КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.21.286296
УДК 004

Гарасимчук Олег Ігорович
кандидат технічних наук, доцент
кафедра захисту інформації
Національний університет «Львівська Політехніка», м. Львів, Україна
ORCID ID 0000-0002-8742-8872
oleh.i.harasymchuk@lpnu.ua

Партика Андрій Ігорович
кандидат технічних наук,
кафедра захисту інформації
Національний університет «Львівська Політехніка», м. Львів, Україна
ORCID ID 0000-0003-3037-8373
andrii.i.partyka@lpnu.ua

Нємкова Олена Анатоліївна
доктор технічних наук, професор
кафедра безпеки інформаційних технологій
Національний університет «Львівська Політехніка», м. Львів, Україна
ORCID ID 0000-0003-0690-2657
olena.a.niemkova@lpnu.ua

Совин Ярослав Романович
кандидат технічних наук, доцент
кафедра захисту інформації
Національний університет «Львівська Політехніка», м. Львів, Україна
ORCID ID 0000-0002-5023-8442
yaroslav.r.sovyn@lpnu.ua

ІНТЕГРОВАНИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ДОСЛІДЖЕННЯ КІБЕЗЛОЧИНІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА ДОПОМОГОЮ СИСТЕМИ МОНІТОРИНГУ ІНЦИДЕНТІВ ВІРУСІВ-ВИМАГАЧІВ

Анотація. У сучасному світі, де цифровізація стрімко зростає, кібербезпека виходить на значущий план у захисті національної безпеки, економіки та суспільного добробуту. Критична інфраструктура, як-от енергетика, транспорт, фінансові служби та медичні установи, особливо вразлива перед обличчям загроз кібербезпеки, зокрема від вірусів-вимагачів. Пропонований нами інтегрований підхід до зміцнення кібербезпеки та розслідування кіберзлочинів у цих сферах акцентує на важливості системи моніторингу інцидентів. Він опирається на три ключові стовпи: розробку передових систем моніторингу, що впроваджують штучний інтелект для оперативного виявлення та аналізу загроз; глибоку комплексну оцінку ризиків для виявлення потенційних вразливостей; та активну міжвідомчу співпрацю для координованого реагування на інциденти. Детальний розгляд технічних аспектів системи моніторингу, включно з її архітектурою та алгоритмами машинного навчання, висвітлює її здатність до прогнозування та виявлення кіберзагроз в реальному часі. Також обговорюються правові та етичні виміри збору та обробки даних, що є критично важливими для забезпечення приватності та довіри. Аналізуючи випадки з реальної практики, ми демонструємо, як інтегрований підхід може значно підвищити рівень кібербезпеки, забезпечуючи ефективне виявлення, швидке реагування та нейтралізацію кіберзагроз. Особлива увага приділяється успішним випадкам виявлення та блокування атак, що підкреслює значення комплексного підходу до захисту критичної інфраструктури. У заключній частині статті ми розглядаємо перспективи розвитку кібербезпеки критичної

інфраструктури, акцентуючи на необхідності неперервного оновлення технологій, вдосконалення методик оцінки ризиків та розширення рамок міжвідомчої та міжнародної співпраці. Підкреслюється важливість адаптації до змінюваного кіберландшафту та впровадження інноваційних рішень для зміцнення стійкості перед обличчям новітніх загроз. Ця стаття вносить вагомий вклад у формування інтегрованих стратегій кібербезпеки, підкреслюючи, що поєднання передових технологій моніторингу, глибокої оцінки ризиків та міцної міжвідомчої співпраці може суттєво підвищити здатність суспільства ефективно протистояти кіберзагрозам та забезпечити безпеку критичної інфраструктури.

Ключові слова: критична інфраструктура; віруси-вимагачі; моніторинг; кіберзлочин; інформаційні системи; аудит кібербезпеки; штучний інтелект; інформаційна безпека; кібербезпека; information security management system; фреймворк інформаційної безпеки.

ВСТУП

У сучасній цифровій епосі, коли технології стрімко розвиваються та проникають у всі сфери нашого життя, питання кібербезпеки набуває особливої актуальності. Значне зростання кіберзагроз, зокрема вірусів-вимагачів, ставить під загрозу не лише окремі компанії чи організації, але й цілі держави, їх економіку та безпеку. Критична інфраструктура, яка включає енергетичні системи, транспортні мережі, фінансові установи та медичні заклади, є особливо вразливими до таких атак. Відсутність ефективного захисту та стратегій реагування може призвести до катастрофічних наслідків, включаючи втрату життя, економічні збитки та соціальну нестабільність. У цьому контексті, розробка та впровадження інтегрованого підходу до забезпечення кібербезпеки та дослідження кіберзлочинів, спрямованих на критичну інфраструктуру, стає нагальною потребою.

Постановка проблеми. Основною проблемою у забезпеченні кібербезпеки критичної інфраструктури є висока складність та динамічність кіберзагроз. Віруси-вимагачі, які блокують доступ до важливих даних або систем до виплати викупу, стали одним з найбільш розповсюджених та руйнівних інструментів кіберзлочинців. Їхня здатність швидко адаптуватися до заходів безпеки ускладнює розробку ефективних методів захисту та відновлення після атак. Додатковою проблемою є відсутність єдиної стратегії або стандартів у сфері кібербезпеки, що ускладнює координацію між різними організаціями та державними установами. Це створює "слабкі ланки" у системі безпеки критичної інфраструктури, якими можуть скористатися зловмисники. Іншою значною проблемою є нестача кваліфікованих фахівців у галузі кібербезпеки, які могли б ефективно протистояти сучасним кіберзагрозам, розробляти та впроваджувати комплексні системи захисту. Нарешті, ще одним викликом є забезпечення балансу між потребою у зборі та аналізі даних для ефективного моніторингу кіберзагроз та необхідністю захисту конфіденційності та особистих даних користувачів. У вступі та розділі проблематики нашої статті ми прагнемо не лише висвітлити актуальність та складність викликів у сфері кібербезпеки критичної інфраструктури, але й закласти основу для обговорення інтегрованого підходу, який дозволить ефективно протистояти цим загрозам.

Аналіз останніх досліджень і публікацій. Вивчаючи найновіші наукові дослідження в цій галузі слід зупинитись на кількох ключових моментах, які були отримані в ряді важливих публікацій.

Стаття “Дослідження структури системи виявлення та протидії атакам вірусів-вимагачів на базі endpoint detection and response ” [15] Д. Журавчака, В. Дудикевича та

А. Толкачової є комплексним дослідженням структури систем для виявлення та протидії атакам вірусів-вимагачів на основі технологій Endpoint Detection and Response (EDR). У ньому окреслено виклики та обмеження поточних систем виявлення, підкреслюючи необхідність регулярних оновлень та адаптацій для реагування на еволюцію атак вірусів-вимагачів. У дослідженні запропоновано набір функціональних та нефункціональних вимог до ефективних систем протидії вірусам-вимагачам, включаючи можливості виявлення та реагування в реальному або наближеному до реального часу, здатність аналізувати та класифікувати різні типи вірусів-вимагачів, а також інтеграцію з іншими системами безпеки та інструментами. Також проведено детальний аналіз існуючих систем виявлення та протидії, таких як системи виявлення вторгнень (IDS), системи EDR та сучасні антивірусні рішення, порівнюючи їхні сильні та слабкі сторони. Крім того, представлено алгоритм оцінки якості продуктів для виявлення та протидії вірусам-вимагачам, перевірений на тестах і експериментах, що демонструє його ефективність. Документ є цінним ресурсом для організацій, які прагнуть покращити свої захисти проти атак вірусів-вимагачів, пропонуючи практичні рекомендації та огляд поточного стану та майбутніх напрямків стратегій виявлення та протидії вірусам-вимагачам.

У дослідженні “Аналіз наявних підходів до протидії несанкціонованому доступу в інформаційних мережах держави на основі теорії ігор» [6] акцентується на розробці математичних моделей для кількісного оцінювання захищеності автоматизованих систем. Це означає, що автори використовують теорію матричних ігор як основний інструмент для моделювання процесів нападу та захисту інформації в інформаційних мережах. Важливість дослідження полягає в тому, що воно надає методику для ідентифікації найбільш небезпечних засобів несанкціонованого доступу (НСД), визначення найефективніших засобів захисту інформації, а також оцінки мінімального збитку, який може бути заподіяний в результаті атак. Літературний огляд, ймовірно, включає роботи, що розглядають теорію ігор у контексті кібербезпеки, а також дослідження, присвячені різним аспектам захисту інформаційних систем від несанкціонованого доступу. Це може включати аналіз потенційних загроз, методи оцінки ризиків, а також розробку і впровадження ефективних засобів захисту.

Метою цієї статті є розробка та обґрунтування інтегрованого підходу до забезпечення кібербезпеки критичної інфраструктури, з особливим акцентом на протидію кіберзлочинам, зокрема атакам вірусів-вимагачів. Цей підхід передбачає створення комплексної системи, яка включає в себе не лише технічні засоби захисту, але й стратегії реагування на інциденти, оцінку ризиків, а також міжвідомчу та міжнародну співпрацю. Мета розгалужується на кілька ключових завдань:

•Аналіз сучасного стану кіберзагроз для критичної інфраструктури, з особливою увагою до вірусів-вимагачів, їхніх методів атак та потенційного впливу на критичні системи.

• Розробка методології інтегрованого підходу, яка включатиме в себе передові технології моніторингу та аналізу кіберзагроз, комплексну оцінку ризиків, а також ефективні стратегії реагування на інциденти.

• Визначення ролі міжвідомчої та міжнародної співпраці у забезпеченні кібербезпеки критичної інфраструктури, включаючи обмін інформацією про загрози, спільні навчання та розробку спільних стандартів безпеки.

• Розробка рекомендацій для підвищення ефективності кібербезпеки критичної інфраструктури, заснованих на аналізі сучасних викликів та потенційних загроз.

• Оцінка правових та етичних аспектів збору та обробки даних у контексті моніторингу кіберзагроз, з метою забезпечення балансу між потребами безпеки та захистом особистих даних.

Мета статті полягає не лише у теоретичному внеску в наукове дослідження у сфері кібербезпеки, але й у розробці практичних рекомендацій, які можуть бути використані урядовими агенціями, компаніями критичної інфраструктури та міжнародними організаціями для підвищення їхньої стійкості до кіберзагроз.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

В умовах стрімкого розвитку цифрових технологій та зростання їх впливу на всі сфери суспільного життя, питання кібербезпеки набуває особливої актуальності. Особливо це стосується критичної інфраструктури, такої як енергетичні системи, транспортні мережі, фінансові установи та медичні заклади, які є найбільш вразливими до кібератак, зокрема атак вірусів-вимагачів [4]. Ці загрози можуть не тільки призвести до значних економічних втрат, але й становити загрозу національній безпеці.

Крім вірусів-вимагачів, існує кілька інших видів шкідливих програм, які становлять загрозу для кібербезпеки [13]:

- Троянські коні: Шкідливі програми, що маскуються під законні програми. Вони можуть викрадати дані, встановлювати додаткове шкідливе програмне забезпечення або надавати несанкціонований доступ до системи зловмисникам.

- Шпигунське ПЗ (спайвар): Програми, розроблені для збору інформації про користувача або організацію без їх відома, включаючи особисті дані, паролі та іншу конфіденційну інформацію.

- Віруси: Програми, що можуть самостійно копіюватися та поширюватися, інфікуючи файли, що призводить до різних небажаних наслідків, від відображення непристойних повідомлень до повного знищення даних на жорсткому диску.

- Черв'яки: Самостійні шкідливі програми, що поширюються через мережеві з'єднання, безпосередньо копіюючи себе на інші комп'ютери, часто використовуючи вразливості в програмному забезпеченні.

- Адвар: Непрохане програмне забезпечення, яке автоматично відображає або завантажує рекламу під час встановлення іншої програми, часто без відома користувача.

Сучасні кіберзагрози вимагають нових підходів до захисту, оскільки кіберзлочинці швидко адаптуються до заходів безпеки, а стандартні антивірусні рішення часто виявляються недостатньо ефективними. В цьому контексті, розробка та впровадження інтегрованого підходу до забезпечення кібербезпеки та розслідування кіберзлочинів стає нагальною потребою [14].

Інтегрований підхід передбачає використання передових технологій моніторингу, що базуються на штучному інтелекті та машинному навчанні для аналізу поведінки системи та виявлення аномалій, що можуть свідчити про потенційні загрози [2]. Такі системи дозволяють не тільки ідентифікувати відомі загрози, але й прогнозувати нові, аналізуючи поведінку системи та використовуючи дані про раніше виявлені атаки. Основні компоненти цього підходу включають:

1. Розробку та впровадження систем моніторингу інцидентів, що базуються на штучному інтелекті та машинному навчанні для аналізу поведінки системи та виявлення аномалій, які можуть свідчити про потенційні загрози.

2. Комплексну оцінку ризиків, що включає ідентифікацію активів, оцінку потенційних загроз та вразливостей, аналіз наслідків та ймовірності реалізації ризиків. На основі цієї оцінки розробляються стратегії мінімізації та управління ризиками.

3. Ефективну міжвідомчу співпрацю, яка включає обмін розвідданими про кіберзагрози, спільні тренінги та навчання, для створення єдиної системи реагування на кіберінциденти. Це дозволяє не тільки оперативно реагувати на потенційні загрози, але й розробляти та впроваджувати уніфіковані стандарти кібербезпеки.

Такий інтегрований підхід демонструє свою ефективність у виявленні, блокуванні атак вірусів-вимагачів, та зменшенні негативного впливу на критичну інфраструктуру, а також в адаптації до постійно змінюваного кіберландшафту та впровадженні інноваційних рішень для забезпечення стійкості критичної інфраструктури до майбутніх кіберзагроз [5].

Оцінка ризиків є ключовим елементом інтегрованого підходу до забезпечення кібербезпеки. Цей процес включає наступні кроки:

1. Ідентифікація активів: Визначення та класифікація інформаційних ресурсів, систем, та сервісів, які потребують захисту. Це можуть бути фізичні та віртуальні сервери, бази даних, корпоративні мережі, програмне забезпечення, та інформація.

2. Оцінка потенційних загроз та вразливостей: Аналіз потенційних загроз для ідентифікованих активів та визначення вразливостей, які можуть бути використані для їх компрометації. Загрози можуть включати малвар, віруси-вимагачі, троянські програми, фішинг, DoS-атаки тощо.

3. Аналіз наслідків та ймовірності реалізації ризиків: Оцінка потенційного впливу кіберзагроз на організацію та визначення ймовірності їх виникнення. Це дозволяє визначити рівень ризику для кожного активу.

4. Розробка стратегій мінімізації та управління ризиками: На основі оцінки ризиків розробляються стратегії для їх мінімізації або нейтралізації. Це може включати заходи щодо зміцнення інформаційної безпеки, розробку планів відновлення після інцидентів, навчання персоналу тощо.

Ефективна міжвідомча співпраця, що включає обмін розвідданими про кіберзагрози, спільні тренінги та навчання, є важливою для створення єдиної системи реагування на кіберінциденти. Це дозволяє не тільки оперативно реагувати на потенційні загрози, але й розробляти та впроваджувати уніфіковані стандарти кібербезпеки. Воно включає кілька ключових аспектів, які спрямовані на створення єдиної системи реагування на кіберінциденти:

1. Обмін розвідданими про кіберзагрози: Важливим аспектом є обмін інформацією між різними організаціями та установами, включаючи державні агенції, приватний сектор та міжнародні партнери. Це дозволяє учасникам своєчасно отримувати інформацію про нові та поточні загрози, методи їх реалізації та можливі способи протидії.

2. Спільні тренінги та навчання: Регулярне проведення спільних тренінгів та навчальних програм для фахівців з кібербезпеки сприяє підвищенню їх кваліфікації та обміну досвідом між різними організаціями. Це включає навчання з використання новітніх технологій, методів аналізу та реагування на кіберінциденти.

3. Розробка та впровадження уніфікованих стандартів кібербезпеки: Співпраця в цій сфері дозволяє розробити та впровадити загальноприйняті стандарти та норми, які стосуються захисту інформаційних систем, критеріїв безпеки та методів реагування на інциденти [3, 7, 9, 11]. Це сприяє уніфікації підходів до забезпечення кібербезпеки та полегшує координацію дій між різними учасниками.

Така співпраця є ключовою для створення ефективної системи захисту критичної інфраструктури від кіберзагроз, оскільки дозволяє об'єднати ресурси, знання та досвід різних організацій для створення комплексної стратегії захисту [12].

Практичне застосування інтегрованого підходу вже демонструє свою ефективність. Кейси з реальної практики показують, що впровадження систем моніторингу дозволяє не тільки ефективно виявляти та блокувати атаки вірусів-вимагачів, але й значно зменшувати негативний вплив на критичну інфраструктуру.

Перспективи розвитку кібербезпеки критичної інфраструктури вимагають неперервного оновлення знань та технологій захисту. Розширення глобальної співпраці, адаптація до постійно змінюваного кіберландшафту та впровадження інноваційних рішень є ключовими для забезпечення стійкості критичної інфраструктури до майбутніх кіберзагроз.

Таблиця 1

Ключові компоненти інтегрованого підходу до кібербезпеки

Аспект	Технології	Виклики	Рішення
Моніторинг інцидентів	SIEM системи, лог-аналіз	Велика кількість даних	Автоматизація, машинне навчання
Аналіз загроз	Штучний інтелект, аналітика поведінки	Еволюція кіберзагроз	Постійне оновлення баз знань
Оцінка ризиків	Квантові оцінки, статистичний аналіз	Суб'єктивність оцінок	Стандартизація, автоматизовані інструменти
Міжвідомча співпраця	Спільні оперативні центри	Розрізнення юрисдикцій	Міжнародні домовленості, протоколи

1. Аспект "Моніторинг інцидентів" описує використання SIEM систем та лог-аналізу для стеження за безпековими подіями. Виклик полягає у великій кількості даних, які потрібно обробити, тоді як рішення включає автоматизацію та використання машинного навчання для ефективнішого аналізу та відповіді [8, 10].

2. Аспект "Аналіз загроз" зосереджується на використанні штучного інтелекту та аналітики поведінки для ідентифікації потенційних загроз. Головним викликом є еволюція кіберзагроз, а відповідь на це - постійне оновлення баз знань.

3. Аспект "Оцінка ризиків" включає квантові оцінки та статистичний аналіз для визначення потенційних ризиків. Виклик полягає в суб'єктивності оцінок, а рішенням є стандартизація та використання автоматизованих інструментів.

4. Аспект "Міжвідомча співпраця" відображає важливість спільних оперативних центрів у координації зусиль різних органів. Виклики включають розрізнення юрисдикцій, а рішення - розробка міжнародних домовленостей та протоколів [1].

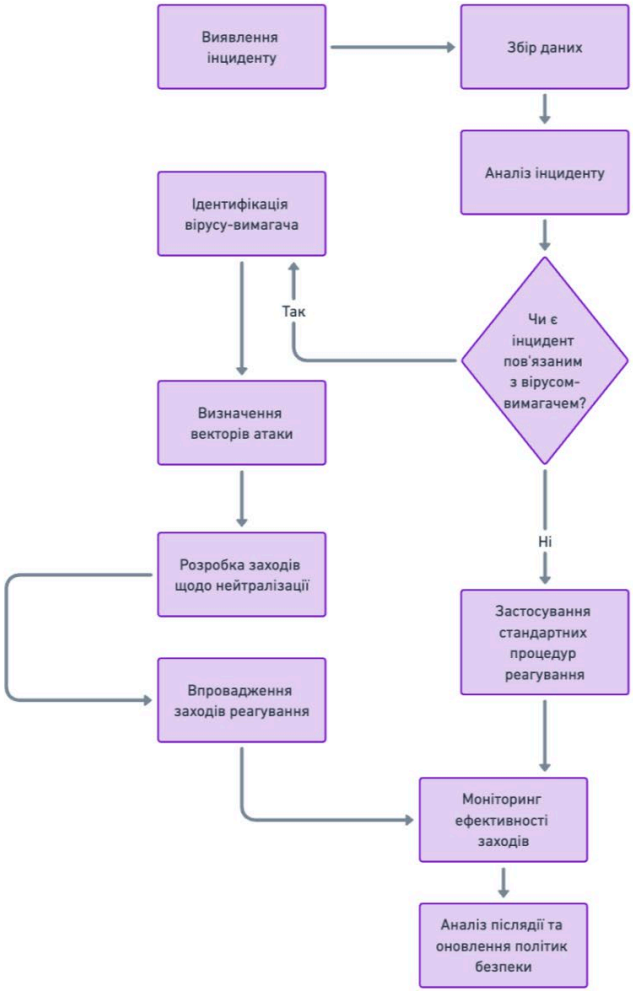

Рис. 1. Інтегрований підхід до забезпечення кібербезпеки

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Ми детально проаналізували, як інтегрована система моніторингу може допомогти виявити та запобігти атакам вірусів-вимагачів, а також зменшити негативний вплив на критичну інфраструктуру. Система дозволяє оперативно реагувати на інциденти, використовуючи алгоритми штучного інтелекту для прогнозування та аналізу потенційних загроз, а також надає інструменти для аналітиків кібербезпеки для більш ефективного розслідування інцидентів.

У результаті проведеного дослідження можна стверджувати, що інтегрований підхід до забезпечення кібербезпеки та розслідування кіберзлочинів є ключовим у зміцненні захисту критичної інфраструктури в умовах постійно зростаючих кіберзагроз.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В ході дослідження ми ознайомилися з сучасними викликами та загрозами кібербезпеки, зокрема з проблематикою вірусів-вимагачів, що впливають на критичну інфраструктуру. Стаття надає інтегрований підхід до забезпечення кібербезпеки та розслідування кіберзлочинів, який включає в себе розробку та впровадження системи моніторингу інцидентів вірусів-вимагачів.

Висновки цієї статті підкреслюють важливість постійного оновлення знань у галузі кібербезпеки та вдосконалення технологій захисту. Також ми рекомендуємо розробку міжнародних стандартів та протоколів для обміну інформацією про кіберзагрози між різними країнами та організаціями, що займаються забезпеченням кібербезпеки критичної інфраструктури.

Завдяки комплексному підходу та розробці відповідних систем моніторингу, можливо не тільки ефективно протидіяти кіберзагрозам, але й мінімізувати ризики для критичної інфраструктури, яка є життєво важливою для функціонування сучасного суспільства.

Основним завданням для майбутнього є продовження роботи над створенням єдиної, інтегрованої системи кібербезпеки, що дозволить оперативно виявляти та нейтралізувати кіберзагрози будь-якого роду, забезпечуючи тим самим безперебійну роботу критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ковалів, М., Скриньковський, Р., Назар, Ю., & Єсімов, С. (2020). Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України. http://dspace.lvduvs.edu.ua/handle/1234567890/3731
2. Сініцин, І., Ігнатенко, П., Слабоспицька, О., & Артеменко, О. (2021). Комплексний підхід до побудови системи кіберзахисту критичної інформаційної інфраструктури держави. Захист інформації. http://dspace.nbuv.gov.ua/bitstream/handle/123456789/144499/08-Sinitsyn.pdf?sequence=1
3. CORDIS, cordis.europa.eu. (2023, 11 грудня). Система обробки інцидентів кібербезпеки, попередження та реагування на них для європейських критичних інфраструктур | проект cybersane | інформаційний бюлетень | H2020 | CORDIS | Європейська комісія. CORDIS | Європейська комісія. https://cordis.europa.eu/project/id/833683
4. Звітність про кіберінциденти для критичної інфраструктури - міркування для космічної галузі. (б. д.). Berkeley Technology Law Journal. https://btlj.org/2024/01/cyber-incident-reporting-for-critical-infrastructure-considerations-for-the-space-industry/
5. Кібербезпека та захист IT-інфраструктури. (2014). Elsevier. https://doi.org/10.1016/c2011-0-08750-1
6. Дудикевич, В. Б., Опірський, І. Р., и Сусукайло, В. А. (2016). Аналіз існуючих підходів до боротьби з несанкціонованим доступом до інформаційних мереж держави на основі теорії ігор. Науковий вісник ДНУ, 26(3), 345-349. https://doi.org/10.15421/40260357
7. Військове відомство США, Міністерство оборони (Dod) та Клементе, Д. (Clemente, J.) (2018). Кібербезпека для критичної енергетичної інфраструктури - посилення безпеки електромереж, атаки на український та західний енергетичні сектори, управління критичною інфраструктурою, гарантії, пом'якшення наслідків. Незалежно опублікована.
8. Мітропулос, С., Пацос, Д. та Дулігеріс, К. (2006). Про обробку та реагування на інциденти: Сучасний підхід. Комп'ютери та безпека, 25(5), 351-370. https://doi.org/10.1016/j.cose.2005.09.006
9. Нейттаанмакі, П., та Лехто, М. (2022). Кібербезпека: Захист критичної інфраструктури. Springer International Publishing AG.
10. Папастергіу, С., Муратідіс, Х., Калогеракі, ЕМ. (2019). Система обробки, попередження та реагування на інциденти кібербезпеки для європейських критичних інформаційних інфраструктур (CyberSANE). In: Макінтайр, Я., Іліадіс, Л., Маглогіанніс, І., Джейн, К. (Ред.) Інженерні застосування нейронних мереж. EANN 2019. Комунікації в комп'ютерних та інформаційних науках, том 1000. Springer, Cham. https://doi.org/10.1007/978-3-030-20257-6_41

11. Uchenna D Ani, Jeremy D McK Watson, Nilufer Tuptuk, Steve Hailes, Madeline Carr, Carsten Maple. (2022). Покращення кібербезпеки критично важливої національної інфраструктури за допомогою моделювання та імітації. http://arxiv.org/abs/2208.07965v1
12. У.Д. Ані; Д.Д. МакК. Ватсон; Д.Р.К. Нерс; А. Кук; К. Мейплз. (2019). Огляд підходів до захисту критичної інфраструктури: Покращення безпеки шляхом реагування на динамічний ландшафт моделювання. https://doi.org/10.1049/cp.2019.0131
13. фон дер Ассен, Я., Фенг, К., Хуертас Сельдран, А., Олеш, Р., Бове, Г. та Стіллер, Б. (2024). GuardFS: файлова система для інтегрованого виявлення та зменшення впливу програм-вимагачів на базі linux. http://arxiv.org/pdf/2401.17917v1.pdf
14. Журавчак, Д. (2021). Система запобігання розповсюдженню програм-вимагачів з використанням python, auditd та linux. Електронне наукове фахове видання "Кібербезпека: Освіта, наука, техніка". https://doi.org/10.28925/2663-4023.2021.12.108116
15. Журавчак, Д., Дудикевич, В., & Толкачова, А. (2023). Дослідження структури системи виявлення та запобігання атакам програм-вимагачів на основі виявлення та реагування на кінцевих точках. Кібербезпека: Освіта, наука, техніка, 3(19), 69-82. https://doi.org/10.28925/2663-4023.2023.19.6982

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023

Oleh I. Harasymchuk
PhD, Associated professor
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID 0000-0002-8742-8872
oleh.i.harasymchuk@lpnu.ua

Andrii I. Partyka
PhD, Senior Lecturer
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID 0000-0003-3037-8373
andrii.i.partyka@lpnu.ua

Elena A. Nyemkova
PhD, Associated professor
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID 0000-0003-0690-2657
olena.a.niemkova@lpnu.ua

Yaroslav R. Sovyn
Ph.D., Associate Professor
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID 0000-0002-5023-8442
yaroslav.r.sovyn@lpnu.ua

AN INTEGRATED APPROACH TO CYBERSECURITY AND CYBERCRIME INVESTIGATION OF CRITICAL INFRASTRUCTURE THROUGH A RANSOMWARE INCIDENT MONITORING SYSTEM

Abstract. In today's rapidly growing digitalised world, cybersecurity is becoming increasingly important in protecting national security, the economy and public welfare. Critical infrastructure, such as energy, transport, financial services and healthcare, is particularly vulnerable to cybersecurity threats, including ransomware. Our proposed integrated approach to strengthening cybersecurity and investigating cybercrime in these sectors emphasises the importance of an incident monitoring system. It relies on three key pillars: the development of advanced monitoring systems that incorporate artificial intelligence to rapidly detect and analyse threats; in-depth comprehensive risk assessments to identify potential vulnerabilities; and active interagency cooperation for coordinated incident response. A detailed look at the technical aspects of the monitoring system, including its architecture and machine learning algorithms, highlights its ability to predict and detect cyber threats in real time. It also discusses the legal and ethical dimensions of data collection and processing, which are critical to ensuring privacy and trust. By analysing real-life cases, we demonstrate how an integrated approach can significantly improve cybersecurity by ensuring effective detection, rapid response and neutralisation of cyber threats. Special attention is paid to successful cases of detecting and blocking attacks, which emphasises the importance of a comprehensive approach to protecting critical infrastructure. In the final part of the article, we consider the prospects for the development of critical infrastructure cybersecurity, focusing on the need for continuous technology upgrades, improved risk assessment methods, and expanded interagency and international cooperation. The importance of adapting to the changing cyber landscape and implementing innovative solutions to strengthen resilience in the face of emerging threats is emphasised. This article makes a significant contribution to the development of integrated cybersecurity strategies, emphasising that the combination of advanced monitoring technologies, in-depth risk assessment and strong interagency cooperation can significantly increase society's ability to effectively counter cyber threats and ensure the security of critical infrastructure.

Keywords: critical infrastructure; ransomware; monitoring; cybercrime; information systems; cybersecurity audit; artificial intelligence; information security; cybersecurity; information security system; information security framework.

REFERENCES

1. Kovaliv, M., Skrynkovskyi, R., Nazar, Y., & Esimov, S. (2020). Legal support of cybersecurity of critical information infrastructure of Ukraine. http://dspace.lvduvs.edu.ua/handle/1234567890/3731.
2. Sinitsyn, I., Ihnatenko, P., Slabospytska, O., & Artemenko, O. (2021). An integrated approach to building a cyber defense system for the critical information infrastructure of the state. Information Protection. http://dspace.nbuv.gov.ua/bitstream/handle/123456789/144499/08-Sinitsyn.pdf?sequence=1.
3. CORDIS, cordis.europa.eu. (December 11, 2023). Cyber security incident handling, warning and response system for the european critical infrastructures | cybersane project | fact sheet | H2020 | CORDIS | european commission. CORDIS | European Commission. https://cordis.europa.eu/project/id/833683
4. Cyber incident reporting for critical infrastructure - considerations for the space industry. Berkeley Technology Law Journal. https://btlj.org/2024/01/cyber-incident-reporting-for-critical-infrastructure-considerations-for-the-space-industry/.
5. Cyber security and IT infrastructure protection. (2014). Elsevier. https://doi.org/10.1016/c2011-0-08750-1
6. Dudykevych, V. B., Opirskyy, I. R., & Susukaylo, V. A. (2016). The analysis of existing approaches to deal with unauthorized access to the information networks of the state on the basis of game theory. Scientific Bulletin of UNFU, 26(3), 345-349. https://doi.org/10.15421/40260357
7. Military, U. S., Department of Defense (Dod) & Clemente, J. (2018). Cyber security for critical energy infrastructure - enhancing electrical grid security, attacks on ukrainian and western energy sectors, critical infrastructure management, safeguards, mitigation. Independently Published.
8. Mitropoulos, S., Patsos, D., & Douligeris, C. (2006). On incident handling and response: A state-of-the-art approach. Computers & Security, 25(5), 351-370. https://doi.org/10.1016/j.cose.2005.09.006
9. Neittaanmaki, P., & Lehto, M. (2022). Cyber security: Critical infrastructure protection. Springer International Publishing AG.
10. Papastergiou, S., Mouratidis, H., Kalogeraki, EM. (2019). Cyber Security Incident Handling, Warning and Response System for the European Critical Information Infrastructures (CyberSANE). In: Macintyre, J., Iliadis, L., Maglogiannis, I., Jayne, C. (Eds) Engineering Applications of Neural Networks. EANN 2019. Communications in Computer and Information Science, Vol 1000. Springer, Cham. https://doi.org/10.1007/978-3-030-20257-6_41
11. Uchenna D Ani, Jeremy D McK Watson, Nilufer Tuptuk, Steve Hailes, Madeline Carr, Carsten Maple. (2022). Improving the cybersecurity of critical national infrastructure using modeling and simulation. http://arxiv.org/abs/2208.07965v1
12. U.D. Ani ; J.D. McK Watson ; J.R.C. Nurse ; A. Cook ; C. Maples (2019). A review of critical infrastructure protection approaches: Improving security through responsiveness to the dynamic modelling landscape. https://doi.org/10.1049/cp.2019.0131
13. von der Assen, J., Feng, C., Huertas Celdrán, A., Oleš, R., Bovet, G., & Stiller, B. (2024). GuardFS: A file system for integrated detection and mitigation of linux-based ransomware. http://arxiv.org/pdf/2401.17917v1.pdf.
14. Zhuravchak, D. (2021). Ransomware spread prevention system using python, auditd and linux. Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique". https://doi.org/10.28925/2663-4023.2021.12.108116
15. Zhuravchak, D., Dudykevych, V., & Tolkachova, A. (2023). Study of the structure of the system for detecting and preventing ransomware attacks based on endpoint detection and response. Cybersecurity: Education, Science, Technique, 3(19), 69-82. https://doi.org/10.28925/2663-4023.2023.19.6982