УДК 004.056.5:004.75:355.45

док. філ. з інформ. техн. **Коваль М.О.** (ВІКНУ)
к.пед.н. **Кравченко О.І.** (ВІКНУ)
Карпенко А.О. (ВІКНУ)
Шамрай Н.М. (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2025/89-05

АНАЛІЗ ВРАЗЛИВОСТЕЙ ТА КІБЕРАТАК НА ІНФОРМАЦІЙНІ РЕСУРСИ, ЩО ОБРОБЛЯЮТЬСЯ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

У статті розглянуто стан забезпечення захищеності критичних інфраструктури а також техносфери в цілому. Як правило виділяють об'єкти чотирьох типів, що відрізняються як ступінь потенційної небезпеки та висунутими вимогами щоб мати змогу захистити їхі: об'єкти технічного управління, виробничі об'єкти що є небезпечними, критично значущі об'єкти, стратегічно пріоритетні об'єкти військового призначення, які можуть впливати на стан національної безпеки.

Інформаційні технології дозволяють отримати важливий ефект тонкого регулювання інформаційного впливу залежно від одержувача. Можна виготовити багато варіантів віртуальної реальності, більш того, її (реальність) можна набудовувати на конкретного споживача у момент запиту на одержання.

Показано, що для ефективного функціонування інформаційної системи (ІС) доцільно використовувати у складі системи управління ІР відповідну підсистему забезпечення безпеки з можливістю проведення оцінювання та управління станом захищеності ІС в режимі реального часу та в швидкозмінній природі кібератак.

Сформульовано поняття інформаційна зброя, яка об'єднує в собі електронний і людський аспекти. інформаційних технологій, тому повсякденна робота багатьох автоматизованих систем (АС) і інформаційних систем (ІС) має життєве важливе значення. З іншого боку, головним стратегічним об'єктом впливу інформаційної зброї залишаються люди. В інформаційних системах повинна бути можливість, виявлення та запобігання вторгнень, які реалізуються множиною різнонаправлених за фізичним змістом атак. З метою здійснення такої можливості система захисту інформації (СЗІ) повинна мати у складі систему управління подіями інформаційної безпеки

Ключові слова: інформаційні ресурси, інформаційна система, кіберзагроза, інформаційна зброя, комбінації кібератак, система захисту інформації.

Вступ та постановка проблеми.

Сучасні об'єкти критичної інфраструктури функціонують як складні технічні системи, що відзначаються багаторівневою структурою, тісною взаємодією елементів та інтеграцією кіберфізичних компонентів. Їх робота відбувається в умовах постійної невизначеності та динамічного зростання загроз, серед яких вагоме місце посідають кіберінциденти, техногенні аварії, природні явища та помилки персоналу. Така сукупність факторів ускладнює процес забезпечення їх надійності та потребує застосування комплексних підходів до захисту, що поєднують організаційні та технічні рішення.

Рівень захищеності зазначених систем визначається їх здатністю протистояти переходу окремих елементів у критичні стани та запобігати розвитку руйнівних сценаріїв під час експлуатації. Водночас досягнення необхідного рівня безпеки ускладнюється низкою чинників невизначеності, зокрема нестабільністю параметрів середовища функціонування, обмеженістю достовірної інформації про внутрішні процеси, а також недосконалістю засобів контролю і математичного опису поведінки систем. Додатковий вплив мають експлуатаційні навантаження та зміна характеристик ключових елементів упродовж життєвого циклу.

У структурі техносфери прийнято виокремлювати декілька категорій об'єктів залежно від рівня потенційної небезпеки та вимог до їх захисту. До них належать об'єкти технічного регулювання, небезпечні виробничі комплекси, критично важливі об'єкти, що підлягають

категоризації в межах системи критичної інфраструктури, а також стратегічні об'єкти військового призначення. Надійність функціонування останніх має особливе значення для підтримання обороноздатності та загального рівня національної безпеки.

Значення критичної інфраструктури для держави визначається тим, що вона забезпечує безперервність ключових процесів у таких сферах, як енергетика, транспорт, зв'язок, медицина та інші життєво важливі галузі. Порушення роботи відповідних систем може мати масштабні наслідки — від економічних втрат до соціальної нестабільності та виникнення загроз безпеці держави і населення [1].

В умовах триваючої збройної агресії проти України особливої актуальності набуває питання стійкості функціонування таких об'єктів. Противник, поряд із застосуванням традиційних засобів ураження, активно використовує інструменти кіберпростору для впливу на системи управління та дестабілізації роботи вразливих елементів інфраструктури. При цьому навіть впровадження сучасних заходів захисту не гарантує повної безпеки, оскільки цифровізація та інтеграція систем у єдине інформаційне середовище створюють нові вразливості.

Таким чином, забезпечення надійного захисту складних технічних систем, що входять до складу критичної інфраструктури, стає одним із ключових завдань сучасного етапу розвитку держави. Це потребує перегляду існуючих підходів до оцінювання ризиків, підвищення рівня адаптивності систем безпеки та впровадження інноваційних методів протидії як фізичним, так і кіберзагрозам [2].

Аналіз досліджень та публікацій.

Аналіз ведення сучасних гібридних війн у світі та проведення кібернетичних операцій, свідчить про розвиток форм, способів та методів, які застосовуються для проведення кібератак на систему управління ІР та ІС. В ході попередніх досліджень [1] визначено, що для ефективного функціонування ІС доцільно використовувати у складі системи управління ІР відповідну підсистему забезпечення безпеки з можливістю проведення оцінювання та управління станом захищеності ІС в режимі реального часу та в умовах постійних змін в природі кібератак.

До основних особливостей відносяться: різна розмірність мереж, територіально рознесені складові ІС, вихід елементів ІС за межі контрольованої зони. Зазначені особливості ІС роблять їх привабливими з точки зору організації та впровадження швидкої взаємодії між територіально-рознесеними підрозділами державних установ, однак, можуть бути використані зловмисниками для здійснення кібератак з метою вчинення деструктивних дій. Звичайно, функціонування ІС в кіберпросторі залежить від множини природних, техногенних та антропогенних чинників, які можуть нашкодити процесу передачі інформації. Але найбільшу шкоду ІС може завдати навмисні атаки та вплив на існуючі вразливості системи безпеки, що здійснюються на різних рівнях базової еталонної моделі взаємодії відкритих систем.

Інформаційні системи описуються в працях вітчизняних та закордонних вчених: Субача І.Ю., Бурячка В.Л., Гнатюка С.О., Корченко О.Г., Юдіна О.К., Бучика С.С., Євсеєва С.П., Дудикевича В.Б., Казмирчук С.В., Albers, O. T. Ptaceka, G. Elmasry, P. Camp та інших.

Водночас, основними вимогами, які пред'являються до захищеності ІР в ІС є: робота в режимі реального часу; врахування загроз характерних інформаційно-телекомунікаційним системам; можливість застосовування в системах з високою динамікою зміни топології; децентралізація управління та наявність ієрархічно-розподільної структури; мінімальне завантаження мережі службовою інформацією.

Виходячи з вказаного, одним з найважливіших питань, які необхідно вирішити в процесі експлуатації ІС є гарантування інформаційної, програмної та апаратної безпеки, які визначають ступінь захищеності інформаційних ресурсів від вразливостей та кібератак.

На сьогодні спостерігається невідповідність між вказаними можливостями існуючих методів управління станом захищеності ІС та вимогами до методів управління станом захищеності ІР в ІС. Як наслідок вирішення питань безпеки в ІС та управління станом захищеності інформаційний систем від вразливостей та кібератак є актуальним і потребує подальших досліджень.

Мета статті є визначення ефективності захищеності інформаційних ресурсів на основі аналізу, вразливостей від зовнішніх та внутрішніх кібератак.

Викладення основного матеріалу.

В умовах функціонування системи кібербезпеки в різних режимах особливої ваги набуває забезпечення захищеності інформаційних ресурсів (ІР) у кіберпросторі. Це, у свою чергу, обумовлює необхідність підвищення ефективності системи управління (СУ) та відповідної підсистеми забезпечення безпеки (ПЗБ), які мають забезпечувати своєчасне виявлення і коректну інтерпретацію впливу кіберзагроз та несанкціонованих втручань. Така оцінка здійснюється на основі аналізу змін сукупності окремих показників, що характеризують рівень захищеності інформаційних ресурсів.

При цьому ключовим аспектом процесу прийняття управлінських рішень у підсистемі кібербезпеки є встановлення об'єктивного ступеня впливу конкретних загроз на загальний стан безпеки інформаційних ресурсів. Саме точність та обґрунтованість такої оцінки визначає ефективність реагування системи на дестабілізуючі фактори.

Одним з важливих факторів розвитку інформаційних технологій є глобальне об'єднання програмних продуктів, технічних засобів та мереж передачі інформації. Таке поєднання надає сучасним технічним засобам нові можливості, зручності у користуванні та керуванні. Проте зворотною стороною таких переваг є додаткові вразливості програмно-керованих технічних засобів. Крім відомих технічних каналів витоку інформації слід враховувати загрози несанкціонованого віддаленого доступу до технічних засобів, наявні в них уразливості та незадекларовані функції, а також можливості впровадження шкідливого програмного забезпечення та програмних закладок. Зазначені вразливості можуть "експлуатуватись" з метою порушення конфіденційності, цілісності, достовірності та доступності інформації, яка обробляється технічними засобами, а також порушення конфіденційності інформації, яка циркулює в місцях їх встановлення.

Сучасне робоче місце в загальному випадку обладнане рядом технічних засобів, які перейшли від "звичайних" технічних засобів до програмно-керованих технічних засобів. Технічні засоби зазначених систем мають у своєму складі модулі або інтерфейси передачі даних, які у певних умов можуть бути використані в якості каналів несанкціонованого керування технічними засобами. Використання програмно-керованих технічних засобів, які мають у своєму складі модулі та інтерфейси передачі даних, потребує вжиття додаткових заходів із захисту інформації, враховуючи сучасні загрози [3].

Порушення захищеності при використанні ІС розподіляються на такі види:

- несанкціонований доступ (НСД) до роботи автоматизованих систем (АС), мереж, баз даних;
- створення руйнівного програмного забезпечення (ПЗ) або технічних засобів, та їх збут або розповсюдження;
- несанкціонований збут або поширення інформації з обмеженим доступом, яка зберігається в АС, мережах або на носіях такої інформації;
- злочини, що здійснені шляхом використання ІС та інформаційної зброї, як засобу досягнення злочинної мети тощо[4].

Поняття інформаційна зброя об'єднує в собі електронний і людський аспекти. З одного боку, суспільство все більше підпадає у залежність від інформаційних технологій, тому повсякденна робота багатьох АС і ІС має життєво важливе значення. З іншого боку, головним стратегічним об'єктом впливу інформаційної зброї залишаються люди. Основними завданнями застосування інформаційної зброї у мережі є:

- порушення цілісності службової та доступної інформації;
- пошкодження систем захисту;
- обмеження порядку доступу до ресурсу законних користувачів, спотворення роботи технічних засобів, комп'ютерних систем.

Види інформаційної зброї у глобальних мережах [5]:

- деструктивні програми типу "комп'ютерні віруси" – програми, що мають здібності до самовідтворення, і, як правило, здатні здійснювати дії, які можуть порушити роботу системи

і/або викликати порушення політики безпеки. Мають можливість впроваджуватися у програми, передаватися лініями зв'язку, мережами передачі даних, виводити з ладу системи керування і т.д.;

- деструктивні програми типу "троянський кінь" – програми, які працюють у звичному режимі, окрім виконання функцій документування, можуть здійснювати приховані дії від особи авторизованого користувача в інтересах розробника цієї програми;

- засоби подавлення інформаційного обміну та фальсифікації в ІС, передусім, військовогота дердавного призначення;

- засоби блокуванн тестових програм;

Ці засоби надають можливості супротивнику завдавати інформаційних ударів. Наприклад, порушити комунікації, паралізувати телефонну мережу, заплутати фінанси, порушити функціонування космічних апаратів.

Універсальність, прихованість, широкий спектр форм програмно-апаратної реалізації, характеризують інформаційну зброю як надзвичайно небезпечною: вона легко маскується під засоби захисту, як бепека інтелектуальної власності. Вона також дозволяє навіть проводити наступальні дії анонімно, без оголошення війни.

З метою запобігання або нейтралізації наслідків застосування інформаційної зброї необхідно вжити наступних заходів [5, 6]:

- збереження матеріально-технічних об’єктів, що є базовою основою ІР;
- забезпечення стабільного функціонування банків і баз даних;
- захист інформації від НСД, перекручування або знищення;
- збереження якості інформації (своєчасності, точності, повноти і необхідної приступності).

Атаки здійснюються з метою порушення конфіденційності, цілісності та працездатності ІР, що зберігається та оброблюється в інформаційних системах (ІС). З цією метою, як свідчить досвід застосування, використовують вразливості ІС, тобто неспроможність системи протистояти певній загрозі або сукупності загроз [5,6,7]. Загальна структура реалізації атак представлена на рис. 1.

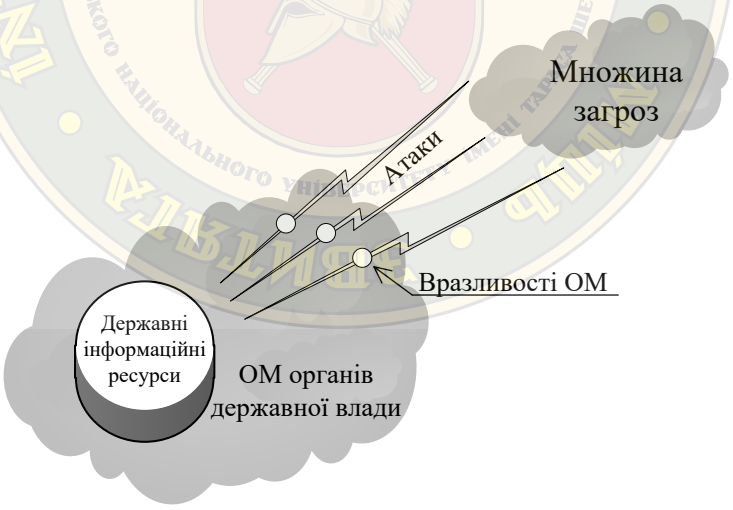

Рисунок 1 – Загальна структура реалізації атак

Для одержання інформації про можливі атаки на інформацію, вимога щодо захисту якої встановлена законодавством, інформаційніі наслідки їхнього прояву, а також виявлення найбільш небезпечних кібератак використовують модель поводження інформаційних систем та ІС при впливі на них кібератак (рис. 2), де КБА – комбінації кібератак, S – підмножина станів ІС, ВФ – виконання функцій ІР, ІНПІС – інтенсивності переходів ІС, МСЗІР – модель системи захисту інформаційних ресурів [8].

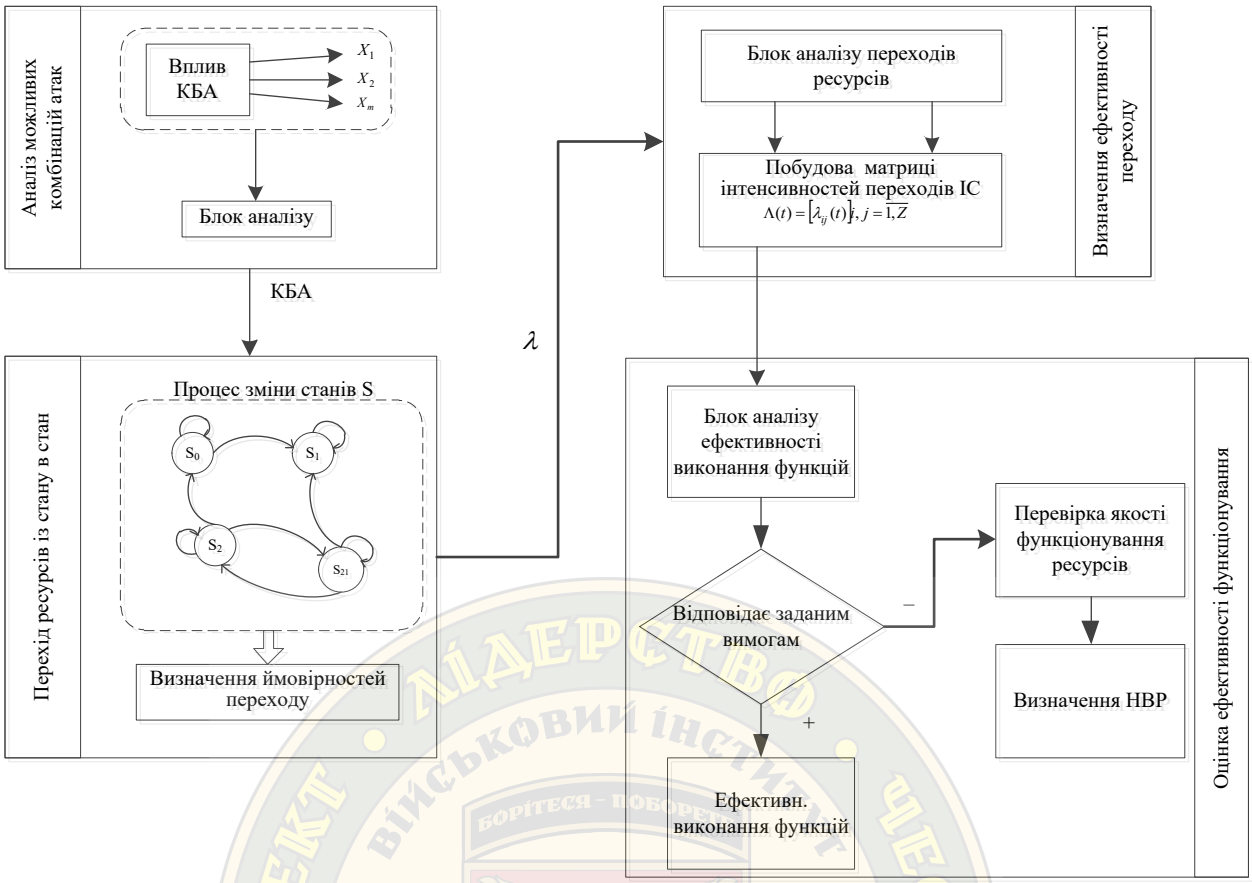

Рисунок 2 – Модель поводження системи при впливі атак

Більш детально доцільно розглянути сучасні бази даних, що містять описи типових вразливостей і загроз, які взаємодіють між собою на різних рівнях моделі OSI model.

У межах цієї моделі взаємодія між системами фактично реалізується через дві взаємопов'язані схеми – горизонтальну та вертикальну:

- у горизонтальній (розподіленій) моделі розглядається безпосередній обмін даними між однойменними рівнями різних кінцевих вузлів (хостів). Для забезпечення такої взаємодії необхідною умовою є використання однакових протоколів на відповідному рівні в обох системах;

- у вертикальній (ієрархічній) моделі описується взаємодія між сусідніми рівнями в межах однієї системи із застосуванням відповідних інтерфейсів. При цьому кожен рівень надає сервіси вищому рівню та використовує можливості нижчого. Виняток становлять крайні рівні: прикладний рівень орієнтований на взаємодію з користувачем, тоді як фізичний рівень не використовує сервіси інших рівнів.

Перші випадки інформаційної безпеки, що офіційно мають місце в базах даних вразливостей, з'явилися в 1988 році [8, 9]. З тих пір ведеться постійний пошук вразливостей та їх реєстрація як в рамках відкритих проектів, так і приватними компаніями, науково-дослідними інститутами та дослідниками. Серед лідерів детектування вразливостей слід згатати нижче перелічених розробників відповідних баз даних вразливостей: United State Computer Emergency Readiness Team та база Vulnerability Notes Database (VND); компанія MITRE та її база вразливосей Common Vulnerabilities and Exposures (CVE) [9]; компанія IBM та база вразливостей X-Force [10]; National Institute of Standardsand Technology та база National Vulnerabilities Database (NVD) [11].

Розглянемо деякі з перелічених баз вразливостей:

- CVE – довідково-пошукова система посилань вразливостей. Головною складовою системи є CVE ідентифікатори – унікальні ідентифікатори, які присвоюються кожній відомій вразливості в сфері інформаційної безпеки. Система включає в себе понад 98000 записів про

окремі вразливості [10]. Основна різниця в тому, що вона є найбільшою, повною та систематизованою. До основних складових структури записів вразливостей відносяться:

1) статус – в цьому полі може знаходитись або значення Entry (Запис перевірений), або значення Candidate (вразливість, яка ще не первірялась);

2) фаза –це поле включає значення етапу удосконалення вразливості, а також дату присвоєння зазначеного етапу. Може приймати наступні значення: Proposed – фаза пропозиції вразливості; Interim – проміжна фаза вразливості; Modified – фаза модифікації вразливості;– Assigned – фаза встановлення вразливості;

3) опис – поле включає в себе опис вразливості;

4) посилання –тут знаходяться посилання на інші джерела із зазначенням точної адреси інтернет-ресурсу опису вразливості та ідентифікатора джерела;

5) голоси – це імена членів голосування, які прийняли рішення щодовнесення вразливості в базу;

6) коментарі – вноситься данні про автора коментаря та самий текстовий зміст.

Додаткова в елементах записів вразливостей може знаходитись тип вразливості, ім'я та ідентифікатор. Ім'я вразливості має формат "CVE-YYYYNNNN", де YYYY – це рік виявлення вразливості, а NNNN – її порядковий номер.

До недоліків бази CVE входить – відсутність певного механізму опису відношення вразливостей до конкретних продуктів, а також присвоєння вразливостям метрик і визначення ступеня небезпеки [12].

Національна база даних вразливостей США (NVD) – сховище даних вразливостей, засноване на стандартах протоколу автоматизації змісту безпеки. База NVD об'єднала в собі опис вразливостей, назви програмного забезпечення з цими вразливостями і оцінки небезпеки вразливостей. За станом на 2017 рік база даних вразливостей NVD біля 70000 записів вразливостей [13].

Структура запису вразливості в базі NVD є розширеною формою подання записи в базі CVE, за рахунок наявності наступних полів: конфігурація вразливих продуктів з урахуванням залежностей; список вразливих продуктів; показникі, що характеризують вразливість в форматі "Загальної системи оцінки вразливостей"; тип доступу для реалізації вразливості. Встановлено, що 82,77% вразливостей належать додаткам, 12,28% – операційним системам і 3,59% – апаратному забезпеченню.

Важливою собливістю бази NVD від є застосування Common Platform Enumeration,як одного з кращих словників продуктів серед існуючих аналогів завдяки значного числа записів та уніфікованого формату імен програмно-апаратного забезпечення [11]. Однак у даного формату представлення записів є недоліки:

– неоднозначність різних полів формату;

– використання не всіх існуючих записів даного словника базою NVD.

База вразливостей OSVDB організова для групи фахівців в області безпеки. Мета проекту полягає в тому, щоб забезпечити точну, Дана база містить деталізовану, інформацію про вразливість систем забезпечення безпеки. В ній знаходиться понад 110 000 вразливостей [13].

Як правило, реалізація внутрішньосегментної (внутрішньої) атаки є значно простішою порівняно з міжсегментною (зовнішньою). Водночас зовнішні атаки становлять більшу загрозу, ніж внутрішні. Це пояснюється тим, що під час їх здійснення об’єкт впливу та зловмисник можуть перебувати на значній відстані один від одного, що ускладнює застосування ефективних заходів захисту та протидії.

Під порушенням безпеки розуміється несанкціонований доступ до інформаційної системи, який виникає внаслідок дій, що суперечать встановленій політиці безпеки або обходять засоби захисту інформації. Атаку доцільно трактувати як спробу реалізації певної загрози. У свою чергу, загроза — це будь-які умови чи події, здатні призвести до порушення нормального функціонування інформаційних, програмних або апаратних компонентів системи, а також спричинити збитки чи інші негативні наслідки [13, 14].

Розглянемо нині існуючі типи атак на ІС обробки ІР (таблиця 1), та їх параметри [43, 44].

Таблиця 1 – Класифікація атак

Ознака атаки	Тип атаки	Характеристики атаки
За характером впливу	пасивні	Атаки, які безпосередньо не впливають на роботу системи, але можуть нашкодити її політиці безпеки. Складно виявити. Після атаки не залишається не має слідів. Приклад: здійснення прослуховування зв'язку в мережі.
	активні	Атаки, що безпосередньо шкодять роботі системи (зміна конфігурації ІС, порушення працездатності тощо) і порушують прийняту в ній політику безпеки. Як правило всі типи віддалених атак є активними. Необхідно обов'язково виявляти, так як після здійснення атаки в системі відбуваються значні зміни.
За метою впливу	порушення конфіденційності	Перехоплення інформації. Приклад: прослуховування каналу в мережі.
	порушення цілісності	Спотворена інформація. Прикл.: застосування помилкового об'єкта в ІС.
	порушення доступності	Не відбувається НСД (цілісність не порушена), проте доступ до легальних користувачів неможливий. Приклад: відмова в обслуговуванні зареєстрованих користувачів.
За умовою початку здійснення впливу	атака на запит від об'єкта, що атакується	У разі запиту атакуючий очікує передачі від потенційної мети атаки запиту певного типу, який і буде умовою початку здійснення впливу. Ініціатором здійснення початку атаки є об'єкт, що атакується. Приклад: DNS- і ARP-запити в стеці TCP / IP.
	атака по настанню події, що очікується на об'єкті	Якщо подія має місце, атакуючий робить постійне спостереження за станом операційної системи віддаленого об'єкта атаки і при виникненні певних обставин в цій системі починаються неполадки. Ініціатором здійснення початку атаки є об'єкт, на який здійснюється атака. Приклад: переривання сеансу роботи користувача з сервером в мережевих операційних системах без видачі команди LOGOUT.
	безумовна атака	У разі безумовної атаки початок її здійснюється по відношенню до мети атаки, тобто атака зрозпочинається негайно і незалежно від стану системи об'єкта атаки. Ініціатором здійснення початку атаки є атакуючий.
За наявністю зворотного зв'язку з об'єктом, який атакується	зі зворотним зв'язком	Атака із зворотним зв'язком – атака, за час якої атакуючий отримує відповіді від об'єкта на частину своїх дій. Це необхідно для продовження атаки і/або здійснювати її більш ефективно, реагуючи на зміни, що відбуваються в системі.
	без зворотного зв'язку (односпрямована атака)	Атака без зворотного зв'язку – атака, яка відбувається без реакції на поведінку системи, що атакується. Приклад: відмова в обслуговуванні.
За кількістю атакуючих	розподілена	Атака, вироблена двома чи більше атакуючими на одну інформаційну систему (ІС), об'єднаними певним задумом та часом початку здійснення.
	нерозподілена	Нерозподілена атака проводиться одним атакуючим.

Ознака атаки	Тип атаки	Характеристики атаки
По розташуванню атакуючого щодо атакуємого об'єкта	внутрисегментна	Атака, в якій суб'єкт і об'єкт атаки знаходяться всередині одного сегменту мережі (сегмент – фізичне об'єднання станцій з використанням комунікаційних пристроїв не вище канального рівня).
	міжсегментна	Міжсегментна атака – атака, при якій суб'єкт і об'єкт атаки знаходяться в різних сегментах мережі.

Особливу увагу доцільно приділити останньому типу атак. У контексті віддалених впливів ключове значення має розташування суб'єкта та об'єкта атаки, оскільки вони можуть перебувати як в одному, так і в різних мережевих сегментах. У разі внутрішньої атаки обидві сторони знаходяться в межах одного сегмента. Якщо ж мова йде про міжсегментну атаку, то суб'єкт і об'єкт розміщені в різних сегментах мережі. Така класифікаційна ознака дозволяє оцінювати "ступінь віддаленості" атаки.

На практиці внутрішні атаки зазвичай реалізуються значно простіше, ніж міжсегментні. Водночас зовнішні (віддалені) атаки вважаються більш небезпечними порівняно з внутрішніми. Це пов'язано з тим, що при їх здійсненні зловмисник і цільовий об'єкт можуть знаходитися на значній відстані один від одного, що ускладнює своєчасне застосування заходів протидії.

Опис стратегій реалізації можливих атак на інформаційні системи наведено в межах проєкту MITRE, зокрема в базі знань MITRE ATT&CK [13]. Вона являє собою структуровану матрицю, яка відображає етапи розвитку атаки, а також відповідні тактики і техніки, що застосовуються зловмисниками. Дана база знань сформована на основі аналізу реальних кіберінцидентів і узагальнення практичного досвіду.

Таким чином, використання моделі MITRE ATT&CK дає змогу не лише класифікувати кіберзагрози, а й описувати механізми їх реалізації, визначати, які програмні засоби чи дії застосовуються. Крім того, це дозволяє ідентифікувати зловмисника з урахуванням етапів атаки та умов її здійснення, зокрема його розташування відносно об'єкта впливу.

Аналіз сучасних наукових публікацій свідчить, що атаки, які застосовуються для здійснення вторгнень в інформаційні системи, зазвичай поділяють на п'ять основних категорій. Кожна з них об'єднує певну сукупність типів атак, що використовуються для досягнення цілей зловмисника. Як правило, окремі типи атак впливають на відповідні рівні мережевої моделі OSI model та виконують визначені функції, спрямовані на дестабілізацію роботи мережі [14]. До основних категорій належать:

- DoS-атаки (Denial of Service) – це мережеві впливи, спрямовані на порушення доступності сервісів шляхом створення умов відмови в обслуговуванні. Вони реалізуються через генерацію надмірного обсягу трафіку, що призводить до перевантаження ресурсів і блокування роботи сервера. Серед найбільш поширених прикладів: *back, land, neptune, pod, smurf, teardrop* та інші;
- U2R-атаки (User to Root) – спрямовані на отримання користувачем із обмеженими правами доступу рівня адміністратора. До типових реалізацій належать: *buffer_overflow, loadmodule, perl, rootkit*;
- R2L-атаки (Remote to Local) – передбачають несанкціоноване отримання доступу до системи віддаленим користувачем, який не має облікового запису. Найпоширеніші приклади: *ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster*;
- Probe-атаки – полягають у дослідженні мережі, зокрема скануванні портів, з метою збору інформації про її структуру та вразливості. До них належать: *ipsweep, nmap, portsweep, satan* та інші подібні методи.

Кожен вид атак має набір параметрів, за якими їх можна ідентифікувати та класифікувати до певного типу [15]. Приклад подібних параметрів наведено нижче:

0,icmp,ecr_i,SF,1032,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,511,511,0.00,0.00,0.00,0.00,1.00,0.00, 0.00,255,255,1.00, 0.00,1.00,0.00,0.00,0.00,0.00,0.00,smurf.

Ця послідовність параметрів з'єднання включає такі характеристики: тривалість з'єднання, тип протоколу, послуга мережі, обсяг даних у повідомленні (байти), стан з'єднання, кількість термінових пакетів, спроби встановлення з'єднання тощо.

Як правило атаки спрямовуються на інформаційні ресурси (ІР) у вигляді повідомлень – текстових даних, аудіо- або відеоматеріалів. Структура такого повідомлення містить передзаголовок, заголовок, контрольну суму, текст повідомлення та його завершення. Ці елементи аналізуються системою виявлення атак для ідентифікації потенційних загроз.

Зазначені типи атак здатні впливати на різні аспекти функціонування інформаційної системи (ІС), зокрема на управління ресурсами системи, розмежування доступу користувачів до даних чи функцій, характеристики енергоспоживання, обмін інформаційними пакетами, доступ до кодування та управління даними загалом.

Висновок/ Проведений аналіз атак та вразливостей на ІР, що обробляються в ІС показав різноманіття варіантів будови баз вразливостей. Кожен з варіантів має свої переваги та недоліки, але найбільш важливий напрямом-орієнтованість сучасних баз вразливистей для застосування в експертних системах. Сучасні інформаційні системи, які оообробляють ІР, мають велику кількість зовнішніх і внутрішніх вразливостей, а реалізація їх відбувається за завдяки використанню множини різнонаправлених атак. Поширення вразливостей окремого вузла ІС може викликати появу додаткових загроз безпеці ІР, що в ній оброблюються. Таким сином для визначення множини параметрів при оцінювання захищеності ІР в цілому та виявлення нових вразливостей, доцільно забезпечити функціонування системи управління інформаційної безпеки з урахуванням вищезазначених вимог, параметрів даних та характеристичних особливостей сучасних системи управління ІР.

Важливими складовими є дотримання принципів управління життєвим циклом інформаційних систем, стандартизація та посилена увага до кібербезпеки. Подальший успіх залежить від успішної інтеграції систем, покращення співдії між різними елементами, а також нарощування кадрового потенціалу, що дозволить забезпечити суттєве збільшення рівня ефективності та безпеки функціонування систем.

ЛІТЕРАТУРА:

1. Сальник С.В., Сторчак А.С., Герасімов К.К. Аналіз функціонування систем управління державними інформаційними ресурсами. Щоквартальний науково-технічний журнал Наука і техніка Повітряних Сил Збройних Сил України. 2019. Вип. 2(35). С.47-54.

2.Субач І.Ю, Фесьоха В.В., Голуб О.О, Криховецький В.В. Нечітке визначення "типовості" статистичної поведінки у інформаційно-телекомунікаційних мережах. Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку та автоматизації в операції Об'єднаних сил : зб. матеріалів XI наук.-практ. конф., 8-9 лист. 2018 р. Київ : ВІТІ ім. Героїв Крут, 2018. С. 213.

3. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України" від 17 вересня 2021 року № 473/2021 URL: https:// https://zakon.rada.gov.ua/laws/show/473/2021#Text (дата звернення:23.06.2023).

4. Лепіх Я.І., Гордієнко Ю.О, Дзядевич С.В., Дружинін А.О., Євтух А.А.,. Лєнков С.В., Мельник В.Г., Проценко В.О., Романов В.О. Мікроелектронні датчики нового покоління для інтелектуальних систем. монографія. Одеса: "Астропринт", 2011. 92 с.

5. Корпань Я.В. Класифікація загроз інформаційній безпеці в комп'ютерних системах при віддаленій обробці даних Реєстрація, зберігання і обробка даних. 2015. Вип. 17(2). С. 39-46.

6. Горбенко В.І., Картавих В.Ю., Субач І.Ю. Модель моніторингу домену управління інформаційної мережі військового призначення Системи обробки інформації. 2013. Вип. 4(111). С. 118-122.

7. Tewari N., Bhardwaj A. Flow Statistics Based Detection of Low Rate and High Rate DDoS Attacks // International Journal of Scientific & Engineering Research. 2013. Vol. 4, № 5. P. 348 – 353.

8. Xiao P., He J., Chen Y., Fu Y. A new trusted roaming protocol in wireless mesh networks // International Journalof Sensor Networks. 2013. Vol. 14, Issue 2. P. 109 – 119. doi: 10.1504/IJSNET.2013.056610 89

9. Офіційний сайт Common Vulnerabilities and Exposures. Режим доступу: http://cve.mitre.org

10.Офіційний сайт National Vulnerabilities Database. Режим доступу: http://nvd.nist.gov

11. Офіційний сайт United States Computer Emergency Readiness Team. Режим доступу: http://www.us-cert.gov

12. Zhang Y., Lee W., Huang Y. Intrusion detection techniques for mobile wireless networks. Wireless Networks Journal (ACM WINET). 2003. № 9(5). P. 545–556.

13. Janakiraman R., Waldvogel M., Zhang Qi. A peer-to-peer approach to networkintrusion detection and prevention. Enabling Technologies: Infrastructure for Collaborative Enterprises. 2003. P. 226–231, DOI:10.1109/ENABL. 2003.1231412

14. Alshboul Y., Streff K., Analyzing Information Security Model for Small-Medium Sized Businesses, Twenty-first Americas Conference on Information Systems, Puerto Rico, 2015.

15. Safa N.S., Solms R.V., Furnell S. Information security policy compliance model in organizations. Computers & Security. 2016. Vol. 56. P. 70-82. DOI:10.1016/j.cose.2015.10.006

REFERENCES:

1. Salnyk S.V., Storchak A.S., Herasimov K.K. (2019) Analiz funktsionuvannia system upravlinnia derzhavnymy informatsiinymy resursamy [Analysis of the functioning of state information resource management systems]. *Shchokvartalnyi naukovo-tekhnichnyi zhurnal Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy.* Vyp. 2(35). S.47-54. (in Ukrainian)

2. Subach I.Yu, Fesokha V.V., Holub O.O, Krykhovetskyi V.V. (2018) Nechitke vyznachennia "typovosti" statystychnoi povedinky u informatsiino-telekomunikatsiinykh merezhakh [Unclear definition of the "typicality" of statistical behavior in information and telecommunications networks.]. *Priorytetni napriamky rozvytku telekomunikatsiinykh system ta merezh spetsialnoho pryznachennia. Zastosuvannia pidrozdiliv, kompleksiv, zasobiv zviazku ta avtomatyzatsii v operatsii Obiednanykh syl : zb. materialiv XI nauk.-prakt. konf., 8-9 lyst. 2018 r. Kyiv* : VITI im. Heroiv Krut, 2018. 213. (in Ukrainian)

3. Ukaz Prezydenta Ukrainy (2021) "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Stratehichnyi oboronnyi biuleten Ukrainy" № 473/2021 Available at: https:// https://zakon.rada.gov.ua/laws/show/473/2021#Text . (accessed 23 January 2023). (in Ukrainian)

4. Lepikh Ya.I., Hordiienko Yu.O, Dziadevych S.V., Druzhynin A.O., Yevtukh A.A.,. Lienkov S.V., Melnyk V.H., Protsenko V.O., Romanov V.O. (2011). *Mikroelektronni datchyky novoho pokolinnia dlia intelektualnykh system.* [New generation microelectronic sensors for intelligent systems.] Odesa: "Astroprint". (in Ukrainian)

5. Korpan Ya.V. (2015) Klasyfikatsiia zahroz informatsiinii bezpetsi v kompiuternykh systemakh pry viddalenii obrobtsi danykh Reiestratsiia, zberihannia i obrobka danykh [Classification of threats to information security in computer systems during remote data processing. Data registration, storage and processing.]. 2015. Vyp. 17(2). S. 39-46.

6. Horbenko V.I., Kartavykh V.Yu., Subach I.Yu.(2013) Model monitorynhu domenu upravlinnia informatsiinoi merezhi viiskovoho pryznachennia [Military information network control domain monitoring model] *Systemy obrobky informatsii.* Vyp. 4(111). 118-122.

7. Tewari N., Bhardwaj A. (2013) Flow Statistics Based Detection of Low Rate and High Rate DDoS Attacks *International Journal of Scientific & Engineering Research.* Vol. 4, 5. 348-353. (in English)

8. Xiao P., He J., Chen Y., Fu Y. A(2013) A new trusted roaming protocol in wireless mesh networks .*International Journalof Sensor Networks*,14, Issue 2. P. 109 -119. (in English) https:// doi.org/ 10.1504/IJSNET.2013.056610 89

9.Ofitsiinyi sait Common Vulnerabilities and Exposures. Rezhym dostupu: http://cve.mitre.org(in English)

10. Ofitsiinyi sait National Vulnerabilities Database. Rezhym dostupu: http://nvd.nist.gov(in English)

11.Ofitsiinyi sait United States Computer Emergency Readiness Team. Rezhym dostupu: http://www.us-cert.gov(in English)

12. Zhang Y., Lee W., Huang Y. (2003) Intrusion detection techniques for mobile wireless networks. Wireless Networks Journal (ACM WINET). 2003. № 9(5). P. 545–556. (in English)

13. Janakiraman R., Waldvogel M., Zhang Qi. (2003) A peer-to-peer approach to networkintrusion detection and prevention. Enabling Technologies: Infrastructure for Collaborative Enterprises. . P. 226–231, DOI:10.1109/ENABL. 2003.1231412 (in English)

14. Alshboul Y., Streff K.(2015), Analyzing Information Security Model for Small-Medium Sized Businesses, Twenty-first Americas Conference on Information Systems, Puerto Rico (in English)

15.Safa N.S., Solms R.V., Furnell S.(2016) Information security policy compliance model in organizations. Computers & Security. 2016. Vol. 56. P. 70-82. DOI:10.1016/j.cose.2015.10.006 (in English)

Ph.D. Koval M., Ph.D. Kravchenko O., Shamraii N., Karpenko A.

ANALYSIS OF VULNERABILITIES AND CYBERATTACKS ON INFORMATION RESOURCES PROCESSED WITHIN INFORMATION SYSTEMS

The article examines the state of security across critical infrastructure and the technosphere as a whole. Typically, four types of facilities are distinguished based on their degree of potential dangers and specific protection requirements: technical control facilities, hazardous industrial facilities, critically significant facilities, and strategically priority military facilities able to affect national security.

Information technologies provide a crucial effect by allowing the precise regulation of informational influence based on the recipient. Multiple variations of virtual reality can be generated; moreover, this environment can be dynamically adapted to the needs of a specific user at the very moment they submit a request.

It is demonstrated that for the effective operation of an information system (IS), an appropriate security assurance subsystem should be integrated into the information resource (IR) management system. This subsystem must be capable of assessing and managing the IS security condition in real time, accounting for the rapidly evolving nature of cyberattacks.

The paper formulates the concept of information weaponry, which combines the electronic and human aspects of information technologies. Consequently, the continuous daily operation of various automated systems (AS) and information systems (IS) is of critical importance. Conversely, humans remain the primary strategic target of information weapons. Information systems must possess the capability to detect and prevent intrusions which are realized by a multitude of attacks of different types in terms of their physical nature. To facilitate this, the information security system (ISS) must incorporate a security information and event management (SIEM) system.

Keywords: information resources, information system, cyber threat, information weapons, cyberattack combinations, information security system.