ua/bitstream/NAU/60197/1/%d0%a4%d0%90%d0%95%d0%a2_172_2023_%d0%b4%d0%b8%d0%bf%d0%bb%d0%be%d0%bc_%d0%9b%d0%b8%d1%88%d1%82%d0%b2%d0%b0%20%d0%84.%d0%ae..pdf

17 Мельник, Д., (2022). Захист національної критичної інформаційної інфраструктур: актуальні проблеми та шляхи їх вирішення. *Адміністративне право і процес, 3(38),* 5–16. https://doi.org/10.17721/2227-796X.2022.3.01

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023

Yana Mashtaliar
student
Department of Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0009-0004-9116-2538
yrpuzik.fitm22@kubg.edu.ua

Valerii Kozachok
PhD, associate professor
Associate Professor of the Department of Information and Cyber
Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0003-0072-2567
v.kozachok@kubg.edu.ua

Zoreslava M. Brzhevska
PhD
Associate Professor of the Department of Information and Cyber
Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0002-7029-9525
z.brzhevska@kubg.edu.ua

Oleksandr Bohdanov
Doctor of Science, Professor
Professor of the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0009-0005-2605-6189
o.bohdanov@kubg.edu.ua

Iryna Oksanych
PhD of Technical Sciences, Senior Researcher
Institute of Problems of Mathematical Machines and Systems of NAS of Ukraine, Kyiv, Ukraine
ORCID 0000-0002-1208-3427
inokc2018@gmail.com

Valerii Lytvynov
Doctor of Technical Sciences, Professor
Institute of Problems of Mathematical Machines and Systems of NAS of Ukraine, Kyiv, Ukraine
ORCID 0000-0001-5568-7629
litval@dr.com

RESEARCH OF DEVELOPMENT AND INNOVATION OF CYBER PROTECTION AT CRITICAL INFRASTRUCTURE FACILITIES

Abstract. Critical infrastructure objects — infrastructure objects, systems, their parts and their totality, which are important for the economy, national security and defense, the malfunctioning of which can harm vital national interests. Classification of objects as critical infrastructure is carried out in accordance with the procedure established by the Cabinet of Ministers of Ukraine. The assignment of banks, other entities operating in the financial services markets, state regulation and supervision of the activities of which is carried out by the National Bank of Ukraine, payment organizations, participants of payment systems, operators of payment infrastructure services is carried out in accordance with the procedure established by the National Bank of Ukraine. Classification of objects to critical infrastructure, which carry out activities on the service markets, state regulation and supervision of the activities of which are carried out by state bodies, is carried out in accordance with the procedure established by such state bodies. Given the importance of cyber security in today's world, critical infrastructure objects are becoming a special target for cyber criminals and cyber threats. These facilities include energy systems, transportation, communication networks, medical facilities and other important sectors

that ensure the necessary functioning of society. This article aims to analyze and review modern approaches used to ensure cyber security at critical infrastructure facilities. Research and implementation of the latest strategies and approaches in this area can help increase the level of protection of important systems, as well as detect and respond to new cyber threats, maintaining the reliability and functioning of society as a whole. The main aspects that should be considered when developing innovative approaches to protecting critical infrastructure objects from cyber threats:

- predictive threat analysis: Understanding potential cyber threats and their impact on critical infrastructure facilities. Detection of new attack vectors and vulnerabilities;
- development and implementation of the latest technologies: Use of artificial intelligence, machine learning, blockchain and other innovative technologies in the field of cyber defense to prevent attacks and detect security breaches;
- creation of integrated protection strategies, development of flexible and comprehensive cyber protection strategies that take into account the specifics of each sector of critical infrastructure objects and its needs;
- introduction of international standards and regulations, cooperation at the international level to establish a unified system of cyber protection standards and rules for critical infrastructure facilities.

Cyber defense is constantly evolving, given the constant growth in the number and complexity of cyber threats. To increase the security of critical infrastructure facilities, it is important to consider a number of modern technological trends in cyber protection, namely:

- artificial intelligence and machine learning;
- blockchain and cryptography;
- Internet of Things (IoT) and protection of embedded systems;
- threat analytics and attack detection;
- automated means of protection;
- protection at the level of data processing.

The study and implementation of these technological trends in the critical infrastructure sector allows to respond to the complexity of modern cyber threats and provides an increase in the security of systems in real time.

Keywords: object of critical infrastructure; cyber security; data encryption; authentication; access management; audit; social engineering; phishing.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Some issues of objects of critical information infrastructure, Resolution of the Cabinet of Ministers of Ukraine № 943 (2020) (Ukraine).
2 On the approval of the Regulation on the organization of cyber protection in the banking system of Ukraine and amendments to the Regulation on the identification of critical infrastructure objects in the banking system of Ukraine, Resolution of the Board of the National Bank of Ukraine № 178 (2022) (Ukraine).
3 On critical infrastructure, Law of Ukraine № 1882-IX (2021) (Ukraine).
4 Resolution of the Cabinet of Ministers of Ukraine on the approval of General requirements for cyber protection of critical infrastructure facilities № 518 (2019) (Ukraine).
5 Khlaponin, Yu., Kozubtsova, L., Kozubtsov, I., & Shtonda, R. (2022). Functions of the information protection system and cyber security of critical information infrastructure. *Cybersecurity: education, science, technology, 3(15)*, 124–134.
6 Kozhedub, Yu., Vasylenko, S., Maksimets, A., & Girda, V. (2021). Conceptual model of information protection of objects of critical Information infrastructure of Ukraine. *Information Technology and Security, 9(2(17))*, 151–164.
7 Gulak, G,. Skeeter, I., & Gulak, E. (2021). Methodological principles of the creation and functioning of the cyber security center of the information infrastructure of nuclear energy facilities. *Cybersecurity: education, science, technology, 4(12)*, 172–186.
8 Bygasa, Yu., Belov, D., & Zaborovskyi, V. (2023). Artificial intelligence and copyright and related rights. *Scientific Bulletin of the Uzhhorod National University*. https://doi.org/10.24144/2307-3322.2022.76.2.47
9 Kagarlytskyi, R. (2023). Biometric authentication of a smartphone user using accelerometer data. https://ela.kpi.ua/bitstream/123456789/60442/1/Kaharlytskyi_bakalavr.pdf

10 Polishchuk, V. (2023). Analysis of blockchain technology in the field of cyber security and information protection. https://openarchive.nure.ua/items/388e8be9-5443-46e2-bcd1-a381751127e4

11 Zhurylo, O., Lyashenko, O., & Avetisova, K. (2023). An Overview of End-Device Hardware Security Solutions for Fog Computing in the Internet of Things. *The current state of scientific research and technology in industry, 1(23),* 57–71. https://doi.org/10.30837/ITSSI.2023.23.057

12 Zagornyak, V. (2023). Research of mechanisms of protection against social engineering attacks and development of methods of their detection. https://elartu.tntu.edu.ua/bitstream/lib/41860/2/Dyplom_Zahornyak_V_Y_2023.pdf

13 Davidyuk, A. (2023). System of exchange of knowledge and experience between specialists in cyber security of critical infrastructure. *Scientific and practical conference "Cyber security of energy". Materials,* 67–73. https://www.researchgate.net/profile/Andrii_Davydiuk/publication/372401612_Sistema_obminu_znannami_ta_dosvidom_miz_fahivcami_z_kiberbezpeki_kriticnoi_infrastrukturi/links/64b4604dc41fb852dd7b7020/Sistema-obminu-znannami-ta-dosvidom-miz-fahivcami-z-kiberbezpeki-kriticnoi-infrastrukturi.pdf#page=6

14 Hnatiuk, S., Berdybaev, R., Sydorenko, V., Zhigarevich, O., & Smirnova, T. (2023). A system for correlating events and managing cyber security incidents at critical infrastructure facilities. *Cybersecurity: education, science, technology, 3(19),* 176–196.

15 Kozubtsova, L., et al. (2022). Performance indicators of the functioning of the information security system and cybersecurity of critical information infrastructure objects. *Computer-integrated technologies: education, science, production, 48*, 64–69. https://doi.org/10.36910/6775-2524-0560-2022-48-10

16 Lishtva, E. (2023). Protection of a multimedia network against DDoS attacks based on DPI technology. https://dspace.nau.edu.ua/bitstream/NAU/60197/1/%d0%a4%d0%90%d0%95%d0%a2_172_2023_%d0%b4%d0%b8%d0%bf%d0%bb%d0%be%d0%bc_%d0%9b%d0%b8%d1%88%d1%82%d0%b2%d0%b0%20%d0%84.%d0%ae..pdf

17 Melnyk, D., (2022). Protection of national critical information infrastructure: current problems and ways to solve them. *Administrative law and process, 3(38),* 5–16. https://doi.org/10.17721/2227-796X.2022.3.01