КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.24.229240
УДК 004.056:620.9

Скіцько Олексій Іванович
к.т.н., старший науковий співробітник
Національна академія Служби безпеки України, Київ, Україна
ORCID ID: 0000-0003-4122-0889
oiskitsko@gmail.com

Ширшов Роман Анатолійович
науковий співробітник
Національна академія Служби безпеки України, Київ, Україна
ORCID ID: 0000-0003-3534-8736
signorum@gmail.com

ПОВЕРХНЯ АТАКИ В КОНТЕКСТІ ЇЇ КОРИСТУВАЧІВ («TREAT ACTORS») ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. У сучасному цифровому світі, де інформаційні технології є невід'ємною частиною життя, питання кібербезпеки стає все більш актуальним. Одним із ключових аспектів захисту інформаційних систем є управління поверхнею атаки, яка включає всі можливі точки входу для зловмисників. Формування та управління поверхнею атаки є складним завданням, яке потребує постійної уваги та вдосконалення. Зловмисні актори (загрозливі актори, суб'єкт загрози) (англ. threat actor) відіграють важливу роль у цьому процесі. Вони постійно шукають нові способи проникнення в системи, використовуючи різноманітні методи та техніки. Ці «актори» можуть бути різними за своїм походженням і мотивами: від кіберзлочинців, які переслідують фінансову вигоду, до державних «акторів», які здійснюють шпигунські та саботажні дії. Розуміння типів «зловмисних акторів» та їхніх методів важливо для ефективного управління поверхнею атаки. Зазначене допоможе вчасно виявити та усунути вразливості, покращити конфігурацію систем та мереж, підвищити обізнаність співробітників щодо сучасних кіберзагроз. У статті розглянуто ключові аспекти формування поверхні атаки, звертаючи увагу на роль «зловмисних акторів». Досліджено типи «зловмисних акторів», їхні методи та техніки, сформовано практичні рекомендації щодо зниження ризиків і покращення захисту інформаційних систем. Крім того, важливим є проведення регулярних аудитів безпеки, а також впровадження сучасних технологій захисту, таких як системи виявлення вторгнень, засоби шифрування даних та багатофакторна автентифікація. Таким чином, комплексний підхід до управління поверхнею атаки, який включає розуміння загрозових акторів, використання сучасних технологій захисту та постійне навчання персоналу, є ключовим для ефективного захисту інформаційних систем критичної інфраструктури.

Ключові слова: зловмисний актор; загрозливий актор; суб'єкт загрози; threat actor; поверхня атаки; об'єкт критичної інфраструктури (ОКІ); інтернет речей (IoT).

ВСТУП

У сучасному світі кібербезпеки велике значення має формування поверхні атаки об'єктів критичної інфраструктури, особливо з огляду на діяльність загрозових акторів. Ця стаття спрямована на аналіз компонентів поверхні атаки, які визначають вразливі місця систем і базуються на оцінці ризиків та вразливостей, що можуть впливати на внутрішню структуру критичних об'єктів. З розумінням цих компонентів можна ефективно виконати оцінку вразливостей та розробити стратегії усунення потенційних точок входу, зміцнюючи захист від можливих кібератак. Окрему увагу в роботі приділено класифікації загрозових акторів, що включає розгляд різноманітних типів зловмисників від незалежних хакерів до

організованих злочинних угруповань та державних акторів, їхні мотивації, методи та можливості впливу на об'єкти критичної інфраструктури.

Постановка проблеми. У сфері кібербезпеки, поняття «поверхня атаки» є ключовою для розуміння ризиків, з якими стикаються об'єкти критичної інфраструктури (ОКІ). Поверхня атаки включає всі потенційні точки входу, через які зловмисники можуть спробувати отримати доступ до системи або її компонентів. З постійним зростанням кількості кіберзагроз, належне управління поверхнею атаки стає все більш критичнішою. Найбільш впливовим чинником, який впливає на формування і використання поверхні атаки є «зловмисні актори» (threat actor), власне, «користувачі» поверхні атаки.

Аналіз останніх досліджень і публікацій. В роботах авторів [1] – [12] розглядаються питання формування поверхні атаки в залежності від можливої точки входу та пропонуються механізми запобігання атакам, пов'язані з використанням технічних та організаційних засобів в якості механізму реагування. Також автори наголошують, на необхідності категорування типів «Threat actors» та визначення потенціалу їх впливу на об'єкти критичної інфраструктури, зміщуючи акценти саме на потенціал «Threat actors» для більш проактивного реагування на атаки ОКІ.

Метою статті є аналіз теоретичних положень і практики діяльності суб'єктів загрози на поверхню атаки, розробка визначення «зловмисні актори», приведення структури можливих місць втручання в поверхню атаки. Наведено пропозиції щодо удосконалення діяльності підрозділів безпеки об'єктів критичної інфраструктури у протидії несанкціонованому втручанню до інформаційних ресурсів. Об'єкт дослідження — закономірності, які виникають у процесі діяльності працівників об'єктів критичної інфраструктури під час експлуатації комп'ютерних систем. Предмет дослідження — вплив «зловмисних акторів» на поверхню атаки об'єкта критичної інфраструктури.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Актуальність питання формування поверхні атаки та управління нею обумовлена рядом ключових факторів, серед яких особливу роль відіграють «зловмисні актори» («Threat actors»). В умовах, де інформаційні технології стали основою бізнес-процесів та особистих взаємодій, рівень кіберзагроз постійно зростає. Це, в свою чергу, підвищує важливість розуміння та управління поверхнею атаки для забезпечення безпеки інформаційних систем.

Фактори, що впливають на ефективність управління поверхнею атаки (рис. 1):

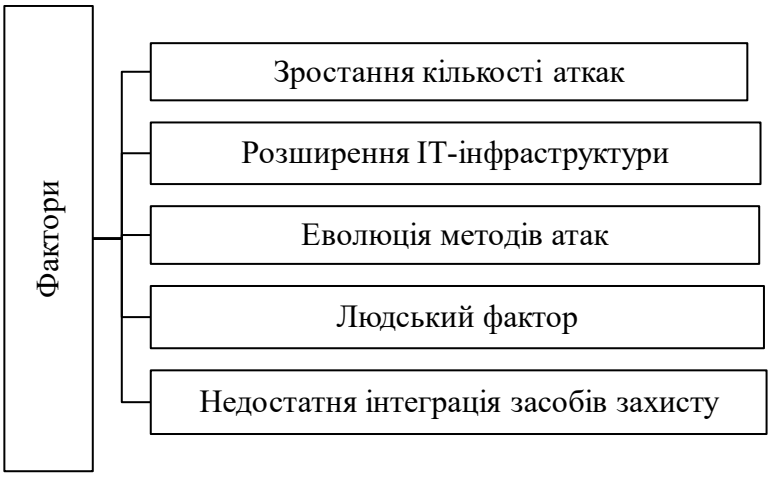

Рис. 1. Факторами впливу на ефективність управління поверхнею атаки

- *Зростання кількості атак.* Кількість кібератак постійно збільшується, і «загловмисні актори» стають дедалі витонченішими у своїх методах. Кіберзлочинці, хактивісти, «державні актори» та інсайдери використовують новітні технології та стратегії для проникнення в системи. З кожним роком спостерігається зростання кількості випадків фішингу, використання шкідливого програмного забезпечення, DDoS-атак та експлуатації вразливостей, що створює значні ризики для ОКІ;
- *Розширення IT-інфраструктури.* Зі збільшенням використання хмарних обчислень, інтернету речей (IoT) та мобільних пристроїв, поверхня атаки ОКІ постійно розширюється, що ускладнює процес ідентифікації та захисту можливих точок входу, враховуючи різноманітність та динамічність сучасних IT-середовищ;
- *Еволюція методів атак.* «Зловмисні актори» постійно вдосконалюють свої методи та техніки, що вимагає від ОКІ постійного оновлення засобів захисту. Зокрема, атаки типу «Zero-Day», які використовують невідомі вразливості, стають все більш поширеними та небезпечними і ускладнюють своєчасне виявлення та нейтралізацію загроз;
- *Людський фактор.* Інсайдерські загрози, соціальна інженерія та інші методи, які експлуатують людську психологію, залишаються одними з найскладніших для протидії. Навіть найкращі технічні заходи безпеки можуть бути недостатніми, якщо співробітники ОКІ не обізнані про сучасні кіберзагрози та не дотримуються політик безпеки;
- *Недостатня інтеграція засобів захисту.* Часто ОКІ використовують різні системи безпеки, які не інтегровані між собою, що ускладнює процес моніторингу та реагування на інциденти. Зазначене призводить до збільшення часу виявлення та нейтралізації атак, що може мати катастрофічні наслідки.

Враховуючи ці фактори, важливість ефективного управління поверхнею атаки стає очевидною. ОКІ повинні постійно вдосконалювати свої методи захисту, впроваджувати багаторівневі стратегії безпеки та підвищувати обізнаність співробітників щодо сучасних загроз. Тільки комплексний підхід до кібербезпеки, який враховує динамічність загроз та роль «зловмисних акторів», дозволить ефективно протидіяти кібератакам та забезпечити надійний захист інформаційних систем.

Розуміння та управління поверхнею атаки є критично важливими аспектами кібербезпеки, які впливають на здатність ОКІ захищати свої інформаційні системи від різноманітних загроз. Враховуючи динамічність і складність сучасного кіберсередовища, а також активну діяльність «зловмисних акторів» («Threat actors»), важливість цього питання стає очевидною з кількох причин, що можна охарактеризувати загальними вимогами до управління поверхнею атаки (рис. 2):

1. *Зниження ймовірності успішних атак.* Ефективне управління поверхнею атаки дозволить мінімізувати кількість точок входу для зловмисників. Виявлення та усунення вразливостей на ранніх етапах знижує ризик успішного проникнення «зловмисних акторів» у систему. Дозволить запобігти витоку конфіденційної інформації, фінансових втрат і порушення функціонування бізнесу.

2. *Забезпечення безперервності процесів.* Кіберзагрози можуть призвести до серйозних перебоїв у роботі ОКІ, включаючи зупинку виробничих процесів, втрату доступу до критичних даних та сервісів. Управління поверхнею атаки забезпечить стабільність та безперервність процесів, що особливо важливо для компаній, які залежать від постійного доступу до інформаційних систем.

3. *Дотримання регуляторних вимог.* Багато галузей мають суворі регуляторні вимоги щодо захисту даних та інформаційних систем. Недотримання цих вимог може призвести до штрафів, судових позовів та інших юридичних наслідків. Управління поверхнею атаки є важливою складовою відповідності таким вимогам, допомагаючи ОКІ уникнути правових проблем.

4. *Зменшення впливу «зловмисних акторів».* «Зловмисні актори» використовують різноманітні методи та техніки для здійснення атак, і їхні дії можуть мати серйозні наслідки для ОКІ. Розуміння поведінки «зловмисних акторів» та адаптація заходів безпеки під їхні методи допомагають знизити вплив атак та підвищити стійкість систем до загроз.

5. *Покращення загального рівня кібербезпеки.* Управління поверхнею атаки сприяє загальному підвищенню рівня кібербезпеки в ОКІ. Регулярне сканування вразливостей, оновлення програмного забезпечення, моніторинг систем та навчання персоналу сформують багаторівневу систему захисту, яка є ефективною проти різноманітних загроз.

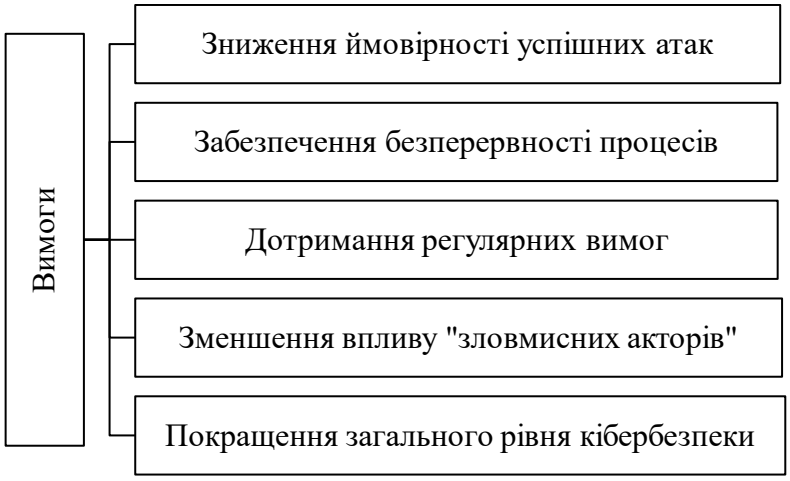

Рис. 2. Загальні вимоги до управління поверхнею атаки

Важливість питання формування та управління поверхнею атаки не можна переоцінити. Це ключовий елемент кібербезпеки, який дозволяє ОКІ ефективно захищати свої інформаційні активи від постійно змінюваних загроз. Застосування структурованих підходів до управління поверхнею атаки та врахування діяльності «зловмисних акторів» забезпечить надійний захист та стійкість інформаційних систем у сучасному кіберсередовищі.

Формування поверхні атаки залишається складним завданням з низкою проблем, що потребують рішення. Однією з головних проблем є динамічність IT-інфраструктури. З постійним впровадженням нових технологій, таких як хмарні обчислення, інтернет речей (IoT) та мобільні пристрої, поверхня атаки постійно змінюється та розширюється. Це ускладнює процес ідентифікації та управління всіма точками входу.

Людський фактор також залишається проблемою. Незважаючи на постійні тренінги, співробітники часто стають жертвами соціальної інженерії, що відкриває нові можливості для зловмисників. Недостатнє розуміння важливості кібербезпеки та нехтування політиками безпеки створюють додаткові ризики. Іншою критичною проблемою є швидка еволюція загроз. Зловмисники постійно розробляють нові методи атак, що робить традиційні методи захисту менш ефективними. Наприклад, атаки типу

«Zero-Day», які використовують невідомі вразливості, є особливо небезпечними, оскільки їх важко виявити та нейтралізувати завчасно.

Вразливості у програмному забезпеченні потребують постійної уваги. Незважаючи на регулярні оновлення та патчі, нові вразливості постійно виявляються, що створює ризик експлуатації. Особливо це стосується великих програмних комплексів, де навіть невеликі помилки можуть мати серйозні наслідки.

Ще однією важливою проблемою є недостатня інтеграція засобів захисту. Часто ОКІ використовують різні системи безпеки, які не інтегровані між собою, що ускладнює процес моніторингу та реагування на інциденти. Це призводить до збільшення часу виявлення та нейтралізації атак.

Окремо важливо відзначити проблему браку фахівців у галузі кібербезпеки. Зростання кількості загроз вимагає збільшення числа кваліфікованих спеціалістів, але попит перевищує пропозицію. Це призводить до перевантаження існуючих команд безпеки та зниження ефективності захисту.

Але основною проблемою для формування поверхні атаки є власне нападник — threat actor. (перекл. авт. «Зловмисний актор, загрозливий актор, суб'єкт загрози (англ. threat actor) — це особа або група осіб, яка має намір завдати шкоди системам або мережам Застосовують різноманітні методи та інструменти для досягнення своїх цілей, що включає в себе використання відкритих вразливостей у програмному забезпеченні, соціальну інженерію, а також фізичний доступ до системи») [3].

Управління поверхнею атаки вимагає комплексного підходу, який включає ідентифікацію, оцінку та мінімізацію кількості точок входу/виходу. Це також включає регулярне оновлення безпеки та проведення аудитів, щоб забезпечити, що жодна нова вразливість не залишиться непоміченою [4].

Враховуючи вищезазначене, важливо розуміти, що управління поверхнею атаки — це не разова дія, а постійний процес, який вимагає неперервного моніторингу, аналізу та вдосконалення систем безпеки.

Введення в експлуатацію, обслуговування та експлуатація будь якого об'єкта критичної інфраструктури цікавить різних осіб або груп (зловмисних), які разом називаються «зловмисними акторами». Ці суб'єкти, а також інші, зовнішні до нормальних операцій життєвого циклу, можуть мати як доброзичливі, так і зловмисні наміри.

Будь-який суб'єкт може представляти загрозу, виходячи зі своєї ролі та доступу [5]. «Актори» внутрішньої групи матимуть авторизований кібернетичний і фізичний доступ до інформаційної системи ОКІ через їхні звичайні робочі обов'язки. На відміну від цього, зовнішня група, за визначенням, не має авторизованого кібернетичного та фізичного доступу до активів інформаційної системи ОКІ. Деякі внутрішні актори повинні мати доступ (або кібернетичний, або фізичний) лише до конкретних заходів або контрактів. Наприклад, польовий технік повинен мати доступ лише під час контракту для конкретної інформаційної системи ОКІ. Однак, навіть після закінчення контракту, цей технік буде мати внутрішню інформацію про технології, архітектуру та операції інформаційної системи. Важливо, щоб ОКІ визнавали та відстежували цих осіб, щоб гарантувати, що вони не зберігають фізичного чи цифрового доступу, більше ніж це необхідно.

Об'єкти критичної інфраструктури повинні оцінювати свої процеси та процедури для підрядних організацій (наприклад, польові техніки, виробники оригінального обладнання [OEM], інтегратори) [6]. Теми для оцінювання включають управління тимчасовими кіберактивами, контроль документації інженерного проектування та специфікації обладнання для мережі та системи управління (наприклад, постачальник, модель, версія апаратного та програмного забезпечення). Прикладами тимчасових

кіберактивів є ноутбуки або інші пристрої для передачі даних, оцінки вразливостей, обслуговування або усунення неполадок. Ці тимчасові кіберактиви є значущими цілями для кібератак, оскільки вони можуть вводити доступ або шкідливе програмне забезпечення до інакше сегментованих мереж або обладнання, можуть не керуватися безпосередньо ОКІ, але навіть якщо ними керують треті сторони, OEM або інші внутрішні актори, ОКІ повинні бути обізнані про їх призначення та забезпечувати політику щодо їх взаємодії з системою.

Зазначене вище дає змогу виокремити наступні групи загроз та провести їх класифікацію (рис. 3):

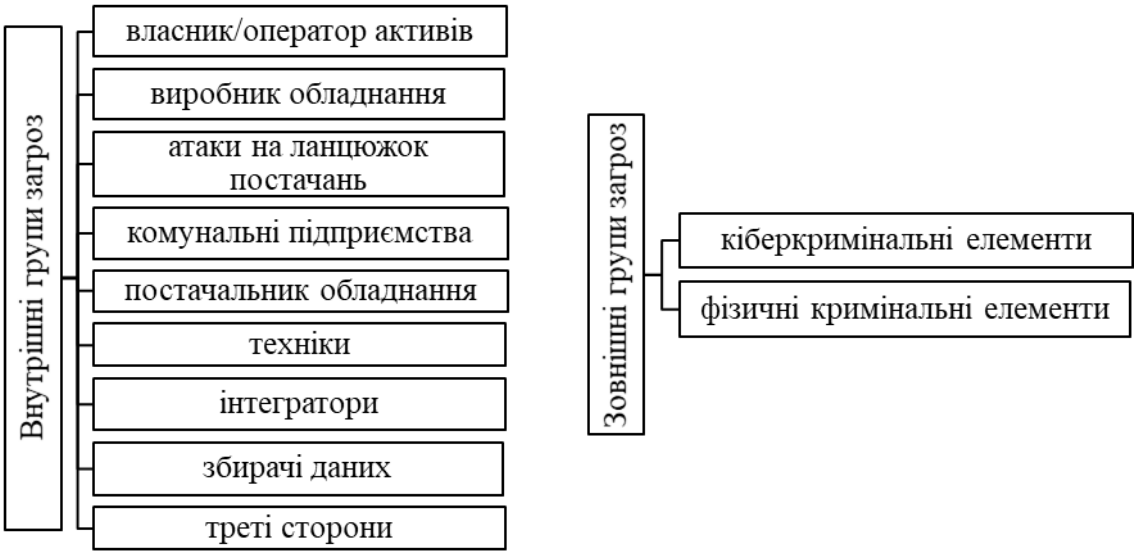

Рис. 3. Загальний класифікатор кіберзагроз

Внутрішні групи загроз:

Власник/оператор активів. Власник/оператор активів здійснює адміністративні операції ОКІ, і його співробітники можуть мати широкі та різноманітні обов'язки. ОКІ виконує контракти щодо своєї діяльності, підтримує договори оренди землі та забезпечує щоденні операції та технічне обслуговування. За своєю роллю, ОКІ підтримує як кібернетичний, так і фізичний доступ до своїх активів, але також має повноваження делегувати завдання та операції іншим організаціям (наприклад, власник активів укладає контракти на щоденні операції, а оператор укладає субпідряд на обслуговування обладнання в польових умовах). Через цю делегацію ОКІ може надавати як кібернетичний, так і фізичний доступ довіреним третім сторонам. Загалом вважається виключенням, що ОКІ може стати зловмисником, кілька занепокоєнь слід врахувати щодо цих груп. Незадоволений або підкуплений співробітник може поділитися критичною інформацією з зовнішніми сторонами, які можуть бути зловмисними. Співробітник може навіть не мати наміру надати доступ зовнішньому ворогу, але натиснувши на фішинговий електронний лист, може встановити шкідливе програмне забезпечення, яке надає противнику початковий доступ до інформаційної системи ОКІ. Зазначають, що найслабшою ланкою в безпеці для більшості ОКІ є люди, і люди з найвищим рівнем фізичного та кібернетичного доступу.

Виробник оригінального обладнання (OEM). OEM (англ. *Original equipment manufacture*) проєктують, будують та впроваджують обладнання для ОКІ. Ця група також включає субпідрядників, які підтримують установку під час будівництва. У

багатьох випадках ОКІ можуть укладати контракти з ОЕМ на довгострокову підтримку та технічне обслуговування своїх продуктів, що може забезпечити довгостроковий дистанційний доступ до інформаційних систем ОКІ для ОЕМ (і їх субпідрядників). ОКІ можуть також зіткнутися з певними вимогами гарантії на придбане обладнання, що вимагає від ОЕМ регулярного або періодичного доступу до обладнання. Нарешті, впровадження великих даних в галузі призвело до появи ряду послуг ОЕМ з моніторингу стану ОКІ. Персонал у цій категорії — наприклад, співробітники ОЕМ, постачальники за субпідрядом з ОЕМ, інтегратори — матимуть різні рівні кібернетичного та фізичного доступу до інформаційних систем ОКІ. Останніми роками спостерігалися цілеспрямовані атаки на ОЕМ, щоб отримати доступ до ОКІ.

Атаки на ланцюжок постачання. ОЕМ можуть бути скомпрометовані через атаку на ланцюжок постачання. Супротивник може почати атаку, скомпрометувавши процеси проектування, виробництва або доставки ОЕМ. Вони можуть навмисно ввести помилку в програмне забезпечення або встановити пристрій моніторингу в апаратне забезпечення. Ці атаки небезпечні, оскільки вони використовують довірчі відносини між ОЕМ і кінцевим користувачем. ОКІ повинні включати процес перегляду ланцюжка постачання як частину своєї перевірки нового обладнання або програмного забезпечення.

Комунальні підприємства. Співробітники комунальних підприємств, мають фізичний і, кібернетичний доступ до систем ОКІ під час нормальних операцій [7]. Цей доступ може також надавати їм фізичний і кібернетичний доступ до активів ОКІ залежно від конструкції. Нормальні бізнес-операції можуть включати запити від комунальних підприємств.

Постачальники обладнання для підстанцій та ОЕМ. Постачальники обладнання для підстанцій та виробники оригінального обладнання (ОЕМ) будуть знати обладнання, що використовується, і можуть мати віддалений доступ до обладнання на підставі контрактів. Атаки, які спрямовані на комунальні підприємства, можуть мати вплив на ОКІ, навіть якщо їх архітектура не є основною ціллю.

Техніки. Техніки можуть бути найняті для обслуговування різних клієнтів/контрагентів ОКІ. Техніки отримують тимчасовий дистанційний або локальний доступ до систем для технічного обслуговування або вирішення проблем. Техніки працюють як на короткострокових, так і на довгострокових контрактах. Техніки зберігатимуть внутрішні знання, але не повинні вважатися авторизованим персоналом поза періодом контракту. З точки зору кіберзагроз, техніки можуть не підпадати під стандарти безпеки, орієнтовані на комунальні підприємства, власників або постачальників. Через характер своєї роботи їм можуть також надаватися підвищені рівні доступу до інформаційних систем ОКІ. Залежно від політики контролю доступу хосту, цей доступ може або не може бути відкликаний, коли технік більше не перебуває на об’єкті. Обладнання, яке використовують техніки, і їхні облікові дані для доступу забезпечують нормальний доступ під час перебування на об’єкті та під час контракту, але якщо це обладнання є тимчасовим, це може представляти вищий ризик як вектор доступу для кібератак.

Інтегратори. Інтегратори ОКІ залучаються для проектування, будівництва або встановлення систем. Вони часто тісно співпрацюють як з ОЕМ, так і з підприємствами. Для виконання роботи їм потрібні знання системи та привілейований доступ для налаштування. Зловмисник може націлитися на інтегратора, щоб викрасти інформацію про систему, яка може бути використана в подальшому для компрометації. Якщо інтегратор все ще має доступ до системи після її введення в експлуатацію, він може стати ціллю для зловмисника, який може використати ці привілеї для компрометації системи. Персонал інтеграторів, що

знаходиться на об'єкті та має доступ до мереж ОКІ, представляє загрозу та ризик, як техніки на короткострокових контрактах, описаних вище.

Треті сторони і збирачі даних. Послуги третіх сторін можуть включати агрегаторів даних, постачальників програмного забезпечення як послуги (Software as a Service (Saas)), постачальників хмарних систем або постачальників зв'язку. Послуги третіх сторін стають все більш поширеними, і більшість ОКІ покладаються хоча б на одну зовнішню послугу. Збір технологічних даних є критичним для процесів багатьох внутрішніх зацікавлених сторін. Дані про продуктивність та моніторинг стану обладнання використовуються для безпечної роботи, мінімізації експлуатаційних витрат, проактивного прогнозування потреб у технічному обслуговуванні. Провайдери SaaS можуть пропонувати послуги для оптимізації процесів, збору даних для моніторингу здоров'я, продуктивності чи інших параметрів, або навіть надання рішень з безпеки [8]. ОКІ повинні ретельно перевіряти своїх постачальників послуг, що включає встановлення вимог до процесів та регулярну звітність від постачальників для забезпечення відповідності політикам організації. Якщо зловмисник отримає доступ до великої кількості зібраних даних, він дізнається цінну інформацію про обладнання, роботу та продуктивність ОКІ.

Зовнішні групи загроз:

Кібер та фізичні кримінальні елементи (зловмисні). Кримінальні елементи відносяться до зловмисних «зовнішніх акторів», які намагаються пошкодити або порушити роботу ОКІ для власної вигоди. Мотиви їхньої кримінальної діяльності різноманітні: експлуатація системи для отримання інформації; створення збоїв; завдання шкоди. Зростаючою загрозою від кримінальних елементів є кібератаки з фінансовою мотивацією. Програми-вимагачі, що впливають на системи управління технологічними процесами, стають все більш поширеними, оскільки злочинці знають, що ці системи надають критичні послуги, і їх виведення з ладу є дорогим і руйнівним. Для запобігання таким загрозам ОКІ повинні впроваджувати надійні заходи безпеки, включаючи регулярне оновлення систем, навчання персоналу з кібербезпеки та створення резервних копій даних. Також важливо розробляти плани реагування на інциденти, щоб швидко і ефективно діяти у разі атаки. Мотиви фінансової вигоди, порушення або пошкодження можуть бути основною метою, порушення або пошкодження роботи ОКІ. «Актори» державного рівня є найбільш значущою загрозою для ОКІ [9]. «Актори» державного рівня використовують різні вектори атак, але ОКІ повинні бути особливо уважними до діяльності з розвідки, яка є помітно важкою для виявлення, і повинні проводити власні внутрішні оцінки загроз, щоб усунути критичні прогалини в безпеці. «Актори» державного рівня будуть використовувати кібертактики, але також можуть скомпрометувати інсайдера (як з його відома, так і без нього) для отримання привілейованих облікових даних, критичної інформації або навіть фізично викрасти активи [10].

Для захисту від зазначених загроз ОКІ необхідно:

1. Впроваджувати засоби моніторингу та виявлення розвідувальної діяльності — розробка та впровадження систем для виявлення незвичайної активності, що може свідчити про проведення розвідки;
2. Проводити регулярні внутрішні оцінки загроз — аналізувати та усувати вразливості у безпеці;
3. Навчати персонал — підвищувати обізнаність співробітників щодо кібербезпеки та тактик, які можуть використовувати зловмисники.

4. Забезпечувати фізичну безпеку об’єктів - впроваджувати заходи для захисту фізичних активів від несанкціонованого доступу.
5. Підтримувати резервні копії даних та плани реагування на інциденти — забезпечувати можливість швидкого відновлення систем та даних у разі атаки.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Зменшення поверхні атаки для ОКІ вимагає комплексного підходу, що враховує кібернетичні та фізичні аспекти захисту. Враховуючи вразливості, пов’язані з внутрішніми та зовнішніми «акторами», пропонується наступні заходи для зменшення поверхні атаки:

1. Управління доступом (контроль доступу) — впровадити багаторівневу систему автентифікації для співробітників та підрядників, що працюють на об’єкті. Це може включати двофакторну автентифікацію (2FA) та біометричні методи. Також слід обмежити доступ до систем і даних застосувавши керування доступом на основі ролей (*англ. Role-Based Access Control, RBAC*), що дозволить надавати доступ лише тим співробітникам, які дійсно потребують його для виконання своїх обов’язків [11]. Запровадити регулярні перевірки облікових записів користувачів та їхніх прав доступу, щоб вчасно виявляти та видаляти застарілі або непотрібні облікові записи, так зване відстеження доступу. Встановити системи моніторингу, що відслідковують активність користувачів і виявляють аномальні дії, які можуть свідчити про злом або несанкціонований доступ [12].

2. Захист від зовнішніх загроз (фізична безпека):
   - встановити огорожі та системи контролю доступу навколо ОКІ, щоб запобігти несанкціонованому доступу до критичних активів;
   - встановити відеоспостереження та датчики руху для моніторингу периметра та виявлення підозрілої активності;
   - використовувати мережеві екрани та системи виявлення вторгнень (англ. *Intrusion Detection System, IDS*) для захисту від несанкціонованого доступу та кібератак;
   - регулярне оновлення програмного забезпечення та операційних систем для усунення відомих вразливостей та зменшення ризику експлуатації.
3. Захист від внутрішніх загроз (управління внутрішніми актами):
   - запровадити програми навчання з кібербезпеки для співробітників, щоб підвищити їхню обізнаність про загрози та навчити практик безпеки;
   - створити політику щодо повідомлення про підозрілі дії всередині ОКІ, що дозволить вчасно виявляти потенційні загрози з боку інсайдерів.
   - моніторинг та аудит, а саме регулярно проводити аудит безпеки для оцінки ефективності існуючих заходів захисту та виявлення можливих вразливостей;
   - впровадити систему логування та аналізу логів для відстеження дій користувачів та виявлення підозрілої активності.
4. Управління контрактами:
   - включати положення про кібербезпеку у договори сторін, щоб забезпечити їх відповідальність за дотримання стандартів безпеки;
   - тимчасовий доступ — надавати виконавцям доступ лише на необхідний період часу та до обмеженого обсягу даних, потрібного для виконання завдань.

5. Захист від «державних акторів»:
   - впровадити системи раннього виявлення розвідувальної діяльності, що дозволить своєчасно виявляти підготовку до атак з боку «державних акторів»;
   - регулярно проводити внутрішні оцінки загроз для виявлення та усунення критичних вразливостей в системах;
   - співпрацювати з державними органами та іншими ОКІ для обміну інформацією про загрози та інциденти кібербезпеки;
   - брати участь у галузевих ініціативах та форумах з кібербезпеки для обміну найкращими практиками та отримання актуальної інформації про нові загрози.

Зазначені заходи значно зменшать поверхню атаки ОКІ та забезпечать безпеку від різноманітних загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Al-Bakri, A., & De Cock, M. (2021). Threat Actor Type Inference and Characterization within Cyber Threat Intelligence. *arXiv:2103.02301*.
2. Fortinet. (2021). *Understanding Today's Threat Actors. Fortinet White Paper.* https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-understanding-todays-threat-actors.pdf
3. Sailio, M., Latvala, O.-M., & Szanto, A. (2020). Cyber Threat Actors for the Factory of the Future. *Appl. Sci. 10(12), 4334.* https://doi.org/10.3390/app10124334
4. «Уроки збройної агресії росії проти україни – воєнно-стратегічні аспекти». (2021). *Збірник матеріалів міжвідомчої науково-практичної конференції кафедри стратегії національної безпеки та оборони.* Національний університет оборони України імені Івана Черняховського.
5. *What is a Threat Actor? | IBM.* (б.д.). IBM - United States. https://www.ibm.com/topics/threat-actor
6. Australian Cyber Security Centre. (2021). *Guidance for the Critical Infrastructure Risk Management Program.* https://www.cisc.gov.au/resources-subsite/Documents/guidance-for-the-critical-infrastructure-risk-management-program.pdf
7. StaffCop Enterprise. (б.д.). *Energy and Utilities Sector Cyber Security*. https://www.staffcop.com/energy-and-utilities-sector-cyber-security/
8. Business Law Today. (2021). *SaaS Agreements: Key Contractual Provisions.* https://businesslawtoday.org/2021/11/saas-agreements-key-contractual-provisions/
9. National Cyber Security Centre. (2021). *NCSC Warns of Enduring Significant Threat to UK's Critical Infrastructure.* https://www.ncsc.gov.uk/news/ncsc-warns-enduring-significant-threat-to-uks-critical-infrastructure
10. Gallagher Security. (б.д.). *Understanding the Impact of Insider Threats.* https://security.gallagher.com/en-HK/Blog/Understanding-the-Impact-of-Insider-Threats
11. Neumetric. (б.д.). *Role-Based Access Control (RBAC) for Cybersecurity*. https://www.neumetric.com/role-based-access-control-rbac-for-cybersecurity/
12. Teramind. (б.д.). User Activity Monitoring.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023

Oleksii Skitsko
PhD, Senior Researcher
National Academy of Security Service of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0003-4122-0889
oiskitsko@gmail.com

Roman Shyrshov
Researcher
National Academy of Security Service of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0003-3534-8736
signorum@gmail.com

ATTACK SURFACE IN THE CONTEXT OF ITS USERS ("TREAT ACTORS") FOR CRITICAL INFRASTRUCTURE FACILITIES

Abstract. In the modern digital world, where information technology is an integral part of life, cybersecurity issues are becoming increasingly relevant. One of the key aspects of protecting information systems is managing the attack surface, which includes all possible entry points for malicious actors. Forming and managing the attack surface is a complex task that requires constant attention and improvement. Malicious actors ("Threat actors") play a crucial role in this process. They constantly seek new ways to penetrate systems, using various methods and techniques. These "actors" can vary in their origins and motivations: from cybercriminals seeking financial gain to state actors conducting espionage and sabotage activities. Understanding the types of "malicious actors" and their methods is essential for effective attack surface management. This understanding helps to timely detect and eliminate vulnerabilities, improve system and network configurations, and raise staff awareness of modern cyber threats. This article examines the key aspects of forming the attack surface, focusing on the role of "malicious actors". It explores the types of "malicious actors", their methods and techniques, and provides practical recommendations for reducing risks and improving the protection of information systems. Additionally, conducting regular security audits and implementing modern protection technologies such as intrusion detection systems, data encryption, and multi-factor authentication are important. Thus, a comprehensive approach to managing the attack surface, which includes understanding "Threat actors", utilizing modern protection technologies, and continuously training personnel, is crucial for effectively protecting the information systems of critical infrastructure.

Keywords: malicious actor; threat actor; attack surface; critical infrastructure object (CIO); Internet of Things (IoT).

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Al-Bakri, A., & De Cock, M. (2021). Threat Actor Type Inference and Characterization within Cyber Threat Intelligence. *arXiv:2103.02301.*
2. Fortinet. (2021). *Understanding Today's Threat Actors. Fortinet White Paper.* https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-understanding-todays-threat-actors.pdf
3. Sailio, M., Latvala, O.-M., & Szanto, A. (2020). Cyber Threat Actors for the Factory of the Future. *Appl. Sci. 10(12), 4334.* https://doi.org/10.3390/app10124334
4. "Lessons of Russia's Armed Aggression against Ukraine - Military and Strategic Aspects" (2021). Collection of materials of the interdepartmental scientific and practical conference of the Department of National Security and Defense Strategy. Ivan Chernyakhovsky National Defense University of Ukraine.
5. *What is a Threat Actor? | IBM.* (n.d.). IBM - United States. https://www.ibm.com/topics/threat-actor
6. Australian Cyber Security Centre. (2021). *Guidance for the Critical Infrastructure Risk Management Program.* https://www.cisc.gov.au/resources-subsite/Documents/guidance-for-the-critical-infrastructure-risk-management-program.pdf

7. StaffCop Enterprise. (n.d.). *Energy and Utilities Sector Cyber Security*. https://www.staffcop.com/energy-and-utilities-sector-cyber-security/
8. Business Law Today. (2021). *SaaS Agreements: Key Contractual Provisions.* https://businesslawtoday.org/2021/11/saas-agreements-key-contractual-provisions/
9. National Cyber Security Centre. (2021). *NCSC Warns of Enduring Significant Threat to UK's Critical Infrastructure.* https://www.ncsc.gov.uk/news/ncsc-warns-enduring-significant-threat-to-uks-critical-infrastructure
10. Gallagher Security. (n.d.). *Understanding the Impact of Insider Threats.* https://security.gallagher.com/en-HK/Blog/Understanding-the-Impact-of-Insider-Threats
11. Neumetric. (n.d.). *Role-Based Access Control (RBAC) for Cybersecurity*. https://www.neumetric.com/role-based-access-control-rbac-for-cybersecurity/
12. Teramind. (n.d.). User Activity Monitoring.