КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1047
УДК 004.738:004.056

Остапчук Вадим Русланович
магістр,
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0009-0002-2952-9189
vrostapchuk.fitm24m@kubg.edu.ua

Осадча Вікторія Вячеславівна
студентка
Свєнтокшиська політехніка, Кельце, Польща
ORCID: 0009-0001-6180-8172
vikosa2007@gmail.com

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

Стрельніков Віталій Ігорович
PhD, доцент кафедри інформаційної та кібернетчної безпеки ім. професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0003-3439-3220
v.strelnikov@kubg.edu.ua

Бодненко Дмитро Миколайович
кандидат педагогічних наук, доцент,
доцент кафедри математики та фізики
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID 0000-0001-9303-6587
d.bodnenko@kubg.edu.ua

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ НА ОБ’ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. У статті досліджується проблема забезпечення інформаційної безпеки автоматизованих систем управління на об'єктах критичної інфраструктури України в умовах зростання кіберзагроз на 87% у світі та 48% в Україні протягом 2024 року. Проаналізовано теоретичні та нормативно-правові основи захисту критичної інфраструктури, класифікацію об'єктів та сучасні тенденції кіберзагроз. Досліджено вітчизняне й міжнародне законодавство у сфері кібербезпеки. Висвітлено порядок створення комплексної системи захисту інформації відповідно до стандартів ISO. Проаналізовано міжнародний досвід США та країн ЄС щодо забезпечення безпеки критичних систем. Розроблено алгоритм визначення актуальності загроз та методику підвищення рівня інформаційної безпеки на основі п'яти функцій: ідентифікація, захист, виявлення, реагування та відновлення. Проведено аналіз SCADA-системи енергетичного підприємства ТОВ "ЕнергоСистема", що управляє трансформаторними підстанціями потужністю 180 МВА. Виявлено критичні вразливості: відсутність сегментації мереж, незашифровані протоколи Modbus TCP/IP та IEC 60870-5-104, слабка автентифікація. Оцінка ризиків за методологією NIST SP 800-82 підтвердила один критичний та чотири високих ризики. Розроблено дев'ять напрямків рекомендацій: сегментація мереж, криптографічний захист каналів зв'язку, двофакторна автентифікація, системи виявлення вторгнень та SIEM-моніторинг, управління оновленнями, автоматизація резервного копіювання, навчання персоналу, розробка політики безпеки, посилення фізичного захисту. Обґрунтовано економічну доцільність інвестицій 4-6 мільйонів гривень, оскільки одна доба простою призводить до втрат понад 50 мільйонів гривень. Результати

мають практичне застосування для підприємств енергетичної, транспортної та оборонної галузей.

Ключові слова: інформаційна безпека; автоматизована система управління; критична інфраструктура; SCADA-системи; кіберзагроза; оцінка ризиків; сегментація мереж; промислові протоколи.

ВСТУП

Постановка проблеми. Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням кіберзагроз для об'єктів критичної інфраструктури, що становить серйозний виклик для національної безпеки України. Автоматизовані системи управління технологічними процесами на енергетичних, транспортних, телекомунікаційних та оборонних об'єктах стають основною мішенню для кібератак, які можуть призвести до катастрофічних наслідків – від масових відключень електроенергії до загрози життю населення. За даними Global Threat Landscape Report 2025, кількість кібератак на критичну інфраструктуру зросла на 87% порівняно з попереднім роком, а в Україні інтенсивність атак збільшилась на 48% [1]. Особливу небезпеку становлять цільові атаки на SCADA-системи та автоматизовані системи управління, які безпосередньо керують технологічними процесами. Досвід кібератак BlackEnergy у 2015 році [2] та Industroyer у 2016 році на українську енергетичну інфраструктуру наочно продемонстрував реальність загроз і критичні наслідки успішних атак на системи управління об'єктами критичної інфраструктури [3]. У зв'язку з цим актуальність дослідження методів і засобів забезпечення інформаційної безпеки автоматизованих систем управління на об'єктах критичної інфраструктури не викликає сумнівів і є важливим науковим та практичним завданням для забезпечення національної безпеки держави.

Аналіз останніх досліджень і публікацій. Проблематика захисту критичної інфраструктури та автоматизованих систем управління знайшла відображення в роботах багатьох вітчизних і зарубіжних дослідників. Теоретичні основи інформаційної безпеки промислових систем розглянуто у працях Бурячка В. П., Складанного П. М., які досліджували архітектуру та вразливості автоматизованих систем управління технологічними процесами [4]. Також дсліджувався розвиток та інновації кіберзахисту [5] та був проведений аналіз технологій розслідування інцидентів безпеки на об'єктах критичної інфраструктури [6].

Міжнародні аспекти захисту критичної інфраструктури висвітлені в стандартах IEC 62443 [7], ISO/IEC 27001 [8] та методологічних документах NIST SP 800-82 [9], які визначають комплексний підхід до управління ризиками інформаційної безпеки. Нормативно-правове регулювання захисту критичної інфраструктури в Україні базується на Законі України "Про критичну інфраструктуру" [10], Доктрині інформаційної безпеки України та інших нормативних актах [11], проте залишається фрагментарним і потребує вдосконалення.

Дослідження сучасних кіберзагроз для SCADA-систем представлені у звітах компанії Positive Technologies [12], яка виявила, що кожну п'яту вразливість в АСУ ТП усувають більше місяця, а для 35% вразливостей існують публічно доступні експлойти.

Аналіз історичних кібератак на промислові системи, зокрема Stuxnet, BlackEnergy та Industroyer, продемонстрував еволюцію методів атак і необхідність посилення захисту промислових протоколів зв'язку. CERT-UA регулярно публікує інформацію про кіберінциденти в Україні, що дозволяє відстежувати актуальні загрози для критичної

інфраструктури. Оцінювання рівня інформаційних ризиків здійснюється за допомогою поетапного аналізу активів, загроз та вразливостей (рис. 1) [13].

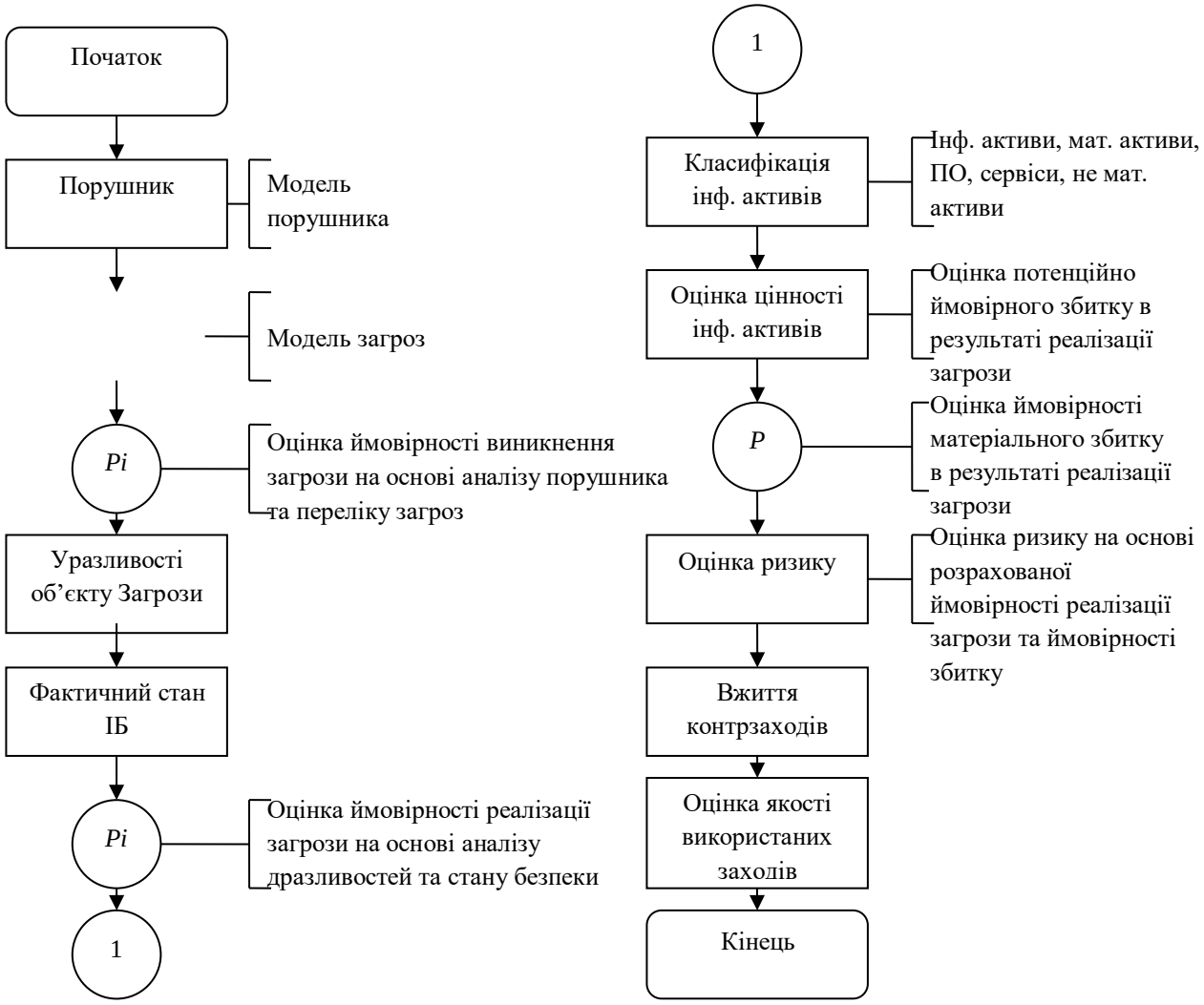

Рис. 1. Структурна схема оцінювання інформаційних ризиків на критично важливих об'єктах

Методологічні підходи до оцінки ризиків інформаційної безпеки АСУ ТП досліджені в роботах, де запропоновані моделі процесу захисту інформації та алгоритми визначення актуальності загроз. Міжнародний досвід побудови систем захисту критичної інфраструктури проаналізовано в документах, що описують підходи США [14] та країн ЄС [15].

Попри значну кількість досліджень, раніше невирішеними залишаються питання адаптації міжнародних стандартів і методологій до специфіки українських об'єктів критичної інфраструктури, розробки практичних рекомендацій щодо захисту SCADA-систем енергетичних підприємств з урахуванням обмежених ресурсів та особливостей архітектури застарілих систем, а також створення комплексної методики оцінки ризиків, яка враховує як технологічні наслідки кібератак, так і їх вплив на національну безпеку в умовах гібридної війни.

Мета статті. Розроблення комплексу практичних рекомендацій щодо забезпечення інформаційної безпеки автоматизованих систем управління на об'єктах критичної інфраструктури на основі аналізу сучасних кіберзагроз, оцінки ризиків та адаптації міжнародних стандартів до специфіки українських енергетичних підприємств.

Для досягнення поставленої мети визначено такі завдання:

1. Проаналізувати теоретичні основи та нормативно-правове регулювання захисту об'єктів критичної інфраструктури в Україні та світі.
2. Дослідити міжнародний досвід побудови систем кіберзахисту критичних інформаційних систем у США, країнах ЄС та розробити алгоритм визначення актуальних загроз безпеці інформації.
3. Розробити методику підвищення рівня інформаційної безпеки автоматизованих систем управління на основі міжнародних стандартів IEC 62443, ISO/IEC 27001 та NIST Cybersecurity Framework.
4. Провести детальний аналіз SCADA-системи енергетичного об'єкта критичної інфраструктури, виявити критичні вразливості та здійснити оцінку ризиків за методологією NIST SP 800-82.
5. Сформулювати комплекс технічних, організаційних та процедурних рекомендацій для підвищення захищеності SCADA-систем з урахуванням економічної доцільності та поетапності впровадження заходів захисту.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

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 [10].

Автоматизовані системи управління (АСУ) – електронні системи, через які інформація, суттєва для ефективних дій військових угруповань, основних формувань, тактичних формувань, військових частин, кораблів, військових підрозділів або зброї, що перебувають під командуванням, вводиться, обробляється та передається [16].

Інформаційна безпека визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через неповноту, невчасність та невірогідність інформації, негативний інформаційний вплив, негативні наслідки застосування інформаційних технологій, несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. Для АСУ критичними є три основні властивості інформації: доступність (можливість отримання інформації у потрібний час), цілісність (відсутність несанкціонованих змін), конфіденційність (захист від несанкціонованого доступу).

Система управління інформаційною безпекою (СУІБ) – ряд процесів і процедур, призначених для управління прийнятними рівнями ризиків, пов’язаних з інформаційною безпекою [17]. Управління інформаційною безпекою критично важливого об’єкта здійснюється відповідно до циклу PDCA (Plan-Do-Check-Act), що передбачає планування, впровадження, перевірку та вдосконалення заходів безпеки (рис. 2).

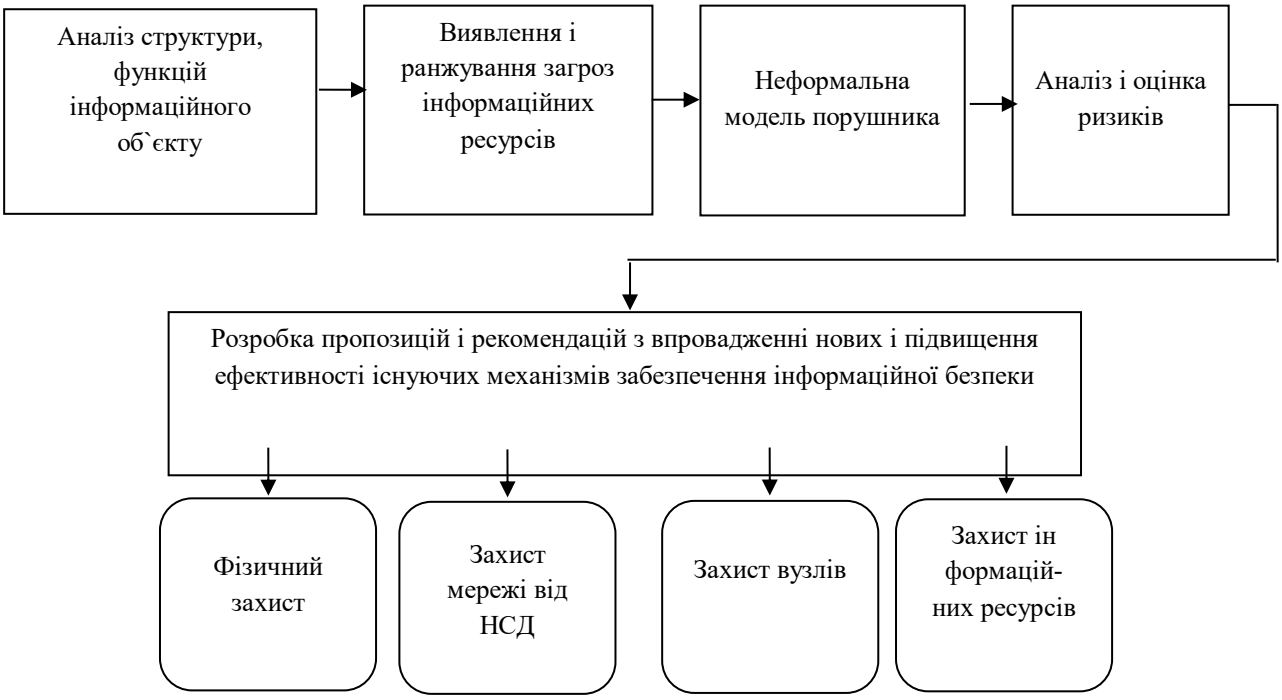

Рис. 2. Сценарій управління інформаційною безпекою критично важливого об'єкта

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У цьому розділі подано науково обґрунтовані результати оцінки інформаційної безпеки автоматизованих систем управління на об'єктах критичної інфраструктури, розроблені на основі проведеного аналізу нормативної бази, міжнародних стандартів, сучасних кіберзагроз і практичного дослідження SCADA-системи енергетичного підприємства. Отримані результати формують комплексний підхід до підвищення рівня захищеності критичних технологічних процесів, враховуючи технічні, організаційні та економічні аспекти.

1. Результати аналізу архітектури та поточного стану безпеки SCADA-системи. Дослідження SCADA-системи ТОВ «ЕнергоСистема» виявило, що її архітектура побудована за принципом централізованого управління трансформаторними підстанціями потужністю 180 МВА. Аналіз мережевої топології показав відсутність сегментації між офісною та технологічною мережами, що створює умови для горизонтального переміщення зловмисника у разі компрометації користувацьких робочих станцій. Значна частина трафіку передається із використанням незашифрованих протоколів Modbus TCP/IP та IEC 60870-5-104, що робить можливим перехоплення та модифікацію керуючих команд. Механізми автентифікації у системі залишаються недостатньо стійкими, що створює додаткові передумови для несанкціонованого доступу до елементів управління.

Проведений аналіз дозволив визначити найбільш критичні вразливості SCADA-інфраструктури, серед яких технологічна залежність від застарілого програмного забезпечення, відсутність централізованого журналювання подій, неповний контроль за оновленнями програмно-апаратних компонентів та низький рівень підготовки персоналу щодо реагування на інциденти. Сукупність цих факторів створює високий

рівень експлуатаційної вразливості системи та підвищує ймовірність реалізації цілеспрямованих атак.

2. Результати оцінки ризиків інформаційної безпеки за методологією NIST SP 800-82. Оцінювання ризиків проводилося відповідно до методології NIST SP 800-82 [9], що дозволило ідентифікувати потенційні загрози, визначити їх ймовірність, наслідки та сформулювати загальний рівень ризику *(*табл.1).

Таблиця 1

Оцінка інформаційних ризиків SCADA-системи

№	Загроза	Ймовірність	Вплив	Рівень ризику
1	Зовнішня кібератака через незахищене з'єднання мереж (тип BlackEnergy)	Висока	Критичний	Критичний
2	Перехоплення та підміна команд управління через незашифровані протоколи	Середня	Критичний	Високий
3	Несанкціонований доступ через компрометацію паролів	Середня	Високий	Високий
4	DoS-атака на SCADA-сервери з метою порушення управління	Середня	Високий	Високий
5	Експлуатація невиправлених вразливостей операційних систем	Середня	Високий	Високий
6	Успішний фішинг персоналу з подальшим проникненням в систему	Середня	Середній	Середній
7	Внесення шкідливого програмного забезпечення через USB-носії	Низька	Високий	Середній

У ході аналізу встановлено, що найбільшу небезпеку становлять кібератаки, спрямовані на порушення доступності та цілісності технологічних процесів. Для SCADA-системи визначено один критичний ризик, пов’язаний із відсутністю сегментації мереж і можливістю зовнішнього втручання у канали керування, та чотири високі ризики, пов’язані з використанням незахищених протоколів, слабкою автентифікацією, низьким рівнем контролю оновлень та відсутністю комплексного моніторингу подій безпеки.

Результати розрахунків продемонстрували, що реалізація навіть одного з високих ризиків може спричинити значне порушення роботи підприємства, а критичний ризик здатний привести до повної зупинки технологічного процесу. Наслідки таких подій мають потенціал створення аварійного стану системи, тривалих відключень електропостачання та значних економічних збитків.

3. Розроблення методики підвищення рівня інформаційної безпеки автоматизованої системи управління. На основі аналізу міжнародних стандартів ISO/IEC 27001, IEC 62443 та NIST Cybersecurity Framework [7, 8, 9] створено методику підвищення рівня інформаційної безпеки, яка ґрунтується на п’яти ключових функціях: ідентифікації, захисту, виявлення, реагування та відновлення.

Запропонована методика адаптована до особливостей українських енергетичних підприємств, зокрема до використання застарілих систем, обмеженого фінансування та складнощів модернізації технологічного обладнання.

Ідентифікація передбачає визначення критичних активів, актуальних загроз, можливих сценаріїв атак і слабких місць системи. Етап захисту включає формування вимог до криптографічного захисту каналів зв’язку, упровадження двофакторної автентифікації та засобів контролю мережевого доступу. Функція виявлення передбачає упровадження IDS/IPS та SIEM-систем, здатних оперативно фіксувати аномалії та інциденти. Реагування спрямоване на розроблення процедур обмеження впливу атаки, а

відновлення передбачає створення резервних копій, підтримку працездатності системи та швидке повернення до штатного режиму роботи.

4. Формування комплексу рекомендацій щодо підвищення кіберзахисту SCADA-системи. На основі проведеного аналізу розроблено науково обґрунтований комплекс рекомендацій із дев'яти напрямів, спрямованих на зниження рівня ризиків та підвищення стійкості SCADA-інфраструктури. Запропоновані заходи охоплюють сегментацію мереж, упровадження криптографічного захисту каналів зв'язку, модернізацію систем автентифікації, створення багаторівневого моніторингу подій, автоматизацію резервного копіювання, розроблення політик безпеки та підвищення кваліфікації персоналу. Кожен із напрямів дозволяє зменшити ризики відповідно до методології NIST SP 800-82 та підвищити загальну надійність критичних систем.

Особливу увагу приділено економічній складовій упровадження заходів захисту. Проведене обґрунтування засвідчує, що інвестиції в межах 4-6 млн грн є повністю виправданими, оскільки один день простою підприємства може спричинити збитки понад 50 млн грн. Таким чином, рекомендовані заходи забезпечують не лише підвищення рівня кіберзахисту, але й значну економічну ефективність.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного дослідження здійснено комплексний аналіз інформаційної безпеки автоматизованих систем управління на об'єктах критичної інфраструктури України та розроблено науково обґрунтовані рекомендації щодо підвищення їх захищеності.

Аналіз SCADA-системи енергетичного підприємства ТОВ "ЕнергоСистема" (180 МВА, 45 тисяч споживачів) виявив сім критичних вразливостей. Оцінка ризиків за методологією NIST SP 800-82 підтвердила наявність одного критичного та чотирьох високих ризиків для безперервності функціонування об'єкта. Розроблена методика підвищення безпеки базується на п'яти функціях (ідентифікація, захист, виявлення, реагування, відновлення) та дев'яти напрямках практичних рекомендацій: сегментація мереж, криптографічний захист каналів зв'язку, двофакторна автентифікація, системи виявлення вторгнень, SIEM-моніторинг, управління оновленнями, автоматизація резервного копіювання, навчання персоналу та розробка політики безпеки.

Економічне обґрунтування довело доцільність інвестицій: впровадження заходів потребує 4-6 мільйонів гривень, тоді як одна доба простою призводить до втрат понад 50 мільйонів гривень. Запропонований поетапний підхід (0-3, 4-6, 7-12 місяців) дозволяє оптимізувати ресурси та мінімізувати ризики під час модернізації. Результати мають практичне значення для підприємств енергетичної, транспортної та оборонної галузей України.

Перспективи подальших досліджень:

- Розробка адаптивних моделей прогнозування кіберзагроз для об'єктів критичної інфраструктури з урахуванням специфіки гібридної війни та геополітичної ситуації в Україні.
- Впровадження технологій штучного інтелекту та машинного навчання для раннього виявлення аномалій у SCADA-системах та автоматизації процесів реагування на інциденти.
- Створення інтегрованих платформ управління ризиками кібербезпеки, які поєднують технічні засоби моніторингу з організаційними процедурами та дозволяють здійснювати комплексну оцінку стану захищеності в режимі реального часу.

- Дослідження методів забезпечення кіберстійкості застарілих промислових систем управління, для яких неможливе оновлення програмного забезпечення через обмеження виробників або відсутність технічної підтримки.
- Розробка галузевих профілів захищеності для різних типів об'єктів критичної інфраструктури (енергетика, транспорт, водопостачання) з урахуванням специфіки технологічних процесів та архітектури систем управління.

Таким чином, результати дослідження формують науково-практичну основу для підвищення стійкості автоматизованих систем управління на об'єктах критичної інфраструктури України до сучасних кіберзагроз та забезпечення національної безпеки держави в інформаційній сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Fortinet. (2025). *Global threat landscape report 2025*. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report-2025.pdf
2. Cybersecurity and Infrastructure Security Agency. (n.d.). *Cyber-attack against Ukrainian critical infrastructure*. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01
3. SecurityWeek. (n.d.). *Industroyer ICS malware linked to Ukraine power grid attack*. https://www.securityweek.com/industroyer-ics-malware-linked-ukraine-power-grid-attack/
4. Kozachok, V. A., Kyrychok, R. V., Skladannyi, P. M., Buriachok, V. L., & Hulak, H. M. (2016). Problems of ensuring security control of corporate networks and ways to solve them. *Scientific Notes of the Ukrainian Research Institute of Communications, 3*(43), 48–61.
5. Mashtaliar, Ya. R., Kozachok, V. A., Brzhevska, Z. M., & Bohdanov, O. M. (2023). Research on the development and innovations of cybersecurity at critical infrastructure facilities. *Cybersecurity: Education, Science, Technique, 2*(22), 156–167.
6. Kozachok, V. A., & Drapatyi, M. V. (2024). Analysis of security incident investigation technologies at critical infrastructure facilities. *Cybersecurity: Education, Science, Technique*, *2*(26), 374–391.
7. International Electrotechnical Commission. (n.d.). *IEC 62443: Security for industrial automation and control systems*. https://tk185.appau.org.ua/downloads/IEC_62443_2_1_ukr_draft.pdf
8. International Organization for Standardization. (n.d.). *ISO/IEC 27001: Information security management systems—Requirements*. https://www.iso.org/standard/27001
9. National Institute of Standards and Technology. (2015). *Guide to industrial control systems (ICS) security (NIST SP 800-82 Rev. 2)*. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf
10. Verkhovna Rada of Ukraine. (2006). *Law of Ukraine "On critical infrastructure"*. https://zakon.rada.gov.ua/laws/show/1882-20#Text
11. Verkhovna Rada of Ukraine. (2017). *Doctrine of information security of Ukraine*. https://zakon.rada.gov.ua/laws/show/47/2017#Text
12. Positive Technologies. (2019). *ICS vulnerabilities research*. https://global.ptsecurity.com/en/research/analytics/ics-vulnerabilities-2019
13. ResearchGate. (n.d.). *Conceptual model of information protection of critical information infrastructure objects of Ukraine*. https://www.researchgate.net/publication/357456211_Conceptual_model_of_information_protection_of_critical_information_infrastructure_objects_of_Ukraine
14. U.S. Department of Homeland Security. (n.d.). *National strategy for the physical protection of critical infrastructure and key assets*. https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf
15. European Commission. (2004). *Critical infrastructure protection in the fight against terrorism*. https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF
16. Verkhovna Rada of Ukraine. (n.d.). *Automated control and monitoring systems (definition)*. https://zakon.rada.gov.ua/laws/term/319/sp:max15
17. Verkhovna Rada of Ukraine. (n.d.). *Information security management system (definition)*. https://zakon.rada.gov.ua/laws/term/66349

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Ostapchuk Vadym
Master
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0009-0002-2952-9189
vrostapchuk.fitm24m@kubg.edu.ua

Osadcha Viktoriia
Student
Kielce University of Technology. Kielce, Poland
ORCID: 0009-0001-6180-8172
vikosa2007@gmail.com

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

Strelnikov Vitalii
PhD, Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0003-3439-3220
*v.*strelnikov@kubg.edu.ua

Dmytro Bodnenko
PhD of Pedagogical Sciences, Associate Professor,
Associate Professor at the Department of Mathematics and Physics
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID 0000-0001-9303-6587
d.bodnenko@kubg.edu.ua

ENSURING INFORMATION SECURITY OF AUTOMATED CONTROL SYSTEMS AT CRITICAL INFRASTRUCTURE FACILITIES

Abstract. The paper proposes a formal model for the adaptive selection of cryptographic parameters for protecting communication channels in corporate computer networks based on dynamic trust assessment and integrated risk. The relevance of the study stems from the fact that common practices of static configuration of encryption algorithms, modes of operation, and cryptographic strength parameters do not account for changes in access context and the behavior of interacting entities, which leads either to excessive computational overhead or to the emergence of vulnerability windows during threat escalation. The scientific novelty lies in interpreting the cryptographic profile as a controllable dynamic state of the security system, where trust acts as a direct control parameter of the cryptographic configuration rather than merely a factor in access decision-making. A protected channel is formalized as a state tuple combining the subject, resource, context, trust level, risk, and cryptographic profile, while adaptive parameter selection is described by a mapping that establishes a correspondence between (resource criticality, context) and a set of cryptographic characteristics (algorithm, mode, strength parameter, session lifetime). An optimization formulation for profile selection is developed that accounts for the trade-off between cryptographic strength and operational costs, along with an event-driven mechanism for updating the cryptographic state (Rekey/Upgrade/Revoke) in response to trust degradation, risk increase, or critical security events. Scenario analysis (normal operation, contextual/behavioral anomaly, critical event) demonstrates the model's ability to coherently enhance strength and reduce cryptographic session lifetimes in high-risk situations, thereby reducing the potential attack window while maintaining acceptable performance under low-risk conditions. The obtained results

provide a theoretical foundation for deploying adaptive cryptographic profiles in TLS/VPN and Zero Trust–oriented corporate environments.

Keywords: dynamic trust; integrated risk; channel cryptographic profile; event-driven update; crypto-agility; Zero Trust; corporate computer networks.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Fortinet. (2025). *Global threat landscape report 2025*. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report-2025.pdf
2. Cybersecurity and Infrastructure Security Agency. (n.d.). *Cyber-attack against Ukrainian critical infrastructure*. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01
3. SecurityWeek. (n.d.). *Industroyer ICS malware linked to Ukraine power grid attack*. https://www.securityweek.com/industroyer-ics-malware-linked-ukraine-power-grid-attack/
4. Kozachok, V. A., Kyrychok, R. V., Skladannyi, P. M., Buriachok, V. L., & Hulak, H. M. (2016). Problems of ensuring security control of corporate networks and ways to solve them. *Scientific Notes of the Ukrainian Research Institute of Communications*, *3*(43), 48–61.
5. Mashtaliar, Ya. R., Kozachok, V. A., Brzhevska, Z. M., & Bohdanov, O. M. (2023). Research on the development and innovations of cybersecurity at critical infrastructure facilities. *Cybersecurity: Education, Science, Technique*, *2*(22), 156–167.
6. Kozachok, V. A., & Drapatyi, M. V. (2024). Analysis of security incident investigation technologies at critical infrastructure facilities. *Cybersecurity: Education, Science, Technique*, *2*(26), 374–391.
7. International Electrotechnical Commission. (n.d.). *IEC 62443: Security for industrial automation and control systems*. https://tk185.appau.org.ua/downloads/IEC_62443_2_1_ukr_draft.pdf
8. International Organization for Standardization. (n.d.). *ISO/IEC 27001: Information security management systems—Requirements*. https://www.iso.org/standard/27001
9. National Institute of Standards and Technology. (2015). *Guide to industrial control systems (ICS) security (NIST SP 800-82 Rev. 2)*. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf
10. Verkhovna Rada of Ukraine. (2006). *Law of Ukraine "On critical infrastructure"*. https://zakon.rada.gov.ua/laws/show/1882-20#Text
11. Verkhovna Rada of Ukraine. (2017). *Doctrine of information security of Ukraine*. https://zakon.rada.gov.ua/laws/show/47/2017#Text
12. Positive Technologies. (2019). *ICS vulnerabilities research*. https://global.ptsecurity.com/en/research/analytics/ics-vulnerabilities-2019
13. ResearchGate. (n.d.). *Conceptual model of information protection of critical information infrastructure objects of Ukraine*. https://www.researchgate.net/publication/357456211_Conceptual_model_of_information_protection_of_critical_information_infrastructure_objects_of_Ukraine
14. U.S. Department of Homeland Security. (n.d.). *National strategy for the physical protection of critical infrastructure and key assets*. https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf
15. European Commission. (2004). *Critical infrastructure protection in the fight against terrorism*. https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF
16. Verkhovna Rada of Ukraine. (n.d.). *Automated control and monitoring systems (definition)*. https://zakon.rada.gov.ua/laws/term/319/sp:max15
17. Verkhovna Rada of Ukraine. (n.d.). *Information security management system (definition)*. https://zakon.rada.gov.ua/laws/term/66349

Отримано редакцією журналу / Received: 27.01.26
Прорецензовано / Revised: 18.02.26
Схвалено до друку / Accepted: 26.03.26