КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.856
УДК 004. 056.3+004.056.5

Фесьоха Віталій Вікторович
доктор філософії, доцент, докторант
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0001-6612-1970
vitaliifesokha@gmail.com

Субач Ігор Юрійович
доктор технічних наук, професор, завідувач кафедри
Інститут спеціального зв'язку та захисту інформації
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0000-0002-9344-713X
igor_subach@ukr.net

КОНЦЕПТУАЛЬНА ОСНОВА ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ В УМОВАХ ЕВОЛЮЦІЇ КІБЕРЗАГРОЗ

Анотація. У статті розглянуто проблематику забезпечення кіберстійкості спеціальних інформаційно-комунікаційних систем (ІКС) в умовах стрімкої еволюції кіберзагроз, зокрема тих, що створені або керовані за допомогою технологій штучного інтелекту. На підставі аналізу сучасних стандартів, рекомендацій та фреймворків показано, що хоча існуючі стратегії кіберстійкості є концептуально цінними та містять прогресивні рішення, проте мають низку обмежень у контексті протидії поліморфним, метаморфним, адаптивним, змагальним та інтелектуально керованим кібератакам. Серед ключових проблем виокремлено відсутність врахування еволюційної природи кіберзагроз, асинхронності кіберподій в системі, складності інтерпретації дій модулів прийняття рішень та обмеженої здатності до накопичення і використання знань в процесах кіберзахисту. Встановлено, що в умовах зростання варіативності та непередбачуваності кібератак виникає об'єктивна потреба в нових методологічних засадах, здатних забезпечити стійке функціонування ІКС навіть в умовах багаторівневого деструктивного впливу. З метою усунення зазначених обмежень запропоновано нові принципи кіберстійкості: еволюційності, часової відносності подій, ситуаційної обізнаності та інтелектуального управління знаннями. Кожен із принципів обґрунтовано в контексті його впливу на кіберстійкість ІКС, описано механізми реалізації та можливі інструменти технічного впровадження. Особливу увагу приділено поєднанню принципу еволюційності з методами топологічного аналізу даних для виявлення структурних закономірностей у динаміці розвитку кіберзагроз. Запропоновані принципи розглядаються як концептуальна основа для побудови самонавчальних, адаптивних і прозорих архітектур кіберзахисту нового покоління, здатних до динамічного оновлення в умовах мінливого та агресивного кіберсередовища.

Ключові слова: кіберстійкість; інформаційно-комунікаційна система; рівень функціональності; кіберзагрози; штучний інтелект; принципи кіберстійкості.

ВСТУП

Спеціальні інформаційно-комунікаційні системи постійно перебувають в полі зору кіберзлочинців, оскільки є критично важливими компонентами забезпечення безперебійного функціонування державних, військових, економічних і соціальних процесів [1]. Крім того, ситуація все більше ускладнюється через стрімкий розвиток самих

кіберзагроз, які часто змінюють свою структуру, тактику й інструменти, набуваючи дедалі більшої прихованості та деструктивного потенціалу [2]. У зв'язку з цим виникає об'єктивна потреба в пошуку нових підходів до захисту критично важливих ІКС.

Постановка проблеми. Стійка тенденція до зростання кількості, складності та непередбачуваності кібератак на спеціальні ІКС висуває нові вимоги до існуючих підходів забезпечення їх стійкого функціонування [1], [2]. У даному контексті концепція кіберстійкості, яка ґрунтується на постулаті про неминучість кібератаки, має суттєву перевагу над традиційними підходами до забезпечення кібербезпеки ІКС, зокрема в аспекті їх функціональності [3] – [5], оскільки включає не лише запобігання та протидію кібератакам, а й управління збоями, відновлення після кібератак, а також підтримання здатності ІКС постійно забезпечувати запланований (прийнятний) результат у будь-який час незалежно від рівня кіберзагроз [2] – [7].

Однак, попри концептуальну перевагу, існуючі стратегії кіберстійкості, хоч і містять прогресивні рішення, часто виявляються недостатніми для ефективної протидії новим кіберзагрозам. Так, у 2023–2025 роках низка масштабних кібератак на ключову інфраструктуру України призвела не лише до технічних збоїв, а й до серйозних соціально-економічних втрат, серед яких найбільш показовими були:

1. На оператор мобільного зв'язку «Київстар» російським хакерським угрупованням «Сонцепік» було здійснено кібератаку 12 грудня 2023 року [8] – [9]. Метою впливу було виведення з ладу ядра мережі, що відповідає за обробку та маршрутизацію трафіку між користувачами та сервісами оператора. Зловмисникам вдалося не лише вивести з ладу головний пункт управління мережею, а й видалити конфігурацію на транзитних базових станціях, внаслідок чого в 24 мільйонів абонентів зник стільниковий зв'язок, перестала функціонувати значна частина банкоматів і платіжних терміналів декількох українських банків, а орієнтовна втрата прибутку материнської телекомунікаційної компанії «Київстар» сягнула 95 мільйонів доларів Сполучених Штатів Америки (США). Завдяки допомозі відомих компаній Microsoft, Cisco та Ericsson вдалося відновити надання всіх послуг лише 15 грудня 2023 року.

2. На тлі російської збройної агресії проти України, державні реєстри та сайт Міністерства юстиції України зазнали масштабної кібератаки 19 грудня 2024 року, в результаті чого було призупинено роботу Єдиних і Державних реєстрів (ЄДР) Міністерства юстиції України, надання послуг, пов'язаних з ідентифікацією та верифікацією даних, реєстрів актів цивільного стану громадян, юридичних і фізичних осіб, а також прав на нерухоме майно та їх обтяжень [10]. До того ж, певних порушень у функціонувані зазнав портал державних сервісів «Дія». Відновлення роботи ЄДР юридичних осіб, фізичних осіб-підприємців та громадських формувань після масштабної кібератаки розпочалося лише 9 січня 2025 року, тоді як відновлення електронної інформаційної взаємодії з державними органами — Державною податковою службою, Державною службою статистики України, Пенсійним фондом України, Міністерством цифрової трансформації та іншими відомствами, які використовують дані ЄДР у своїй діяльності відбулося 10 січня 2025 року [11].

3. 23 березня 2025 року було здійснено потужну кібератаку на державну залізничну службу України, яка вивела з ладу онлайн-систему продажу квитків, спричинивши великі черги на залізничних вокзалах. Кібератака була системною, нетиповою та багаторівневою [12], [13]. Над вирішенням проблеми працювали фахівці з «Укрзалізниці», кібердепартаменту Служби безпеки України та Державної служби спеціального зв'язку та захисту інформації України. Попри кібератаку, вдалося забезпечити 96% вчасного прибуття потягів. Однак, стабільна робота онлайн-сервісів із

продажу квитків і відновлення послуг у застосунку відбулося лише 29 березня, після розгортання сервісів на іншій платформі.

Крім того, стрімкий розвиток галузі штучного інтелекту (ШІ) відкриває нові можливості для кіберзлочинців, зокрема щодо автоматизації кібератак, поглибленого аналізу вразливостей в ІКС, створення високоваріативного шкідливого коду із використанням генеративних, мовних моделей та нейроеволюційних алгоритмів ШІ з метою ефективного обходу традиційних засобів кіберзахисту, а також імітації стилю поведінки легітимних користувачів системи, що призводить до появи нових типів адаптивних та інтелектуально керованих кібератак, які істотно ускладнюють завдання забезпечення кіберстійкості ІКС [14].

Таким чином, зростаюча складність та масштабність сучасних підходів до реалізації деструктивного впливу, посилена використанням технологій ШІ, вимагає перегляду та подальшого розвитку концептуальної основи забезпечення кіберстійкості ІКС, що в свою чергу актуалізує проведення подальших наукових досліджень щодо запобігання та протидії адаптивним та інтелектуально керованим сценаріям реалізації кіберзагроз на ключову інфраструктуру.

Аналіз останніх досліджень і публікацій. Проблематика забезпечення кіберстійкості ІКС все більше привертає увагу як наукової спільноти [2], [7], [14] – [21], так і фахівців із практичної площини кібербезпеки [22] – [24]. Упродовж останніх років сформувалися кілька основних напрямів досліджень, спрямованих на підвищення здатності ІКС протидіяти цілеспрямованим деструктивним впливам:

- ***кіберстійкість на етапі проєктування*** — забезпечення кіберстійкості ІКС ще на етапі її проєктування, із включенням механізмів безпечного відновлення та недопущення поширення відмов *[2], [18], [19];*
- ***інтелектуальна реконфігурація термінальних компонентів*** — застосування програмно-реконфігурованої логіки та вбудованих засобів самодіагностики з елементами ШІ для автоматичного виявлення кіберінцидентів і відновлення функціональності *[15];*
- ***мультиагентні адаптивні системи без надмірності*** — забезпечення функціональної стійкості розподілених ІКС через адаптивне використання наявних ресурсів, протидію DDoS-атакам, взаємодію агентів засобами стеганографії *[16];*
- ***кількісне вимірювання кіберстійкості*** — впровадження метрик кіберстійкості на основі емпіричного аналізу працездатності (наприклад, площа під кривою функціональності), з акцентом на застосування в ІКС військового призначення *[17];*
- ***застосування технологій ШІ:*** інтеграція моделей ШІ для виявлення аномалій, прогнозування кіберзагроз, автоматизації реагування та адаптації до нових кібератак (акцент на SIEM, IDS системах, технології аналізу поведінки UEBA та Big Data) *[20];*
- ***кіберстійкість кіберфізичних систем*** — класифікація кіберзагроз і методів захисту **кіберфізичних систем**, зокрема через підходи до стійкого керування (Resilient Control) та стійкості через проєктування (Resilience-by-Design) із використанням сегментації, різноманіття, теорії ігор *[18];*
- ***навчання з підкріпленням для реалізації механізмів кіберстійкості*** — застосування машинного навчання з підкріпленням для реалізації моделі P2R2 (Preparation, Prevention, Response, Recovery), включно з реакцією на кібератаки нульового дня, періодичною зміною характеристик ІКС,

приманками (імітаційними ресурсами) та захистом від кібератак на алгоритми навчання *[21]*.

Наведений огляд літератури свідчить про те, що сучасні напрями підвищення кіберстійкості ІКС, хоча й орієнтуються на інтелектуалізацію, адаптивність та проактивний захист через моделювання, навчання та багаторівневу взаємодію компонентів, все ж потребують нових методологічних підходів, які б враховували еволюційну природу кіберзагроз, часову відносність кіберподій, а також забезпечували ситуаційну обізнаність про внутрішні процеси для створення більш стійких ІКС до кіберзагроз.

Метою статті є виявлення та систематизація проблем забезпечення кіберстійкості ІКС в умовах еволюції кіберзагроз, а також визначення концептуальної основи для її підвищення.

Для досягнення мети вирішуються наступні взаємопов'язані завдання:

1. Аналіз існуючих підходів до забезпечення кіберстійкості ІКС.
2. Характеристика типів кіберзагроз, що демонструють ознаки еволюційного розвитку та/або динамічно розвиваються.
3. Визначення перспективних напрямків підвищення кіберстійкості ІКС з врахуванням виявленої проблематики.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Аналіз існуючих підходів до забезпечення кіберстійкості ІКС. Попри наявні відмінності в термінологічному трактуванні поняття кіберстійкості (cyber resilience) в сучасному науково-практичному дискурсі [3], [5], [25], можна виокремити основні компоненти, що формують її узагальнену структурну модель [26], [27]:

- *запобігання (prevention)* — виявлення та усунення потенційних загроз;
- *протидія (resistance)* — зменшення впливу кібератак на функціонування ІКС;
- *відновлення (recovery)* — повернення до нормального функціонування;
- *адаптація (adaptation)* — навчання на подіях, оновлення стратегій протидії та конфігурацій захисту.

У даному контексті кіберстійкість доцільно розглядати як результат інтеграції трьох взаємопов'язаних ключових підходів до кіберзахисту: проактивного, реактивного та постінцидентного (рис. 1), що в сукупності забезпечують здатність ІКС функціонувати безперервно навіть в умовах цілеспрямованих деструктивних впливів.

Рис. 1. Кіберстійкість як результат інтеграції ключових підходів до кіберзахисту

Функціональні перетини між зазначеними підходами утворюють багаторівневу архітектуру кіберстійкості:

- *на стику проактивного та реактивного підходів реалізуються механізми* раннього виявлення та швидкого реагування, зокрема засобами поведінкового аналізу;
- ***перетин реактивного та постінцидентного підходів*** охоплює здатність до ізоляції кіберінциденту, утримання критичних функцій та негайного початку процесів відновлення ще до повного усунення загрози;
- ***проактивний і постінцидентний підходи*** взаємодіють в межах механізмів адаптації: результати розслідування інцидентів стають основою для оновлення моделей кіберзагроз, політик безпеки та конфігурацій ІКС, тим самим підсилюючи здатність системи до самонавчання.

Саме такий інтегрований підхід покладено в основу більшості сучасних стратегій забезпечення кіберстійкості [26], [28], [29], що формуються на основі міжнародних стандартів, рекомендацій і регуляторних документів, які в свою чергу визначають методологічні основи, функціональні вимоги та архітектурні засади побудови стійких ІКС. В таблиці 1 наведено огляд загальновизнаних і найбільш поширених регуляторних документів щодо забезпечення кіберстійкості ІКС [27], [30] – [36].

Таблиця 1

Поширені регуляторні документи щодо забезпечення кіберстійкості ІКС

Найменування	Фокус	Підхід до кіберстійкості	Сильні сторони	Обмеження
ISO/IEC 27001	Інформаційна безпека	Орієнтація на управління ризиками	Універсальність, чітка структура контролів, міжнародне визнання	Не охоплює повністю аспекти відновлення та адаптації
NIST Cybersecurity Framework	Управління кіберризиками	Гнучка шестифункціональна модель: Govern–Identify–Protect–Detect–Respond–Recover	Широке прийняття, простота інтеграції, адаптивність	Добровільний характер, потребує доповнення технічними деталями
NIST SP 800-160 Vol.2	Інженерія життєвого циклу систем	Побудова стійких систем (Resilience Engineering)	Системне мислення, вбудована стійкість, орієнтація на критичні функції	Висока складність впровадження, орієнтація на системних інженерів
ISO/IEC 27031	Безперервність інформаційно-комунікаційних технологій	Підготовка, реагування, відновлення	Сильний акцент на безперервну підтримку функціонування, взаємозв'язок з ISO 22301	Фокус обмежений IT-середовищем
ENISA Guidelines	Критична інфраструктура ЄС	Системний підхід до забезпечення стійкості	Практичні кейси, рекомендації для державного/приватного сектору	Орієнтованість на політику, не завжди детальні технічні вказівки

Symantec Cyber Resilience Blueprint	Комерційні рішення	4-фазна модель: Prevent–Detect–Respond–Recover	Простота, орієнтація на автоматизацію та рішення	Приватна ініціатива, відсутність нормативного статусу
Digital Operational Resilience Act	Фінансовий сектор ЄС	Юридична відповідальність за кіберстійкість	Конкретні вимоги до фінансових установ, відповідальність за тестування	Обмежене застосування поза фінансовою сферою
Cyber Resilience Review	Самооцінювання	Оцінка зрілості кіберстійкості	Структурований інструмент для організацій, безкоштовний	Рекомендаційний характер, потребує зовнішньої підтримки

Як свідчить проведений аналіз, розглянуті нормативно-методичні документи охоплюють різні аспекти забезпечення кіберстійкості, формуючи багатоаспектну методологічну базу від проєктування стійких ІКС до організаційного управління безпекою та самодіагностики. Деякі з них, зокрема ISO/IEC 27001 та ISO/IEC 27031 закладають передумови для підвищення кіберстійкості систем, переважно орієнтуючись на формування системного підходу до управління ризиками, безперервності функціонування та підготовки до кіберінцидентів. Тоді як, NIST Cybersecurity Framework і Symantec Cyber Resilience Blueprint пропонують фреймворки з чітко визначеними фазами реагування на кіберзагрози, які, в свою чергу є зручними для адаптації під специфіку конкретних організацій. Якщо NIST Cybersecurity Framework є універсальною моделлю національного масштабу, то Symantec Cyber Resilience Blueprint є практичним інструментом з акцентом на інтеграцію безпеки у бізнес процеси.

Особливу цінність у технічному плані має NIST SP 800-160 Vol.2, який єдиний серед розглянутих документів пропонує інженерний підхід до кіберстійкості на етапі проєктування ІКС, реалізуючи принципи resilience engineering. На відміну від вищезазначених фреймворків, він не лише регламентує управління, а й детально описує архітектурні тактики та цілі кіберстійкості. Водночас ENISA Guidelines і Cyber Resilience Review демонструють важливість взаємозв'язку між стратегічними підходами та інструментами самооцінювання. ENISA Guidelines надає міжінституційні рекомендації, тоді як Cyber Resilience Review орієнтований на оперативний рівень (виявлення слабких місць і підвищення зрілості без залучення зовнішніх аудиторів).

Окрему увагу заслуговує регламент Digital Operational Resilience Act, який єдиний серед проаналізованих документів має юридично зобов'язувальний характер. Він не лише формулює вимоги до кіберстійкості, а й передбачає їхнє обов'язкове тестування, управління та прозорість у фінансовому секторі. Digital Operational Resilience Act вказує на поступовий перехід від добровільних рекомендацій до жорстких регуляторних норм щодо кіберстійкості.

Оскільки NIST Cybersecurity Framework 2.0 є найпоширенішим, універсальним та широко адаптованим у різних галузях інструментом для управління кіберризиками, розгляд особливостей реалізації кіберстійкості доцільно здійснювати саме на його прикладі. На рис. 2 наведено функції, що формують модель забезпечення кіберстійкості ІКС.

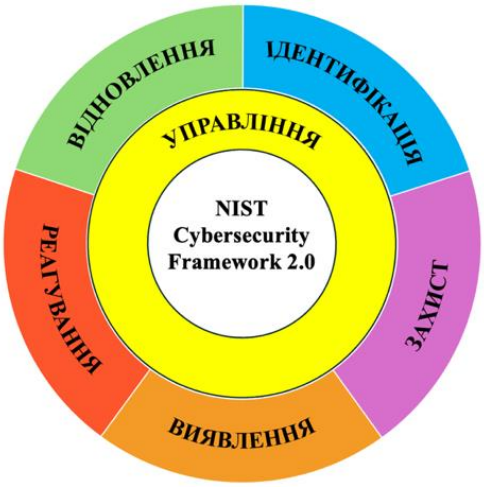

Рис. 2. Функціональна модель кіберстійкості NIST Cybersecurity Framework 2.0

Так, NIST Cybersecurity Framework 2.0 [30] базується на шести взаємопов'язаних функціях, що охоплюють повний життєвий цикл управління кіберризиками. Функція *«Управління»* встановлює політики, ролі, відповідальність і загальні принципи управління безпекою в організації. *«Ідентифікація»* полягає у виявленні активів, ризиків та залежностей, що потребують захисту. *«Захист»* зосереджується на впровадженні заходів, які знижують ймовірність реалізації кіберзагроз. *«Виявлення»* передбачає моніторинг та виявлення аномальної або шкідливої активності. *«Реагування»* визначає дії, які мають бути виконані у разі кіберінциденту, для його локалізації та пом'якшення наслідків. *«Відновлення»* охоплює заходи з відновлення функціонування систем і процесів після інциденту.

Узагальнюючи, можна стверджувати, що в сукупності зазначені документи формують цілісну систему координат для побудови ефективної стратегії кіберстійкості, яка базується на спільних фундаментальних принципах [29], які визначають логіку протидії кіберзагрозам і забезпечення функціональної стійкості ІКС:

- *проактивності* — спрямованості на попередження кібератак ще до їхньої реалізації (полювання на загрози). Як правило, передбачає аналіз поведінкових аномалій, оцінку ризиків і використання методів прогнозного аналізу для виявлення потенційних кіберзагроз;
- *безперервного навчання* — постійного вдосконалення підходів до виявлення та протидії кібератакам шляхом навчання алгоритмів на актуальних даних. Передбачає використання методів машинного навчання, аналізу історичних даних про кібератаки, а також симуляцій нових сценаріїв реалізації загроз;
- *адаптивності* — здатності ІКС змінювати власні механізми захисту у відповідності до змін у кіберсередовищі. Передбачає використання динамічних стратегій безпеки, гнучке оновлення політик та алгоритмів захисту, оперативне реагування на кіберінциденти;
- *багаторівневості* — комплексного підходу до кіберзахисту шляхом інтеграції технічних (мережеві екрани, IDS/IPS, SIEM), організаційних (контроль доступу, реагування на інциденти) і процедурних (аудит, резервне копіювання) заходів;
- *відновлюваності* — здатності ІКС швидко відновлювати рівень функціонування після впливу кібератак, мінімізуючи їх наслідки.

Забезпечується через механізми аварійного відновлення, дублювання критичних компонентів і резервного копіювання.

Однак, ефективність застосування систем і технологій кіберзахисту, реалізованих на основі зазначених принципів знижується в умовах стрімкої еволюції кібератак, що додатково посилюється використанням загальнодоступних технологій ШІ стороною кібервпливу [29]. Це зумовлено низкою виявлених обмежень:

- вузьким підходом до аналізу природи еволюції кібератак, зокрема їхніх технік і методів застосування;
- відсутністю урахування динаміки еволюції кібератак та можливостей генеративних моделей ШІ для їх створення під час прогнозування загроз;
- відсутністю урахування часової відносності кіберподій в ІКС, що ускладнює відслідковування достовірності їхньої хронології;
- складністю інтерпретації критичної інформації у випадку використання штучних нейронних мереж для прийняття рішень в ІКС.

Таким чином, виявлені обмеження сучасних підходів до забезпечення кіберстійкості ключових ІКС вказують на недостатнє врахування темпів і характеру трансформації сучасних кіберзагроз. Для глибшого розуміння викликів щодо забезпечення кіберстійкості ІКС доцільно проаналізувати типи загроз, які зазнають еволюційних змін, активно адаптуються до умов середовища та використовують можливості ШІ для ускладнення виявлення і протидії.

Характеристика типів кіберзагроз, що демонструють ознаки еволюційного розвитку та/або динамічно розвиваються. В останнє десятиліття кіберзагрози зазнали суттєвих трансформацій як за своєю структурною складністю, так і за механізмами адаптації, що дозволяє зловмисникам значно підвищувати їх ефективність [14]. Замість кібератак, які достатньо легко виявляються методами сигнатурного аналізу, переважають динамічні, еволюційні форми деструктивних впливів, серед яких ключову роль відіграють поліморфні, метаморфні та інтелектуально керовані загрози, згенеровані із застосуванням технологій ШІ. В табл. 2 наведено огляд типів кіберагроз для ІКС, які демонструють ознаки еволюційного розвитку та/або динамічно розвиваються.

Таблиця 2

Типи кіберзагроз, що демонструють ознаки еволюційного розвитку

Тип загрози	Характеристика	Ключові технології	Загроза для ІКС
Поліморфні	Змінюють власний код при кожному виконанні, зберігаючи функціональність	Шифрування, вставки програмного «сміття», обфускація коду	Ухилення від сигнатурного виявлення
Метаморфні	Генерують повністю нову структуру коду, змінюючи частково внутрішню логіку	Генератори коду, обфускація, переструктурування програмної логіки	Високий рівень мінливості, ускладнення зворотної інженерії
Адаптивні	Змінюють свою поведінку в реальному часі у відповідь на реакції цільової системи	Підкріплювальне навчання , зворотній зв’язок з атакованим середовищем	Тривале проникнення, активне ухилення
Створені засобами генеративного ШІ	Створені засобами ШІ нові, невідомі форми деструктивного впливу або трафіку, подібні до легітимних	Generative Adversarial Networks, LLM, нейроеволюція	Маскування під нормальну активність, обхід систем кіберзахисту

Імітаційні	Імітують поведінку легітимних користувачів або процесів	Імітаційне навчання, моделі поведінки, LLM	Ухилення від поведінкових фільтрів, соціальна інженерія
Автономні	Приймають рішення та діють без участі людини, виконуючи багатоступеневі кібератаки	Автономні агенти, багатоагентні системи, планування сценаріїв	Автоматизовані кампанії, кібератаки по ланцюгу поставок
Змагальні	Впливають на роботу моделей ШІ, подаючи спеціально модифіковані вхідні дані для спотворення класифікації або ухвалення рішень	Adversarial examples, FGSM, PGD, data poisoning, model evasion	Обхід систем кіберзахисту, маніпуляція поведінковим аналізом, руйнування класифікаторів

Поліморфні кібератаки змінюють свій код при кожному запуску, зберігаючи логіку виконання. Часто застосовуються в експлойтах до мережевих протоколів, зокрема SMB і RDP, дозволяючи проникати через вразливості в фреймворках керування ІКС [37].

Метаморфні кібератаки змінюють власну структуру, логіку, обхідні гілки коду або інструкції. Для ключових ІКС дані загрози особливо небезпечні, оскільки здатні проникати на різні рівні систем [37].

Сучасні кібератаки дедалі частіше використовують елементи ШІ. Мова йде не лише про автоматизацію сканування, а й про автономні [38] системи прийняття рішень на стороні зловмисника [13]. Наприклад, нейроеволюційні алгоритми та генетичні алгоритми застосовуються для створення модифікованого шкідливого програмного забезпечення, яке здатне обходити детектори, змінювати IP-адреси, імітувати поведінку легітимних процесів [39]. Особливо небезпечними є кібератаки з підкріплювальним навчанням, коли сторона впливу адаптує власні дії на основі реакцій системи: уникає виявлення, залишаючись активним упродовж тривалого часу [40].

Створені засобами генеративного ШІ кібератаки використовують потужність нейромереж — Generative Adversarial Networks, великі мовні моделі та нейроеволюційні алгоритми для створення зловмисного трафіку, подібного до легітимного, що дає змогу обманювати поведінкові системи виявлення [41].

Імітаційні кібератаки копіюють поведінку легітимних користувачів з метою уникнення виявлення або здійснення соціальної інженерії без участі людини, часто у складі багатоагентних систем. Здатні самостійно планувати та виконувати складні сценарії впливу, адаптуючи свої дії до архітектури цільової системи [42].

Особливу небезпеку для ІКС становлять кібератаки на алгоритми машинного навчання, що інтегровані в системи кіберзахисту. Вони можуть проявлятися у вигляді модифікованих вхідних даних, які система помилково класифікує як безпечні або через розмиття поведінкових меж, отруєння навчальних даних, що призводить до хибної генералізації та прихованих тригерів у моделі, які активуються за заданих умов [43].

Підсумовуючи, можна сказати, що розглянуті типи кіберзагроз становлять серйозну небезпеку для ключових ІКС через їхню здатність змінювати структуру, логіку або поведінку в реальному часі, а також у зв’язку з високим ступенем взаємозалежності компонентів ІКС і жорсткими вимогами до безперервності їх функціонування. Інтелектуально керовані кібератаки дозволяють зловмиснику гнучко адаптувати дії до середовища ІКС, що перетворює атаку з разової деструктивної дії на довготривалу стратегічну кампанію. Відтак, ІКС потрапляють у поле дії якісно нових кібератак, які не мають сталої сигнатури, адаптуються до цільової системи, можуть діяти на декількох рівнях одночасно, а також використовують слабкі місця систем кіберзахисту.

Зазначене свідчить про необхідність переосмислення підходів до забезпечення кіберстійкості ІКС, зокрема в контексті врахування природи еволюції кіберзагроз, часових викривлень в ланцюгах подій та обмеженої прозорості дій інтелектуальних систем кіберзахисту в процесі ухвалення рішень.

Визначення перспективних напрямків підвищення кіберстійкості ІКС. Враховуючи виявлені обмеження підходів до забезпечення кіберстійкості ІКС і високий рівень потенційної загрози з боку кібератак, що демонструють ознаки еволюційного розвитку, виникає необхідність визначення перспективних напрямків вдосконалення систем кіберзахисту. Так, доцільним є розширення наявних підходів до забезпечення кіберстійкості ІКС шляхом впровадження нових принципів, здатних забезпечити ефективну протидію складним, адаптивним та інтелектуально керованим кіберзагрозам.

Запропоновано такі принципи:

1. *Еволюційності* — спрямованості на глибоке розуміння закономірностей розвитку як технік кібератак, так і стратегій кіберзахисту. Передбачає побудову карти еволюції кібератак, яка дозволить не лише візуалізувати тренди, а й знаходити неочевидні взаємозв'язки між техніками застосування та ознаками, характерними для окремих етапів їх розвитку. Реалізація даного принципу надасть змогу створювати прогнозні моделі, що поєднують аналіз еволюційних процесів кібератак із можливостями генеративних моделей та нейроеволюційних алгоритмів ШІ для подальшого створення правил виявлення потенційних кіберзагроз. Крім того, його реалізація може ефективно здійснюватися з використанням засобів топологічного аналізу даних, які дозволяють виявляти сталі структурні характеристики в складних, динамічних просторах ознак. Принцип еволюційності, також, може бути застосований і до стратегій кіберзахисту, сприяючи адаптивному удосконаленню механізмів протидії. Додатково даний принцип забезпечує взаємозв'язок між принципами проактивності, адаптивності, безперервного навчання та інтелектуального управління знаннями, формуючи цілісну концепцію динамічного й самонавчального кіберзахисту.

2. *Часової відносності подій* — спрямованості на врахування часових спотворень, затримок і асинхронності в спостереженні за подіями в ІКС. Так, в сучасних ІКС події надходять із численних джерел з різною затримкою, що зумовлює порушення хронологічної узгодженості та ускладнює формування достовірної картини інцидентів. Принцип передбачає відмову від припущення про абсолютність часових міток і перехід до аналізу подій в множині допустимих послідовностей, узгоджених із реальністю. Замість жорсткої часової шкали застосовується ймовірнісна топологія подій, яка дозволяє інтерпретувати часові зсуви, спричинені як технічними факторами, так і навмисними діями зловмисників. Для реалізації принципу можуть бути використані засоби топологічного аналізу даних, графові моделі, здатні адаптивно відображати відносність подій у часі. Додатково принцип забезпечує взаємозв'язок із принципами ситуаційної обізнаності та інтелектуального управління знаннями, оскільки точне трактування часових міток є необхідною умовою для коректної інтерпретації подій та формування контексту рішень.

3. *Ситуаційної обізнаності* — спрямованості на забезпечення прозорості, інтерпретованості та контрольованості рішень, які приймає система кіберзахисту. Реалізація принципу передбачає впровадження механізмів, що дозволяють відслідковувати й пояснювати логіку виявлення кібератак (які ознаки стали підставою для класифікації події як загрози), адаптації стратегії протидії (які саме зміни були внесені) та оновлення знань (які нові правила було згенеровано). Ключовим елементом принципу є представлення знань у формі, зрозумілій для людини, зокрема у вигляді

онтологій, семантичних мереж або декларативних структур, що дає змогу формалізувати дані про типи кібератак, адаптаційні механізми та історію змін у системі. Додатково принцип забезпечує інтеграцію з принципами інтелектуального управління знаннями, часової відносності подій та еволюційності, оскільки саме прозоре представлення подій, рішень і змін є основою для формування узгодженого інформаційного контексту, на якому базується навчання та адаптація.

4. *Інтелектуального управління знаннями* — спрямованості на автоматизоване накопичення, організацію, оновлення та використання знань у системі кіберзахисту засобами технологій ШІ. Реалізація принципу передбачає супровід активної пам'яті системи в процесі самонавчання, зокрема використання мовних моделей ШІ для автоматизованого пошуку інформації про кібератаки, її структурованої інтеграції, а також контрольованого формування нових правил на основі отриманих даних із відкритих джерел або карти еволюції кібератак. Даний принцип забезпечує актуалізацію знань щодо нових типів кібератак, технік їх реалізації та контрзаходів. Крім того, принцип сприяє глибшому дослідженню кіберінцидентів в ІКС і вдосконаленню стратегій захисту. У взаємодії з принципами еволюційності, проактивності, безперервного навчання, інтерпретованості та адаптивності, інтелектуальне управління знаннями забезпечує не лише цілісне ведення та оновлення критично важливої інформації, а й контроль за її використанням у процесі прийняття рішень засобами ШІ.

Запропоновані принципи формують концептуальну основу для подальшого розвитку інтелектуальних систем кіберзахисту, здатних діяти в умовах адаптивності кіберзагроз і високої динаміки інформаційного середовища.

З метою ілюстрації потенційного впливу запропонованих принципів на кіберстійкість ІКС розглянуто модель її оцінювання, запропоновану в [2]. Серед аналогічних підходів [26], [30], [44] дана модель є найбільш придатною для оцінювання ІКС, оскільки забезпечує кількісне представлення даного показника, легко адаптується до різних типів систем, а також підтримує обчислення інтегральної оцінки. На рис. 3 зображено ілюстративний приклад типового графіка зміни рівня функціональності $F(t)$ ІКС відповідно до підходу Resilience Profile: система зазнає кібератаки в момент t_1, після чого функціональність деградує до певного рівня в межах інтервалу [0..1], і з моменту t_2 розпочинається процес відновлення. Площа під графіком функції $F(t)$ інтерпретується як інтегральна оцінка кіберстійкості ІКС.

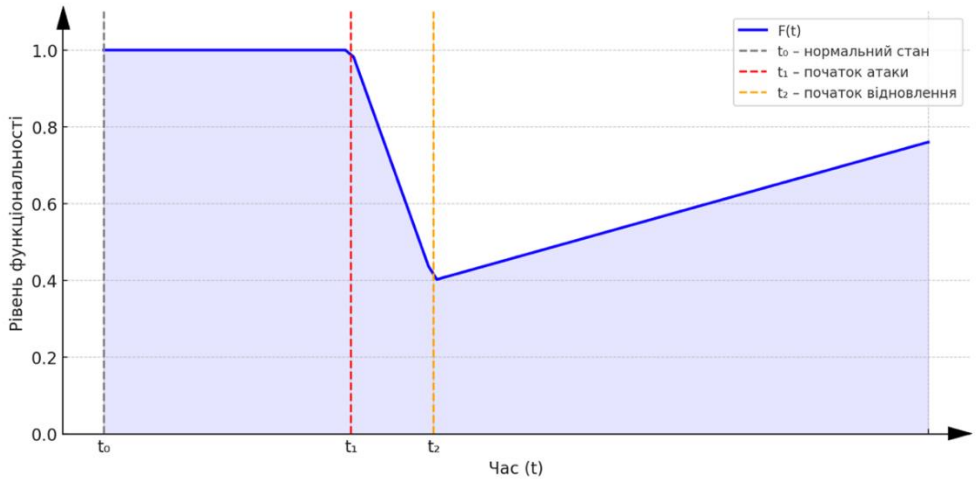

Рис. 3. Приклад типового графіка зміни рівня функціональності $F(t)$ ІКС

У табл. 3 представлено потенційний вплив від впровадження запропонованих принципів на показники кіберстійкості ІКС, де T_{dis} — час до моменту порушення функціональності, ΔF — деградація функціональності під час кібератаки, T_{rec} — необхідний час для відновлення, R_{score} — інтегральний показник кіберстійкості.

Таблиця 3

Потенційний вплив від впровадження запропонованих принципів на показники кіберстійкості

Принцип	T_{dis}	ΔF	T_{rec}	R_{score}
Еволюційності	Дає змогу передбачити атаки завдяки аналізу еволюції, збільшуючи час до інциденту	Зменшує глибину впливу атак через ранню ідентифікацію критичних точок	Допомагає підібрати ефективну траєкторію відновлення з історичних даних	Підвищує загальну кіберстійкість завдяки прогнозуванню розвитку атак
Часової відносності подій	Виявляє маніпуляції з часом, що дозволяє раніше помітити підготовку атаки	Уточнює вплив затримок і помилок, зменшуючи втрати функціональності	Уточнює послідовність подій для швидкої і правильної реакції	Формує точнішу модель подій, що покращує узагальнений рівень стійкості
Ситуаційної обізнаності	Забезпечує кращу орієнтацію в подіях, що пришвидшує виявлення загрози	Підвищує точність реакцій, зменшуючи помилки в обробці загроз	Дозволяє точніше інтерпретувати зміни в системі	Забезпечує прозорість функціонування та контроль
Інтелектуального управління знаннями	Оперативно оновлює знання, підвищуючи готовність до нових атак	Надає актуальні знання для пом’якшення впливу кібератак	Швидко інтегрує нові методики відновлення на основі знань	Інтелектуальне оновлення знань постійно адаптує систему до нових загроз

На основі викладеного можна стверджувати, що включення нових принципів кіберстійкості створює підґрунтя для побудови більш стійких ІКС. Завдяки спрямованості на глибоке розуміння еволюції загроз, відображення часової неоднозначності, прозорість рішень та автоматизоване управління знаннями, система кіберзахисту отримує здатність не лише протистояти атакам, а й самостійно вдосконалювати механізми протидії в динамічному кіберсередовищі.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

З огляду на зростання складності та варіативності сучасних кіберзагроз, зокрема посилених використанням технологій ШІ, традиційні підходи до забезпечення кіберстійкості ІКС потребують переосмислення і подальшого розвитку. Ефективна протидія адаптивним та інтелектуально керованим кібератакам вимагає не лише технічної модернізації систем кіберзахисту, а й оновлення концептуальної основи, яка визначають архітектуру, логіку реагування та здатність до адаптації.

З урахуванням виявлених обмежень сучасних підходів та еволюційного характеру кібератак, обґрунтовано доцільність впровадження нових принципів кіберстійкості: еволюційності, часової відносності подій, ситуаційної обізнаності та інтелектуального

управління знаннями. Їх узгоджене застосування дозволяє сформувати цілісну концепцію інтелектуального, динамічного та прозорого кіберзахисту, орієнтованого на стійке функціонування ІКС навіть за умов складних і багаторівневих загроз.

Таким чином, реалізація запропонованих принципів не лише сприятиме вирішенню наявної проблематики сучасних стратегій забезпечення кіберстійкості, а й відкриває потенційний шлях до побудови інтелектуальних систем кіберзахисту нового покоління, здатних не просто протидіяти кібервпливу, а й активно адаптуватися, самонавчатися та підтримувати безперервність критичних функцій в умовах постійно змінного ландшафту кіберзагроз.

Перспективним напрямком подальших наукових досліджень є реалізація принципу еволюційності шляхом розробки моделі еволюції кібератак на основі топологічного аналізу даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gerasimov B.M., Subach I.Y., Khusainov P.V., & Mishchenko V.O. (2008). Analysis of the tasks of monitoring information networks and methods of increasing the efficiency of their functioning. *Modern information technologies in the sphere of security and defense, 3(3),* 24–27.
2. Kott, A., & Linkov, I. (2019). *Cyber Resilience of Systems and Networks*. Springer International Publishing. https://doi.org/10.1007/978-3-319-77492-3
3. Kostromina, M. O. (2022). Cyber Resilience and Cyber Security: What's the Difference? *Modern Information Security*, 52(4). https://doi.org/10.31673/2409-7292.2022.040012
4. Korystyn, O., & Demediuk, S. (2023). Actualization of cyber resilience and historical origins of the concept of "resilience". *Analytical and Comparative Jurisprudence, (6),* 708–713. https://doi.org/10.24144/2788-6018.2023.06.122
5. Ivanchenko, Ye., Korchenko, O., Zarytskyi, O., Zybin, S., & Vyshnevska, N. (2023). Analysis of the concept of cyber resilience of critical infrastructure. *Ukrainian Information Security Research Journal, 25(4),* 221–233. https://doi.org/10.18372/2410-7840.25.18228
6. Cyber resilience – what it is, how to ensure it, and how to manage it. (2018). Spilno. https://spilno.org/article/kiberstiikist-scho-tse-yak-zabezpechyty-ta-yak-upravlyaty.
7. Bagheri, S., & Ridley, G. (2017). Organisational Cyber Resilience: Research opportunities. *In Australasian Conference on Information Systems*.
8. Kyivstar is not working. What happened and can the problem be circumvented?. (2023). BBC News Ukraine. https://www.bbc.com/ukrainian/articles/cz92xrkklwro.
9. Melnyk, T. (2023). *How hackers broke into Kyivstar: explained by company director Alexander Komarov – Forbes*. https://forbes.ua/innovations/pro-kiberataku-na-kiivstar-vidnovlennya-zvyazku-ta-dopomogu-microsoft-cisco-ericsson-blits-intervyu-prezidenta-kompanii-komarov-12122023-17855
10. Russian hackers broke into Ukraine's state registries. What is known. (n. d.). BBC News Ukraine. https://web.archive.org/web/20241220165826/https:/www.bbc.com/ukrainian/articles/c7ve1298ndgo.amp
11. Restoration of the Unified State Register after a cyberattack. (2025). Ministry of Justice of Ukraine. https://minjust.gov.ua/news/ministry/vidnovlennya-roboti-edinogo-derjavnogo-reestru-pislya-kiberataki.
12. Dysa, Y., & Balmforth, T. (2025). *Ukraine sees Russian effort to sow chaos as cyberattack hits rail service*. Reuters. https://www.reuters.com/world/europe/ukraine-railway-says-its-online-systems-targeted-large-scale-cyberattack-2025-03-24/
13. The Ukrzaliznytsia failure was caused by an "enemy cyberattack." Online services are down, tickets are available at ticket offices. (2025). *BBC News Ukraine*. https://www.bbc.com/ukrainian/articles/ce98ex5jem1o
14. Fesokha, V. (2024). Features of the confrontation between defensive and offensive artificial intelligence in cyberspace. *International Science Journal of Engineering & Agriculture, 3(4),* 105–114. https://doi.org/10.46299/j.isjea.20240304.11
15. Toliupa, S., Samokhvalov, Y., Khusainov, P., & Shtanenko, S. (2023). Self-diagnosis as a way to increase the cyber resistance of terminal components of a technological system. *Cybersecurity: Education, Science, Technique, 2(22),* 134–147. https://doi.org/10.28925/2663-4023.2023.22.134147

16. Lukova-Chuiko, N. (2018). Methodological foundations for ensuring the functional stability of distributed information systems against cyber threats [Doctoral dissertation]. State University of Telecommunications.
17. Kott, A., & Linkov, I. (2021). To Improve Cyber Resilience, Measure It. *Computer*, *54(2)*, 80–85. https://doi.org/10.1109/mc.2020.3038411
18. Segovia-Ferreira, M., Rubio-Hernan, J., Cavalli, A. R., & Garcia-Alfaro, J. (2024). A Survey on Cyber-Resilience Approaches for Cyber-Physical Systems. *ACM Computing Surveys*. https://doi.org/10.1145/3652953
19. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). Developing cyber-resilient systems: A systems security engineering approach. *National Institute of Standards and Technology, 2(1)*. https://doi.org/10.6028/NIST.SP.800-160v2r1.
20. Lunhol, O. (2024). Overview of cybersecurity methods and strategies using artificial intelligence. *Cybersecurity: Education, Science, Technique*, *1(25)*, 379–389. https://doi.org/10.28925/2663-4023.2024.25.379389
21. Huang, Y., Huang, L., & Zhu, Q. (2022). Reinforcement Learning for feedback-enabled cyber resilience. *Annual Reviews in Control*. https://doi.org/10.1016/j.arcontrol.2022.01.001
22. Improving cyber resilience with Fidelis Elevate. (n. d.). Wise IT. https://wiseit.com.ua/building-cyber-resilience/.
23. Key strategies for building cyber resilience in 2024. (2024). *World Economic Forum*. https://www.weforum.org/stories/2024/04/cybersecurity-key-strategies-cyber-resilience-2024/
24. State Special Communications Service and eGA launch project to improve cyber resilience of critical infrastructure. (2025). *State Service for Special Communications and Information Protection of Ukraine*. https://cip.gov.ua/ua/news/ssscip-and-ega-to-enhance-cyber-resilience-of-ukrainian-critical-infrastructure
25. On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021, "On the Cybersecurity Strategy of Ukraine," Decree of the President of Ukraine № 447/2021 (2021) (Ukraine). https://zakon.rada.gov.ua/laws/show/447/2021#Text
26. Bodeau, D. J., Graubart, R. D., McQuaid, R. M., & Woodill, J. (2018). Cyber resiliency metrics, measures of effectiveness, and scoring (MITRE Technical Report No. MTR180314). *The MITRE Corporation.* https://www.mitre.org/sites/default/files/2021-11/prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf.
27. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems*. ISO. https://www.iso.org/standard/82875.html
28. European Union Agency for Cybersecurity. (2021). *ENISA Threat Landscape 2021*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.
29. Fesokha, V., & Subach, I. (2025, April). Principles of ensuring cyber resilience of information and communication systems based on artificial intelligence technologies. *Cybersecurity issues in information and communication systems: abstracts of reports from the VIII International Scientific and Practical Conference*, 56–57.
30. National Institute of Standards and Technology. (2024). *Cybersecurity Framework 2.0*. https://www.nist.gov/cyberframework.
31. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). Developing cyber-resilient systems: A systems security engineering approach. *National Institute of Standards and Technology, 2(1)*. https://doi.org/10.6028/NIST.SP.800-160v2r1.
32. International Organization for Standardization & International Electrotechnical Commission. (2025). *ISO/IEC 27031:2025 – Cybersecurity – Information and communication technology readiness for business continuity*. ISO. https://www.iso.org/standard/27031.html.
33. European Union Agency for Cybersecurity. (2016). *National Cyber Security Strategy Good Practice Guide*. ENISA. https://www.enisa.europa.eu/publications/ncss-good-practice-guide.
34. Symantec Corporation. (2014). *The Cyber Resilience Blueprint: A New Perspective on Security*. Symantec. https://www.ten-inc.com/presentations/Symantec-The-Cyber-Resilience-Blueprint.pdf.
35. European Insurance and Occupational Pensions Authority. (n. d.). *Digital Operational Resilience Act (DORA)*. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.
36. Cybersecurity and Infrastructure Security Agency. (n. d.). *Cyber Resilience Review (CRR)*. U.S. Department of Homeland Security. https://www.cisa.gov/resources-tools/services/cyber-resilience-review-crr.

37. Fesokha, V., Kysylenko, D., & Nesterov, O. (2023). Analysis of the capacity of existing anti-virus protection systems and their based methods for detecting new malware in military information systems. *Communication, informatization and cybersecurity systems and technologies*, *3(3)*. https://doi.org/10.58254/viti.3.2023.16.143
38. AI-Generated Cyber Threats the Rise of Autonomous Hacking Systems. (2024). *IJARCCE*, *13(12)*. https://doi.org/10.17148/ijarcce.2024.131263
39. Oh, S. H., Kim, J., Nah, J. H., & Park, J. (2024). Employing Deep Reinforcement Learning to Cyber-Attack Simulation for Enhancing Cybersecurity. *Electronics*, *13(3), 555*. https://doi.org/10.3390/electronics13030555
40. Kim, M.-S. (2024). Deep Reinforcement Learning-Based Adversarial Attack and Defense in Industrial Control Systems. *Mathematics*, *12(24), 3900*. https://doi.org/10.3390/math12243900
41. Duy, P. T., Tien, L. K., Khoa, N. H., Hien, D. T. T., Nguyen, A. G.-T., & Pham, V.-H. (2021). DIGFuPAS: Deceive IDS with GAN and function-preserving on adversarial samples in SDN-enabled networks. *Computers & Security*, *109*, *102367*. https://doi.org/10.1016/j.cose.2021.102367
42. Lin, C., Chen, S., Zeng, M., Zhang, S., Gao, M., & Li, H. (2022). Shilling Black-Box Recommender Systems by Learning to Generate Fake User Profiles. *IEEE Transactions on Neural Networks and Learning Systems*, 1–15. https://doi.org/10.1109/tnnls.2022.3183210
43. Zhang, C., Costa-Perez, X., & Patras, P. (2022). Adversarial Attacks Against Deep Learning-Based Network Intrusion Detection Systems and Defense Mechanisms. *IEEE/ACM Transactions on Networking*, 1–18. https://doi.org/10.1109/tnet.2021.3137084
44. Vugrin, E. D., & Turgeon, J. T. (2012). *Advancing Cyber Resilience Analysis with Performance-Based Metrics* (SAND2012-2427). Sandia National Laboratories. https://www.sandia.gov/app/uploads/sites/141/2022/02/cyber_resil_102212.pdf

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Vitalii Fesokha
PhD in Information systems and technologies, Associate Professor, Postdoctoral researcher
Kruty Heroes Military Institute of Telecommunications and Information
Technologies, Kyiv, Ukraine
ORCID ID 0000-0001-6612-1970
vitaliifesokha@gmail.com

Ihor Subach
Doctor of Technical Science, Professor, Head of the Department
Institute of Special Communications and Information Protection
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID ID: 0000-0002-9344-713X
igor_subach@ukr.net

CONCEPTUAL FRAMEWORK FOR ENHANCING CYBER RESILIENCE OF INFORMATION AND COMMUNICATION SYSTEMS IN THE CONTEXT OF EVOLUTION OF CYBER THREATS

Abstract. The article discusses the issue of ensuring the cyber resilience of critical information and communication systems in the context of the rapid evolution of cyber threats, in particular those created or controlled using artificial intelligence technologies. Based on an analysis of current standards, recommendations, and frameworks, it is proven that although existing cyber resilience strategies are conceptually valuable and contain progressive solutions, they have a number of limitations in the context of countering polymorphic, metamorphic, adaptive, competitive, and intellectually controlled cyber attacks. Among the key problems are the failure to take into account the evolutionary nature of cyber threats, the asynchrony of cyber events in the system, the complexity of interpreting the actions of decision-making modules, and the limited ability to accumulate and use knowledge in cyber defense processes. It has been established that, given the growing variability and unpredictability of cyberattacks, there is an objective need for new methodological principles capable of ensuring the stable functioning of ICS even under conditions of multi-level destructive influence. In order to eliminate these limitations, new principles of cyber resilience have been proposed: evolution, temporal relativity of events, situational awareness, and intelligent knowledge management. Each of the principles is justified in the context of its impact on the cyber resilience of ICS, and the mechanisms for implementation and possible tools for technical implementation are described. Particular attention is paid to combining the principle of evolution with methods of topological data analysis to identify structural patterns in the dynamics of cyber threats. The proposed principles are considered as a conceptual basis for building self-learning, adaptive, and transparent cyber defense architectures of the new generation, capable of dynamic updating in a changing and aggressive cyber environment.

Keywords: cyber resilience; information and communication system; level of functionality; cyber threats; artificial intelligence; principles of cyber resilience.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Gerasimov B.M., Subach I.Y., Khusainov P.V., & Mishchenko V.O. (2008). Analysis of the tasks of monitoring information networks and methods of increasing the efficiency of their functioning. *Modern information technologies in the sphere of security and defense, 3(3),* 24–27.
2. Kott, A., & Linkov, I. (2019). *Cyber Resilience of Systems and Networks*. Springer International Publishing. https://doi.org/10.1007/978-3-319-77492-3
3. Kostromina, M. O. (2022). Cyber Resilience and Cyber Security: What's the Difference? *Modern Information Security*, 52(4). https://doi.org/10.31673/2409-7292.2022.040012
4. Korystyn, O., & Demediuk, S. (2023). Actualization of cyber resilience and historical origins of the concept of "resilience". *Analytical and Comparative Jurisprudence, (6),* 708–713. https://doi.org/10.24144/2788-6018.2023.06.122

5. Ivanchenko, Ye., Korchenko, O., Zarytskyi, O., Zybin, S., & Vyshnevska, N. (2023). Analysis of the concept of cyber resilience of critical infrastructure. *Ukrainian Information Security Research Journal, 25(4),* 221–233. https://doi.org/10.18372/2410-7840.25.18228
6. Cyber resilience – what it is, how to ensure it, and how to manage it. (2018). Spilno. https://spilno.org/article/kiberstiikist-scho-tse-yak-zabezpechyty-ta-yak-upravlyaty.
7. Bagheri, S., & Ridley, G. (2017). Organisational Cyber Resilience: Research opportunities. *In Australasian Conference on Information Systems*.
8. Kyivstar is not working. What happened and can the problem be circumvented?. (2023). BBC News Ukraine. https://www.bbc.com/ukrainian/articles/cz92xrkklwro.
9. Melnyk, T. (2023). *How hackers broke into Kyivstar: explained by company director Alexander Komarov – Forbes*. https://forbes.ua/innovations/pro-kiberataku-na-kiivstar-vidnovlennya-zvyazku-ta-dopomogu-microsoft-cisco-ericsson-blits-intervyu-prezidenta-kompanii-komarov-12122023-17855
10. Russian hackers broke into Ukraine's state registries. What is known. (n. d.). BBC News Ukraine. https://web.archive.org/web/20241220165826/https:/www.bbc.com/ukrainian/articles/c7ve1298ndgo.amp
11. Restoration of the Unified State Register after a cyberattack. (2025). Ministry of Justice of Ukraine. https://minjust.gov.ua/news/ministry/vidnovlennya-roboti-edinogo-derjavnogo-reestru-pislya-kiberataki.
12. Dysa, Y., & Balmforth, T. (2025). *Ukraine sees Russian effort to sow chaos as cyberattack hits rail service*. Reuters. https://www.reuters.com/world/europe/ukraine-railway-says-its-online-systems-targeted-large-scale-cyberattack-2025-03-24/
13. The Ukrzaliznytsia failure was caused by an "enemy cyberattack." Online services are down, tickets are available at ticket offices. (2025). *BBC News Ukraine*. https://www.bbc.com/ukrainian/articles/ce98ex5jem1o
14. Fesokha, V. (2024). Features of the confrontation between defensive and offensive artificial intelligence in cyberspace. *International Science Journal of Engineering & Agriculture, 3(4),* 105–114. https://doi.org/10.46299/j.isjea.20240304.11
15. Toliupa, S., Samokhvalov, Y., Khusainov, P., & Shtanenko, S. (2023). Self-diagnosis as a way to increase the cyber resistance of terminal components of a technological system. *Cybersecurity: Education, Science, Technique, 2(22),* 134–147. https://doi.org/10.28925/2663-4023.2023.22.134147
16. Lukova-Chuiko, N. (2018). Methodological foundations for ensuring the functional stability of distributed information systems against cyber threats [Doctoral dissertation]. State University of Telecommunications.
17. Kott, A., & Linkov, I. (2021). To Improve Cyber Resilience, Measure It. *Computer, 54(2),* 80–85. https://doi.org/10.1109/mc.2020.3038411
18. Segovia-Ferreira, M., Rubio-Hernan, J., Cavalli, A. R., & Garcia-Alfaro, J. (2024). A Survey on Cyber-Resilience Approaches for Cyber-Physical Systems. *ACM Computing Surveys*. https://doi.org/10.1145/3652953
19. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). Developing cyber-resilient systems: A systems security engineering approach. *National Institute of Standards and Technology, 2(1)*. https://doi.org/10.6028/NIST.SP.800-160v2r1.
20. Lunhol, O. (2024). Overview of cybersecurity methods and strategies using artificial intelligence. *Cybersecurity: Education, Science, Technique, 1(25),* 379–389. https://doi.org/10.28925/2663-4023.2024.25.379389
21. Huang, Y., Huang, L., & Zhu, Q. (2022). Reinforcement Learning for feedback-enabled cyber resilience. *Annual Reviews in Control*. https://doi.org/10.1016/j.arcontrol.2022.01.001
22. Improving cyber resilience with Fidelis Elevate. (n. d.). Wise IT. https://wiseit.com.ua/building-cyber-resilience/.
23. Key strategies for building cyber resilience in 2024. (2024). *World Economic Forum*. https://www.weforum.org/stories/2024/04/cybersecurity-key-strategies-cyber-resilience-2024/
24. State Special Communications Service and eGA launch project to improve cyber resilience of critical infrastructure. (2025). *State Service for Special Communications and Information Protection of Ukraine*. https://cip.gov.ua/ua/news/ssscip-and-ega-to-enhance-cyber-resilience-of-ukrainian-critical-infrastructure
25. On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021, "On the Cybersecurity Strategy of Ukraine," Decree of the President of Ukraine № 447/2021 (2021) (Ukraine). https://zakon.rada.gov.ua/laws/show/447/2021#Text
26. Bodeau, D. J., Graubart, R. D., McQuaid, R. M., & Woodill, J. (2018). Cyber resiliency metrics, measures of effectiveness, and scoring (MITRE Technical Report No. MTR180314). *The MITRE Corporation.*

https://www.mitre.org/sites/default/files/2021-11/prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf.
27. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems*. ISO. https://www.iso.org/standard/82875.html
28. European Union Agency for Cybersecurity. (2021). *ENISA Threat Landscape 2021*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.
29. Fesokha, V., & Subach, I. (2025, April). Principles of ensuring cyber resilience of information and communication systems based on artificial intelligence technologies. *Cybersecurity issues in information and communication systems: abstracts of reports from the VIII International Scientific and Practical Conference*, 56–57.
30. National Institute of Standards and Technology. (2024). *Cybersecurity Framework 2.0*. https://www.nist.gov/cyberframework.
31. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). Developing cyber-resilient systems: A systems security engineering approach. *National Institute of Standards and Technology, 2(1)*. https://doi.org/10.6028/NIST.SP.800-160v2r1.
32. International Organization for Standardization & International Electrotechnical Commission. (2025). *ISO/IEC 27031:2025 – Cybersecurity – Information and communication technology readiness for business continuity*. ISO. https://www.iso.org/standard/27031.html.
33. European Union Agency for Cybersecurity. (2016). *National Cyber Security Strategy Good Practice Guide*. ENISA. https://www.enisa.europa.eu/publications/ncss-good-practice-guide.
34. Symantec Corporation. (2014). *The Cyber Resilience Blueprint: A New Perspective on Security*. Symantec. https://www.ten-inc.com/presentations/Symantec-The-Cyber-Resilience-Blueprint.pdf.
35. European Insurance and Occupational Pensions Authority. (n. d.). *Digital Operational Resilience Act (DORA)*. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.
36. Cybersecurity and Infrastructure Security Agency. (n. d.). *Cyber Resilience Review (CRR)*. U.S. Department of Homeland Security. https://www.cisa.gov/resources-tools/services/cyber-resilience-review-crr.
37. Fesokha, V., Kysylenko, D., & Nesterov, O. (2023). Analysis of the capacity of existing anti-virus protection systems and their based methods for detecting new malware in military information systems. *Communication, informatization and cybersecurity systems and technologies, 3(3).* https://doi.org/10.58254/viti.3.2023.16.143
38. AI-Generated Cyber Threats the Rise of Autonomous Hacking Systems. (2024). *IJARCCE, 13(12).* https://doi.org/10.17148/ijarcce.2024.131263
39. Oh, S. H., Kim, J., Nah, J. H., & Park, J. (2024). Employing Deep Reinforcement Learning to Cyber-Attack Simulation for Enhancing Cybersecurity. *Electronics, 13(3), 555.* https://doi.org/10.3390/electronics13030555
40. Kim, M.-S. (2024). Deep Reinforcement Learning-Based Adversarial Attack and Defense in Industrial Control Systems. *Mathematics, 12(24), 3900*. https://doi.org/10.3390/math12243900
41. Duy, P. T., Tien, L. K., Khoa, N. H., Hien, D. T. T., Nguyen, A. G.-T., & Pham, V.-H. (2021). DIGFuPAS: Deceive IDS with GAN and function-preserving on adversarial samples in SDN-enabled networks. *Computers & Security, 109, 102367*. https://doi.org/10.1016/j.cose.2021.102367
42. Lin, C., Chen, S., Zeng, M., Zhang, S., Gao, M., & Li, H. (2022). Shilling Black-Box Recommender Systems by Learning to Generate Fake User Profiles. *IEEE Transactions on Neural Networks and Learning Systems*, 1–15. https://doi.org/10.1109/tnnls.2022.3183210
43. Zhang, C., Costa-Perez, X., & Patras, P. (2022). Adversarial Attacks Against Deep Learning-Based Network Intrusion Detection Systems and Defense Mechanisms. *IEEE/ACM Transactions on Networking*, 1–18. https://doi.org/10.1109/tnet.2021.3137084
44. Vugrin, E. D., & Turgeon, J. T. (2012). *Advancing Cyber Resilience Analysis with Performance-Based Metrics* (SAND2012-2427). Sandia National Laboratories. https://www.sandia.gov/app/uploads/sites/141/2022/02/cyber_resil_102212.pdf