УДК 004.056.53
DOI: 10.31673/2409-7292.2024.040002

Дженюк Н. В.

МЕТОДОЛОГІЧНІ ОСНОВИ ЗАХИСТУ В СОЦІОКІБЕРФІЗИЧНИХ СИСТЕМАХ

Предмет розгляду у статті є методологічні основи захисту інформації в соціокіберфізичних системах (СКФС), які інтегрують фізичні, цифрові та соціальні компоненти, що функціонують у критичній інфраструктурі. Розглянуто принципи забезпечення безпеки та принципи ефективного управління безпекою в соціокіберфізичних системах, використання яких є необхідним для зниження ризиків атак та підвищення стійкості систем до сучасних загроз. Досліджено існуючі моделі побудови систем захисту кіберфізичних систем, зокрема багаторівневі підходи до безпеки, структури захисту з урахуванням загроз для внутрішнього та зовнішнього контурів соціокіберфізичних систем. Проаналізовано основні вразливості СКФС на фізичному, кібернетичному та соціальному рівнях, з акцентом на ризики атак соціальної інженерії, компрометації даних, перехоплення інформації та недостатню стійкість до багатовекторних атак. Розглянуто модель класифікації індикаторів компрометації "The Pyramid of Pain", що складається з шести рівнів та демонструє взаємозв'язок між типами індикаторів, що використовуються для виявлення діяльності зловмисника. Досліджено сучасні методи і технології кіберзахисту в СКФС. Доведено, що багаторівневий підхід до захисту соціокіберфізичних систем є найбільш ефективним у сучасних умовах, оскільки враховує складність інтеграції фізичних, кібернетичних і соціальних компонентів. Впровадження адаптивних моделей безпеки, що базуються на аналізі великих даних, машинному навчанні та прогнозуванні загроз, значно підвищує стійкість систем до сучасних кіберзагроз. Тому комплексний підхід до захисту з урахуванням специфіки кожного компонента (соціального, кібернетичного чи фізичного) сприяє зниженню ризиків атак та забезпечує безперервність функціонування критичної інфраструктури.

Ключові слова: соціокіберфізична система, інформаційні ресурси, багаторівневий підхід, моделі захисту, вразливості.

Вступ

Соціокіберфізичні системи сучасності являють собою комплексні структури, які об'єднують фізичні, цифрові та соціальні компоненти. Вони охоплюють різні сфери інфраструктури, такі як комунікаційні мережі, транспорт, управління ресурсами та надання державних послуг. Завдяки впровадженню таких передових технологій, як Інтернет речей (IoT), штучний інтелект (AI) і великі дані (Big Data), ці системи стають більш ефективними та багатофункціональними, але водночас зростають ризики кібератак і компрометації даних.

Розвиток цифрових технологій призводить до збільшення обсягу інформації, що обмінюється між компонентами систем. Це створює нові виклики для забезпечення безпеки, зокрема конфіденційності, цілісності та доступності даних. Оскільки такі системи є ключовими елементами критичної інфраструктури, їхній захист від кібератак стає важливим завданням для забезпечення національної безпеки.

Масштабне застосування цих технологій вимагає комплексних підходів до кібербезпеки. Серед них – впровадження надійних протоколів захисту, аналіз потенційних ризиків, моніторинг мережевого трафіку та створення механізмів оперативного реагування на загрози. Ці підходи, з одного боку, сприяють пришвидшенню впровадження "розумних" технологій, розширенню спектру послуг і переходу до сучасних технологій mesh- і NGN-мереж. З іншого боку, вони підкреслюють необхідність забезпечення кібербезпеки на всіх етапах розвитку та застосування таких систем [1 – 3].

Аналіз літературних джерел та формулювання проблеми

Загалом, соціокіберфізична система (СКФС) являє собою поєднання двох систем: кіберфізичної (КФС) та соціальної. КФС стосується нового покоління систем, що інтегрують обчислювальні та фізичні можливості, тісно пов'язані з четвертою промисловою революцією [4]. У статті [5] представлено багаторівневу методологію безпеки кіберфізичних систем та інтернету речей у процесі інтелектуалізації інфраструктури суспільства. Основою підходу є парадигма "багаторівнева система – багаторівнева безпека", що враховує фізичний, комунікаційний та кібернетичний простори. Запропоновано ієрархічну модель безпеки інтернету речей, побудовану за концепцією "об'єкт – загроза – захист", яка охоплює загрози на кожному рівні архітектури. Висвітлено ефективність моделей захисту безпровідних

технологій зв’язку та їх інтеграцію в багаторівневі системи для забезпечення безпечного обміну інформацією. Розроблена методологія спрямована на створення надійних систем, здатних протидіяти сучасним загрозам у контексті індустрії 4.0.

У роботі [6] досліджується використання технології ультраширокосмугових сигналів для захисту інформації в кіберфізичному просторі. Серед переваг зазначають високу надійність і стійкість до перешкод, здатність функціонувати в умовах значного рівня завад. До недоліків належать складність реалізації таких систем, можливі обмеження у сумісності з наявним обладнанням, а також необхідність спеціалізованих знань для розробки та обслуговування. Цей підхід забезпечує високий рівень захисту даних у кіберфізичних системах, однак вимагає ретельного аналізу та планування під час проєктування захисних систем. У статті [7] модель інформаційної безпеки “розумного міста” розроблена на основі концепції “об'єкт – загроза – захист” та передбачає багаторівневий підхід до захисту інформації. Вона включає фізичний, комунікаційний та кібернетичний простори, забезпечуючи конфіденційність, цілісність і доступність даних. Особлива увага приділяється безпеці MEMS-давачів як елементів інтернету речей, використанню хмарних технологій для аналізу та збереження даних, а також криптографічним методам шифрування для захисту каналів зв’язку. Запропонована модель дозволяє ефективно протидіяти сучасним загрозам у різних сегментах “розумного міста”, таких як енергетика, екологія, медицина та інфраструктура. Це рішення сприяє створенню надійної кіберфізичної системи для підтримки функціонування міської інфраструктури в умовах цифрової трансформації.

Робота [8] ґрунтовно аналізує концепцію подвійного контуру захисту в соціокіберфізичних системах, акцентуючи увагу на важливості комплексного підходу до безпеки, який охоплює як внутрішні, так і зовнішні заходи захисту. У ній підкреслюється актуальність цієї проблеми в умовах широкого спектру загроз – від соціальної інженерії до кібератак, та пропонується системний підхід до оцінки ризиків і розробки захисних стратегій. Водночас реалізація такого підходу може бути ускладненою через потребу в глибокій інтеграції між різними компонентами системи та значні ресурсні витрати. У статті [9] розглядається управління даними соціокіберфізичної системи (D-CPSS) із застосуванням концепції 7C Framework. Описано, як кіберфізичні системи (CPS) інтегруються із соціальними системами, створюючи керовані даними кіберфізичні та соціальні системи (D-CPSS). Така інтеграція забезпечує низку переваг, зокрема підвищення ефективності, продуктивності та гнучкості. Проте, залишаються виклики у розумінні та впровадженні D-CPSS. Для кращого усвідомлення D-CPSS пропонується структура 7C, яка забезпечує цілісне уявлення про систему, враховуючи різні компоненти та їх взаємозв’язки.

У роботі [10] представлено всебічний огляд соціальної інженерії в кібербезпеці. Стаття починається з визначення соціальної інженерії та виділення ключових відмінностей між соціальною інженерією та традиційними методами зламу. Далі розглядаються різні типи атак соціальної інженерії. Автори надають детальні описи кожного типу атак, а також приклади реальних інцидентів. Однією з сильних сторін статті є ґрунтовне дослідження механізмів, які роблять атаки соціальної інженерії успішними.

Аналіз публікацій дозволяє зробити висновок, що під час створення соціокіберфізичних систем та систем забезпечення їхнього безпечного функціонування питання, пов’язані з інформаційними процесами соціального компоненту, недостатньо досліджені. Це зумовлено тим, що обробка та сприйняття інформації людиною суттєво відрізняються від аналогічних процесів у кіберфізичній системі. Тому питання оцінки, обміну та обробки інформації є актуальними та обґрунтовують необхідність аналізу методологічних основ захисту інформаційних ресурсів в соціокіберфізичних системах.

Мета роботи та цілі дослідження

Метою роботи є дослідження методологічних основ захисту інформації в соціокіберфізичних системах, що інтегрують фізичні, кібернетичні та соціальні компоненти, з урахуванням зростаючих ризиків кіберзагроз та викликів сучасних технологій.

© Дженюк, Н. В. (2024). Методологічні основи захисту в соціокіберфізичних системах. Сучасний захист інформації, 4(60), 16–29. https://doi.org/10.31673/2409-7292.2024.040002.

Для вирішення поставленої мети розглянуто такі завдання:

– Аналіз існуючих методів захисту соціокіберфізичних систем і їх компонентів.

– Визначення основних вразливостей і загроз для соціальних, кіберфізичних та інформаційно-комунікаційних систем.

– Формування рекомендацій щодо вибору моделей захисту для забезпечення надійного функціонування соціокіберфізичних систем.

Методологічні основи захисту в соціокіберфізичних системах

Соціокіберфізичні системи потребують нових підходів до обробки даних, які включають ідентифікацію, аналіз та інтеграцію різноманітних типів інформації, що відрізняються за масштабами і структурою. Одночасно актуальним є розвиток бездротових технологій, інтегрованих із мобільними інтернет-ресурсами, які, з одного боку, сприяють підвищенню ефективності роботи смарт-систем, а з іншого – створюють умови для проведення цільових атак, зокрема шляхом поєднання кіберзагроз із методами соціальної інженерії. Зростання обчислювальних потужностей, а також поява квантових обчислень ставлять під сумнів надійність сучасних криптографічних алгоритмів. Розвиток інформаційних технологій і мереж нового покоління “G”) значно ускладнює ситуацію, адже призводить до збільшення кількості атак на кіберфізичні та інформаційно-комунікаційні системи, які є основою критичної інфраструктури.

Кібербезпеку можна визначити як стан захищеності кіберпростору держави в цілому або окремих об’єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам [11].

Принципи забезпечення безпеки в СКФС

Сучасні соціокіберфізичні системи поєднують фізичні, кібернетичні та соціальні компоненти, тому їхній захист потребує врахування багатовимірного характеру та застосування інтегрованого підходу. Забезпечення безпеки таких систем базується на кількох ключових принципах (Рис. 1).

Комплексний підхід до безпеки передбачає охоплення всіх рівнів СКФС. На фізичному рівні забезпечується захист пристроїв і обладнання, на кіберрівні – безпека даних, комунікацій та програмного забезпечення, а на соціальному рівні здійснюється управління людським фактором і навчання користувачів. Для підвищення надійності захисту застосовується принцип багаторівневого захисту, який включає автентифікацію користувачів, шифрування даних, використання міжмережевих екранів і систем виявлення вторгнень.

Не менш важливим є принцип мінімізації привілеїв, згідно з яким користувачам і компонентам системи надаються лише ті права доступу, які необхідні для виконання їхніх функцій. Для забезпечення стійкості до атак СКФС має здатність до виявлення загроз і швидкого відновлення після інцидентів. Це досягається шляхом резервування ресурсів, впровадження систем моніторингу та реагування, а також розробки політик відновлення.

Сучасні виклики вимагають адаптивності систем безпеки, яка забезпечується регулярним оновленням програмного забезпечення, аналізом нових вразливостей і гнучкістю у налаштуванні політик захисту. Важливим фундаментом є принцип конфіденційності, цілісності та доступності, що гарантує обмеження доступу до даних, захист від несанкціонованих змін і забезпечення доступності сервісів у потрібний момент.

Особливу увагу приділяють контролю людського фактора через навчання користувачів правилам безпеки, захист від атак соціальної інженерії та впровадження багатофакторної автентифікації. Для безпечних комунікацій широко застосовуються сучасні криптографічні алгоритми та протоколи захисту даних, зокрема VPN і SSL/TLS. Постійний моніторинг і аналіз системи за допомогою засобів SIEM дозволяють виявляти потенційні загрози та оперативно реагувати на них.

© Дженюк, Н. В. (2024). Методологічні основи захисту в соціокіберфізичних системах. Сучасний захист інформації, 4(60), 16–29. https://doi.org/10.31673/2409-7292.2024.040002.

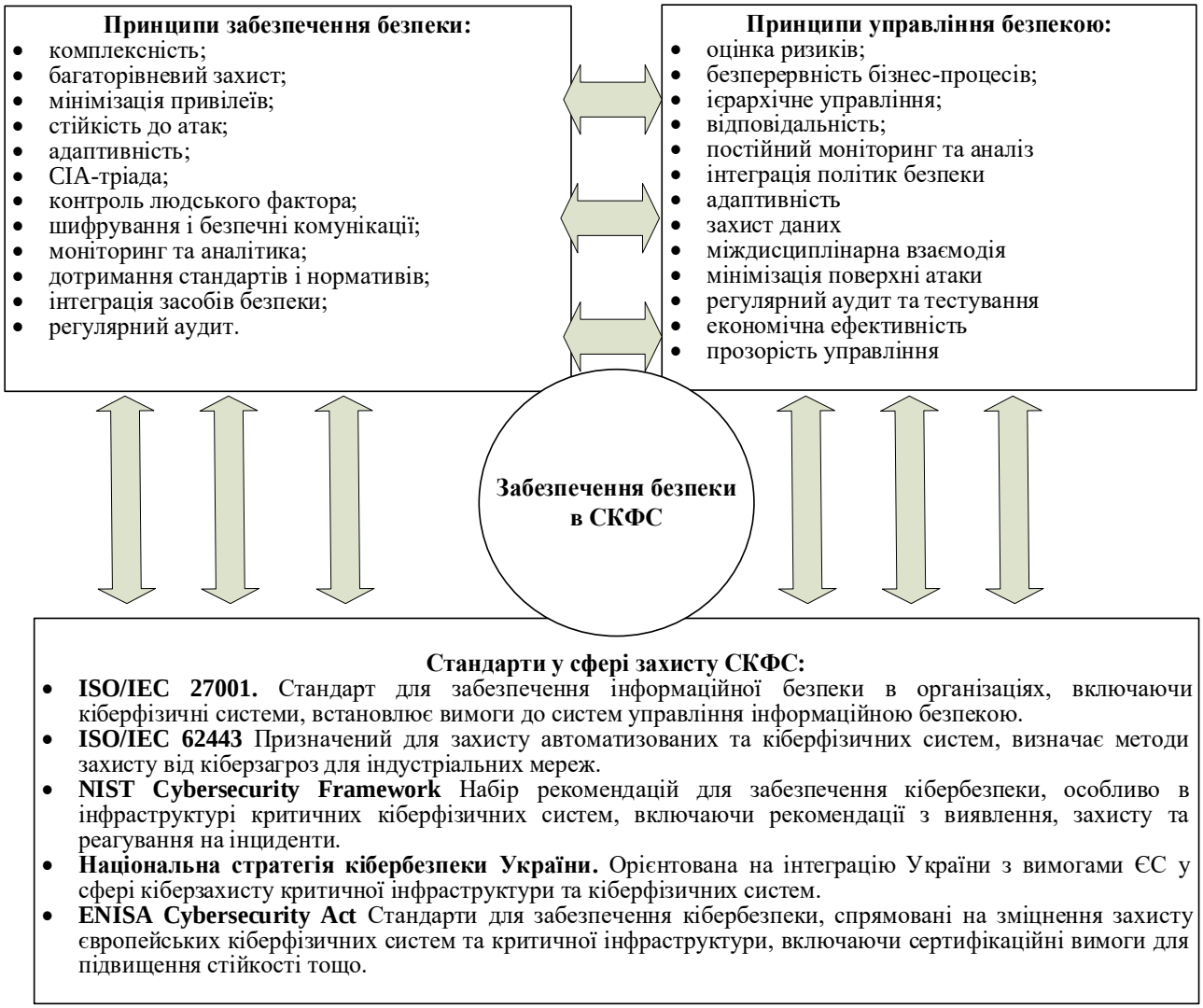

Рис. 1. Забезпечення безпеки в СКФС

Значущим є дотримання міжнародних стандартів безпеки, таких як ISO/IEC 27001, NIST Cybersecurity Framework і IEC 62443, що забезпечують високу якість організації захисту. Інтеграція засобів безпеки фізичного, мережевого та програмного рівнів дозволяє створити єдину, узгоджену систему захисту, а регулярний аудит, тестування на проникнення та оцінка ризиків забезпечують актуальність і надійність захисних механізмів.

Застосування таких принципів дозволяє знижувати ризики атак, підтримуючи стабільність і функціональність соціокіберфізичних систем у сучасному технологічному середовищі.

Принципи управління безпекою в СКФС

Для зниження ризиків атак та підвищення стійкості систем до сучасних загроз необхідне ефективне управління безпекою в соціокіберфізичних системах. Воно ґрунтується на багатошаровому підході, який враховує складність і взаємозалежність фізичних, кібернетичних і соціальних компонентів. Ефективний захист починається з оцінки ризиків. Це включає аналіз загроз для різних складових системи, розрахунок ймовірності атак та оцінку потенційних збитків. Пріоритетність заходів захисту визначається на основі рівня ризику, що дозволяє зосередити ресурси на найбільш критичних аспектах (Табл. 1).

Забезпечення безперервності бізнес-процесів є одним із ключових завдань управління. Це досягається шляхом розробки планів безперервності діяльності, резервування критичних

© Дженюк, Н. В. (2024). Методологічні основи захисту в соціокіберфізичних системах. Сучасний захист інформації, 4(60), 16–29. https://doi.org/10.31673/2409-7292.2024.040002.

ресурсів, створення аварійних копій даних і впровадження стратегій відновлення після інцидентів. Управління безпекою здійснюється на стратегічному, операційному та технічному рівнях, що дозволяє чітко розподілити обов'язки між керівництвом, адміністраторами та користувачами.

Таблиця 1

Рівень вразливості технологій у соціокіберфізичних системах

Технологія	Соціоплатформа (Соцмережі, Криптовалютні біржі)	Кіберпростір (Хмари, LTE, WAN)	Кіберсистема (Бездротові, Mesh, Сенсорні мережі)
Хмарні технології	30%	55%	25%
WAN (Широкосмугові мережі)	40%	50%	35%
LTE технології	45%	60%	40%
Бездротові технології	50%	40%	65%
Mesh мережі	25%	40%	70%
Сенсорні мережі	20%	35%	75%

Постійний моніторинг та аналіз стану системи є необхідною умовою для виявлення потенційних загроз і реагування на них. Використання сучасних засобів, таких як системи SIEM, дозволяє відстежувати аномалії та аналізувати журнали подій. Єдність політик безпеки є ще одним важливим аспектом, адже всі компоненти системи, від фізичних до соціальних, мають діяти згідно з узгодженими правилами.

Система безпеки повинна бути адаптивною, здатною швидко реагувати на нові виклики. Це забезпечується регулярним оновленням програмного забезпечення, впровадженням інноваційних технологій і використанням засобів штучного інтелекту для передбачення загроз. Захист даних включає забезпечення конфіденційності, цілісності та доступності інформації через шифрування і багатофакторну автентифікацію.

Регулярний аудит та тестування допомагають перевіряти ефективність реалізованих заходів захисту. Це включає проведення тестів на проникнення, оцінку відповідності системи міжнародним стандартам і аналіз ефективності. При цьому заходи безпеки мають бути економічно обґрунтованими. Баланс між витратами і рівнем ризику досягається завдяки оптимізації ресурсів та використанню хмарних рішень.

Кібербезпека стає все більш універсальною сферою, де значну роль відіграють людський фактор, соціальні та культурні аспекти, особливості взаємодії з технологіями, а також психологічні аспекти, такі як довіра до технологій і схильність до ризику. Крім того, успішні атаки можуть використовувати специфічні вразливості у соціокіберфізичних системах, зокрема слабкі місця в налаштуваннях безпеки, незахищені канали зв'язку або незахищені компоненти IoT. Ці фактори та методи атак використовуються для пояснення успішності атак на соціокіберфізичні системи [12].

Таким чином, атака на соціокіберфізичні системи означає використання людської вразливості та/або слабких місць програмного забезпечення для підриву кібербезпеки. Це робить соціокіберфізичні системи постійною, універсальною загрозою безпеці (Рис. 2).

Проблеми загроз для систем СКФС пояснює концепція "піраміди безпеки", розроблена у 2013 році фахівцем з безпеки Девідом Дж. Б'янко (рис. 3). Вона відображає впорядкований список індикаторів для визначення дій зловмисників, де складність і зусилля для виявлення цих індикаторів зростають в напрямку до вершини піраміди. Чим вище індикатор у піраміді, тим важче його ідентифікувати та перетворити на дієві заходи.

Індикатори з "Pyramid of Pain" допомагають визначити складність для зловмисника при блокуванні або зміні різних аспектів атаки:

Геш-значення (Hash Values) – це найнижчий рівень уразливостей, зміна геш-значень легко робиться зловмисниками, тому їхня вразливість є тривіальною.

© Дженюк, Н. В. (2024). Методологічні основи захисту в соціокіберфізичних системах. Сучасний захист інформації, 4(60), 16–29. https://doi.org/10.31673/2409-7292.2024.040002.

IP-адреси (IP Addresses) – їх легко змінити, але блокування певних IP-адрес може тимчасово обмежити зловмисника.

Домени (Domain Names) – блокування доменів є простим, але теж не вирішує проблему повністю, оскільки зловмисники можуть реєструвати нові домени.

Артефакти мережі або хосту (Network/Host Artifacts) – такі артефакти можуть включати файли, залишені на зараженому хості, і їх виявлення є більш складним для зловмисників.

Інструменти (Tools) – це програми, які використовуються для здійснення атак. Якщо зловмисник не має доступу до своїх інструментів, його можливості сильно обмежуються.

Тактики, техніки та процедури (TTPs) – найвищий рівень складності. Ці тактики важко змінювати, і вони показують, наскільки добре зловмисник володіє своїми навичками.

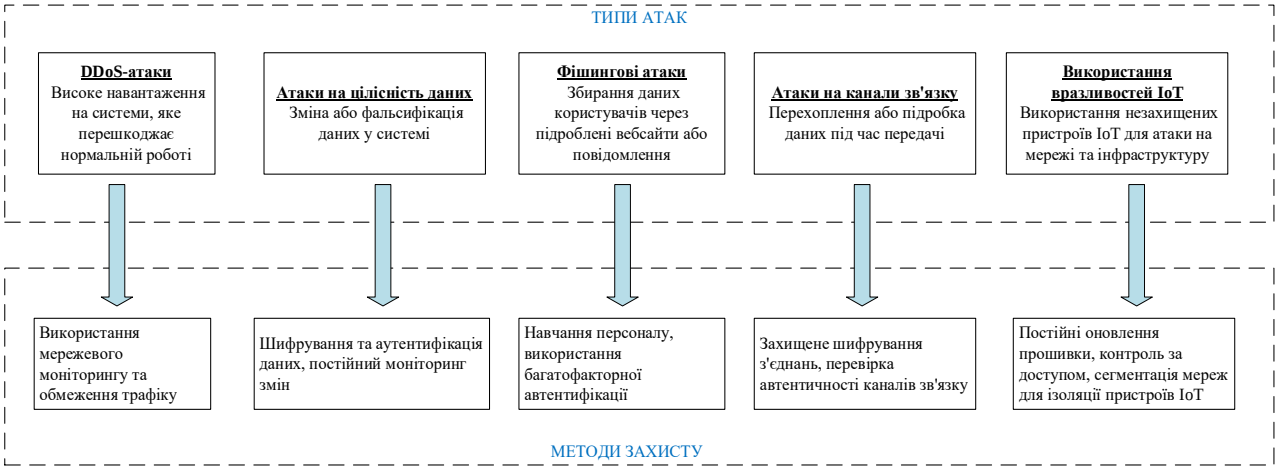

Рис. 2. Методи захисту від атак на СКФС.

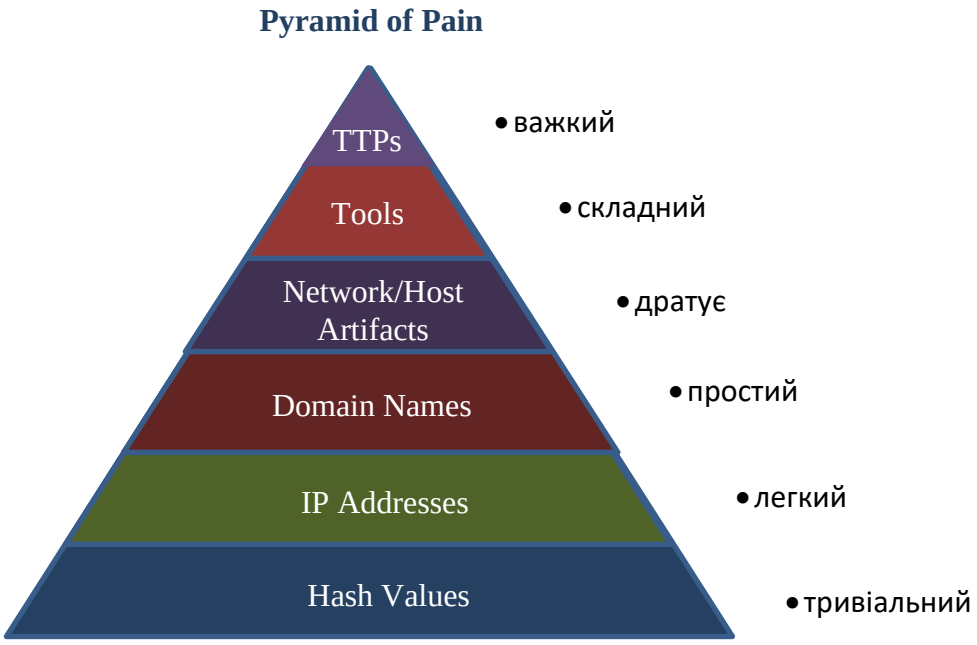

Рис. 3. Піраміда безпеки [13].

Для аналізу існуючих методів захисту в соціокіберфізичних системах необхідно враховувати і функціональні можливості кожного елемента інфраструктури цих систем. Такий

© Дженюк, Н. В. (2024). Методологічні основи захисту в соціокіберфізичних системах. Сучасний захист інформації, 4(60), 16–29. https://doi.org/10.31673/2409-7292.2024.040002.

підхід акцентує увагу на розробці нових багаторівневих і багатоконтурних систем безпеки, здатних ефективно протистояти сучасним векторним кібератакам (Рис. 4).

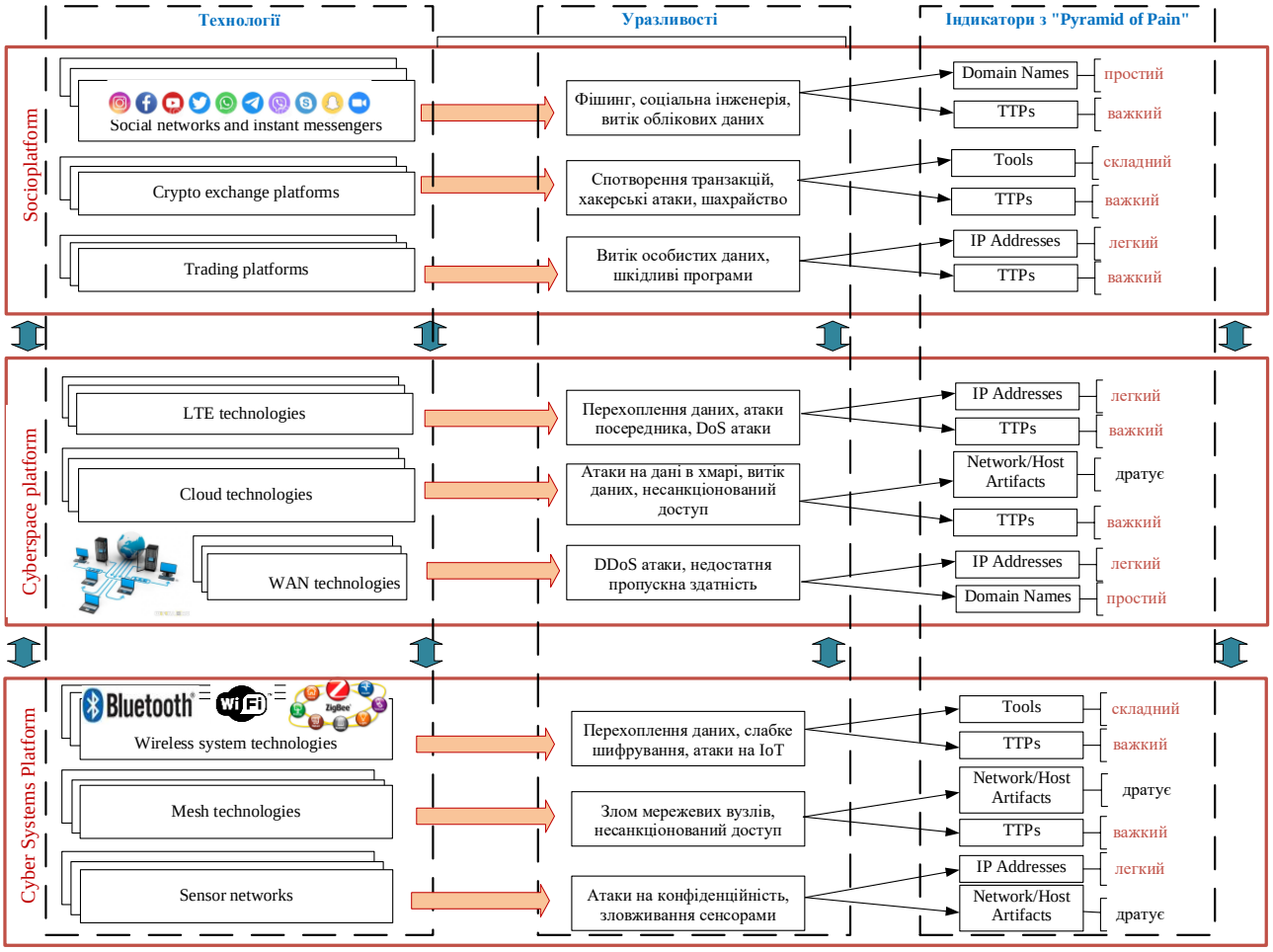

Рис. 4. Вразливості та захисні механізми для соціокіберфізичних систем

На рис. 4 зображена структурно-логічна схема, що демонструє вразливості та захисні механізми соціокіберфізичних систем із урахуванням рівнів складності для зловмисників при блокуванні чи обмеженні різних індикаторів кіберзагроз, таких як геш-значення, тактики, техніки та процедури (TTPs). Ця схема дозволяє оцінювати інтеграцію соціальних ресурсів і кіберпростору як сукупність технологій, що використовуються в окремих компонентах таких платформ, як соціальні мережі, кіберпростір і кіберфізичні мережі.

Socioplatform є найбільш уразливою для соціальної інженерії та атак на облікові дані, при цьому такі індикатори, як Domain Names та TTPs, грають ключову роль у виявленні атак.

Cyberspace platform стикається з ризиками на рівні мережевих технологій, таких як хмара та LTE. Індикатори, як-от Network/Host Artifacts і TTPs, є важливими для аналізу атак на ці платформи.

Cybersystem platform має ризики, пов'язані з IoT і бездротовими технологіями, зокрема слабке шифрування та несанкціонований доступ до сенсорних мереж, де критичними є Tools і TTPs.

Моделі побудови систем захисту соціокіберфізичних систем

Моделі побудови систем захисту соціокіберфізичних систем (СКФС) орієнтовані на розробку інтегрованих рішень, які гарантують стійкість, гнучкість і надійний захист фізичних, кібернетичних і соціальних елементів. Процес синтезу базується на багаторівневій архітектурі, врахуванні ризиків та застосуванні сучасних методологій і технологій (Рис. 5).

© Дженюк, Н. В. (2024). Методологічні основи захисту в соціокіберфізичних системах. Сучасний захист інформації, 4(60), 16–29. https://doi.org/10.31673/2409-7292.2024.040002.

Також потрібно враховувати загрози для внутрішнього та зовнішнього контурів соціокіберфізичних систем [14–16].

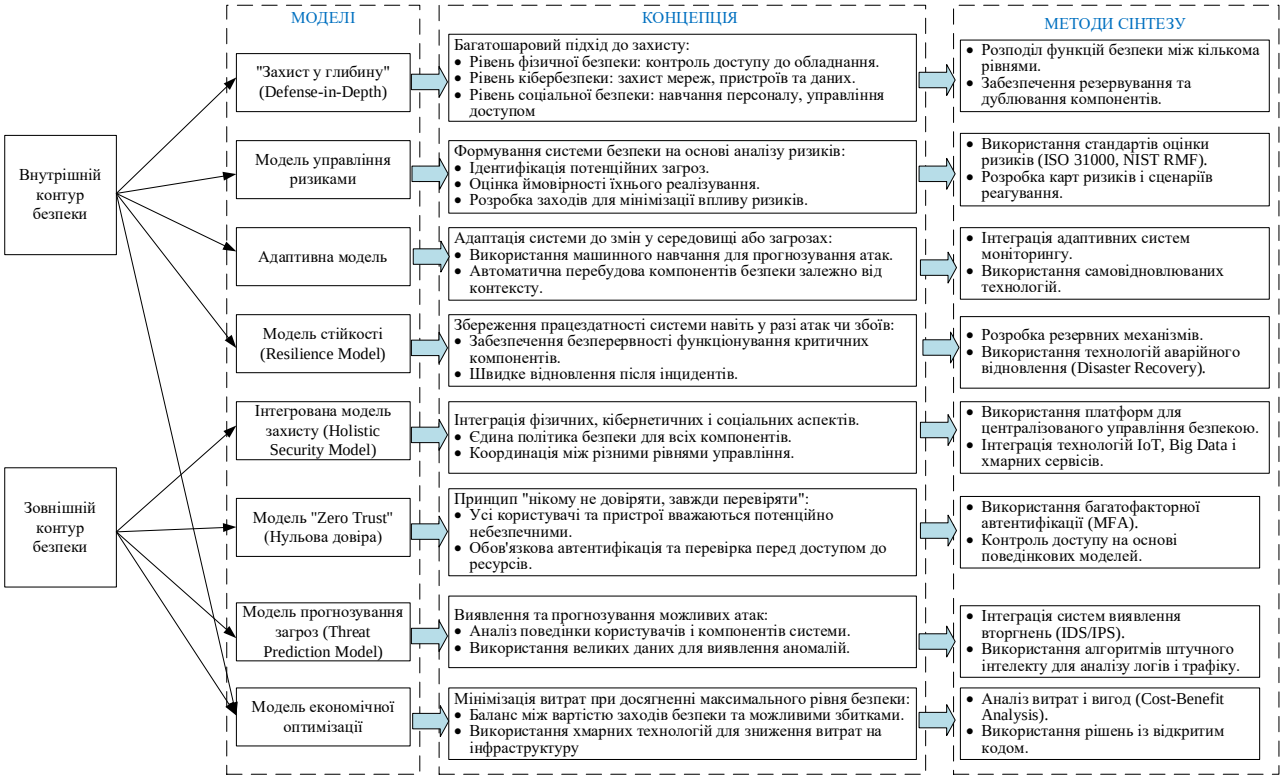

Рис. 5. Моделі систем захисту СКФС

Модель “Захист у глибину”. Модель “Захист у глибину” передбачає багатошаровий підхід, де кожен рівень захисту працює автономно, але разом формує міцний бар’єр для загроз. Першим рівнем є *фізична безпека*, що забезпечує захист інфраструктурних компонентів, таких як сервери, комунікаційні пристрої або кабельні з’єднання. Другий рівень охоплює *кібербезпеку*, спрямовану на захист мереж, даних та пристроїв від загроз. На цьому етапі використовуються такі заходи, як шифрування даних, впровадження систем виявлення та запобігання вторгненням (IDS/IPS), а також регулярне сканування на вразливості. Третім рівнем є *соціальна безпека*, яка враховує людський фактор. Тут важливу роль відіграє навчання персоналу основам кібергігієни, зокрема уникненню фішингових атак і застосуванню складних паролів. Окрім того, запроваджуються політики управління доступом, такі як багатофакторна автентифікація, яка ускладнює доступ до системи для зловмисників навіть у разі компрометації пароля [17–18].

Модель управління ризиками. Модель управління ризиками базується на проактивному аналізі ризиків, який включає ідентифікацію загроз, оцінку їхньої ймовірності та розробку заходів для мінімізації впливу. Ця модель дозволяє враховувати як технічні аспекти, так і організаційні фактори, створюючи комплексну систему захисту. У соціокіберфізичних системах, які характеризуються високим рівнем інтеграції технологій та людського фактору, така модель дозволяє зосередити ресурси на захисті найбільш критичних компонентів. В цій моделі формування системи безпеки складається з трьох етапів – ідентифікація загроз, оцінка ймовірності реалізації загроз та розробка заходів для мінімізації ризиків [19–21].

Адаптивна модель. Адаптивна модель безпеки базується на здатності систем динамічно реагувати на зміни в середовищі, поведінці користувачів або характері загроз. Головною особливістю адаптивної моделі є її інтерактивність і можливість самонавчання. Система

використовує алгоритми машинного навчання (ML) для аналізу великих обсягів даних у реальному часі [22]. Система також автоматично перебудовує свої компоненти, зокрема змінює конфігурацію міжмережевих екранів, оновлює політики доступу або перенаправляє трафік у разі виявлення проблемних вузлів. Ця здатність до динамічної трансформації робить адаптивну модель особливо ефективною для середовищ із високим рівнем змін [17].

Модель стійкості (Resilience Model). Основна концепція моделі стійкості (Resilience Model) полягає у здатності системи забезпечувати безперервне функціонування навіть під час атак, технічних збоїв чи непередбачуваних подій. Одним із ключових принципів моделі є забезпечення безперервності функціонування критично важливих компонентів. Для цього впроваджується сегментація системи, що дозволяє ізолювати важливі елементи від менш значущих, а також механізми пріоритизації ресурсів [23].

Інтегрована модель захисту (Holistic Security Model). Інтегрована модель захисту передбачає створення єдиної політики безпеки, яка охоплює всі аспекти функціонування СКФС. Це означає, що правила та процедури безпеки повинні бути уніфікованими для фізичних, кібернетичних і соціальних складових системи. Такий підхід дозволяє уникнути розрізнених методів забезпечення захисту, які часто стають причиною вразливостей через недостатню координацію між різними підсистемами.

Інтеграція технологій IoT (інтернету речей), Big Data і хмарних сервісів є ще одним важливим аспектом. IoT використовується для моніторингу фізичних компонентів системи, наприклад, завдяки датчикам руху чи температури, які працюють у режимі реального часу. Технології Big Data дозволяють аналізувати великі обсяги даних, що надходять від цих сенсорів, а також прогнозувати потенційні загрози. Машинне навчання допомагає оцінювати поведінкові дані користувачів, дозволяючи своєчасно ідентифікувати підозрілі дії. Хмарні сервіси забезпечують централізоване зберігання даних, резервне копіювання та оперативний доступ до необхідних ресурсів навіть у випадку фізичних пошкоджень інфраструктури [18].

Модель “Zero Trust” (Нульова довіра). Модель “Zero Trust”, або “Нульова довіра” базується на принципі, що жодному користувачу чи пристрою не можна довіряти без попередньої перевірки, незалежно від того, чи вони перебувають усередині, чи поза межами мережі організації. У цьому підході кожен запит на доступ ретельно перевіряється, а ресурси стають доступними лише за умови відповідності строгим правилам безпеки. Це дозволяє зменшити ризики як зовнішніх, так і внутрішніх загроз [24–25].

Модель прогнозування загроз (Threat Prediction Model). Модель прогнозування загроз спрямована на проактивне виявлення потенційних кіберзагроз, дозволяючи запобігти атакам ще до їхньої реалізації. Цей підхід базується на аналізі поведінки користувачів, компонентів системи та виявленні аномалій за допомогою технологій роботи з великими даними. Завдяки цьому організації можуть ефективно підвищувати стійкість своїх інформаційних систем [26–28].

Модель економічної оптимізації. Модель економічної оптимізації в кібербезпеці спрямована на досягнення високого рівня захисту при мінімальних витратах. Цей підхід базується на ретельному аналізі витрат і вигод, а також на впровадженні технологій, які дозволяють знизити витрати без втрати ефективності захисту.

СКФС – це складні інтегровані платформи, які знаходять широке застосування в таких галузях, як енергетика, транспорт, медицина й промисловість. Захист цих систем потребує особливого підходу, який враховує технічні, організаційні й людські фактори. Методологічні основи забезпечення безпеки СКФС базуються на комплексному підході, що включає інтеграцію різних підходів і технологій (Рис. 6).

Основою захисту СКФС є *системний підхід*, який розглядає безпеку як комплекс взаємопов’язаних заходів, спрямованих на інтеграцію всіх компонентів системи. Це включає врахування ризиків на технічному, соціальному й організаційному рівнях. Крім того, створення моделей загроз, які враховують специфіку кожного компонента, дозволяє прогнозувати потенційні атаки та розробляти ефективні стратегії їх запобігання. Ефективний

© Дженюк, Н. В. (2024). Методологічні основи захисту в соціокіберфізичних системах. Сучасний захист інформації, 4(60), 16–29. https://doi.org/10.31673/2409-7292.2024.040002.

захист СКФС базується на детальному *аналізі ризиків*. Для цього використовуються такі методи, як оцінка ризиків за стандартами ISO 31000 або NIST, а також SWOT-аналіз безпеки. Визначення ймовірності атак і наслідків від них допомагає розробити стратегії мінімізації ризиків [19].

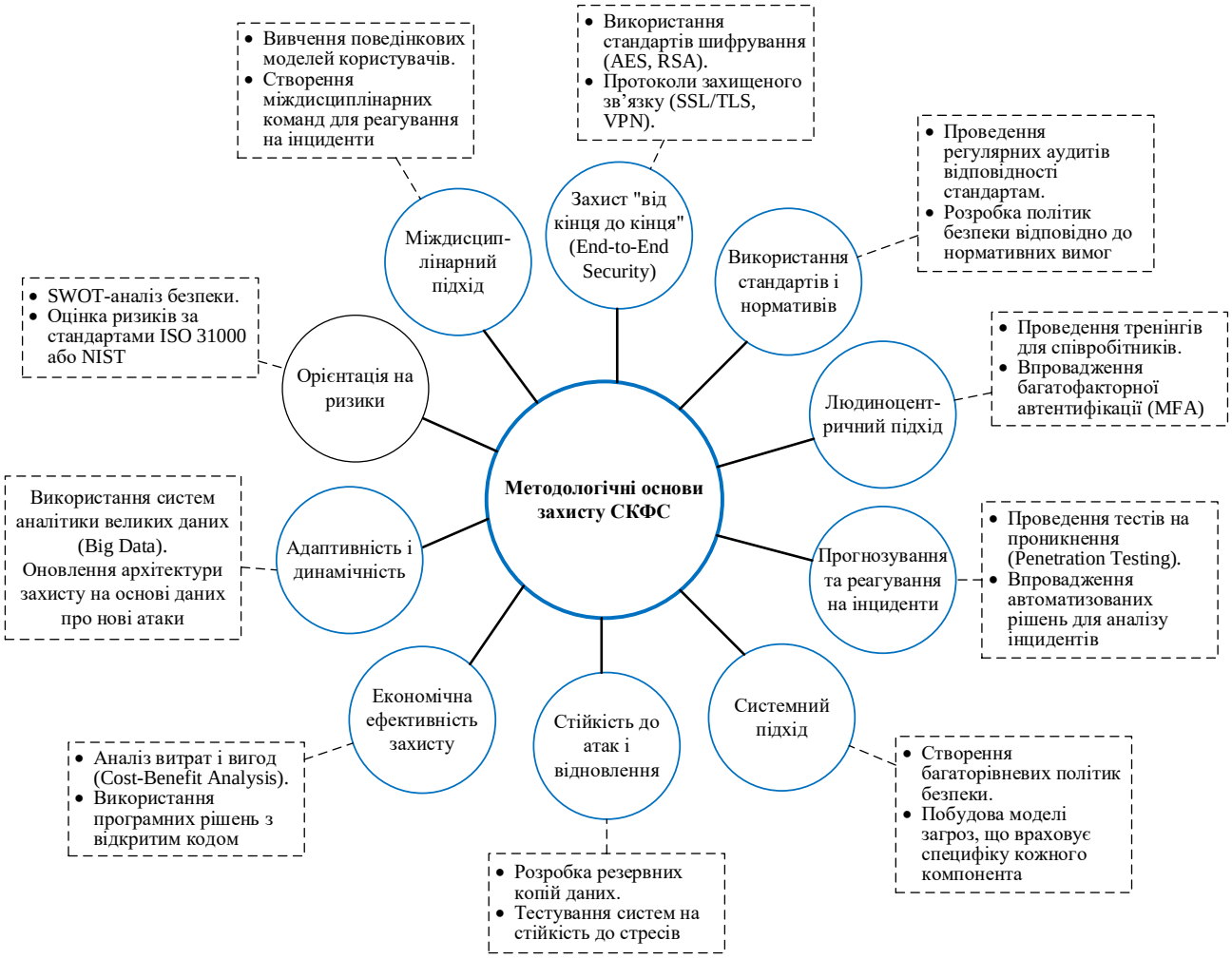

Рис. 6. Основні методологічні основи захисту СКФС

СКФС об'єднують не лише технічні компоненти, але й соціальні й організаційні аспекти, тому захист вимагає *залучення експертів із різних галузей*. Інженери займаються розробкою технічних рішень, соціологи вивчають вплив людського фактора, а економісти аналізують фінансову доцільність заходів. Міждисциплінарні команди, які працюють над реагуванням на кіберінциденти, можуть оперативно адаптуватися до нових загроз, комбінуючи знання з різних сфер. Сучасні загрози еволюціонують з високою швидкістю, тому системи захисту повинні бути *адаптивними*. Регулярне оновлення політик і технологій дозволяє оперативно реагувати на нові виклики. Використання технологій машинного навчання забезпечує прогнозування атак, аналіз великих даних (Big Data) і оновлення архітектури захисту на основі нових відомостей про загрози.

Одним із ключових принципів є *забезпечення захисту на всіх етапах життєвого циклу* даних і компонентів системи. Це включає шифрування даних, захист комунікацій між компонентами та багатофакторну автентифікацію користувачів.

Людський фактор залишається одним із найважливіших елементів безпеки. Навчання користувачів базовим принципам кібергігієни, проведення тренінгів і впровадження

© Дженюк, Н. В. (2024). Методологічні основи захисту в соціокіберфізичних системах. Сучасний захист інформації, 4(60), 16–29. https://doi.org/10.31673/2409-7292.2024.040002.

багатофакторної автентифікації (MFA) знижують ризики, пов'язані з атаками соціальної інженерії.

Міжнародні стандарти, такі як ISO/IEC 27001, NIST Cybersecurity Framework та IEC 62443, задають чіткі вимоги до забезпечення безпеки СКФС. Їх дотримання дозволяє створювати системи захисту, які відповідають найвищим вимогам і можуть бути перевірені на відповідність під час аудитів [17].

Ефективний захист включає не лише запобігання атакам, але й *швидке реагування на інциденти*. Системи виявлення вторгнень (IDS/IPS), плани реагування на інциденти (IRP) і автоматизовані аналітичні рішення дозволяють зменшити час реакції та мінімізувати наслідки атак.

Ефективний захист повинен відповідати реальним можливостям організації. Використання хмарних рішень та програм із відкритим кодом дозволяє знизити витрати без втрати якості. Аналіз витрат і вигод (Cost-Benefit Analysis) допомагає визначити *оптимальний рівень інвестицій у безпеку*.

Резервування критичних компонентів, створення резервних копій даних і *тестування систем на стійкість* дозволяють забезпечити працездатність навіть у разі успішної атаки.

Одним із найбільших викликів є забезпечення безпеки сервісів, оскільки вони становлять точку взаємодії між користувачами, інформаційними ресурсами та мережами. До того ж, ці сервіси можуть бути вразливими до цільових атак, які комбінуються з методами соціальної інженерії, що використовуються для введення в оману користувачів і забезпечення доступу до критично важливих даних. Враховуючи цей контекст, важливо класифікувати сервіси за моделями синтезу систем безпеки СКФС, що дозволить більш точно визначити рівень їхньої вразливості та відповідні механізми захисту від потенційних загроз (Табл. 2).

Забезпечення безпеки сервісів у соціокіберфізичних системах набуває особливого значення, оскільки кожен із них виконує унікальну роль у загальній інфраструктурі. Наприклад, смарт-міста, Інтернет речей (IoT), автоматизовані виробничі системи, медичні інформаційні системи, інтелектуальні транспортні системи, хмарні платформи та мобільні безпровідні мережі з БПЛА характеризуються специфічними вразливостями та рівнем загроз. Їхня взаємодія між користувачами, інформаційними ресурсами та мережами створює критичні точки доступу для потенційних атак.

У цьому контексті концепція "Pyramid of Pain" є ефективним інструментом для аналізу. Вона дозволяє оцінити рівень складності для зловмисників у виконанні атак залежно від типу системи. Наприклад, хмарні платформи можуть бути вразливими до атак на доступність та цілісність даних, тоді як мобільні безпровідні мережі з БПЛА схильні до ризиків перехоплення і маніпуляції сигналами (Табл. 3).

При розрахунку загального рівня безпеки системи враховуються рівні складності впровадження заходів безпеки з урахуванням критеріїв із "Pyramid of Pain" (1).

$$S = \sum_{i=1}^{n} \omega_i \cdot V_i, \tag{1}$$

де S – загальний рівень безпеки системи, залежить від рівня впливу кожного механізму безпеки та від типу системи,

ω_i – ваговий коефіцієнт впливу i-го рівня загрози (визначається значимістю рівня з Pyramid of Pain),

V_i – оцінка вразливості i-го рівня (тривіальна = 1, легка = 2, проста = 3, неприємна = 4, складна = 5, важка = 6),

n – кількість рівнів (у нашому випадку 6).

Такий підхід забезпечує цілісний погляд на вразливості соціокіберфізичних систем, враховуючи різні рівні ризиків для кожного сервісу. Він сприяє розробці адаптивних механізмів кіберзахисту, які відповідають конкретним потребам і особливостям кожного типу системи, підвищуючи їхню стійкість до цільових атак і методів соціальної інженерії.

© Дженюк, Н. В. (2024). Методологічні основи захисту в соціокіберфізичних системах. Сучасний захист інформації, 4(60), 16–29. https://doi.org/10.31673/2409-7292.2024.040002.

Таблиця 2

Таблиця моделей синтезу систем безпеки СКФС із вразливостями

Модель	Сервіси	Можливі вразливості
“Захист у глибину”	Фізична безпека, кібербезпека, соціальна безпека	Вразливі фізичні точки (доступ до обладнання), недостатній контроль доступу в мережах, атаки соціальної інженерії, недотримання політик користувачами.
Управління ризиками	Аналіз ризиків, побудова сценаріїв реагування	Недостатнє врахування загроз, неточна оцінка ризиків, відсутність сценаріїв реагування на рідкісні, але критичні події.
Адаптивна модель	Системи моніторингу, машинне навчання	Недостатня якість даних для навчання, помилкові спрацьовування, складність у забезпеченні своєчасної адаптації систем.
Модель стійкості	Критичні сервіси, резервування компонентів	Вразливості в резервних механізмах, затримки у відновленні, недостатня стійкість до багатовекторних атак.
Інтегрована модель захисту	Платформи централізованого управління, IoT, Big Data, хмарні сервіси	Вразливості IoT-пристроїв, слабкі місця в обробці великих даних, несанкціонований доступ до хмарних платформ, конфлікти політик між різними рівнями системи.
“Zero Trust”	Системи автентифікації, поведінкові моделі	Недостатньо надійні механізми перевірки, відсутність багатофакторної автентифікації, ризики компрометації облікових записів, уразливості в системах обробки поведінкових даних.
Прогнозування загроз	IDS/IPS, аналіз логів і трафіку	Низька якість аналізу через недостатні дані, пропущені атаки через недостатню швидкість обробки, помилкові позитивні спрацювання.
Економічна оптимізація	Хмарні сервіси, рішення з відкритим кодом	Недостатній захист хмарних платформ, вразливості у програмному забезпеченні з відкритим кодом, економія на критичних компонентах безпеки.

Таблиця 3

Рівень вразливості та складність застосування механізмів кіберзахисту

Механізми безпеки	**Смарт-міста**	**Інтернет речей (IoT)**	**Автоматизовані виробничі системи**	**Медичні інформаційні системи**	**Інтелектуальні транспортні системи**	**Хмарні платформи**	**Мобільні безпровідні мережі з БПЛА**
Геш-значення (Hash Values)	Низька (Тривіальна)	Середня (Тривіальна)	Середня (Тривіальна)	Низька (Тривіальна)	Низька (Тривіальна)	Середня (Тривіальна)	Середня (Тривіальна)
IP-адреси (IP Addresses)	Середня (Легка)	Середня (Легка)	Середня (Легка)	Низька (Легка)	Низька (Легка)	Середня (Легка)	Середня (Легка)
Домени (Domain Names)	Середня (Проста)	Середня (Проста)	Середня (Проста)	Середня (Проста)	Низька (Проста)	Середня (Проста)	Середня (Проста)
Артефакти мережі/хосту (Network/Host Artifacts)	Середня (Неприємна)	Висока (Неприємна)	Висока (Неприємна)	Середня (Неприємна)	Середня (Неприємна)	Висока (Неприємна)	Висока (Неприємна)
Інструменти (Tools)	Середня (Складна)	Висока (Складна)	Висока (Складна)	Висока (Складна)	Середня (Складна)	Висока (Складна)	Висока (Складна)
Тактики/техніки/процедури (TTPs)	Висока (Важка)	Висока (Важка)	Висока (Важка)	Висока (Важка)	Висока (Важка)	Висока (Важка)	Висока (Важка)

Таблиця відображає рівень вразливості та складність застосування механізмів кіберзахисту для різних типів соціокіберфізичних систем із врахуванням їхніх особливостей. Одним із найпростіших індикаторів компрометації є геш-значення. Вони легко змінюються зловмисниками, тому захист на основі гешування є тривіальним і забезпечує низький рівень безпеки для більшості платформ. Схожа ситуація спостерігається і з IP-адресами та доменами.

© Дженюк, Н. В. (2024). Методологічні основи захисту в соціокіберфізичних системах. Сучасний захист інформації, 4(60), 16–29. https://doi.org/10.31673/2409-7292.2024.040002.

Блокування IP-адрес або доменів може тимчасово обмежити доступ зловмисників, проте такі заходи є лише частковим рішенням, адже зловмисники швидко змінюють або реєструють нові ресурси.

Складнішими для обходу є мережеві або хост-артефакти, які дозволяють виявляти сліди діяльності атакуючих. Їхнє використання вимагає більш розвинених технологій і процедур для ефективного захисту. Більше того, обмеження доступу до спеціалізованих інструментів для атак значно ускладнює діяльність зловмисників. Водночас найвищий рівень складності становлять тактики, техніки та процедури (TTPs). Їх блокування створює серйозні перешкоди для зловмисників, адже зміна цих параметрів вимагає великих зусиль і ресурсів. У соціокіберфізичних системах, таких як мобільні безпровідні мережі з БПЛА, важливу роль відіграє автентифікація. Вона забезпечує надійний захист, запобігаючи несанкціонованому доступу до ключових компонентів, таких як дрони або базові станції. Аналіз мережевих артефактів і блокування інструментів атак також є ефективними заходами захисту для цих систем, які використовуються в умовах високих вимог до безперебійності та безпеки.

Дослідження показало, що найефективніший кіберзахист досягається через багаторівневий підхід, який поєднує базові заходи, як-от аналіз геш-значень, із більш складними методами, зокрема виявленням TTPs. Цей підхід дозволяє зменшити ризики для всіх типів платформ, враховуючи їхню специфіку, і підвищити стійкість до кіберзагроз.

Висновки

У статті проведено аналіз існуючих методів захисту соціокіберфізичних систем і їх компонентів. В результаті дослідження було встановлено, що для зниження ризиків атак та підвищення стійкості соціокіберфізичних систем (СКФС) необхідно застосовувати принципи забезпечення безпеки та ефективного управління безпекою, які враховують всі рівні взаємодії між фізичними, кібернетичними та соціальними компонентами системи. Проаналізовано основні вразливості СКФС на кожному з рівнів, зокрема ризики, пов’язані з атаками соціальної інженерії, компрометацією даних, перехопленням інформації та багатовекторними атаками. Застосування багаторівневих підходів до захисту, що охоплюють як внутрішні, так і зовнішні контури системи, є найбільш ефективним для забезпечення безпеки. Модель класифікації індикаторів компрометації “The Pyramid of Pain” продемонструвала важливість використання різних рівнів індикаторів для виявлення зловмисних дій. Доведено необхідність адаптивності систем кібербезпеки, які повинні бути здатними до динамічної перебудови та реагування на нові виклики. Використання алгоритмів машинного навчання для аналізу великих обсягів даних у реальному часі дозволяє своєчасно виявляти аномалії та прогнозувати потенційні загрози. Застосування криптографічних методів забезпечує конфіденційність і цілісність даних навіть у разі перехоплення. Системи виявлення та запобігання вторгненням ефективно виявляють спроби несанкціонованого доступу та блокують загрози на ранніх етапах. Окрему увагу приділено концепції “нульової довіри” (Zero Trust), яка передбачає ретельну перевірку кожного запиту на доступ незалежно від джерела. Такий підхід мінімізує ризики компрометації внутрішніх систем і підвищує рівень загальної безпеки.

Результати дослідження підтвердили, що комплексний, багаторівневий та адаптивний підхід до захисту СКФС є найефективнішим у сучасних умовах. Він дозволяє знижувати ризики атак, підвищувати рівень захисту даних і забезпечувати безперервне функціонування критичної інфраструктури навіть в умовах технічних збоїв або кібератак.

Перелік посилань

1. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC Technology Center, 2023. – 168 p. https://doi.org/10.15587/978-617-7319-72-5

2. Шиян, А. “Методологія комплексного захисту людини та соціальних груп від негативного інформаційно-психологічного впливу”, Інформаційна безпека, № 1(22), с. 94 – 98, 2016.

3. Scheau, C., Arsene A., and Dinca G. “Phishing and e-commerce: an information security management problem”, Journal of Defence Resources Management, vol.7, № 1 (12), pp. 129 – 140, 2016.

© Дженюк, Н. В. (2024). Методологічні основи захисту в соціокіберфізичних системах. Сучасний захист інформації, 4(60), 16–29. https://doi.org/10.31673/2409-7292.2024.040002.

4. Lezoche, M., Panetto, H. Cyber-Physical Systems, a new formal paradigm to model redundancy and resiliency. Enterprise Information Systems. 1–22 (2018), https://doi.org/10.1080/17517575.2018.1536807.

5. Дудикевич, В. Б., Микитин, Г. В., Бортнік, Л. Л., Стосик, Т. Р. Методологія безпеки кіберфізичних систем та інтернету речей в інтелектуалізації об'єктів інфраструктури. Computer systems and network. Vol. 6, No. 1, 2024. P. 44-53. https://doi.org/10.23939/csn2024.01.044.

6. Dzheniuk, N., Yevseiev, S., Lazurenko, B., Serkov, O., & Kasilov, O. (2023). A Method of protecting information in cyber-physical space. Advanced Information Systems, 7(4), 80–85. https://doi.org/10.20998/2522-9052.2023.4.11

7. Дудикевич, В. Б., Микитин, Г. В., Галунець, М. О. Системна модель інформаційної безпеки "Розумного міста". Системи обробки інформації, 2020, випуск 2 (161) С. 93-98. https://doi.org/10.30748/soi.2020.161.11

8. Pohasii, S., Milevskyi, S., Tomashevsky, B., & Voropay, N. (2022). Development of the double-contour protection concept in socio-cyberphysical systems. Advanced Information Systems, 6(2), 57–66. https://doi.org/10.20998/2522-9052.2022.2.10

9. Yevseiev, S., Milevskyi, S., Bortnik, L., Alexey, V., Bondarenko, K., Pohasii, S. Socio-Cyber-Physical Systems Security Concept. 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications. June 9-11, 2022, Ankara, Turkey. https://doi.org/10.1109/HORA55278.2022.9799957

10. Zuoguang Wang, Hongsong Zhu, and Limin Sun. 2021. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. IEEE Access 9 (2021), 11895–11910. https://doi.org/10.1109/ACCESS.2021.3051633

11. Бурячок, В. Л. Основи формування державної системи кібернетичної безпеки: монографія/ В. Л. Бурячок. – К.: НАУ, 2013. – 432 с.

12. Wang, L. Sun, and H. Zhu, "Визначення соціальної інженерії у кібербезпеці", IEEE Access, vol. 8, стр. 85094–85115, 2020, https://doi:10.1109/access.2020.2992807.

13. Nataliia Dzheniuk, Serhii Yevseiev, Stanislav Milevskyi, Natalya Voropay, Roman Korolov. Sociocyberphysical system wireless air network topology synthesis model. Vol. 30 No. 1 (2024): Ukrainian Scientific Journal of Information Security. Pp. 51-57. https://doi.org/10.18372/2225-5036.30.18603

14. Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A.., Mykus, S., Milov, O.., Prokopenko, O., Sievierinov O., & Chopenko, D. (2021). Development of a concept for building a critical infrastructure facilities security system. Eastern-European Journal of Enterprise Technologies, 3(9(111), 63–83. https://doi.org/10.15587/1729-4061.2021.233533.

15. Androshchuk A., Yevseiev, S., Melenchuk, V., Lemeshko, O., & Lemeshko, V. (2020). Improvement of project risk assessment methods of implementation of automated information components of non-commercial organizational and technical systems. Eureka: Physics and Engineering, (1), 48-55. https://doi.org/10.21303/2461-4262.2020.001131/

16. Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC Technology Center, 2021. – 188 p. https://doi.org/10.15587/978-617-7319-31-2

17. NIST Cybersecurity Framework. Retrieved from https://www.nist.gov/cyberframework. Accessed: Nov. 20, 2024.

18. European Union Agency for Cybersecurity (ENISA). Good Practices for Security of Critical Information Infrastructures. ENISA Reports, 2018. https://doi.org/10.2824/800176.

10.Barabash O., Laptiev O., Grushina O. The conceptual model of the intelligent network. Сучасний захист інформації, No4 (56), 2023, P. 1-9. https://doi.org/ 10.31673/2409-7292.2023.030202

11.Король О.Г., Лаптєва Т.О., Метод використання кіберрозвідки для виявлення індикаторів компрометації на базі матриці Mitre Att&ck. Сучасний захист інформації. 2024. No 3(59). С.69-74. DOI: 10.31673/2409-7292.2024.03000720. NIST Risk Management Framework (RMF). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final. Accessed: November 20, 2024.

21. FAIR (Factor Analysis of Information Risk) – методологія кількісної оцінки ризиків. Retrieved from https://www.fairinstitute.org/. Accessed: November 20, 2024.

22. Лахно В. А. Побудова адаптивної системи розпізнавання кіберзагроз на основі нечіткої кластерізації ознак / В. А. Лахно // Східно-Європейський журнал передових технологій. - 2016. - № 2(9). - С. 18-25. - Режим доступу: http://nbuv.gov.ua/UJRN/Vejpte_2016_2%289%29__3

23. Дробик О. В., Лаптєв О. А., Пархоменко І. І., Богуславська О. В., Пепа Ю. В., Пономаренко В. В. Розпізнавання радіосигналів на основі апроксимації спектральної функції у базисі передатних функцій резонансних ланок другого порядку. Сучасний захист інформації. 2024. №2. С.13-23.

24. Microsoft Zero Trust Model. Офіційний сайт. Retrieved from https://www.microsoft.com/security/business/zero-trust. Accessed: November 20, 2024.

25. Zscaler Zero Trust Exchange. Офіційний сайт. Retrieved from https://www.zscaler.com/solutions/zero-trust. Accessed: November 20, 2024.

26. Splunk. Офіційний сайт. Retrieved from https://www.splunk.com. Accessed: November 20, 2024.

27. Snort. Офіційний сайт. Retrieved from https://www.snort.org. Accessed: November 20, 2024.

28. Palo Alto Networks. Офіційний сайт. Retrieved from https://www.paloaltonetworks.com. Accessed: November 20, 2024.

Надійшла 24.11.2024