УДК 004.056 DOI: 10.30748/soi.2019.157.17

С.В. Сальник, А.С. Сторчак, А.Є. Крамський

Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут ім. І. Сікорського", Київ

АНАЛІЗ ВРАЗЛИВОСТЕЙ ТА АТАК НА ДЕРЖАВНІ ІНФОРМАЦІЙНІ РЕСУРСИ, ЩО ОБРОБЛЯЮТЬСЯ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

В статті розглянуто вразливості та атаки на державні інформаційні ресурси, що обробляються засобами інформаційно-телекомунікаційних систем для визначення множини параметрів при оцінці захищеності державних інформаційних ресурсів. Розглянуто порушення у сфері використання електронно-обчислювальних засобів, телекомунікаційних систем і комп'ютерних мереж. Представлено загальну структуру реалізації атаки. Проведено аналіз вразливостей інформаційно-телекомунікаційних систем обробки державних інформаційних ресурсів та атак на системи обробки державних інформаційних ресурсів. Розглянуто сучасні бази даних, які містять детальний опис вразливостей та атак. Представлено класифікацію атак та параметри цих атак. Описано стратегії здійснення атак. Розглянуто основні фази та особливості проведення атак. Висунуто перелік вимог до методів виявлення атак. Визначено, що реалізація загроз відбувається за допомогою множини різнонаправлених атак. Запропоновано для визначення множини параметрів при оцінці захищеності державних інформаційних ресурсів, що обробляються засобами інформаційно-телекомунікаційних систем, забезпечити функціонування систем виявлення атак та визначення вразливостей з урахуванням вимог до методів виявлення атак, параметрів даних та характеристичних особливостей сучасних систем виявлення атак.

Ключові слова: *державні інформаційні ресурси, інформаційно-телекомунікаціні системи, атаки на державні інформаційні ресурси, фази атак, класифікація атак, вразливості систем.*

Вступ

На фоні ключової ролі системи забезпечення кібербезпеки вкрай значущою стає вимога забезпечення безпеки державних інформаційних ресурсів (ДІР) в кіберпросторі та, як наслідок, спроможності системи управління та підсистем забезпечення безпеки або кібербезпеки здійснювати достовірне та своєчасне визначення впливу загроз на стан безпеки державних інформаційних ресурсів на основі оцінки зміни значень множини окремих показників. Центральним питанням для прийняття рішень в підсистемі забезпечення кібербезпеки є питання достовірного визначення впливу окремих загроз на стан безпеки державних інформаційних ресурсів в цілому.

З позиції теорії систем, дані системи відносяться до класу складних систем, математично строге моделювання яких, як правило, становить актуальне завдання [1]. Ситуація ускладнюється тим, що різні об'єкти кіберзахисту відносяться до компетенції різних суб'єктів національної системи кібербезпеки та мають індивідуальну схильність до використання нормативних документів.

Дослідженню вразливостей інформаційно-телекомунікаційних систем (ІТС) присвячені роботи В.М. Базилевича, С.В. Віхорева, С.В. Казмирчук, М.Г. Луцького, Г.Ф. Конаховича, О.К. Юдіна, І.Б. Яковіва, О.Г. Корченка та інших [1–6]. Але недостатньо дослідженою залишилась задача визначення основних типів вразливостей ІТС.

Метою даної роботи є аналіз вразливостей та атак на державні інформаційні ресурси, що обробляються засобами ІТС для визначення множини параметрів при оцінці захищеності ДІР.

Об'єктом розгляду даної статті є процес забезпечення безпеки ДІР, яка обробляється в ІТС.

Предметом дослідження є вразливості ІТС, в яких обробляються ДІР, та атаки зловмисників, які використовуються при проведенні вторгнень.

Виклад основного матеріалу

Державні інформаційні ресурси (ДІР) являють собою систематизовану інформацію, що є доступною за допомогою інформаційних процесів, що використовують засоби обчислювальної техніки та забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування. Під обробкою ДІР розумітимемо виконання однієї або кількох операцій, а саме: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів. Від надійного виконання зазначених операцій та рівня захищеності ДІР в значній мірі залежить функціону-

вання ІТС та ефективна робота державних установ та організацій.

Порушення рівня захищеності у сфері використання електронно-обчислювальних засобів, телекомунікаційних систем і комп'ютерних мереж розподіляються на такі види:

– несанкціонований доступ до роботи автоматизованих систем, комп'ютерних мереж, баз даних;

– створення з метою використання, поширення або збуту шкідливих програмних продуктів або технічних засобів, а також їх розповсюдження або збут;

– несанкціонований збут або поширення інформації з обмеженим доступом, яка зберігається в автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;

– злочини, що здійснені шляхом використання комп'ютерної системи як засобу досягнення злочинної мети тощо.

Атаки реалізуються зловмисниками для порушення конфіденційності, цілісності або доступності ДІР, що зберігається, обробляється та циркулює в ІТС. З цією метою, як правило, використовують вразливості ІТС, тобто нездатність системи протистояти реалізації певної загрози або сукупності загроз. Структура реалізації атак представлена на рис. 1.

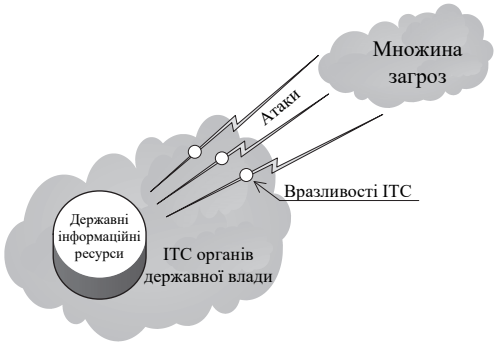

Рис. 1. Загальна структура реалізації атак

Проведемо аналіз таких характеристик безпеки ДІР, як: загрози на ДІР, аналіз можливих вразливостей ДІР та атак на ДІР. Також розглянемо сучасні бази даних, які містять детальний опис вразливстей атак та загроз, які взаємодіють між собою на рівнях моделі OSI.

У рамках моделі OSI, взаємодія між системами відбувається фактично у вигляді двох моделей – горизонтальної та вертикальної (ієрархічної та розподільної):

– у рамках горизонтальної (розподільчої) моделі розглядається пряма взаємодія (обмін даними) однакових рівнів у двох кінцевих точках (хостах); для організації такої взаємодії в кожній з кінцевих точок повинні підтримуватися однакові протоколи для даного рівня;

– у вертикальній (ієрархічній) моделі розглядається обмін інформацією (взаємодія) між сусідніми рівнями однієї системи з використанням інтерфейсів; у цій моделі кожен рівень може надавати свої послуги вищому рівню, і користуватися послугами нижчого рівня (крайні рівні моделі в цьому сенсі є винятком – прикладний рівень надає свої послуги користувачу, а фізичний рівень не користується сервісом інших рівнів).

Перші інциденти порушення інформаційної безпеки, офіційно зареєстровані в базах даних вразливостей, з'явилися в 1988 році [7–10]. З тих пір ведеться постійний пошук вразливостей та їх реєстрація як в рамках різних відкритих проектів, так і комерційними компаніями, дослідницькими інститутами та дослідниками. Серед лідерів детектування вразливостей можливо зазначити наступних розробників відповідних баз даних вразливостей: компанія MITRE та її база вразливосей Common Vulnerabilities and Exposures (CVE) [7]; National Institute of Standardsand Technology та база National Vulnerabilities Database (NVD) [8]; United State Computer Emergency Readiness Team та база Vulnerability Notes Database (VND) [9], компанія IBM та база вразливостей X-Force [10] та інші [11–13].

Розглянемо більш детально деякі з зазначених баз вразливостей:

– CVE – довідково-пошукова система посилань та позначень вразливостей. Важливою складовою системи є CVE ідентифікатори – унікальні ідентифікатори, що надаються кожній відомій вразливості в сфері інформаційної безпеки. Система містить більше 98000 записів про окремі вразливості [7]. Основна відмінність полягає в тому, що вона є найбільш повною та систематизованою, тому її використовують як основу для визначення відповідності записів вразливостей в інших базах. До основних елементів структури записів вразливостей відносяться:

1) статус – в цьому полі може міститися або значення Entry (перевірений запис), або значення Candidate (ще не перевірена вразливість);

2) фаза – в цьому полі міститься значення етапу розвитку вразливості, а також дата присвоєння зазначеного етапу. Можуть бути наступні значення:

– Proposed – фаза пропозиції вразливості;

– Interim – проміжна фаза вразливості;

– Modified – фаза модифікації вразливості;

– Assigned – фаза встановлення вразливості;

3) опис – поле містить опис вразливості;

4) посилання – в даному полі містяться посилання на інші джерела із зазначенням конкретної адреси інтернет-ресурсу опису вразливості і ідентифікатора джерела;

5) голоси – поле містить імена членів голосування, які прийняли рішення про занесення вразливості в базу;

6) коментарі – вноситься ім'я автора коментаря та його текстовий зміст.

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

Процес додавання вразливості в базу містить три етапи:

1) обробку – аналіз, дослідження і процес приведення вразливості до формату CVE;

2) присвоєння – призначення конкретному запиу вразливості ідентифікатора CVE;

3) публікацію – створення нового запису і публікація його на інтернет-ресурсі CVE, як тільки ідентифікатор CVE офіційно присвоєно.

До недоліків бази CVE слід віднести – відсутність механізму опису належності вразливостей до конкретних продуктів, а також присвоєння вразливостям метрик і розрахунку ступеня небезпеки [7].

– 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. На 2017 рік база даних вразливостей NVD мала близько 70000 записи вразливостей [8].

Структура запису вразливості в базі NVD є розширеною формою подання запису в базі CVE, за рахунок наявності наступних полів: конфігурація вразливих продуктів з урахуванням залежностей; список вразливих продуктів; показники, 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.

Відмінною особливістю бази NVD є використання Common Platform Enumeration, що є одним з кращих словників продуктів серед відомих аналогів за рахунок великого числа записів і уніфікованого формату імен програмно-апаратного забезпечення [8]. Однак у даного формату представлення записів продуктів є недоліки, а саме:

– неоднозначність значень різних полів формату;

– недостатнє використання записів даного словника базою NVD.

– База вразливостей OSVDB створена для спільноти фахівців в області безпеки. Мета проекту полягає в тому, щоб забезпечити точну, деталізовану, актуальну інформацію про вразливість для систем забезпечення безпеки. Дана база містить понад 110 000 вразливостей [13].

Структура даної бази не суттєво відрізняється від раніше розглянутої бази NVD, однак варто відзначити наявність основних полів, таких як: "Ідентифікатор OSVDB"; "Дата виявлення"; "Ім'я виробника"; "Ім'я продукту"; "Версія продукту"; "Посилання"; "Рішення"; "Метрики вразливості".

– База вразливостей X-Force є проектом компанії IBM, що знаходиться у відкритому доступі в мережі Інтернет. Поля даних, що описують записи вразливостей цієї бази, не суттєво відрізняються від полів баз вразливостей, описаних раніше. Однак в їх склад входять елементи, що вказують на перевагу бази X-Force, таких як: поле "Наслідки", які представляють в формалізованому вигляді можливий результат експлуатації вразливості; поле TemporalScore, що є елементом системи метрик CVSS, використовуваної для оцінювання тимчасових характеристик вразливості [10].

Також слід відзначити наявність в даній базі описів і висновків про можливі вразливості. Зазначена база містить більше 70000 записів вразливостей, які поділяються на вразливості вищого, середнього та низького рівнів. Вразливості низького рівня небезпеки становлять всього 12%, середнього і високого рівня небезпеки 62 та 26% відповідно.

Зазначені вразливості можуть бути використані зловмисником для здійснення вторгнень у ІТС з метою порушення цілісності, доступності та конфіденційності інформації, яка передається в ІТС, або для деструктивного впливу на сам процес функціонування ІТС.

Таким чином, у ІТС має бути передбачена можливість щодо виявлення та запобігання вторгнень, які реалізуюсься множиною різнонаправлених за своїм фізичним змістом атак. Для забезпечення такої можливості система управління містить у своєму складі підсистему управління безпекою, функціонування якої повинно здійснюватися на основі відповідних методів виявлення атак або вторгнень (МВА).

Під вторгненням розуміємо несанкціонований вхід в ІТС в результаті дій, що порушують політику безпеки або обходять систему захисту. Питання захисту будь-якої ІТС від вторгнень та атак являє собою задачу, забезпечення якої покладається на МВА. Внаслідок чого при побудові МВА необхідно враховувати широкий спектр атак, які здатні впливати на ІТС практично на всіх рівнях мережевої моделі OSI.

Під атакою розуміємо спробу реалізації загрози. В свою чергу загроза являє собою будь-які обставини або події, що можуть бути причиною порушення функціонування інформаційним, прог-

рамним та апаратним складовим інформаційної системи, політиці безпеки, нанесення збитків, тощо.

Розглянемо нині використовуємі типи атак на ІТС обробки ДІР (табл. 1), та їх параметри.

Таблиця 1

Класифікація атак

Ознака атаки	Тип атаки	Характеристика атаки
За характером впливу	пасивні	Атаки, що не мають безпосереднього впливу на роботу системи, але можуть порушувати її політику безпеки. Практично неможливо виявити. Після атаки не залишається ніяких слідів. Приклад: прослуховування каналу зв'язку в мережі.
	активні	Атаки, що безпосередньо впливають на роботу системи (зміна конфігурації ІТС, порушення працездатності і т.д.) і порушують прийняту в ній політику безпеки. Практично всі типи віддалених атак є активними. Існує можливість виявлення, так як в результаті здійснення атаки в системі відбуваються певні зміни.
За метою впливу	порушення конфіденційності	Перехоплення інформації. Приклад: прослуховування каналу в мережі.
	порушення цілісності	Спотворення інформації. Приклад: впровадження помилкового об'єкта в ІТС.
	порушення доступності	Не відбувається несанкціонованого доступу (зберігається цілісність і конфіденційність), проте доступ до інформації легальних користувачів неможливий. Приклад: відмова в обслуговуванні (DoS).
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	У разі настання події, атакуючий здійснює постійне спостереження за станом операційної системи віддаленої цілі атаки і при виникненні певної події в цій системі починається вплив. Ініціатором здійснення початку атаки є об'єкт, що атакується. Приклад: переривання сеансу роботи користувача з сервером в мережевих операційних системах без видачі команди LOGOUT.
	безумовна атака	У разі безумовної атаки початок її здійснення безумовно по відношенню до мети атаки, тобто атака здійснюється негайно і безвідносно до стану системи і атакується об'єкта. Ініціатором здійснення початку атаки є атакуючий.
За наявністю зворотного зв'язку з об'єктом, який атакується	зі зворотним зв'язком	Атака зі зворотним зв'язком – атака, під час якої атакуючий отримує відповідь від об'єкта на частину своїх дій. Ці відповіді потрібні, щоб мати можливість продовжити атаку 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 (DoS).
По розташуванню атакуючого щодо атакує-мого об'єкта	внутрисегментна	Атака, при якій суб'єкт і об'єкт атаки знаходяться всередині одного сегменту мережі (сегмент – фізичне об'єднання станцій за допомогою комунікаційних пристроїв не вище канального рівня).
	міжсегментна	Міжсегментна атака – атака, при якій суб'єкт і об'єкт атаки знаходяться в різних сегментах мережі.
За кількістю атакуючих	розподілена	Атака, вироблена двома або більше атакуючими на одну і ту ж обчислювальну систему, об'єднаними єдиним задумом і в часі.
	нерозподілена	Нерозподілена атака проводиться одним атакуючим.

Опис стратегій здійснення атак, що використовуються при проведення атак на інформаційні системи, представлено в проекті корпорації The MITRE Adversarial Tactics, Techniques and Common Knowledge [15]. В свою чергу база даних (атак) та модель для оцінки поведінки зловмисників (при здійсненні вторгнень) являє собою матрицю ATT@CK, яка описує найбільш небезпечні фази атаки на ІТС, а саме:

– отримання початкового доступу (Initial Access) – представляє вектори, які використовують зловмисники для отримання доступу до мережі;

– виконання (Execution) – застосування методів, що призводять до виконання коду зловмисника в локальній або віддаленій системі;

– закріплення в атакуємій системі (Persistence) – будь-які зміни доступу або конфігурації системи, які забезпечують постійну присутність зловмисника в цій системі;

– підвищення привілеїв (Privilege Escalation) – зловмисник має скористатись слабкими місцями системи для отримання прав локального адміністратора або рівня system/root;

– обхід захисту (Defense Evasion) – набір атрибутів, які застосовує зловмисник для ухилення від виявлення;

– отримання облікових даних (Credential Access) – методи отримання доступу або контролю обліковими даними системи, домена або служби, що використовуються в системі;

– огляд (Discovery) – методи отримання зловмисником відомостей про систему і внутрішню мережу;

– горизонтальне просування (Lateral Movement) – методи збору інформації із системи без використання додаткових інфструментів;

– збір даних (Collection) – методи збору інформації;

– витік (Exfiltration) – матоди та атрибути видалення файлів і інформації з цільовою системи;

– управління і контроль (Command and Control) – взаємодія зловмисника з підконтрольними системами.

Аналіз останніх публікацій свідчить про те, що існуючі атаки, які застосовуються для проведення вторгнень в ІТС, поділяються на 5 категорій. Кожна з категорій містить множину типів атак, які використовуються для реалізації мети вторгнення. В свою чергу, кожен тип атаки несе загрозу мережі на відповідних рівнях мережевої моделі OSI та виконує свою функцію щодо здійснення деструктивного впливу на мережу [14]. До вказаних категорій атак відносять:

– Side-channel атаки (атаки сторонніми каналами) – атаки, спрямовані на вразливості в практичній реалізації криптосистеми. На відміну від теоретичного криптоанализа, атаки по сторонніх каналах використовуть інформацію про фізичні процеси в пристрої, які не розглядаються в теоретичному описі криптографічного алгоритму. До найчастіше застосованих Side-channel атак належать: probing attack, timing attack, fault–induction attack, power analysis attack, electromagnetic analysis attacks та інші атаки;

– DoS атаки – це мережеві атаки, спрямовані на створення ситуацій, коли у системі, що піддається вторгненню, відбувається відмова в обслуговуванні. Вказані атаки характеризуються генерацією великого об`єму трафіка, що призводить до перенавантаження та блокування сервера. До найчастіше застосованих DoS атак належать: back, land, neptune, pod, smurf, teardrop attacks та інші атаки;

– U2R атаки – пропонують отримання зареєстрованим користувачам привілеїв адміністратора. До U2R атак відносять наступні типи атак: buffer_overflow, loadmodule, perl, rootkit;

– R2L атаки, що характеризуються отриманням доступу незареєстрованого користувача до мережі з боку віддаленої станції. Поділяють R2L атаки на: ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster та інші атаки;

– Probe-атаки – сканування мережевих портів з метою отримання конфіденційної інформації. Probe-атаки поділяються на наступні типи: ipsweep, nmap, portsweep, satan та інші.

Кожна атака характеризується наявністю множини параметрів, при ідентифікації яких можливо співвіднести до окремого типу атак. Приклад параметрів атаки зазначено нище:

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,

та являє собою послідовність параметрів з'єднання, таких як: тривалість з'єднання, тип протоколу, послуга мережі, кількість байтів в повідомленні, стан з'єднання, кількість термінових пакетів, кількість невдалих спроб встановлення з'єднання, тощо.

Зазвичай атака поступає на інформаційно-телекомунікаційний ресурс у вигляді повідомлення з мовою, відео, аудію інформацією або даними. Дане повідомлення складається з наступних елементів: передзаголовок, заголовок, контрольна сума, текст повідомлення, завершення повідомлення, яке і ідентифікуються системою виявлення атак на предмет встановлення атаки. Вказані типи атак за своєю функцією можуть впливати на: управління ІТС, розмежування доступу, обмін пакетами, енергетичні характеристики, доступ до кодування, управління інформацією та інше.

З урахуванням особливостей функціонування ІТС, які обробляють ДІР, доцільно висунути перелік вимог до МВА, з метою їх застосування у ІТС:

– інтелектуалізація процесу встановлення вразливостей та виявлення атак;

– високу точність виявлення атак;

– високу швидкість виявлення атак;

– можливість виявлення нових атак;

– робота в умовах непередбачуваності;

– можливість самонавчання та ін.

Системи виявлення атак (СВА) служать механізмами моніторингу та спостереження підозрілої активності. Вони можуть виявити атакуючих, які змогли обійти Firewall, і видати звіт про це адміністратору, який, у свою чергу, зробить подальші кроки щодо запобігання атаки.

Висновки

Проведений аналіз вразливостей та атак на ДІР, що обробляються засобами ІТС, показав різноманіття підходів до побудови баз вразливостей, кожен має свої переваги та недоліки, але найбільш вагомим є орієнтованість сучасних баз вразливистей для використання в експертних системах. Сучасні ІТС обробки ДІР мають велику кількість зовнішніх і внутрішніх вразливостей, а реалізація їх відбувається за допомогою множини різнонаправлених атак. Поширення вразливостей окремого вузла ІТС може викликати появу додаткових загроз безпеці ДІР, що в ній оброблюються. Тому для визначення множини параметрів при оцінці захищеності ДІР в цілому та виявлення нових вразливостей доцільно забезпечити функціонування СВА з урахуванням вищезазначених вимог, параметрів даних та характеристичних особливостей сучасних СВА. Виходячи із сказаного, подальша робота буде направлена саме на аналіз сучасних СВА та МВА з метою встановлення можливостей їх застосування в системах забезпечення безпеки ДІР в ІТС.

Список літератури

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

2. Аналіз вразливостей корпоративних інформаційних систем / Д. Мехед, Ю. Ткач, В. Базилевич, В. Гур'єв, Я. Усов // Захист інформації. – 2018. – № 20(1). – С. 61-66. https://doi.org/10.18372/2410-7840.20.12453.

3. Грищук Р. Джерела первинних даних для розроблення шаблонів потенційно небезпечних кібератак / Р. Грищук, В. Охрімчук, В. Ахтирцева // Захист інформації. – 2016. – № 18(1). – С. 21-29.

4. Яковів І. Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека / І. Яковів // Information Technology and Security. – 2017. – № 5(9). – С. 134-144.

5. Корпань Я.В. Класифікація загроз інформаційній безпеці в комп'ютерних системах при віддаленій обробці даних / Я.В. Корпань // Реєстрація, зберігання і обробка даних. – 2015. – № 17(2). – С. 39-46.

6. Труш О.В. Цілісність інформації в інформаційно-телекомунікаційних системах спеціального призначення: загрози та методи захисту / О.В. Труш, О.А. Хахлюк // Сучасний захист інформації. – 2013. – № 2. – С. 31-35.

7. Офіціальний сайт Common Vulnerabilities and Exposures [Електронний ресурс]. – 2019. – Режим доступу: http://cve.mitre.org.

8. Офіціальний сайт National Vulnerabilities Database [Електронний ресурс]. – Режим доступу: http://nvd.nist.gov.

9. Офіціальний сайт United States Computer Emergency Readiness Team [Електронний ресурс]. – Режим доступу: http://www.us-cert.gov.

10. Офіціальний сайт X-Force [Електронний ресурс]. – Режим доступу: http://xforce.iss.net.

11. Офіціальний сайт Secuni [Електронний ресурс]. – Режим доступу: http://secunia.com.

12. Офіціальний сайт BugTraq [Електронний ресурс]. – Режим доступу: http://securityfocus.com.

13. Офіціальний сайт Open Source Vulnerabilities Data Base [Електронний ресурс]. – Режим доступу: http://osvdb.org.

14. Офіціальний сайт KDD Cup 1999 Data [Електронний ресурс]. – Режим доступу: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.

15. Офіціальний сайт The MITRE Corporation [Електронний ресурс]. – Режим доступу: http://attack.mitre.org.

References

1. Buryachok, V.L. (2013), "*Osnovy formuvannya derzhavnoyi systemy kibernetychnoyi bezpeky*" [*Basis for the formation of the state system of cybernetic security*], NAU, Kyiv, 432 p.

2. Mehed, D., Tkach, Yu., Bazilevich, V., Guriev, V. and Usov, Y. (2018), "Analiz vrazlyvostey korporatyvnykh informatsiynykh system" [Analysis of corporate information systems vulnerability], *Ukrainian Information Security Research Journal*, Vol. 20(1), pp. 61-66. https://doi.org/10.18372/2410-7840.20.12453.

3. Grishchuk, R., Okhrimchuk, V. and Akhtyrtseva, V. (2016), "Dzherela pervynnykh danykh dlya rozroblennya shabloniv potentsiyno nebezpechnykh kiberatak" [Sources of primary data for developing templates for potentially dangerous cyber attacks], *Ukrainian Information Security Research Journal*,Vol. 18(1), pp. 21-29.

4. Yakoviv, I. (2017), "Informatsiyno-telekomunikatsiyna systema, kontseptual′na model′ kiberprostoru i kiberbezpeka" [Information-telecommunication system, conceptual model of cyberspace and cybersecurity], *Information Technology and Security*, Vol. 5, No. 2 , pp. 134-144.

5. Korpan′, YA. (2015), “Klasyfikatsiya zahroz informatsiyniy bezpetsi v komp'yuternykh systemakh pry viddaleniy obrobtsi danykh” [Classification of information security threats to computer systems for remote data processing], *Data Recording, Storage & Processing*,Vol. 17(2), pp. 39-46.

6. Trush, O. and Khakhlyuk, O. (2013), “Tsilisnist′ informatsiyi v informatsiyno-telekomunikatsiynykh systemakh spetsial′noho pryznachennya: zahrozy ta metody zakhystu” [Target information in informational and telecommunication systems special purpose: threats and protection methods], *Modern Information Security*, Vol. 3, pp. 31-35.

7. The official site of Common Vulnerabilities and Exposure (2019), *Common Vulnerabilities and Exposures*, available at: www.cve.mitre.org.

8. The official site of National Vulnerabilities Database, available at: www.nvd.nist.gov.

9. The official site of United States Computer Emergency Readiness Team, available at: www.us-cert.gov.

10. The official site of X-Force, available at: www.xforce.iss.net.

11. The official site of Secuni, available at: www.secunia.com.

12. The official site of BugTraq, available at: www.securityfocus.com.

13. The official site of Open Source Vulnerabilities Data Base, available at: www.osvdb.org.

14. The official site of KDD Cup 1999 Data, available at: www.kdd.ics.uci.edu/databases/kddcup99/kddcup99.

15. The official site of The MITRE Corporation, available at: www.attack.mitre.org.

Надійшла до редколегії 11.03.2019
Схвалена до друку 23.04.2019

Відомості про авторів:

Сальник Сергій Васильович
кандидат технічних наук
заступник завідувача кафедри
Інституту спеціального зв’язку та захисту інформації
Національного технічного університету України
“Київський політехнічний інститут ім. І. Сікорського”,
Київ, Україна
https://orcid.org/0000-0003-4463-5705

Сторчак Антон Сергійович
старший викладач кафедри Інституту спеціального
зв’язку та захисту інформації Національного технічного
університету України “Київський політехнічний інститут
ім. І. Сікорського”,
Київ, Україна
https://orcid.org/0000-0002-5267-3122

Крамський Антон Євгенійович
аспірант кафедри Інституту спеціального зв’язку
та захисту інформації Національного технічного
університету України “Київський політехнічний інститут
ім. І. Сікорського”,
Київ, Україна
https://orcid.org/0000-0003-1431-242X

Information about the authors:

Sergey Salnyk
Candidate of Technical Sciences
Deputy Head of the Department of Institute
of Special Communications and Information Protection
of National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute”,
Kyiv, Ukraine
http:orcid.org/0000-0003-4463-5705

Anton Storchak
Senior Instructor of Institute
of Special Communications and Information Protection
of National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute”,
Kyiv, Ukraine
https://orcid.org/0000-0002-5267-3122

Kramskyi Anton
Doctoral Student of Institute of Special Communications
and Information Protection
of National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute”,
Kyiv, Ukraine
https://orcid.org/0000-0003-1431-242X

АНАЛИЗ УЯЗВИМОСТЕЙ И АТАК НА ГОСУДАРСТВЕННЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ, КОТОРЫЕ ОБРАБАТЫВАЮТСЯ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

С.В. Сальник, А.С. Сторчак, А.Е. Крамской

В статье рассмотрены уязвимости и атаки на государственные информационные ресурсы, которые обрабатываются средствами информационно-телекоммуникационных систем, для определения множества параметров при проведении оценки защищенности государственных информационных ресурсов. Рассмотрены нарушения в сфере использования электронно-вычислительных средств, телекоммуникационных систем и компьютерных сетей. Представлена общая структура реализации атаки. Показана взаимосвязь между такими характеристиками информационной безопасности: угрозы информации, уязвимости системы обработки государственных информационных ресурсов, атаки на информационно-телекоммуникационную систему. Проанализированы уязвимости информационно-телекоммуникационных систем обработки государственных информационных ресурсов и атаки на системы обработки государственных информационных ресурсов. Рассмотрены современные базы данных (CVE, NVD, X-Force, OSVDB и другие), которые содержат детальное описание уязвимостей и атак. Представлена классификация атак и параметры этих атак. Описаны стратегии осуществления атак. Рассмотрены основные фазы и особенности проведения атак. Выдви-

нуты требования к методам и систем обнаружения атак. Определено, что реализация угроз государственным информационным ресурсам осуществляется с помощью множества разнонаправленных атак с использованием уязвимостей информационно-телекоммуникационных систем. Предложено для определения множества параметров при оценке защищенности государственных информационных ресурсов, обрабатываемых средствами информационно-телекоммуникационных систем, обеспечить функционирование систем обнаружения атак и определения уязвимостей с учетом требований к методам обнаружения атак, параметров данных и характеристических особенностей современных систем обнаружения атак.

***Ключевые слова**: государственные информационные ресурсы, информационно-телекоммуникационные системы, атаки на государственные информационные ресурсы, фазы атак, классификация атак, уязвимости систем.*

ANALYSIS OF VARIABILITY AND ATTACK ON STATE INFORMATION RESOURCES PROCESSED IN INFORMATION AND TELECOMMUNICATION SYSTEMS

S. Salnyk, A. Storchak, A. Kramskyi

Vulnerabilities and attacks on state information resources, which are processed with the help of information and telecommunication systems for determine a variety of parameters when assessing the security of state information resources are considered. The violations in the use of electronic computing facilities, telecommunication systems and computer networks are considered. The general structure of the attack implementation is presented. The interrelation between such characteristics of information security: information threats, vulnerabilities of the state information resources processing system, attacks on the information and telecommunication system is shown. The vulnerabilities of information and telecommunication systems for processing state information resources and attacks on state information resources processing systems are analysed. Modern databases (CVE, NVD, X-Force, OSVDB and others) that contain a detailed description of vulnerabilities and attacks are considered. A classification of attacks and the parameters of these attacks are presented. Attack strategies, their main phases and features are described. Requirements for methods and systems for detecting attacks are described. It was determined that the realization of threats to state information resources is carried out using a variety of multidirectional attacks using vulnerabilities of information and telecommunication systems. It was proposed to determine the set of parameters in assessing the security of state information resources processed by means of information and telecommunication systems, to ensure the functioning of attack detection systems and vulnerability determination taking into account the requirements for attack detection methods, data parameters and characteristic features of modern attack detection systems.

***Keywords:** state information resources, information and telecommunication systems, attacks on state information resources, phases of attacks, classification of attacks, vulnerabilities.*