Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Факультет комп'ютерних наук
Спеціальність 125 «Кібербезпека»
Освітня програма «Безпека інформаційних та комунікаційних систем»

«Допущено до захисту»
Зав.кафедрою БІСТ
Сергій РАССОМАХІН

_____

« » 2022 р.

Пояснювальна записка

до кваліфікаційної роботи магістра

на тему: «Розробка методу класифікації рівня небезпеки вразливостей сучасних розподілених систем»

оцінка « » Керівник проф. Олійников Р.В.

Голова ЕК Рецензент Шумов О.І.

Доценко С.І. _____ Виконавець : студент групи КБ-61

Пономаренко В.В.

Харків – 2022

РЕФЕРАТ

Кваліфікаційна робота магістра складається зі змісту, вступу, чотирьох розділів, висновків, списку використаної літератури. Загальний об’єм роботи становить 94 сторінки, робота містить 7 таблиць, 6 ілюстрацій, використано 58 джерел.

Об’єкт дослідження - процес класифікації рівня небезпеки вразливостей сучасних розподілених систем.

Предмет дослідження - методи виявлення вразливостей.

Мета роботи - підвищення безпеки сучасних розподілених систем. Підвищення безпеки системи вимагає використання обґрунтованих засобів та методів пошуку недоліків. Від оперативної ідентифікації загроз суттєво залежить надійність системи.

Результати роботи - в результаті проведеного дослідження запропоновано метод класифікації вразливостей, розглянуті поширені загрози розподілених обчислень, проаналізовані стандарти кібербезпеки та шляхи їх впровадження в організацію. Також надано опис дискретної задачі оптимізації та розглянуті існуючі алгоритми вирішення зазначеної оптимізаційної задачі.

У кваліфікаційній роботі магістра досліджуються моделі розподілених обчислювальних систем, порівнюються їх переваги та недоліки. Перераховані задачі проектуванні розподіленої обчислювальної системи загального призначення. Розглянуті ряд завдань, які постають перед ІТ-фахівцем під час проведення аудиту безпеки та запропоновано ряд рішень щодо вирішення цих завдань, таких як скорочення витрат ресурсів, поліпшення процесу визначення аналітично доведених найпріорітетніших напрямів дій попередження загроз, спрощення аналітичної діяльності фахівця. В дослідженні порушені питання загроз кібербезпеки, класифікації мережевих атак, безпека розподілених обчислень. Розглядається наукова література стосовно методів протидії потенційним загрозам.

Ключові слова: РОЗПОДІЛЕНА СИСТЕМА, КІБЕРБЕЗПЕКА, ВРАЗЛИВІСТЬ, СТАНДАРТ, АЛГОРИТМ, БЕЗПЕКА РОЗПОДІЛЕНИХ ОБЧИСЛЕНЬ, КОМБІНАТОРНА ЗАДАЧА, КЛАСИФІКАЦІЯ.

ABSTRACT

The master's qualification work consists of a table of contents, introduction, four chapters, conclusions, list of references. The total volume of work is 94 pages, the work contains 7 tables and 6 illustrations, 58 sources are used.

The object of research is the process of classifying the hazard level of vulnerability of modern distributed systems.

The subject of the research is methods for detecting vulnerabilities.

The purpose of the work is to improve the security of modern distributed systems. Improving the security of the system requires the use of reasonable tools and methods to find flaws. The reliability of the system significantly depends on the rapid identification of threats.

Results of the work - as a result of the research, a method for classifying vulnerabilities is proposed, common threats to distributed computing are considered, cybersecurity standards and ways to implement them in the organization are analyzed. The discrete optimization problem is also described and the existing algorithms for solving this optimization problem are considered.

In the master's qualification work, models of distributed computing systems are studied, their advantages and disadvantages are compared. The tasks of designing a general-purpose distributed computing system are listed. A number of tasks that are faced by an IT specialist during a security audit are considered and a number of solutions to solve these problems are proposed, such as reducing resource costs, improving the process of determining analytically proven priority areas of action for preventing threats, simplifying the analytical activities of a specialist. The study covers issues of cybersecurity threats, classification of network attacks, and security of distributed computing. The scientific literature on methods of countering potential threats is considered.

Keywords: DISTRIBUTED SYSTEM, VULNERABILITY, DISTRIBUTED COMPUTING SECURITY, COMBINATORIAL PROBLEM, CLASSIFICATION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

ОС - операційна система

ПЗ - програмне забезпечення

ПК - персональний комп’ютер

API - Application Programming Interface (інтерфейс прикладного програмування)

AWS - Amazon Web Services (комерційна публічна хмара Amazon)

BSI - British Standards Institution (британський інститут стандартів)

CAS - Community Authorization Service (служба авторизації спільноти)

COBIT - Control Objectives for Information and Related Technologies (завдання управління для інформаційних і суміжних технологій)

CVE - Common Vulnerabilities and Exposures (база даних загальновідомих вразливостей інформаційної безпеки)

CVSS - Common Vulnerability Scoring System (стандарт для розрахунку кількісних оцінок вразливості)

DDoS - Distributed Denial of Service (розподілена атака типу «відмова в обслуговуванні»)

DoS - Denial of Service (атаки типу «відмова в обслуговуванні»)

DSM - Distributed Shared Memory (розподілена спільна пам'ять)

EALS - Enterprise Authorization and Licensing System (система авторизації та ліцензування підприємства)

GPS - Global Positioning System (глобальна система позиціонування)

IaaS - Infrastructure as a Service (інфраструктура як послуга)

IP - Internet Protocol (міжмережевий протокол)

ISA - International Society of Automation (міжнародне товариство автоматизації)

ISO - International Organization for Standardization (міжнародна організація по стандартизації)

LAN - Local Area Network (локальна обчислювальна мережа)

MAC - Media Access Control (управління доступом до посередників)

MitM - Man in the Middle (атака посередника)

MPI - Message Passing Interface (інтерфейс передачі повідомлень)

NIST - National Institute of Standards and Technology (національний інститут стандартів і технологій)

NIST CSF - NIST Cybersecurity Framework (фреймворк кібербезпеки)

NVD - National Vulnerability Database (національна база даних вразливостей)

OSVDB - Open Source Vulnerability Database (база даних вразливостей з відкритим кодом)

PaaS - Platform as a Service (платформа як послуга)

PCI DSS - Payment Card Industry Data Security Standard (стандарт безпеки даних індустрії платіжних карток)

PDCA - Plan-Do-Check-Act (планування-дія-перевірка-коригування)

P2P - Peer-to-Peer (однорангова мережа)

SaaS - Software as a service (програмне забезпечення як послуга)

SAN - Storage Area Network (мережа зберігання даних)

SLA - Service Level Agreement (угода про рівень сервісу)

SSI - Server Side Includes (включення на стороні сервера)

SSL - Secure Sockets Layer (рівень захищених сокетів)

TLS - Transport Layer Security (протокол захисту транспортного рівня)

ULC - User-Level Interactions (взаємодії на рівні користувача)

VND - Vulnerability Notes Database (база даних нотаток про вразливості)

VO - Virtual Organization (системи рівня віртуальної організації)

VOMS - Virtual Organization Membership Service (служба членства у віртуальній організації)

VPC - Virtual Private Cloud (хмарна виділена мережа)

VPN - Virtual Private Network (віртуальна приватна мережа)

WAN - Wide Area Network (глобальна обчислювальна мережа)

ВСТУП

Забезпечення належної безпеки інформаційних ресурсів є актуальним завданням у кіберпросторі. Згідно зі звітом Cisco Annual Internet Report (AIR), до 2023 року користувачами Інтернету стануть 66% населення Землі. До глобальної мережі будуть підключені більше 28 мільярдів пристроїв[1]. Зазначимо той факт, що на фоні росту кількості інтернет користувачів і підключених пристроїв буде спостерігатися зростання кібератак. Щодня інформаційні ресурси піддаються зазіханням сторонніми особами. Тому, критично важливим є ефективна протидія та мінімізація можливих збитків від потенційних загроз. Одним із способів протидії загрозам є своєчасне виявлення існуючих вразливостей системи. Виникає потреба в обґрунтованому наданні пріоритету виправлення знайденим недолікам, для того щоб першочергово усунути найбільш критичні вразливості. Отже актуальною є розробка методу класифікації рівня небезпеки вразливостей.

Метою досліджень є підвищення безпеки сучасних розподілених систем. Підвищення безпеки системи вимагає використання обґрунтованих засобів та методів пошуку недоліків. Від оперативної ідентифікації загроз суттєво залежить надійність системи.

Розподілені системи були створені з метою досягнення таких властивостей: прозорості, відкритості, надійності, продуктивності та масштабованості. Інтеграція різних розподілених компонентів створює нові проблеми безпеки. Отже, безпека є однією з провідних проблем при розробці розподілених систем. Питання безпеки в моделях розподілених обчислювальних систем часто знаходять відображення в сучасних наукових дослідженнях. Значна кількість робіт присвячена аналізу потенційних загроз, визначенню ефективних засобів і методів протидії поширеним недолікам інформаційних систем. Незважаючи на широке охоплення проблем безпеки в різноманітних наукових публікаціях, слід зазначити, що триваючий процес інтеграції різних розподілених компонентів в поточні та перспективні системи створює нові виклики для забезпечення надійної безпеки. Саме тому, такі задачі як своєчасне виявлення,

ідентифікація, нейтралізація недоліків в розподілених системах і надалі потребують уваги та вдосконалення.

Фахівці в області аудиту безпеки інформації в процесі своєї діяльності стикаються з вирішенням ряду інформаційно-аналітичних задач, таких як: аналіз інформаційних ризиків для своєчасного попередження потенційних загроз і збитків, виявлення недоліків у використовуваних механізмах захисту і підвищення їх ефективності, розробка рекомендацій щодо мінімізації ризиків та впровадження нових засобів захисту інформації. В сучасній практиці фахівцям з інформаційної безпеки нерідко доводиться здійснювати свою діяльність в умовах обмеженості задіяних ресурсів. Підсумкові результати аудиту в значній мірі залежать від кваліфікації залучених експертів, складності досліджуваного об'єкта і ступеня ефективності використовуваних методів та засобів. Для розгляду взяті наступні практичні задачі які постають перед фахівцем з інформаційної безпеки під час аудиту, а саме: задача класифікації виявлених вразливостей, задача вибору кращої стратегії усунення найкритичніших серед виявлених вразливостей. Розглянута модель задачі оцінки рівня небезпеки вразливостей та підхід для її подальшої реалізації на основі вирішення задачі дискретної оптимізації. Зазначена модель зведена до формулювання задачі про покриття множини та допустимістю застосування механізмів захисту інформації для попередження недоліків.

1 ОПИС ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ

1.1 Розподілена система

В наукових працях зарубіжних авторів зустрічаються різні визначення стосовно розподілених систем. Так наприклад, одне з найперших визначень розподіленої системи було надано професорами Амстердамського університету: Ендрю Таненбаум та Мартен ван Стін. Вони визначили розподілену систему як «сукупність незалежних комп'ютерів, яка представляється своїм користувачам як єдина узгоджена система»[2]. Британські інформатики Джордж Кулуріс, Джин Долімор, Тім Кіндберг, Гордон Блер визначили розподілену систему як «систему, в якій апаратні та програмні компоненти встановлюються на географічно віддалених комп'ютерах, які координують та співпрацюють у своїх діях, передаючи повідомлення між собою»[3]. Поєднуючи зазначені визначення, можна стверджувати, що розподілена обчислювальна система - це системна архітектура, яка взаємодіє з безліччю розсіяних апаратних засобів та програмного забезпечення для координації дій багатьох процесів, що працюють на різних автономних комп'ютерах через мережу зв'язку, так, що всі компоненти (апаратне та програмне забезпечення) взаємодіють разом для виконання набору пов'язаних завдань, які спрямовані на досягнення спільної мети[4]. У такому обчислювальному середовищі користувачі можуть рівномірно отримувати доступ до локальних або віддалених ресурсів і запускати процеси з будь-якої точки системи. У розподіленій системі вузли взаємодіють, надсилаючи та отримуючи повідомлення через мережу. Різні розподілені ресурси спільно використовуються через мережу між вузлами у вигляді мережевих служб, що надаються серверами. Мережа, кластери, сітки та хмари формують основу розподілених систем.

1.2 Переваги та задачі проектування розподілених обчислювальних систем

Розподілена система має ряд переваг перед централізованою системою, насамперед такі як економічність, швидкість, невід'ємний розподіл та поступове зростання. Крім того, розподілені обчислення забезпечують наступні переваги[5]

- Підвищена продуктивність: наявність декількох вузлів у розподіленій системі дозволяє паралельно обробляти додатки і тим самим підвищувати продуктивність додатків та системи в цілому.
- Спільний доступ до ресурсів: розподілені системи забезпечують ефективний доступ до різних системних ресурсів. Користувачі можуть спільно використовувати спеціальні і іноді дорогі апаратні та програмні ресурси, такі як сервер баз даних, обчислювальний сервер, сервер віртуальної реальності, сервер мультимедійної інформації.
- Підвищена розширюваність: розподілені системи розроблені таким чином, щоб бути модульними та адаптивними. Для певних обчислень система налаштує себе на включення великої кількості вузлів та ресурсів, тоді як в інших випадках вона буде складатися лише з декількох ресурсів. Крім того, ємність файлової системи і обчислювальна потужність можуть бути збільшені поступово. Найбільш відмінною особливістю розподіленої системи порівняно з централізованою є її модульна розширюваність.
- Підвищена надійність, доступність і відмовостійкість: об'єднання безлічі обчислювальних ресурсів і ресурсів зберігання в розподіленій системі робить привабливим та економічно ефективним впровадження надмірності з метою підвищення надійності і відмовостійкості системи. Система може вийти з ладу в одному вузлі, розподіляючи свої завдання на інший доступний вузол.

Проектування розподіленої обчислювальної системи загального призначення є складним процесом. Цей процес пов'язаний з багатьма труднощами, які доводиться долати дизайнерам, для того щоб досягти зазначених переваг. На фоні розширення сфери застосування і масштабу розподілених систем та додатків виникають нові задачі проектування[3]. Серед основних задач, такі як:

- Гетерогенність: розподілені системи дозволяють користувачам отримувати доступ до служб та запускати програми через неоднорідну сукупність комп'ютерів та мереж. Гетерогенність (тобто

різноманітність і відмінність) відноситься до всього нижчепереліченого: мереж, комп'ютерного обладнання, операційних систем, мов програмування і реалізацій різних розробників.

- Відкритість: відкритість комп'ютерної системи - це характеристика, яка визначає, чи можна розширювати та повторно впроваджувати систему різними способами. Відкритість розподіленої системи визначається, перш за все, ступенем, як нові служби спільного використання ресурсів можуть бути додані і доступні для використання різними клієнтськими програмами. Відкритість не може бути досягнута до тих пір, поки специфікація та документація ключових програмних інтерфейсів компонентів системи не буде доступна розробникам програмного забезпечення.
- Масштабованість: розподілені системи ефективно працюють у різних масштабах, починаючи від невеликої інтрамережі до Інтернету. Кількість комп'ютерів і серверів в Інтернеті різко зросла. Система описується як масштабована, якщо вона буде залишатися ефективною при значному збільшенні кількості ресурсів і числа користувачів.
- Прозорість розподілу: прозорість визначається як приховування від користувача та прикладного програміста розділення компонентів у розподіленій системі. Таким чином, система сприймається як єдине ціле, а не як набір незалежних компонентів. Проблема прагнення до прозорості розподілу в дуже великих системах полягає в тому, що продуктивність знизиться до неприйнятного рівня. Більш того, затримки в мережі мають природну нижню межу, яка стає помітною при роботі з далекомагістральними з'єднаннями.
- Планування: децентралізована організація планувальника зводить нанівець обмеження централізованої організації щодо стійкості, масштабованості та автономності. Цей підхід добре масштабується як для дрібномасштабного середовища спільного використання ресурсів (наприклад, спільного використання ресурсів у межах одного

адміністративного підрозділу), так і для великомасштабного середовища. Однак цей підхід створює серйозні проблеми управління розподіленою інформацією, забезпечення загальносистемної координації, безпеки, автентичності користувачів ресурсів та неоднорідності політики постачальника ресурсів.

- Безпека та довіра: багато інформаційних ресурсів, які надаються та підтримуються в розподілених системах, мають високу внутрішню цінність для своїх користувачів. Тому їх безпека має велике значення. Децентралізована організація розподілених систем створює серйозні проблеми в області безпеки і довірчого управління. Впровадження захищеної розподіленої системи вимагає рішень, здатних ефективно вирішувати різні проблеми безпеки.

1.3 Моделі розподілених обчислювальних систем

Розподілена обчислювальна система побудована на великій кількості автономних комп'ютерних вузлів. Ці вузли пов'язані між собою системними мережами (SAN), локальними мережами (LAN) або глобальними мережами (WAN) ієрархічним чином. Завдяки сучасним мережевим технологіям кілька комутаторів локальної мережі можуть легко з'єднати сотні машин в робочий кластер. Глобальна мережа може з'єднати багато локальних кластерів, щоб сформувати дуже великий кластер кластерів. У цьому сенсі можна побудувати масштабну систему, в якої мільйони комп'ютерів будуть підключені до прикордонних мереж в різних доменах Інтернету. Розподілені обчислення можна розділити на чотири класи, а саме: кластерні обчислення, мережі P2P, сіткові обчислення та хмарні обчислення. (Див. Таблиці 1.1-1.2). Масивні системи вважаються високомасштабованими і можуть забезпечити підключення до веб-масштабу як фізично, так і логічно. З точки зору кількості вузлів, ці чотири системні класи можуть включати сотні, тисячі або навіть мільйони комп'ютерів як вузли-учасники. Ці машини працюють колективно, спільно або злагоджено на різних рівнях[6].

Таблиця 1.1 – Класифікація паралельних і розподілених обчислювальних систем

Функціональність, додатки	Комп'ютерні кластери	Однорангові мережі
Архітектура, підключення до мережі та розмір	Мережа обчислювальних вузлів, з'єднаних SAN, локальною мережею або WAN ієрархічно	Гнучка мережа клієнтських комп'ютерів, логічно з'єднаних оверлейной мережею
Контроль та управління ресурсами	Однорідні вузли з розподіленим управлінням, що працюють під управлінням UNIX або Linux	Автономні клієнтські вузли, вільний вхід і вихід, з самоорганізацією
Додатки та мережеві сервіси	Високопродуктивні обчислення, пошукові системи, веб-сервіси і т. д.	Найбільш привабливий для бізнес - обміну файлами, доставки контенту і соціальних мереж
Репрезентативні операційні системи	Пошукова система Google, SunBlade, IBM Road Runner, Cray XT4 і т. д.	Gnutella, eMule, BitTorrent, Napster, KaZaA, Skype, JXTA

Таблиця 1.2 – Класифікація паралельних і розподілених обчислювальних систем

Функціональність, додатки	Дані / обчислювальні сітки	Хмарні платформи
Архітектура, підключення до мережі та розмір	Різнорідні кластери, з'єднані високошвидкісними мережевими з'єднаннями по обраним сайтам ресурсів	Віртуалізований кластер серверів у центрах обробки даних через SLA
Контроль та управління ресурсами	Централізоване управління, орієнтоване на сервер, з автентифікованою безпекою	Динамічне надання ресурсів серверам, сховищам і мереж
Додатки та мережеві сервіси	Розподілені суперкомп'ютери, глобальне вирішення проблем та послуги центрів обробки даних	Вдосконалений веб-пошук, службові обчислення та аутсорсингові обчислювальні послуги
Репрезентативні операційні системи	TeraGrid, GriPhyN, UK EGEE, D-Grid, ChinaGrid та ін.	Google App Engine, IBM Blue cloud, AWS і Microsoft Azure

1.4 Кластерні обчислення

Комп'ютерні кластери - це набір комп'ютерів згрупованих разом, які взаємодіють через високошвидкісну мережу, і їх можна представити користувачам як єдиний комп'ютер. Будь-яке завдання, призначене кластеру, буде виконуватися на всіх вузлах кластера паралельно, розбиваючи все завдання на менші автономні завдання. Потім результати менших завдань будуть об'єднані, щоб сформувати кінцевий результат. Кластерні обчислення допомагають організаціям збільшити свої обчислювальні потужності, використовуючи стандартні та загальнодоступні

технології. Кластери використовуються в основному для запуску наукових, інженерних, комерційних та промислових застосувань, що вимагають високої доступності та високої пропускної здатності обробки. Розглянемо архітектуру типового серверного кластера, побудованого навколо мережі взаємозв'язків з низькою затримкою та високою пропускною здатністю. (Див. Рисунок 1.1). Кластер серверів, з'єднаних між собою широкосмуговою мережею SAN або локальною мережею із спільними пристроями вводу-виводу та дисковими масивами; кластер діє як єдиний комп'ютер, підключений до Інтернету[6].

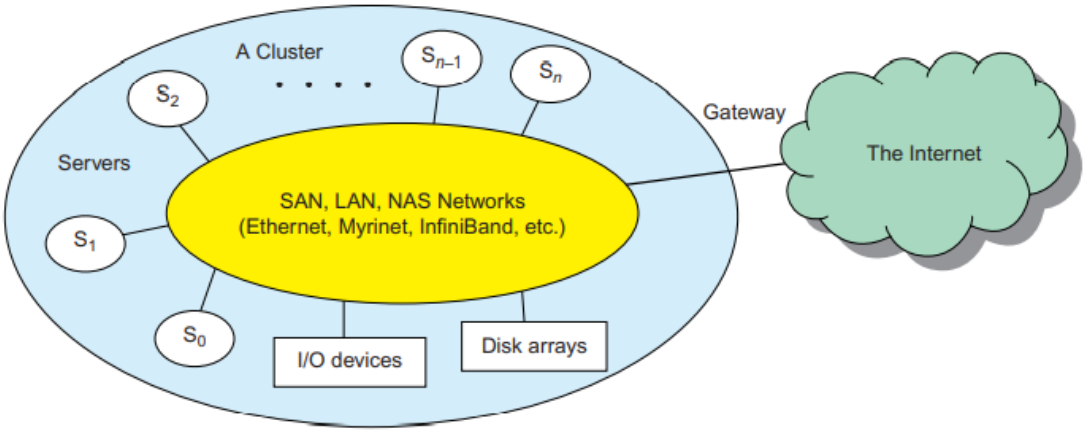

Рисунок 1.1 - Архітектура типового серверного кластера

Ідеальний кластер повинен об'єднати кілька системних зображень в єдине системне зображення (SSI)[7]. Розробники кластерів прагнуть, щоб кластерна операційна система або якесь проміжне програмне забезпечення підтримували SSI на різних рівнях, включаючи спільний доступ до процесорів, пам'яті та вводу-виводу на всіх вузлах кластера. SSI - це ілюзія, створена програмним або апаратним забезпеченням, яке представляє набір ресурсів як єдиний інтегрований, потужний ресурс. SSI робить кластер схожим на єдину машину для користувача. Кластер з декількома системними зображеннями - це не що інше, як набір незалежних комп'ютерів. Проміжне програмне забезпечення або розширення ОС були розроблені в просторі користувача для досягнення SSI на вибраних функціональних рівнях. Без цього проміжного програмного забезпечення вузли кластера не зможуть ефективно працювати разом для досягнення спільних обчислень. Програмні середовища та програми повинні покладатися на проміжне

програмне забезпечення для досягнення високої продуктивності. Переваги кластера полягають у масштабованій продуктивності, ефективній передачі повідомлень, високій доступності системи, безперебійній відмовостійкості та управлінні завданнями в масштабах кластера[6].

1.5 Peer-to-Peer (P2P)

Як приклад добре налагодженої розподіленої системи добре зарекомендувала себе архітектура клієнт-сервер. У цьому сценарії клієнтські комп'ютери (ПК та робочі станції) підключаються до центрального сервера для роботи з комп'ютерами, електронною поштою, програмами для доступу до файлів та баз даних. Архітектура P2P пропонує розподілену модель мережевих систем. Мережа P2P орієнтована на клієнта, а не на сервер. У системі P2P кожен вузол діє як клієнт і сервер, забезпечуючи частину системних ресурсів. Однорангові комп'ютери - це просто клієнтські комп'ютери, підключені до Інтернету. Всі клієнтські машини діють автономно, вільно приєднуючись до системи або залишаючи її. Це означає, що між одноранговими вузлами не існує відносин "ведучий-ведений". Не потрібна централізована координація або центральна база даних. Іншими словами, жодна однорангова машина не має глобального уявлення про всю систему P2P. Система самоорганізується з розподіленим управлінням.

Розглянемо структуру мережі P2P на двох рівнях абстракції. Структура системи P2P шляхом зіставлення фізичної IP-мережі з накладеною мережею, побудованою за допомогою віртуальних посилань. (Див. Рисунок 1.2)[6].

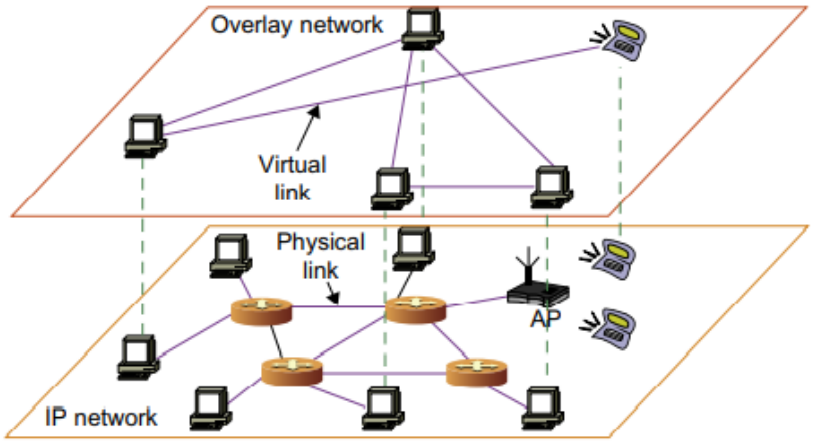

Рисунок 1.2 - Структура P2P системи

Спочатку однорангові вузли абсолютно не пов'язані між собою. Кожна однорангова машина добровільно приєднується до мережі P2P або залишає її. Тільки залучені однорангові вузли формують фізичну мережу в будь-який час. На відміну від кластера або сітки, мережа P2P не використовує виділену мережу взаємозв'язків. Фізична мережа - це просто спеціальна мережа, сформована в різних доменах Інтернету випадковим чином за допомогою протоколів TCP/IP та NAI. Таким чином, фізична мережа динамічно змінюється за розміром та топологією завдяки безкоштовному членству в мережі P2P.

Елементи даних або файли поширюються серед однорангових вузлів. Виходячи з потреб у спілкуванні або спільному використанні файлів, ідентифікатори вузлів формують накладену мережу на логічному рівні. Існує два типи накладених мереж: неструктуровані та структуровані. Неструктурована накладена мережа характеризується випадковим графіком. Фіксованого маршруту для надсилання повідомлень або файлів між вузлами не існує. Структуровані накладені мережі працюють відповідно до певної топології підключення та правил вставки та видалення вузлів з графіка накладення. Це накладання являє собою віртуальну мережу, сформовану шляхом логічного зіставлення кожної фізичної машини з її ідентифікатором за допомогою віртуального зіставлення. (Див. Рисунок 1.2). Коли новий одноранговий вузол приєднується до системи, його одноранговий ідентифікатор додається як вузол в накладеній мережі. Коли існуючий одноранговий вузол залишає систему, його ідентифікатор автоматично видаляється з накладеної мережі. Отже, саме накладена мережа P2P характеризує логічний зв'язок між одноранговими вузлами.

В залежності від застосування мережі P2P поділяються на чотири групи. (Див. Таблиця 1.3). Перше сімейство призначене для розподіленого обміну файлами цифрового контенту в мережі P2P. Це включає в себе багато популярних P2P-мережі, такі як Gnutella, Napster і BitTorrent. Спільні мережі P2P включають, серед іншого, чат MSN або Skype, миттєві повідомлення та дизайн співпраці. Третя сім'я призначена для розподілених обчислень P2P у конкретних додатках. Інші

платформи P2P, такі як JXTA.net підтримують іменування, виявлення, зв'язок, безпеку та агрегацію ресурсів у деяких програмах P2P[6].

Таблиця 1.3 - Основні категорії сімейств мереж P2P

Системні характеристики	Розподілений обмін файлами	Платформа для спільної роботи	Розподілені P2P-обчислення	Платформа P2P
Додатки	Поширення контенту в форматі MP3, відео, відкритого програмного забезпечення	Обмін миттєвими повідомленнями, спільний дизайн та ігри	Наукові дослідження та соціальні мережі	Відкриті мережі для громадських ресурсів
Операційні проблеми	Слабка безпека та серйозні порушення авторських прав в Інтернеті	Відсутність довіри, порушення приватності, спам	Недоліки в безпеці, егоїстичні партнери	Відсутність стандартів або протоколів захисту
Приклади систем	Gnutella, Napster, eMule, BitTorrent, Aimster, KaZaA, etc.	ICQ, AIM, Groove, Magi, Multiplayer Games, Skype, etc.	SETI@home, Geonome@home, etc.	JXTA, .NET, FightingAid @home, etc.

Переваги систем зв'язку P2P полягають у тому, що загальносистемна координація може бути розподілена, відтворена та сегментована (наприклад, кожен набір даних отримує унікальний торрент у BitTorrent). Координація в системах P2P обчислювально дешева і може виконуватися практично будь-яким вузлом у системі, а вимоги до координаційної мережі невеликі, що дозволяє вузлам з великими відмінностями в якості каналу брати участь у мережах. Мережі P2P в цілому

утворюють стійкі та масштабовані віртуальні інфраструктури, які добре підходять для відображення в розподілені гетерогенні мережі, такі як Інтернет. Однак загальна застосовність P2P-інфраструктур для обчислювальної науки невелика, і застосування P2P-мереж, як правило, обмежується додатками для поширення даних з низькими вимогами до безпеки[8].

1.6 Grid обчислення

Grid (розподілені або сіткові обчислення) - це тип розподіленої обчислювальної системи, в якій сукупність різнорідних комп'ютерів і ресурсів розподілена по декількох адміністративних доменах з метою надання користувачам легкого доступу до цих ресурсів. Grid визначається як паралельна та розподілена система, яка здатна динамічно вибирати, ділитися та агрегувати географічно розподілені ресурси під час виконання на основі їх доступності, можливостей, продуктивності і вартості, що відповідають вимогам користувачів до якості обслуговування[4].

Grid обчислення можна розглядати як гетерогенні кластери, з'єднані високошвидкісними мережами. Вони мають централізований контроль, орієнтовані на сервер з автентифікованою безпекою[2]. Grid обчислення об'єднують обчислювальні ресурси, розподілені по великій географічній території, що належать різним особам і організаціям. За допомогою мережевих обчислень організація може прозоро інтегрувати, оптимізувати та ділитися розсіяними, неоднорідними пулами хостів, серверів, сховищ, даних, мереж та датчиків в єдину синергетичну систему. Grid система, розподілена по різнорідних обчислювальних платформах. (Див. Рисунок 1.3)[4]. Однією з основних стратегій обчислювальної мережі є використання проміжного програмного забезпечення для розділення та розподілу частин програми між кількома комп'ютерами. Проміжне програмне забезпечення - це програмне забезпечення, яке забезпечує обмін даними та управління ними в розподілених додатках. Призначення проміжного програмного забезпечення полягає в тому, щоб дозволити різним комп'ютерам запускати додаток по всій мережі комп'ютерів. Без цього комунікація по всій системі була б неможлива. Як і програмне забезпечення в цілому, для проміжного програмного

забезпечення не існує єдиного формату. Проміжне програмне забезпечення і вузол управління «ґрід-обчислювальної» системи відповідають за безперебійну роботу системи. Разом вони розділяють і розподіляють частини програми на кілька тисяч комп'ютерів і контролюють обсяг доступу кожного комп'ютера до ресурсів мережі і навпаки. Проміжне програмне забезпечення «ґрід» дозволяє різнорідним системам працювати спільно, створюючи видимість великого віртуального обчислювального середовища, пропонуючи при цьому безліч віртуальних ресурсів.

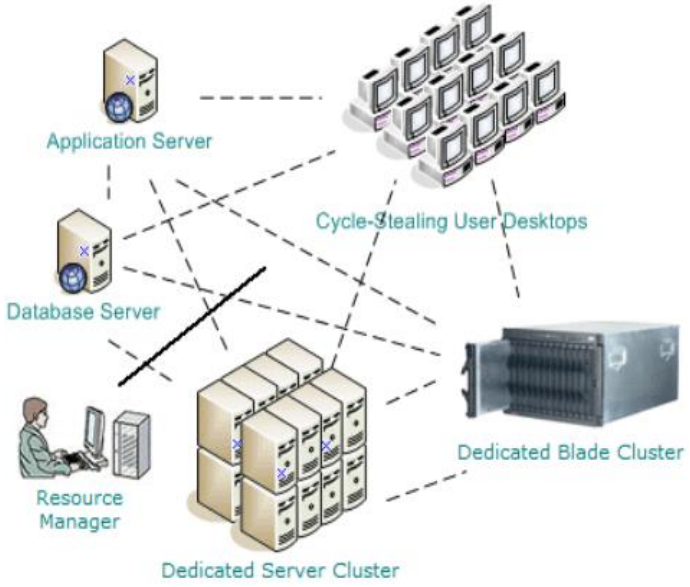

Рисунок 1.3 – Grid обчислювальна система

Подібно до електромережі комунального підприємства, обчислювальна «сітка» пропонує інфраструктуру, яка об'єднує комп'ютери, програмне забезпечення / проміжне програмне забезпечення, спеціальні прилади, а також людей і датчики. Мережа часто будується через магістральні мережі LAN, WAN або Internet в регіональному, національному або глобальному масштабі. Підприємства або організації представляють мережі як інтегровані обчислювальні ресурси. Їх також можна розглядати як віртуальні платформи для підтримки віртуальних організацій. Комп'ютери, що використовуються в мережі, - це насамперед робочі станції, сервери, кластери та суперкомп'ютери. Персональні комп'ютери, ноутбуки та КПК можуть використовуватися як пристрої доступу до мережевої системи.

Існує три основних типи комп'ютерних «сіток»: обчислювальні «сітки», «сітки» даних та сервісні «сітки»[9]:

- Обчислювальні «сітки» (computational grids): зосередження на виділенні ресурсів спеціально для обчислювальної потужності (розв'язування рівнянь та складних математичних задач). Хоча машини, що беруть участь у сітці такого типу, зазвичай є високопродуктивними серверами. Програми з нескінченними циклами можуть бути використані для руйнування вузлів цієї «сітки» і зменшення функціональності.
- Інформаційні «сітки» (data grids): відповідає за зберігання та надання доступу до великих обсягів даних, часто в декількох організаціях. Однак користувачі можуть перезаписувати дані інших користувачів, якщо вони перевищують доступний їм простір. Це призводить до пошкодження даних інших користувачів.
- Сервісні «сітки» (service grids): надають послуги, які недоступні на одному комп'ютері. Однак користувачі можуть використовувати сервісні «сітки» для запуску атаки «відмови в обслуговуванні» (DoS) проти іншого сайту.

Перераховані вище типи «сіток» представляють три загальні категорії «ґрід-обчислювальних» систем, деякі «ґрід» системи можуть використовувати аспекти інших або всіх трьох типів «сіток», що робить їх гібридними «ґрід-обчислювальними» системами. За національними проектами «ґрід» слідують розробки промислових «ґрід-платформ» IBM, Microsoft, Sun, HP, Dell, Cisco, EMC, Platform Computing та інші. Швидко з'явилися нові постачальники мережевих послуг (GSP) та нові мережеві програми, подібні до зростання Інтернету та веб-сервісів за останні два десятиліття. Використання «ґрід-технології» дозволяє науковому співтовариству вивчати проблеми, занадто масштабні для вирішення за допомогою звичайних обчислювальних технологій. Використання «сіток» призвело до створення нових типів додатків та нових способів використання

існуючих обчислювальних технологій. Додатки Grid в залежності від вимог можуть бути розділені на такі категорії, як[8]:

- Обчислювальні витрати. Наприклад зусилля з інтерактивного моделювання, проект SIMRI, та дуже масштабні програми для моделювання та аналізу, такі як Astrophysics Simulation Collaboratory.
- Інтенсивне використання даних. Наприклад проекти експериментального аналізу даних, такі як European Data Grid[10], та програми для аналізу зображень та датчиків, такі як SETI@home[11].
- Розподілені зусилля для співпраці, такі як інструменти вимірювання в Інтернеті, ROADnet, сегментоване моделювання та аналіз, такі як Folding@home, або віддалені проекти візуалізації, такі як віртуальна обсерваторія[12].

Підводячи підсумок, інфраструктура обчислювальної «сітки» повинна забезпечувати гнучкий та безпечний доступ до ресурсів та їх використання за допомогою скоординованих моделей спільного використання ресурсів для динамічних колекцій окремих осіб та організацій. Ресурси та користувачі повинні бути організовані у віртуальних організаціях, а системи повинні бути позбавлені централізованого контролю.

1.7 Хмарні обчислення

Національний інститут стандартів і технологій (NIST) надав наступне визначення хмарних обчислень: «Хмарні обчислення - це модель забезпечення повсюдного, зручного доступу до мережі на вимогу до спільного пулу користувацьких обчислювальних ресурсів (наприклад, мереж, серверів, сховищ, додатків та служб), які можна швидко підготувати та випустити з мінімальними зусиллями щодо управління або взаємодії з постачальником послуг. Ця хмарна модель складається з п'яти основних характеристик, трьох моделей обслуговування та чотирьох моделей розгортання»[13].

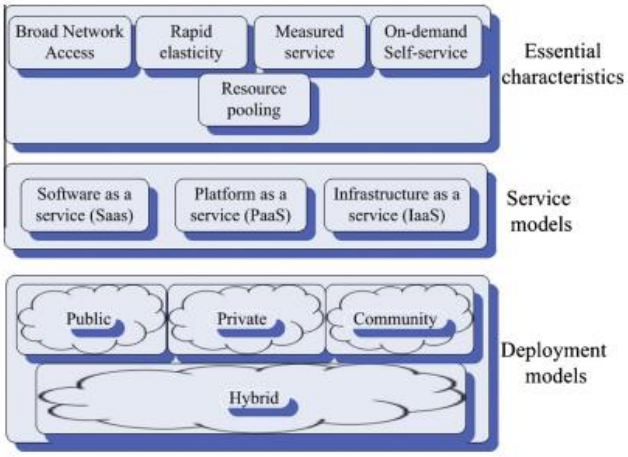

Рисунок 1.4 - Хмарна модель відповідно до визначення NIST

Парадигма хмарних обчислень виникла в результаті злиття ряду тенденцій розробки програмного забезпечення та побудови інфраструктури, наприклад, автономні обчислення, «сіткові» обчислення, віртуалізацію та сервісно-орієнтовану розробку програмного забезпечення. Технологічному розвитку хмарних обчислень сприяла розробка ефективної технології апаратної паравіртуалізації і гіпервізорів (моніторів віртуальних машин), таких як Xen, VMware і KVM[14].

Характеристики хмарних обчислень[13]:

- Самообслуговування на вимогу. Користувачі можуть запитувати послуги з хмари та керувати ними без будь-якої взаємодії людини з постачальником хмарних послуг (CSP). Надання послуг і пов'язаних з ними ресурсів здійснюється в міру необхідності. Зазвичай це робиться за допомогою веб-служб та інтерфейсів управління.
- Широкий доступ до мережі. Сервіси, додатки і дані, присутні в хмарі, повинні бути доступні користувачам з використанням стандартних механізмів і протоколів. Характеристика також вимагає, щоб доступність послуг підтримувала неоднорідне тонке або товсте середовище (наприклад, мобільні телефони, ноутбуки, робочі станції).
- Об'єднання ресурсів. Обчислювальні ресурси провайдера об'єднуються для обслуговування декількох споживачів за допомогою мультитенантної моделі, при цьому різні фізичні та віртуальні ресурси

динамічно призначаються та переназначаються відповідно до споживчого попиту. Існує відчуття незалежності місця розташування в тому сенсі, що клієнт, як правило, не має контролю або знань про точне розташування наданих ресурсів, але може мати можливість вказати місце на більш високому рівні абстракції (наприклад, країна, штат або центр обробки даних). Приклади ресурсів включають зберігання, обробку, оперативну пам'ять та пропускну здатність мережі.

- Швидка еластичність. Можливості можуть бути еластично надані і вивільнені, в деяких випадках автоматично, для швидкого розширення за межі і всередину відповідно до попиту. Споживачеві можливості, доступні для забезпечення, часто здаються необмеженими і можуть бути використані в будь-якій кількості в будь-який час.
- Розмірений сервіс. Хмарні системи автоматично контролюють та оптимізують використання ресурсів, використовуючи можливості вимірювання на певному рівні абстракції, що відповідає типу послуги (наприклад, зберігання, обробка, пропускна здатність та активні облікові записи користувачів). Використання ресурсів можна відстежувати, контролювати та повідомляти про це, забезпечуючи прозорість як для постачальника, так і для споживача використовуваної послуги.

Хмарні обчислювальні середовища пропонують кілька рівнів віртуалізації, а послуги, пропоновані хмарами, часто класифікуються за моделями багаторівневого обслуговування як: інфраструктура як послуга (IaaS), платформа як послуга (PaaS), програмне забезпечення як послуга (SaaS). (Див. Рисунок 1.5)[8].

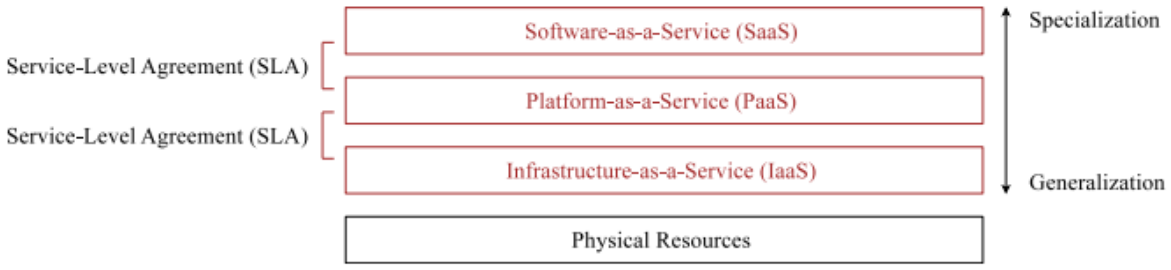

Рисунок 1.5 – Моделі сервісів хмарних обчислень

Хмарні середовища віртуалізують доступ до інфраструктур, платформ і додатків (програмного забезпечення) і реалізують їх, а також забезпечують обчислювальну потужність за рахунок моделей дозованого обслуговування. Надання хмарних сервісів регулюється угодами про рівень обслуговування.

1.7.1 Модель обслуговування IaaS

Моделі обслуговування «Інфраструктура як послуга» (IaaS) стосуються надання можливостей динамічної інфраструктури у вигляді віртуалізованих середовищ, що пропонуються як дозовані послуги на узгоджені періоди часу. Доступ до служб IaaS зазвичай здійснюється через абстрактні хмарні інтерфейси, які надають API для створення віртуальних серверів та координації користувацьких інфраструктурних середовищ. Хмарна інфраструктура - це сукупність апаратного та програмного забезпечення, що забезпечує п'ять основних характеристик хмарних обчислень. Хмарну інфраструктуру можна розглядати як таку, що містить як фізичний рівень, так і рівень абстракції. Фізичний рівень складається з апаратних ресурсів, необхідних для підтримки наданих хмарних сервісів, і зазвичай включає сервер, сховище та мережеві компоненти. Рівень абстракції складається з програмного забезпечення, розгорнутого на фізичному рівні, яке виявляє основні характеристики хмари. Концептуально рівень абстракції знаходиться вище фізичного рівня[13]. Використання віртуалізованих хмарних інфраструктур полегшує управління очікуваними і несподіваними піками вимог до обчислювальної потужності, адаптацію до регіональних відмінностей у використанні шаблонів та мінімізація витрат на надмірне надання апаратного забезпечення. Як правило, хмарні інфраструктури використовують механізми шлюзів, які приймають або відхиляють запити на створення екземплярів служб на основі внутрішніх моделей завантаження та пропускної здатності інфраструктури. Умови надання послуг у хмарах можуть бути визначені та відрегульовані за допомогою угод про рівень обслуговування (SLAs). Моделі обслуговування IaaS знайшли широке визнання в промисловості, де провайдери пропонують доступ до віртуалізованих інфраструктурних послуг у загальнодоступних хмарних середовищах, таких як Amazon Elastic Compute Cloud (EC2) і Simple Storage Service

(S3)[15-16], Microsoft Azure[17]. Для побудови приватних хмарних інфраструктур існує ряд хмарних наборів інструментів з відкритим вихідним кодом, наприклад, Nimbus, OpenNebula[18-19].

1.7.2 Модель обслуговування PaaS

Моделі обслуговування «Платформа як послуга» (PaaS) стосуються надання обчислювальних платформ в якості сервісів у хмарних середовищах. Використання сервісів PaaS дозволяє розробникам і кінцевим користувачам налаштовувати програмні середовища, використовувати моделі дозованих витрат на придбання програмного забезпечення і адаптуватися до вимог багатокористувацької архітектури. Підтримка механізмів між-машинного зв'язку, таких як веб-служби, дозволяє використовувати можливості PaaS при інтеграції різнорідних програмних середовищ. PaaS включає проміжне програмне забезпечення, бази даних, засоби розробки та деяку підтримку середовища виконання, наприклад Web 2.0 та Java. Платформа включає в себе як апаратне, так і програмне забезпечення, інтегроване зі спеціальними програмними інтерфейсами. Постачальник надає API і програмні засоби (наприклад, Java, Python, Web 2.0, Net). Користувач звільняється від управління хмарної інфраструктури[6].

1.7.3 Модель обслуговування SaaS

«Програмне забезпечення як послуга» (SaaS) - це модель обслуговування, при якій доступ до програмних пакетів пропонується як послуга через моделі дозованої підписки або оплати за використання. SaaS дозволяє кінцевим користувачам уникати жорстких ліцензійних угод і моделей з фіксованою вартістю та визначається безліччю варіантів використання в економічних умовах, таких як хмарні обчислення, де платформи віртуалізовани, пропускна здатність мережі зростає швидше ніж обчислювальні можливості, а обчислювальна техніка є предметом торгівлі. Модель «Програмне забезпечення як послуга» (SaaS) застосовується до бізнес-процесів, галузевих додатків, управління взаємовідносинами зі споживачами (CRM), планування ресурсів підприємства (ERP), людських ресурсів (HR) та програм співпраці. З боку клієнта немає початкових інвестицій у сервери або ліцензування програмного забезпечення. З

боку провайдера витрати досить низькі в порівнянні зі звичайним розміщенням призначених для користувача додатків[6].

Через велику різноманітність хмарних рішень, які зараз пропонує галузь, клієнти повинні спочатку вивчити доступні моделі розгортання в хмарі, щоб проаналізувати їх переваги, недоліки та обмеження, наприклад, з точки зору масштабованості, еластичності, ціноутворення чи міграції. Головним чином, вони повинні оцінюватися з точки зору безпеки. Для цього в літературі обговорюються п'ять моделей. Це публічні, приватні, гібридні та громадські хмари, а також модель під назвою - віртуальна приватна хмара (VPC)[20].

1.7.4 Публічна хмара. Переваги та недоліки

Публічна хмара (Public Cloud). Інфраструктура, що лежить в основі загальнодоступної хмари, як правило, належить постачальнику хмарних послуг. У загальнодоступній хмарі є багато послуг від різних клієнтів, тому доступ до них здійснюється з кількох місць кількома орендарями. Для доступу до служб зазвичай використовуються веб-інтерфейси. Ця модель заснована на бізнес-підході з оплатою за використання і, як правило, є доступною, надаючи послуги з високим ступенем масштабованості. Ресурси хмари розташовані віддалено, що робить цю модель менш безпечною та більш ризикованою, ніж інші моделі розгортання, оскільки моделі надання послуг можуть бути схильні до шкідливої активності. У цьому випадку угоди про рівень обслуговування (SLAs) між клієнтами та постачальниками повинні бути добре деталізовані та проаналізовані[20].

Переваги моделі публічної хмари[21]:

- Мінімальні інвестиції: оскільки це послуга з оплатою за користування, немає суттєвої попередньої плати, що робить її чудовою для підприємств, які потребують негайного доступу до ресурсів.
- Відсутність витрат на налаштування: вся інфраструктура повністю субсидується постачальниками хмарних послуг, тому немає необхідності налаштовувати будь-яке обладнання.
- Управління інфраструктурою не потрібно: використання загальнодоступної хмари не вимагає управління інфраструктурою.

- Відсутність технічного обслуговування: роботи з технічного обслуговування виконуються постачальником послуг (а не користувачами).
- Динамічна масштабованість: для задоволення потреб компанії доступні ресурси на вимогу.

Недоліками моделі публічної хмари є[21]:

- Проблеми безпеки даних та конфіденційності: оскільки хмара відкрита для громадськості, вона не забезпечує повного захисту від кібератак і потенційно має слабкі місця.
- Проблеми з надійністю: оскільки одна і та ж серверна мережа доступна широкому колу користувачів, вона схильна до збоїв і простоїв в роботі.
- Обмеження послуги, ліцензії: хоча існує багато ресурсів, якими потенційний клієнт має змогу поділитися з орендарями, існує ліміт щодо використання.

1.7.5 Приватна хмара. Переваги та недоліки. VPC модель

Приватна хмара (Private Cloud). Приватна хмара має власну інфраструктуру і може бути розміщена у внутрішньому центрі обробки даних організації. Таким чином набагато легше виконувати та ідентифікувати обов'язки з управління та забезпечення безпеки, які можуть бути покладені на саму організацію або на третю сторону. Приватні хмари вимагають великих бюджетів і вимагають висококваліфікованих IT-фахівців для управління ними, підвищення безпеки, контролю, відповідності, стійкості та прозорості[20]. Переваги моделі приватної хмари[21]:

- Кращий контроль: клієнт отримує повний контроль над інтеграцією служб, IT-операціями, політикою та поведінкою користувачів.
- Безпека та конфіденційність даних: підходить для зберігання корпоративної інформації, доступ до якої мають лише авторизовані працівники. Шляхом сегментації ресурсів в рамках однієї і тієї ж інфраструктури можна домогтися поліпшення доступу і безпеки.

- Підтримка застарілих систем: цей підхід призначений для роботи із застарілими системами, які не можуть отримати доступ до загальнодоступної хмари.
- Налаштування: на відміну від розгортання в загальнодоступній хмарі, приватна хмара дозволяє компанії адаптувати рішення до своїх конкретних потреб.

Недоліками моделі приватного хмари є[21]:

- Обмежена масштабованість: приватні хмари мають обмежену масштабованість, оскільки вони масштабуються в межах внутрішніх розміщених ресурсів. Вибір базового обладнання впливає на масштабованість.
- Більш висока вартість: через ряд переваг, які отримає клієнт, інвестиції будуть значно вище, порівняно із загальнодоступною хмарою (оплата програмного забезпечення, обладнання, персоналу і т.д.).

VPC модель полягає у використанні підключення до віртуальної приватної мережі (VPN) для створення віртуальних приватних або напівприватних хмар, вдаючись до захищених каналів, що надаються технологією VPN, і призначаючи ізольовані ресурси клієнтам. VPC встановлюється поверх будь-якої раніше описаної моделі, подібно до VPN, побудованої на інших мережах. Отже, VPC - це особливий випадок приватної хмари, яка існує всередині будь-якої іншої[20]. Ця модель дозволяє організаціям використовувати хмарні сервіси, не турбуючись про роботу в загальних або загальнодоступних середовищах. Прикладом такої моделі є Amazon VPC[22].

1.7.6 Гібридна хмара. Переваги та недоліки

Гібридна хмара (Hybrid Cloud). Гібридна хмара - це суміш двох або більше інших моделей розгортання хмарних обчислень, які управляються централізовано і обмежені захищеною мережею. Гібридна хмара традиційно розглядається як суміш приватних і публічних хмар, що об'єднує переваги кожного з них і долає їх перешкоди. Це дозволяє декільком, але обмеженим і чітко визначеним об'єктам отримувати доступ до хмари через Інтернет більш безпечним способом, ніж

використання загальнодоступної моделі. Це також забезпечує портативність даних і додатків. Ця модель управляється як організацією, так і сторонньою організацією і розміщується як на сайті, так і за межами сайту[20]. Переваги моделі гібридної хмари[21]:

- Гнучкість та контроль: підприємства з більшою гнучкістю можуть розробляти персоналізовані рішення, які відповідають їх конкретним потребам.
- Вартість: оскільки загальнодоступні хмари забезпечують масштабованість, клієнт несе відповідальність за оплату додаткової потужності, лише в тому випадку, якщо вона йому потрібна.
- Безпека: оскільки дані належним чином розділені, ймовірність крадіжки даних значно зменшується.

Недоліками моделі гібридної хмари є[21]:

- Технічне обслуговування: гібридна стратегія хмарних обчислень може вимагати додаткового технічного обслуговування, що призведе до збільшення операційних витрат компанії.
- Складна інтеграція: при створенні гібридної хмари інтеграція даних та додатків може бути складною.

1.7.7 Хмарний сервіс спільноти. Переваги та недоліки

Хмарний сервіс спільноти (Community Cloud). Хмарний сервіс спільноти - це модель, яка контролюється та спільно використовується кількома організаціями. Зазвичай хмара налаштовується таким чином, щоб підтримувати спільні інтереси кількох власників. Хмара спільноти може управлятися комітетом власників або сторонньою організацією і може бути розміщена на місці або за його межами. Члени спільноти можуть вільно отримувати доступ до даних у хмарі. Хмара спільноти усуває ризики безпеки, пов'язані з загальнодоступними хмарами, і витрати на приватні хмари[20]. Переваги хмарних сервісів спільноти[21]:

- Рентабельність: економічна вигода, оскільки хмара спільно використовується кількома організаціями або громадами.
- Безпека: хмара спільноти забезпечує кращу безпеку.

- Загальні ресурси: дозволяє спільно використовувати ресурси, інфраструктуру і т.д., з декількома організаціями.
- Спільна робота та обмін даними: підходить як для спільної роботи, так і для обміну даними.

Недоліки хмарних сервісів спільноти[23]:

- Рідкість: розгортання в хмарі спільноти все ще менш поширене, ніж інші моделі розгортання, оскільки необхідно знайти інші організації з подібними вимогами.
- Відносно висока вартість: порівняно з загальнодоступною хмарною моделлю, моделі хмарних сервісів спільноти мають високу початкову вартість і можуть бути дещо витратними в обслуговуванні, залежно від кількості залучених партнерів.
- Обмежена пропускна здатність і обсяг пам'яті: оскільки декілька організацій спільно використовують однакові ресурси, можуть виникати питання щодо пропускної здатності та ємності зберігання.

1.8 Порівняння переваг та недоліків моделей хмарного розгортання

Розглянемо короткий опис основних характеристик моделей хмарного розгортання. (Див. Таблиці 1.4-1.5). Таблиці надають наочне порівняння між чотирма основними моделями, а також додатково VPC модель[20].

Таблиця 1.4 - Порівняння моделей хмарного розгортання

	Публічна хмара	Приватна хмара	Гібридна хмара	Хмарний сервіс спільноти	VPC хмара
Налаштування та використання	Всередині компанії	IT-фахівці	IT-фахівці	IT-фахівці	IT-фахівці
Конфіденційність та безпека	Низька	Висока	Від низької до високої	Середня	Висока
Контроль даних	Низький	Високий	Середній	Середній	Високий
Загальна надійність	Середня	Висока	Середня / Висока	Середня	Висока

Таблиця 1.5 - Порівняння моделей хмарного розгортання

	Публічна хмара	Приватна хмара	Гібридна хмара	Хмарний сервіс спільноти	VPC хмара
Гнучкість і масштабованість	Висока	Середня	Дуже висока	Середня	Середня
Вартість	Низька	Відносно висока	Середня	Відносно висока	Перемінна
Обладнання	Стороннє	Організації або стороннє	Організації або стороннє	Організації або стороннє	Організації та стороннє

2 СТАНДАРТИ КІБЕРБЕЗПЕКИ

2.1 Поняття стандарт та фреймворк

Стандарт описується як ідеальна умова з мінімальною межею досягнення. Це також стосується технічних специфікацій, які повинні застосовуватися сервісним центром, щоб користувачі послуг могли отримати максимальну функціональність, призначення або прибуток від послуг. Багато міжнародних організацій, асоціацій та консорціумів відіграють життєву важливу роль у розробці стандартів. Стандарти подаються у вигляді документів, що визначають специфікації, процедури та керівні принципи, спрямовані на забезпечення безпеки, узгодженості та надійності продуктів, послуг та систем. Згідно з визначенням, наданим ISO/IEC, стандарти - це документи або правила, розроблені на основі загальної угоди та затверджені юридичною особою, які допомагають досягти оптимальних результатів як керівництво, модель або зразок у конкретному[25]. Стандарт практично відповідає вимогам користувачів, враховує обмеження технології та ресурсів, а також відповідає вимогам перевірки. Спираючись на результати дослідження від міжнародної компанії Ipsos MORI (Інститут соціальних досліджень) зазначимо, що правила або стандарти, пов'язані з кібербезпекою, майже невідомі в діловому світі. Ряд компаній не беруть участі в проектах або тендерах з обов'язковими вимогами щодо дотримання стандартів кібербезпеки, в той час як нові компанії намагаються більш інтенсивно вивчати стандарти безпеки[26]. Дослідження 2019 року показало, що кожна п'ята компанія (18%) і кожна сьома благодійна організація (14%) в даний час потребують постачальника, який може відповідати стандартам кібербезпеки, хоча деякі компанії все ще не вважають постачальників потенційним джерелом кіберризиків[27].

Стандарти інформаційних технологій описують угоду між постачальниками, які погоджуються використовувати одну і ту ж технологію, щоб апаратне забезпечення та системи могли взаємодіяти та забезпечувати доступ до послуг. У розробці стандартів беруть участь багато міжнародних організацій, консорціуми та асоціації. Деякі стандарти "відкриті" для всіх типів підприємств та державних

організацій. Інші є "закритими", специфічними для певних галузей та підприємств. Очікується, що впровадження стандартів забезпечить переваги економії часу та фінансів, що призведе до збільшення виробництва та прибутку, мінімізації ризиків, підвищення обізнаності користувачів та безперервності бізнесу. Кілька організацій з розробки стандартів, таких як ITU-T, розробили стандарти, які називаються "рекомендаціями" для телекомунікаційних мереж, або IEEE-SA (Асоціація стандартів), які сприяли розробці багатьох стандартів для різних галузей, таких як телекомунікації, інформаційні технології та електростанції. Відкриті стандарти можуть використовуватися організаціями будь-якого типу, оплачуючи вартість завантаження копії документа, надаючи користувачеві можливість використовувати частину або всі керівні принципи в міру необхідності або використовувати їх з іншими стандартами. Кілька стандартів можуть бути використані разом з іншими стандартами для доповнення та посилення інших вимог, таких як вимоги ISO, BSI та NIST з їхнім посібником із спеціальних публікацій серії 800. Країна має право видавати свої стандарти або відхиляти правила чи стандарти, опубліковані іншими країнами. Стандартами може бути все, що визначається країною чи організацією для регулювання, моніторингу чи оцінки діяльності. Найбільш поширене використання терміну "стандарт" зазвичай відноситься до документів, які професійні органи встановлюють для використання іншими організаціями (наприклад, програмні стандарти, технічні стандарти) або стандарти технічної практики (наприклад, практичні стандарти кібербезпеки). В загальному сенсі стандарт визначає кроки, які потрібно зробити, для того щоб відповідати вимогам стандарту. Визначається це шляхом пояснення та надавання методів один за одним для завершення процесу. Тоді як структура - це загальне керівництво, яке може бути прийняте підприємствами, компаніями, установами, що охоплює багато компонентів або областей, але не визначає кроки, які слід вжити.

Фреймворк - це використання повного набору правил, ідей чи посібників для опису проблеми або визначення того, що робити. Загалом, фреймворк надає лише загальний опис як основу для створення чогось або досягнення корисної мети[28]. Як правило, фреймворк використовується для підведення підсумків досягнення

цілей, опису сфери охоплення, керівництва впровадженням і оцінкою, а також визначення стандартів якості, які повинні бути досягнуті. Кілька детальних аспектів аналізу іноді пов'язані зі стандартними аспектами. Фреймворки часто вважаються схожими на "моделі" або "методи", оскільки багато фреймворків складаються з однієї або декількох моделей. Існують фреймворки, засновані на методах моделювання (таких як моделі процесів, моделі робочих процесів, моделі життєвого циклу), а деякі базуються на найкращих практиках. Фреймворк надає користувачам більше свободи у виборі частини методу або всього використання. Користувачам надається свобода вибору методів, моделей або технічних практик, котрі входять в рамки, і пропозиції загальних керівних принципів, які можуть бути прийняті, а також пропозиції для організації, щоб мати можливість застосовувати їх в організації. Наприклад, ISO 31000 пропонує структуру для управління організаційними ризиками, і існують загальні методи та керівні принципи для його застосування в організаціях[29].

2.2 Стандарти кібербезпеки

Набори практик або технічних методів, які допомагають організаціям забезпечити своє кібер-середовище, називаються стандартами кібербезпеки. Стандарти кібербезпеки включають користувачів, мережеву інфраструктуру, програмне забезпечення, апаратні засоби, процеси та інформацію на системних носіях, які можуть бути підключені до мережі Інтернет. Сфера застосування стандартів кібербезпеки широка в тому сенсі, що вони охоплюють функції безпеки в додатках і криптографічні алгоритми, які в основному забезпечують перспективу щодо засобів контролю безпеки, процесів, процедур, керівних принципів і базових показників. Експерти з безпеки рекомендують впроваджувати стандарти кібербезпеки як принципово важливий елемент, що складається з набору кращих практик для захисту організацій від загроз і ризиків кібербезпеки. Основною метою стандартів кібербезпеки є запобігання або пом'якшення наслідків кібератак і зниження ризику кіберзагроз. Впровадження стандартів забезпечить переваги економії часу, зниження витрат, збільшення прибутку, підвищення обізнаності користувачів, мінімізації ризиків та забезпечення безперервності бізнесу. Крім того,

використання стандартів полегшує відповідність організації кращим галузевим практикам і процедурам і надає можливість порівняти систему безпеки на міжнародному рівні. Отже, у різних організаціях чи підприємствах було встановлено застосування стандартів кібербезпеки для захисту активів від кіберзагроз. Як результат, різні організації розробили різні стандарти кібербезпеки, щоб забезпечити те, що організації різного розміру та характеру здійснювали відповідні заходи щодо запобігання та пом'якшення кіберзагроз[30]. Розглянемо п'ять найбільш відомих, визнаних на міжнародному рівні організацій, що розробляють стандарти і керівні принципи для контролю безпеки.

2.2.1 Національний інститут стандартів і технологій (NIST)

Стандартна серія SP 800 була розроблена NIST, нерегульованим федеральним агентством, створеним при міністерстві торгівлі США. NIST був заснований в 1901 році, і його місія полягає в тому, щоб поліпшити життя і економічну безпеку за допомогою розвитку технологій, науки і стандартів. Галузі, які підтримуються стандартами та вимірами NIST, включають будівельні та пожежні дослідження, хімічну науку та технології, інформаційні технології, електроніку та електротехніку, матеріалознавство та інженерію, технологічні послуги, машинобудування, фізику, нейтронні дослідження, нанорозмірну науку та технології. NIST опублікував свою групу з 800 документів у 1990 році, яка вважається найстарішою публікацією у своїх стандартах інформаційної безпеки, що охоплює широкий спектр документів, які підтримують різні аспекти інформаційної безпеки. Ця серія стандартів включає рекомендації, керівні принципи, технічні характеристики та звіти, які NIST щороку публікує про свою діяльність у сфері кібербезпеки. Серія стандартів SP 800 спочатку була розроблена для задоволення вимог конфіденційності та безпеки у федеральних інформаційних системах, однак пізніше вона була використана і нефедеральними організаціями. Для використання публікації в системах національної безпеки необхідно отримати дозвіл відповідного федерального органу влади. Серія стандартів SP 800 включає в себе ряд різних публікацій, таких як фреймворк управління ризиками (RMF), фреймворк кібербезпеки (CFS), NIST SP 800-39, NIST SP 800-53, а також NIST SP

800-37, SP800-12. SP800-12 є найпопулярнішим документом в цій серії стандартів, оскільки він пропонує хорошу перспективу підходу NIST.

2.2.2 Міжнародна організація зі стандартів (ISO)

Стандарт ISO/IEC 27000 присвячений безпеці в управлінні інформаційними системами (ISM) та опублікований міжнародною організацією зі стандартизації (ISO) та міжнародною електротехнічною комісією (IEC). Методи і практика для забезпечення ефективного впровадження інформаційної безпеки в організації докладно описані в стандарті ISO 27001, приділяючи особливу увагу забезпеченню безпечного та надійного обміну даними і каналами зв'язку. Сімейство стандартів ISO/IEC 27000 має на меті допомогти організаціям забезпечити безпеку своїх інформаційних активів і охоплює такі області, як розробка системи управління інформаційною безпекою (ISMS), впровадження засобів контролю, управління ризиками, проведення аудитів. Положення про управління забезпечують міцну основу для таких компонентів: керівництво, планування, підтримка, експлуатація, оцінка ефективності та вдосконалення. ISO 27001, який є першою серією стандартів ISO/IEC 27000, датується 2005 роком. Однак в даний час опубліковані і широко використовуються в організаціях чотири стандарти, включаючи 27001, 27002, 27005 і 27006. Посилаючись на дані ISO за 2016 рік, понад 33 000 організацій пройшли сертифікацію ISO 27001. Це число на 21% більше, порівняно з 2015 роком. Враховуючи, що ISO 27001 забезпечує міцну основу для дотримання кількох важливих нормативних актів, тенденція зростання зацікавлених організацій зберігається в наші дні[31].

2.2.3 Американський інститут дипломованих громадських бухгалтерів (AICPA)

Рада зі стандартів аудиту (ASB) AICPA створила положення SSAE, щоб переосмислити та оновити спосіб звітування службових компаній про контроль відповідності. SSAE 18 набув чинності в травні 2017 року, йому передували SSAE 16 (набув чинності в 2011 році) та SAS 70 (набув чинності в квітні 1992 року). Організації досягають відповідності вимогам SSAE та інформаційної безпеки за допомогою звіту про SOC 2. Організації, що відповідають вимогам SOC 2,

демонструють здатність враховувати критерії управління даними клієнтів відповідно до п'яти принципів: безпека, доступність, цілісність обробки, конфіденційність, приватність. Що стосується інформаційної безпеки, організації проходять аудит контролю, пов'язаного із захистом активів, включаючи мережеві та прикладні брандмауери, двофакторну автентифікацію та виявлення вторгнень.

2.2.4 Рада зі стандартів безпеки (PCI SSC).

Стандарт безпеки даних індустрії платіжних карток (PCI DSS) детально описує стандарти інформаційної безпеки для захисту даних кредитних карток. Цей галузевий стандарт безпеки регулюється радою стандартів безпеки PCI SSC, яка була заснована п'ятьма основними брендами кредитних платежів: Visa, MasterCard, American Express, JCB, Discover. Відповідність вимогам PCI DSS має на увазі комплексний підхід до забезпечення інформаційної безпеки даних платіжних карт. Необхідність відповідності PCI DSS встановлюється операторами платіжних систем в рамках їх власних програм з безпеки. Рада PCI SSC дотримується трирічного циклу оновлення стандарту. Перший рік - впровадження стандарту в індустрії, другий рік - збір зворотного зв'язку у вигляді коментарів і побажань від учасників індустрії платіжних карток, третій рік - підготовка нової версії стандарту. Між етапами проводяться конференції, які складаються з американської та європейської сесій. В ході конференцій організації-учасники, міжнародні платіжні системи, QSA-аудитори (кваліфікований спеціаліст з оцінки безпеки), торгово-сервісні підприємства і постачальники послуг обговорюють майбутнє стандарту і супутніх документів. Новітня версія стандарту 4.0 була прийнята в березні 2022 року[32]. PCI DSS зосереджується на шести основних цілях:

- Підтримка безпеки мережі, захист.
- Захист інформації стосовно власника картки.
- Захист систем від злому.
- Обмеження та контроль доступу до системної інформації та операцій.
- Моніторинг та тестування мереж.
- Визначення та підтримка офіційної політики інформаційної безпеки.

2.2.5 Міжнародне товариство автоматизації (ISA)

ISA є одним із лідерів та експертом у розробці стандартів, акредитованих американським національним інститутом стандартів (ANSI), які охоплюють безпеку, ефективність та прибутковість для управління системами автоматизації та контролю. Стандарти серії ISA 62443 надають найкращі практики та засоби контролю інформаційної безпеки для систем управління промисловою автоматизацією. Ці стандарти стосуються вимог та контролю, які підтримують тріаду C-I-A (конфіденційність, цілісність, доступність) протягом усього життєвого циклу автоматизованого управління.

2.4 Фреймворки кібербезпеки

Фреймворк кібербезпеки - це набір керівних принципів, яких компанії повинні дотримуватися, щоб бути краще підготовленими до виявлення та реагування на кібератаки. Фреймворк кібербезпеки включає набір стандартів, методологій, процедур і процесів, які гармонізують політичні, ділові та технологічні підходи до усунення кіберризиків. Він також включає в себе керівництво щодо запобігання та відновлення після атак. Фреймворк кібербезпеки повинен, наскільки це можливо, включати добровільні узгоджені стандарти і кращі галузеві практики.

2.4.1 NIST CSF

NIST CSF допомагає організаціям посилити свої заходи кібербезпеки та забезпечує інтегровану організаційну структуру для різних підходів до безпеки шляхом збору найкращих практик, стандартів та рекомендацій. Іншими словами, фреймворк, що забезпечує засоби вираження вимог до кібербезпеки, який може бути ефективний для виявлення прогалин у практиці кібербезпеки організації. Фреймворк кібербезпеки NIST складається з трьох основних частин: основний фреймворк; рівень реалізації фреймворку; профіль фреймворку. Базова платформа має ряд функцій, таких як[33]:

- Ідентифікація: допомагає організаціям розвивати розуміння того, як управляти ризиками кібербезпеки для систем, людей, активів, даних та можливостей, включаючи управління активами, бізнес-середовище та

управління інформаційними технологіями за допомогою комплексної оцінки ризиків та процесів управління.

- Захист: допомагає організаціям розробляти і впроваджувати відповідні запобіжні заходи для забезпечення надання критично важливих послуг. Цей етап також включає визначення заходів безпеки для захисту даних та інформаційних систем, включаючи контроль доступу, навчання та обізнаність, безпеку даних, процедури захисту інформації та підтримку захисних технологій.
- Виявлення: допомагає організаціям розробляти та впроваджувати відповідні дії для виявлення виникнення події кібербезпеки, а також пропонує рекомендації по виявленню аномалій в безпеці, системах моніторингу і мережах для виявлення інцидентів безпеки.
- Реагування: допомагає організаціям розробляти та впроваджувати відповідні заходи для дій щодо виявленого інциденту кібербезпеки. Це також включає рекомендації щодо планування реагування на події безпеки, процедур пом'якшення наслідків, комунікаційних процесів під час реагування та заходів щодо підвищення відмовостійкості безпеки.
- Відновлення: допомагає організаціям розробляти та впроваджувати відповідні заходи для підтримки планів сталого розвитку та відновлення будь-яких можливостей або послуг, які були порушені через інцидент з кібербезпекою, а також керівних принципів, які компанія може використовувати для відновлення після атак.

2.4.2 COBIT

Завдання управління для інформаційних і суміжних технологій (COBIT - Control Objectives for Information and Related Technologies) методологія управління інформаційними технологіями, що належить і розробляється некомерційною організацією ISACA - асоціацією аудиту та контролю інформаційних систем, заснованою в 1967 році в США у відповідь на зростаючі проблеми комп'ютерних систем. У загальній класифікації COBIT - це високорівневий стандарт інформаційних технологій в системі управління, який концентрується на загальних

концепціях процесів прийняття рішень в управлінні IT, замість того, щоб зосереджуватися на деталях. Методологія COBIT включає 34 основні IT-процеси, охоплює найкращі практики та підходи щодо управління процесами, інфраструктурою, ресурсами, відповідальністю та контролем. Кожен IT-процес в COBIT включає в себе 318 високорівневих деталізованих цілей контролю і ряд цілей контролю. Цілі контролю поділяються на чотири основні категорії, включаючи планування, впровадження, підтримку, а також моніторинг та оцінку. Методологія COBIT добре зарекомендувала себе для впровадження інтегрованого рішення. Однак зазначена методологія не є найкращим рішенням у тих випадках, коли належне впровадження засобів контролю безпеки є першочерговим завданням, оскільки COBIT не надає керівних принципів для досягнення заздалегідь визначених цілей контролю. COBIT - рада стандартів асоціації аудиту та контролю інформаційних систем (ISACA) публікує стандарт під назвою цілі контролю для Інформація та пов'язані з нею технології (COBIT). COBIT надає систему контролю для управління IT.

2.5 Проблеми впровадження та підтримки стандартів

Незважаючи на те, що впровадження одного або декількох стандартів приносить реальні, цінні вигоди, організаціям слід усвідомлювати потенційні проблеми, пов'язані з впровадженням і супроводом[35].

- Час: впровадження та підтримка стандартів інформаційної безпеки це не одноразовий проект. Швидше, це процес, який вимагає відданого, кваліфікованого персоналу, підтримки з боку вищого керівництва, а також постійного моніторингу та вдосконалення. Успішна робота вимагатиме участі всієї організації.
- Вартість: стандарти можуть бути дорогими для впровадження та настільки ж дорогими для підтримки. У випадку ISO 27001, наприклад, на додаток до часу та зусиль, необхідних для виконання вимог стандарту, організації повинні планувати щорічні збори за аудит, які можуть бути суттєвими.

- Участь: участь вищого керівництва та володіння програмою на рівні С є найважливішими елементами для організації ефективного розгортання програми інформаційної безпеки. Команда інформаційної безпеки повинна ділитися показниками, повідомляти про ефективності програми і демонструвати її цінність і стратегічне відповідність бізнес-цілям організації, щоб підтримувати підтримку вищого керівництва.
- Управління змінами: в цілому, всі цінують цінність захисту інформації до тих пір, поки вона не зажадає зміна. Команди безпеки, які впроваджують стандарти, мають завдання знайти делікатний баланс між безпекою та зручністю.
- Постійне вдосконалення: стандарти мають життєвий цикл. Коли стандарт оновлюється, всі відповідні організації несуть відповідальність за те, щоб бути в курсі оновлень і впроваджувати їх до зазначених дат або якомога швидше, якщо терміни не встановлені. У деяких випадках стандарт може застаріти, і новий стандарт повинен бути досліджений і представлений вищому керівництву для затвердження для впровадження.

Стандарти інформаційної безпеки зарекомендували себе як цінні ресурси для обміну інформацією про найкращі практики, встановлені галузевими експертами. Конкретні рекомендації з інформаційної безпеки доступні для урядових установ, громадських організацій і варіюються залежно від таких факторів, як галузь, закони та вимоги до дотримання нормативних вимог.

3 БЕЗПЕКА РОЗПОДІЛЕНИХ СИСТЕМ

3.1 Мотивація та об’єкти атак хакерів

Метою хакера є порушення безпеки комп'ютерів і мереж, що впливають на конфіденційність, цілісність і доступність інформації та послуг в системах. Така діяльність хакерів вважається незаконною, оскільки вони витрачають свій час і ноу-хау на отримання особистої вигоди і порушення безпеки в мережах. Перш ніж перейти до таксономії комп'ютерних загроз, необхідно класифікувати різні типи хакерів. Очікується, що кожен тип хакерів матиме власну мотивацію для своєї діяльності. Найбільш поширені з них включені тут[36]:

- Спосіб розваги. Розвага - єдина мотивація для сценаристів і безлічі несерйозних хакерів. Для них злом захищеної системи - це складна і повна пригод приємна гра, що дозволяє перевірити їх кмітливість і навички.
- Тестування на вразливість. Тестування на вразливість проводиться адміністраторами для виявлення вразливостей і, отже, розробки засобів захисту. Те саме роблять і хакери для виявлення вразливостей у цільових системах та пошуку експлойтів для цих вразливостей. Це майже попередня фаза атаки.
- Крадіжка даних. Хакери проникають в базу облікових даних окремих осіб або організацій.
- Шпигунство. Вид крадіжки, при якому хакер намагається отримати захищену інформацію замість прямої фінансової вигоди. Вкрадена інформація може бути або продана на чорному ринку, або використана противниками для отримання стратегічних переваг.
- Спам. Спам - це не лише небажані електронні листи. Цей спам може бути викликаний певними шкідливими програмами, які проникають у веб-браузер і спорожняють його небажаною рекламою.
- Контроль. Хакер використовує троян або інші засоби для отримання віддаленого контролю над іншою системою. Потім хакер може

перетворити цю скомпрометовану систему на бота або «комп'ютер-зомбі», який він використовує для спаму або розгортання розподілених атак типу «відмова в обслуговуванні».

- Порушення. Порушення надання послуг або доступу до інформації шляхом захоплення веб-сайтів або облікових записів у соціальних мережах, як правило, є актом конкуренції, протесту чи суперництва. Цей ефект призведе до уповільнення або закриття інтернет-активності цілі.

3.2 Класифікація комп’ютерних загроз та атак

Комп'ютерні загрози та атаки включають доступ до інформації, знищення або маніпулювання даними, дестабілізацію комп'ютера або погіршення його продуктивності. Комп'ютерні атаки - це в основному збір інформації, підвищення привілеїв, експлойти з переповненням буфера, віддалений доступ неавторизованих користувачів і атаки типу «відмова в обслуговуванні». Мережеві атаки, які є підмножиною комп'ютерних атак, були в основному атаками на комп'ютерні системи, які формують базову інфраструктуру мережі зв'язку. Мережа допомагає у відправці атаки або може бути засобом атаки. У сценарії атаки задіяні різні етапи, і ці етапи коротко перераховані тут[36]:

- Крок 1: Спуфінг (підробка). Перш ніж приступити до будь-якого з кроків атаки, хакери зазвичай вважають за краще приховувати свою особистість і свої дії. Зазвичай це робиться шляхом підробки, коли зловмисник приховує свою особу і видає себе за когось іншого. Це може бути зроблено за допомогою клонування MAC, підробка IP-адреси або підробки електронної пошти.
- Крок 2: Розвідка. Завжди рекомендується ретельно планувати, перш ніж вживати будь-яких дій, і це також стосується і у випадку злому. Хакери спочатку визначають ціль для запуску атаки, витягують максимум інформації про ціль атаки, розуміють її недоліки, а тільки потім вивчають найкращі способи використання знайдених недоліків.

- Крок 3: Підготовка. Хакер за допомогою інформації, зібраної на попередньому етапі, ідентифікує та розробляє засоби для того, щоб проникнути в комп'ютер або мережу. На цьому етапі хакер збирає інструменти, які він планує використовувати, як тільки отримає доступ до системи, для успішної експлуатації вразливостей в системі.
- Крок 4: Впровадження. На етапі впровадження атака починає працювати. Це відбувається, коли надсилаються фішингові електронні листи або коли підроблені веб-сторінки розміщуються в Інтернеті, і зловмисник терпляче чекає, коли всі необхідні йому дані почнуть надходити.
- Крок 5: Експлуатація. Це стан, коли починають надходити конфіденційні дані. Це найцікавіший етап для хакерів, вони отримують імена користувачів та паролі в системах електронної пошти на базі Інтернету або захищених підключеннях до конфіденційних мереж.
- Крок 6: Встановлення. Після успішної експлуатації зловмисник подбає про те, щоб мати постійний доступ до системи. Це робиться шляхом встановлення постійного бекдора або створення облікових записів адміністратора в системі, вимкнення правил брандмауера та, можливо, навіть активації віддаленого доступу до робочого столу на комп'ютерних системах в мережі.
- Крок 7: Контроль. Як тільки зловмисник отримує доступ до мережі, створює облікові записи адміністратора, або встановлює всі необхідні інструменти для бекдорного входу в систему в будь-який час, зловмисник отримує контроль над ціллю.
- Крок 8: Дії для досягнення поставлених цілей. Маючи повний контроль над цільовою системою, зловмисник може ставити цілі і досягати їх без відома справжнього користувача. Таким чином, атаки класифікуються на основі різних кроків, зроблених хакером під час атаки, починаючи від приховування особи та збору інформації, що є попередньою фазою атаки, і закінчуючи самою атакою.

3.3 Поширенні загрози кібербезпеки

Спільною метою кібератак є відключення або отримання доступу до цільової системи. Мета може бути досягнута шляхом застосування різних атак на цільову систему. Існує кілька кібератак, які навіть розвиваються день у день. Розглянемо ряд поширених кібератак[36]:

Спуфінг - це приховування своєї особистості, для того щоб уникнути виявлення за несанкціоновані дії та спроба видати себе за когось іншого з метою завоювати довіру і отримати конфіденційну системну інформацію. Звичайна підробка, здійснювана шляхом зміни апаратного забезпечення або MAC-адреси, називається клонуванням MAC, зміна IP-адреси або унікального ідентифікатора в мережі називається IP-підробкою, а видача себе за когось іншого в їх цифровому спілкуванні називається підробкою електронної пошти.

Malware - це шкідливе програмне забезпечення, призначене для знищення окремої системи або мережі. До цієї категорії належить базове шкідливе програмне забезпечення, таке як хробаки, віруси та трояни, а також останнє шкідливе програмне забезпечення, таке як шпигунське програмне забезпечення, програми-вимагачі. Шкідливе програмне забезпечення заражає систему або мережу, коли користувач натискає небезпечне посилання через вкладення електронної пошти або при установці ризикованого програмного забезпечення. Головне, що слід зазначити, це те, що шкідливе програмне забезпечення відтворюється або поширюється, коли воно взаємодіє з іншою системою чи пристроєм. Деякі з причин включають блокування доступу до мережі, установку додаткового шкідливого програмного забезпечення, збір інформації[36].

Збір інформації - це практика зловмисника, який отримує безцінні відомості про ймовірні цілі. Це не атака, а лише попередня фаза атаки, і вона повністю пасивна, оскільки явної атаки немає. Системи, включаючи комп'ютери, сервери і мережеву інфраструктуру, включаючи канали зв'язку і міжмережеві пристрої, скануються і досліджуються на предмет отримання такої інформації, як запущена цільова система, список відкритих портів, відомості про операційну систему і її версії і т. д.

Фішинг - це практика надсилання шахрайських повідомлень, які, як видається, надходять з авторитетного джерела, як правило, електронною поштою. Мета полягає в тому, щоб вкрасти конфіденційні дані, такі як дані кредитної картки та дані для входу в систему, або встановити шкідливе ПЗ на комп'ютер жертви. Фішинг стає все більш поширеною кіберзагрозою.

Атаки «людина посередині» (MitM) відбуваються, коли зловмисники підключаються до двосторонньої транзакції. Як тільки зловмисники переривають трафік, вони можуть фільтрувати та красти дані. Зазвичай це відомо як напади підслуховування. Існує кілька варіацій MitM-атак, які включають в себе крадіжку пароля, пересилання облікових даних. Зазвичай при використанні незахищеного загальнодоступного Wi-Fi зловмисники можуть вставляти себе між пристроєм відвідувача і мережею. Сам того не знаючи, відвідувач передає всю інформацію через зловмисника. У деяких випадках зловмисник встановлює деяке програмне забезпечення для збору інформації про жертву за допомогою шкідливого ПЗ[36].

Шпигунське та рекламне ПЗ - це програмне забезпечення, загальною властивістю якого є збір особистої інформації користувачів без їх відома. Рекламне програмне забезпечення призначене для відстеження даних про поведінку користувача під час серфінгу, і на основі цього відображаються спливаючі вікна та рекламні оголошення. Положення про рекламне програмне забезпечення в угоді під час процесу встановлення часто пропускається з найменшою серйозністю. З іншого боку, шпигунське програмне забезпечення встановлюється на комп'ютер і збирає інформацію про діяльність користувача в Інтернеті без його відома. Шпигунське програмне забезпечення містить кейлоггери, які записують все, що вводиться на клавіатурі, що робить його небезпечним через високу загрозу крадіжки особистих даних.

Кейлогер має можливість записувати натискання клавіш, а також робити скріншоти і зберігати їх у файл журналу в зашифрованому вигляді. Програмне забезпечення кейлоггера може записувати всю інформацію, що вводиться на клавіатурі, включаючи паролі, електронну пошту та миттєві повідомлення. Файл журналу, створений кейлоггером, зберігається і відправляється зловмиснику

поштою на віддалену машину з метою вилучення пароля і банківських реквізитів для фінансового шахрайства[36].

Криптоджекінг. Спеціалізована атака, яка включає в себе отримання чужого комп'ютера для виконання роботи по генерації криптовалюти. Зловмисники або встановлюють шкідливе програмне забезпечення на комп'ютер жертви для виконання необхідних обчислень, або іноді запускають код на JavaScript, який виконується в браузері жертви.

Програма-вимагач - це шкідливе програмне забезпечення, яке перешкоджає доступу до комп'ютера або файлів на комп'ютері. Комп'ютери можуть бути заблоковані або файли зашифровані. Відповідно, двома поширеними типами програм-вимагачів є програми-вимагачі для блокування екрана та програми-вимагачі для шифрування. З жертви зажадають викуп за зняття обмеження, і це відобразиться в системі жертви. Також може бути повідомлення про те, що установи виявили незаконну діяльність на цьому комп'ютері і вимагають викуп в якості штрафу, щоб уникнути судового переслідування[36].

Атаки «відмови в обслуговуванні» (DoS), як випливає з назви, забороняють користувачам отримувати доступ або користуватися послугою чи системою. В основному це досягається за рахунок перевантаження смуги пропускання, центрального процесора або пам'яті, при якій доступ до мережі комп'ютера-жертви або сервера, що пропонує послугу, стає неможливим. Таким чином, DoS-атаки переривають роботу комп'ютера або мережевих систем, роблячи їх недоступними або занадто низькими по продуктивності[36].

При розподілених атаках «відмови в обслуговуванні» (DDoS) жертва піддається атаці з великої кількості окремих скомпрометованих систем одночасно[37]. DDoS-атаки зазвичай здійснюються за допомогою ботнетів. Ботмастер - це зловмисник, який побічно атакує машину-жертву, використовуючи армію ботів[38]. DDoS-атаки відбуваються, коли велика кількість скомпрометованих систем діють синхронно і координуються під контролем зловмисника, щоб повністю вичерпати його ресурси і змусити його відмовити в обслуговуванні своїм справжнім користувачам.

Експлойт нульового дня з'являється після оголошення про вразливість мережі, але до впровадження виправлення або рішення. Зловмисники націлюються на розкриту вразливість протягом цього проміжку часу. Виявлення загроз вразливості нульового дня вимагає постійної обізнаності.

Спам - це небажане повідомлення електронної пошти. Надсилання спаму електронною поштою може бути не тільки трудомістким завданням для одержувачів, але й джерелом аплетів Java, які можуть виконуватися автоматично під час читання повідомлення[39].

Крім вищезазначених загроз, інститут SANS визначає наступні шкідливі дії шпигунського ПЗ як найбільш часті шкідливі дії[40]:

- Зміна мережевих налаштувань;
- Відключення антивірусних і антишпигунських засобів;
- Вимкнення центру безпеки Microsoft або автоматичних оновлень;
- Установка підроблених сертифікатів;
- Моніторинг URL-адрес, очищення форм і екрану;
- Включення мікрофона або камери на пристрої;
- ПЗ вдає з себе антишпигунський або антивірусний інструмент;
- Редагування результатів пошуку;
- ПЗ діє як ретранслятор спаму.

3.4 Сучасні загрози та тренди кібербезпеки

Прогнозування загроз і тенденцій комп'ютерної безпеки зазвичай робиться для того, щоб допомогти експертам з безпеки, які вживають активних заходів для захисту безпеки. Зазвичай прогнози на будь-який рік залежать від того, як все відбувалося в попередні роки, і очікувані зміни в основному стосуються тактики і масштабу найбільших і значущих загроз, які були успішно реалізовані. Інвестиції в безпеку виправдані в багатьох організаціях тільки після аналізу цих прогнозів[36].

Фішинг та інші тактики соціальної інженерії, ймовірно, продовжуватимуться і в найближчі роки зі зростаючою складністю та витонченістю. Вони будуть здаватися все більш переконливими, щоб обдурити людей за посиланням або відкритим вкладенням. Навіть при наявності надійних засобів захисту від програм-

вимагачів очікується, що хакери весь час будуть націлюватися на більше число жертв з великими цифровими активами. Зростання популярності криптовалют, також викличе більше атак програм-вимагачів, дозволяючи вимагати оплати інкогніто. Криптоджекінг також можна розглядати як загальну тенденцію майбутнього, оскільки він включає в себе хакерські захоплення з метою видобутку криптовалют. У міру того, як IoT стає все більш популярним і поширеним, атаки IoT будуть набирати обертів. Сюди входять ноутбуки, планшети, розумні пристрої, веб-камери, побутова техніка, динаміки з підтримкою Wi-Fi, побутова техніка, будильники, медичні прилади, виробниче обладнання, автомобілі та мережеві пристрої, такі як маршрутизатори, шлюзи, комутатори, сервери NAS і навіть системи домашньої безпеки. Безпека рідко є першою турботою в конкурентній боротьбі за впровадження нових продуктів і технологій. Таким чином, чим більше пристроїв IoT, тим більший ризик, що це призведе до зростання кількості атак IoT у найближчі роки.

Порушення даних продовжуватимуться в найближчі роки, оскільки дані залишаються цінним об'єктом тяжіння на чорному ринку. Абсолютно нові підходи до захисту даних та інфраструктури необхідні, оскільки все більше і більше даних переміщуються в хмару. Крім того, в найближчі роки буде більше атак, націлених на електричні мережі, автоматизовані транспортні системи, комп'ютеризовані водоочисні споруди і т. д.

Атаки, що фінансуються державою - це коли держави використовують свої кібернетичні навички для проникнення в інші уряди для здійснення атак на критичну інфраструктуру. У міру зростання політичної напруженості спонсоровані державою атаки викрадають політичні та промислові секрети, поширюють дезінформацію, проводять DDoS-атаки, здійснюють помітні витоки даних і т. д.

Іншою метою зловмисника є конфіденційна медична карта пацієнтів. Оскільки індустрія охорони здоров'я звикає до цифрового віку, також спостерігається зростання занепокоєння щодо конфіденційності, безпеки та загроз комп'ютерній безпеці. Є побоювання, що хакер може заволодіти і змінити

дозування ліків, відключити моніторинг життєво важливих показників і т.д. Такі дії несуть в собі великий ризик для життя пацієнтів.

З появою самокерованих автомобілів, напівавтономних транспортних засобів і підключених автомобілів, ризик кібербезпеки в цій сфері є серйозним. З появою високотехнологічних автомобілів у майбутньому, ймовірно, збільшиться не тільки кількість підключених автомобілів, але і кількість та серйозність виявлених системних вразливостей. Для хакерів це означає ще одну можливість скористатися вразливими місцями та створити загрозу для життя.

Безпека кінцевих точок є серйозною проблемою для організацій, оскільки зараження шкідливим програмним забезпеченням пристроїв, що належать працівникам, стала серйозною проблемою безпеки в 2020 році, коли співробітники працювали вдома під час пандемії COVID-19. Коли організації дозволяють працівникам не ризикувати своїм здоров'ям та безпекою та дозволяють їм використовувати власні пристрої, зловмисники націляться на ці пристрої, щоб обійти багаторівневий захист організації. Перевага для хакерів полягає в тому, що персональні пристрої користувачів менш захищені в порівнянні з корпоративними пристроями, оскільки користувачі рідко застосовують додаткові заходи для захисту своїх інтелектуальних пристроїв від загроз. Штучний інтелект також застосовується по обидва боки барикад для захисту комп'ютерів і атак на них. Штучний інтелект використовується для ідентифікації особи, виявлення загроз, однак хакери також використовують його в якості засобу для розробки все більш складних шкідливих програм і методів атак.

3.5 Безпека обчислювальних кластерів

Проблема продуктивності безпеки стає більш складною, оскільки кластерні системи використовують дуже високошвидкісні кластерні з'єднання. Традиційно всі комунікаційні завдання, такі як пакетування і обробка переривань, виконуються операційною системою, споживаючи обчислювальну потужність центрального процесора хоста. Оскільки кластерні з'єднання стають швидшими. Накладні витрати на обробку повідомлень стають все більш помітними. М. Лі розглядає проблеми безпеки в кластерному з'єднанні, особливо при взаємодії на рівні

користувача (ULC), порівняння схем для забезпечення безпеки ULC; хост-процесор, захищений співпроцесор і карта мережевого інтерфейсу з примусовим забезпеченням безпеки (SCENIC). SENIC рекомендується за його низьку наскрізну затримку і високу прозорість безпеки при збереженні переваги ULC в продуктивності за рахунок обходу головного процесора[41].

М. Пурзанді та Д. Гордон представляють підхід до забезпечення безпеки, заснований на тому, що кластерне середовище операторського класу являє собою незалежну модель безпеки, яка включає розподілену автентифікацію і розподілений контроль доступу[42]. Підхід до забезпечення безпеки кластерного середовища HPC фокусується на багатовимірному виявленні, призначеному для забезпечення управління безпекою кластерів в режимі реального часу, яке швидко і автоматично адаптується до мінливих ситуацій. NVisionCC - це перша система виявлення вторгнень, спеціально розроблена для унікальною кластерної середовища HPC[43].

Професори Вей Лі та Рейфорд Б. Вон вивчили вразливості безпеки обчислювальних кластерів, використовуючи графіки експлуатації. Вони змоделювали кілька атак, які можуть бути здійснені на конфіденційність, цілісність і доступність. Їх дослідження показали, що електронні графіки можуть бути спрощені на основі знань домену, таких як конфігурації кластерів та виявлені вразливості. В дослідженні стверджується, що цей метод може бути використаний для сертифікації кластерів за допомогою бази знань про вразливість кластерів[44].

Атака типу «відмова в обслуговуванні» (DoS) є однією з поширених атак на розподілені системи. Ця атака в основному націлена на ресурси таким чином, що ресурси не можуть виконувати свої законні операції. В дослідженні Чанхуа Чжу презентується метод, який використовує ланцюжок Маркова, щоб пом'якшити наслідки DoS-атаки на бездротову сенсорну мережу на основі кластера. Підхід ланцюга Маркова був використаний для отримання ймовірності активних кластерів, інтегрованих ними для кількісної оцінки живучості, яка визначається як здатність надавати базові послуги після атак або системної помилки в різних станах[45].

С. Хало та Р. Нівас запропонували модель безпеки для комп'ютерних мереж, які базуються на архітектурі кластерних обчислень з використанням різних доступних інструменті в у моделі безпеки TCP/IP. Кожен інструмент має свої власні функції безпеки, які роблять систему безпечною. Вони застосували ці засоби безпеки з їх функціями безпеки на різних рівнях архітектури кластерних обчислень, щоб зробити її безпечною та високопродуктивною обчислювальною системою[46].

В підсумку зауважимо, що кластери комп'ютерів вразливі для атак з боку зловмисних елементів, таких як хакери і зломщики, через їх відкритого характеру і використання загальнодоступних ресурсів, таких як Інтернет. Ряд науковців провели значні дослідження щодо безпеки кластерів та запропонували кілька методів, які можуть бути використані для захисту кластерів від цих атак.

3.6 Безпека Grid систем

Безпека була центральною проблемою в грід-обчисленнях з самого початку і розглядалася як найбільш значна проблема для грід-обчислень. М. Ессаїді запропонував класифікацію різних механізмів і рішень, що відносяться до різним компонентам безпеки грід-обчислень. Ця класифікація поділяє безпеку грід-обчислень на п'ять основних категорій: рівень ресурсів, рівень обслуговування, рівень автентифікації та авторизації, інформаційний рівень і рішення на рівні управління[47].

Зокрема, грід-обчислення чутливі до автентифікації і авторизації через їх децентралізований тип. Автентифікація у середовищі грід-обчислень - це перша лінія захисту перед будь-якими іншими аспектами безпеки. Це пов'язано з перевіркою ідентичності об'єкта в мережі. Класифікував методи автентифікації на: автентифікацію kerberos, автентифікацію по паролю, автентифікацію Secure Sockets Layer (SSL) і центри сертифікації (CA). Авторизація - це один із процесів, який визначає, чи авторизована конкретна операція. У грід-обчисленнях системи авторизації можна розділити на дві категорії: системи рівня віртуальної організації (VO) мають централізовану систему авторизації, яка надає користувачам облікові дані для доступу до ресурсів; і системи рівня ресурсів, децентралізовані і

дозволяють користувачам отримувати доступ до ресурсів на основі облікових даних, представлених користувачами.

Автентифікація по паролю. Проста функція, при якій одна сторона представляє системі набір облікових даних (ідентифікатор користувача і комбінацію паролів). Якщо облікові дані відповідають заданому набору в системі, система повертає значення, що представляє авторизацію; інакше це не так. У разі, якщо повідомлення не можуть бути прочитані ненадійним об'єктом, можна використовувати незашифровані паролі, в іншому випадку замість відправки паролів по мережі можна використовувати пароль в якості ключа шифрування[9].

Автентифікація Kerberos. Протокол, який працює на основі «квитків», дозволяючи вузлам, що спілкуються через незахищену мережу, безпечно підтверджувати свою ідентичність один одному[9].

Аутентифікація на рівні захищених сокетів (SSL). Безпека транспортного рівня (TLS) і його попередник Secure Sockets Layer (SSL) - це криптографічні протоколи, які забезпечують безпеку зв'язку через Інтернет. TLS та SSL шифрують сегменти мережевих з'єднань вище транспортного рівня, використовуючи асиметричну криптографію для обміну ключами, симетричне шифрування для конфіденційності та коди автентифікації повідомлень для забезпечення цілісності повідомлень. Кожен клієнт перевіряє справжність сервера, надсилаючи ключ сеансу від клієнта до сервера для налаштування зашифрованого зв'язку. Протокол TLS дозволяє клієнт-серверним додаткам взаємодіяти по мережі способом, призначеним для запобігання підслуховування і несанкціонованого доступу. Як тільки клієнт і сервер вирішили використовувати TLS, вони підключилися за допомогою процедури встановлення зв'язку. Під час цього «рукостискання» клієнт і сервер узгоджують різні параметри, які використовуються для встановлення безпеки з'єднання[9].

Центри сертифікації. Якщо мережевому ресурсу потрібно безпечно взаємодіяти з іншим мережевим ресурсом, йому потрібен сертифікат, підписаний центром сертифікації. Безпека в середовищі grid може ґрунтуватися на документах з цифровим підписом або сертифікатах, які передають ідентифікаційні дані,

авторизацію та атрибути. Цифровий підпис може підтвердити дійсність документа без фізичної присутності підписувача або фізичного володіння документами, підписаними почерком автора. Автентифікація користувачів здійснюється шляхом пред'явлення сертифіката посвідчення особи і підтвердження того, що вони знають відповідний закритий ключ. Ці сертифікати видаються центрами сертифікації, які перевіряють зв'язок між користувачем або системним компонентом та право власності на пару відкритого, приватного ключа. Користувачі створюють і підписують цифровим підписом сертифікати умов використання, які визначають умови, які повинні бути виконані користувачем, перш ніж йому буде надано доступ до ресурсу. Атрибути користувача затверджуються «органами влади», які надають гарантовану інформацію у вигляді сертифікатів атрибутів з цифровим підписом. Як сертифікати умов використання, так і сертифікати атрибутів можуть зберігатися локально для користувача до тих пір, поки вони можуть бути надані сервером, коли вони необхідні для визначення дозволів під час запиту доступу[9].

Віртуальні системи рівня організації. VO визначається як динамічна група індивідів або організації, які визначають умови та правила (бізнес-цілі та політику) для спільного використання ресурсів. Системи авторизації grid рівня VO є централізованою авторизацією для всього VO. Ці типи систем необхідні через наявність VO, який має набір користувачів, і декількох постачальників ресурсів, що володіють ресурсами, які будуть використовуватися користувачами VO. Щоразу, коли користувач хоче отримати доступ до певних ресурсів, що належать постачальнику, користувач отримує облікові дані з системи авторизації, яка надає користувачам певні права. Користувач надає облікові дані ресурсу, щоб отримати до нього доступ. У системах такого типу ресурси мають остаточне право дозволяти або забороняти доступ користувачам. Прикладами систем авторизації сітки рівня VO є CAS (служба авторизації спільноти), VOMS (служба членства у віртуальній організації) та EALS (система авторизації та ліцензування підприємства)[9].

Системи на рівні ресурсів. На відміну від централізованих систем авторизації, децентралізовані системи реалізують рішення про авторизацію доступу до набору ресурсів. Постачальники ресурсів надають привілеї спільноті. Це робиться після

встановлення довірчих відносин із спільнотою. Коли користувач хоче отримати доступ до ресурсу, він вводить свої облікові дані, які містять конкретні твердження політики. Постачальник ресурсів приймає рішення про те, надавати або відхиляти запит на доступ до його ресурсів. Прикладами систем авторизації на рівні ресурсів є системи Akenti, GridMap та PERMIS (перевірка стандартів інфраструктури управління привілеями та ролями)[9].

3.7 Безпека мережі P2P

Одноранговi мережі (P2P) забезпечують потужну платформу для створення різних децентралізованих послуг. Мережі P2P пропонують користувачам багато переваг, але протистояти різним атакам безпеки та захищатися від них стає важко. Оскільки системи P2P за своєю суттю покладаються на залежність одноранговых вузлів один від одного, зловживання довірою між вузлами є суттєвою проблемою. У традиційній моделі клієнт-сервер внутрішні дані не повинні надаватися клієнту. Але в P2P деякі внутрішні компоненти повинні бути доступні пов'язаним вузлам з метою розподілу робочого навантаження. Зловмисники можуть використовувати це для того, щоб скомпрометувати P2P-мережі. Іншими словами, децентралізований характер і відсутність контролюючого органу піддають P2P-системи широкому спектру атак безпеки. Приклади таких атак включають: відмову в обслуговуванні (DoS), несанкціоноване завантаження, атаки типу «забруднення» та атаку ідентифікації, яка дозволяє зловмисному одноранговому вузлу в мережі перехоплювати запит програми та брати на себе відповідальність за будь-який компонент програми. Е. Кутрулі та А. Цалгатіду досліджували та класифікували типи потенційних атак на системи репутації для додатків P2P. Крім того, вони класифікували захисні механізми, які були запропоновані для кожного типу атаки, і виявили конфлікти між захисними механізмами або бажаними характеристиками надійних систем репутації. Більше того, вони запропонували розробникам систем репутації дорожню карту про те, як використовувати результати опитування для розробки надійних систем репутації для P2P-додатків. Потокові додатки через P2P-системи набули величезної популярності. Успіх завжди має на увазі підвищену турботу про безпеку, захищеності і недоторканності приватного життя[48].

3.8 Безпека хмарних обчислень

Характеристики та моделі хмарних обчислень, представлені в попередньому розділі, пропонують клієнтам покращені, оптимізовані та недорогі послуги. Наведені в першому розділі моделі, що забезпечують зазначені характеристики, реалізовані з використанням різних технологій, наприклад віртуалізації і багатокористувацької оренди. Технології разом із хмарними сервісами та моделями розгортання створюють специфічні для хмари ризики безпеки та вразливості на додаток до загальних ризиків із звичайною IT-інфраструктури.

Ризики безпеки в хмарі можуть відрізнятися від ризиків звичайної IT-інфраструктури за характером, інтенсивністю, або за обома критеріями. Об'єднання ресурсів дозволяє використовувати один і той же пул кільком користувачам за допомогою технологій множинної оренди і віртуалізації. Хоча технології забезпечують швидку еластичність та оптимальне управління ресурсами, вони також вносять певні ризики в систему. Багаторазова оренда призводить до ризиків видимості даних для інших користувачів та відстеження операцій. Функція самообслуговування на вимогу надається клієнтам за допомогою веб-інтерфейсів управління, що підвищує ймовірність несанкціонованого доступу до інтерфейсу управління в порівнянні з традиційними системами.

Аналогічно, віртуалізоване середовище представляє власний набір ризиків та вразливостей, що включає шкідливу взаємодію між віртуальними машинами (VM). Аналогічно, з точки зору моделі хмарних сервісів, моделі сервісів залежать одна від одної. Програми SaaS створюються та розгортаються поверх PaaS, а PaaS залежить від базового IaaS. Ця операційна залежність моделей обслуговування один від одного призводить також до залежності безпеки. Наприклад, якщо зловмиснику вдасться взяти під контроль IaaS, результатом буде скомпрометований PaaS, який використовує IaaS. Скомпрометований PaaS може призвести до порушення SaaS. Інакше кажучи, будь-яка скомпрометована модель сервісу надає доступ до іншого рівня моделі сервісу. Модель розгортання приватної хмари успадковує той самий набір вразливостей, що і звичайна IT-інфраструктура. Причина в тому, що приватна хмара призначена для використання однією

організацією. Загальнодоступні, громадські та гібридні хмари мають велику кількість вразливостей та ризиків, характерних для хмари, через присутність користувачів з різних джерел та адміністративний контроль третьої сторони.

Наявність кількох орендарів, що використовують віртуалізовані ресурси, які можуть відповідати тим самим фізичним ресурсам, створює багато проблем із безпекою. Ідеальне розділення численних орендарів та виділених ресурсів є складним завданням і вимагає набагато вищого рівня безпеки.

Розглянемо звіт для фахівців та ентузіастів з безпеки хмарних технологій. Дані звіту надають актуальне уявлення про стан загроз і викликів хмарної безпеки, про те, як вони вплинули на галузь, і що можна зробити для поліпшення як окремої людини, так і галузі в цілому. Дослідження, засноване на опитуванні, ознайомлює з дотримання вимог, ризиків, технологій і високопріоритетними міркуваннями хмарної безпеки, актуальними в даний час.

Таблиця 3.1 - Головні загрози хмарним обчисленням[49]

Рейтинг результатів опитування	Середній бал опитування	Назва проблеми
1	7.729	Недостатня ідентичність, облікові дані, доступ та управління ключами, привілейовані облікові записи
2	7.592	Небезпечні інтерфейси та APIs
3	7.424	Неправильна конфігурація та неадекватний контроль змін
4	7.408	Відсутність архітектури та стратегії хмарної безпеки
5	7.275	Небезпечна розробка програмного забезпечення
6	7.214	Незахищені сторонні ресурси

Продовження Таблиці 3.1 – Головні загрози хмарним обчисленням[49]

7	7.143	Системні вразливості
8	7.114	Випадкове розкриття хмарних даних
9	7.097	Неправильна конфігурація та експлуатація безсерверних та контейнерних навантажень
10	7.088	Організована злочинність / хакери
11	7.085	Ексфільтрація даних хмарного сховища

Порушення даних залишаються проблемою, незважаючи на зростання обізнаності про кібербезпеку та інвестиції. Минулий 2021 рік був особливо важким роком для злому хмарних обчислень, коли інциденти призводили до відключення мереж на кілька тижнів і порушували роботу бізнесу по всій країні. Хоча Amazon Web Services (AWS) стає все більш популярним інструментом, який дозволяє підприємствам завантажувати та розповсюджувати дані з неперевершеною ефективністю, він має унікальний набір вразливостей, які користувачі не помічають. Неправильно налаштовані сегменти Simple Storage Service (S3) можуть становити серйозні ризики для хмарного середовища. Для уточнення, публічний доступ до читання може призвести до витоку даних, тоді як публічний доступ до запису може запустити шкідливе програмне забезпечення або зашифрувати дані для викупу вашої компанії. Виділимо кілька найбільш помітних порушень даних AWS за 2021 рік. У 2021 році відбулися зломи, які торкнулися ряду великих компаній, таких як Twitch, Cosmology Kozmetik, PeopleGIS, Premier Diagnostics, Senior Advisor, Reindeer, Twillo[50]. Причому більшість цих атак були пов'язані зі зловживанням привілеями з боку інсайдерських загроз. Наприклад, Twitch надав доступ до даних в Інтернеті через помилку в зміні конфігурації сервера Twitch, до якого згодом отримала доступ шкідлива третя сторона. Служба тестування на Covid-19 Premier Diagnostics Utah розмістила тисячі сканувань посвідчень особи, включаючи водійські права, картки медичного страхування, паспорти та інші посвідчення особи, в Інтернеті без пароля або будь-якої іншої автентифікації, необхідної для доступу до них[50].

4 РОЗРОБКА МАТЕМАТИЧНОЇ МОДЕЛІ ОЦІНКИ РІВНЯ ЗАГРОЗ

4.1 Огляд і аналіз баз даних вразливостей та дефектів

Створення реєстрів і баз даних з інформацією про виявлені вразливості потребувало уніфікованого способу ідентифікації та класифікації вразливостей. Кожній виявленої вразливості потрібно присвоїти ідентифікатор, дати їй ємний та короткий опис, визначити список вразливого ПЗ і його версій. Крім того, було потрібно оцінити ступінь критичності даної вразливості по ряду різних критеріїв: простоті виявлення зловмисником вразливого ПЗ, легкості експлуатації вразливості і необхідним для цього привілеїв, а також потенційних наслідків експлуатації вразливості для комп'ютерної системи. Ця інформація могла згодом доповнюватися рекомендаціями щодо усунення вразливості або запобігання її експлуатації та статусом вразливості, наприклад: чи присутня вразливість в актуальній версії ПЗ або ж була закрита відповідними оновленнями та патчами.

Бази даних і реєстри вразливостей корисні широкому колу фахівців в області інформаційної безпеки. Мережеві адміністратори або співробітники, відповідальні за безпеку комп'ютерних систем організації, можуть своєчасно дізнатися з баз і реєстрів про появу нових загроз для обслуговуваних систем, визначити пріоритетні заходи реагування на ці загрози, виходячи з оцінки критичності і поширеності в організації вразливого ПЗ. При цьому для фахівців важливі оперативність оновлень баз даних вразливостей, зручність отримання цих оновлень і ступінь покриття обраним реєстром вразливостей, як основних видів ПЗ захищеної комп'ютерної системи, так і всієї безлічі виявлених для цього ПЗ вразливостей. Також значущими характеристиками будуть наявність рекомендацій щодо усунення вразливостей і можливість визначення потенційних векторів атак на захищені комп'ютерні системи. Поява і розвиток незалежних один від одного баз даних та реєстрів вразливостей сприяло проблемі синхронізації інформації між ними, як в частині однозначної ідентифікації вразливостей, так і в класифікації та оцінці вразливостей, викликаних відмінностями в системах оцінки. В даний час можна зустріти ряд як простих, так і складних ієрархічних класифікацій (таксономій) в області

програмної безпеки, які можна розділити на наступні: класифікації загроз і атак; класифікації шкідливих програм; класифікації та реєстри вразливостей; класифікації дефектів.

Таблиця 4.1 - Класифікації в області безпеки програм

Вид	Приклад	Особливості
Класифікації шкідливого програмного забезпечення	Mitre MAEC (Malware Attribute Enumeration and Characterization) - перелік і характеристики ознак шкідливого ПЗ	Мова для опису шкідливого ПЗ, що враховує ознаки поведінки, тип атаки і т. п.
Реєстри та класифікації вразливостей програмних систем	MITRE CVE (Common Vulnerabilities and Exposures) - загальні вразливості та недоліки	База даних відомих вразливостей
	OSVDB (Open Security Vulnerability Database) - база вразливостей відкритого доступу	База даних відомих вразливостей
	US-CERT Vulnerability Notes Database - база вразливостей	Опис знайдених вразливостей і способів їх виявлення
Класифікації загроз безпеці та комп'ютерних атак на ресурси системи	OWASP Top Ten - 10 найпоширеніші загрози для веб-додатків	Десять найбільш актуальних класів загроз, пов'язаних з вразливістю web-додатків

Продовження Таблиці 4.1 - Класифікації в області безпеки програм

	Microsoft STRIDE Threat Model - модель загроз Microsoft	Опис п'яти основних категорій вразливостей
Класифікації дефектів, внесених в процесі розробки	MITRE CWE (Common Weaknesses Enumeration) - загальна класифікація дефектів ПЗ	Система класифікації недоліків ПЗ
	CWE/SANS Top 25 Most Dangerous Software Errors - 25 найбільш небезпечних помилок в розробці ПЗ	25 найбільш поширених і небезпечних помилок, які можуть стати причиною вразливості
	MITRE Common Configuration Enumeration (CCE) - загальний реєстр конфігурацій	Ідентифікація проблемних конфігурацій системи, що встановлює відповідність між різними джерелами
Класифікації дефектів, внесених в процесі впровадження та експлуатації	DPE (Security-Database Default Password Enumeration) - реєстр паролів за замовчуванням	База даних паролів за замовчуванням для мережевих пристроїв, ПЗ і ОС, призначена для тестування з метою виявлення слабких конфігурацій

4.1.1 CVE

Стандарт Common Vulnerabilities and Exposures (CVE), розроблений американською некомерційною дослідницькою корпорацією MITRE Corporation в 1999 році, де-факто є на сьогоднішній день основним стандартом в області уніфікованого іменування та реєстрації виявлених вразливостей програмного забезпечення. Даний стандарт безпосередньо визначає як формат ідентифікаторів і вмісту записів про окремі виявлені вразливості, так і процес резервування ідентифікаторів для нових виявлених вразливостей і поповнення відповідних баз даних[51]. Вже в 2000 році ініціатива MITRE щодо створення єдиного стандарту для реєстрації та ідентифікації виявлених вразливостей ПЗ отримала широку підтримку з боку провідних виробників програмного забезпечення та дослідницьких організацій в області інформаційної безпеки. За даними на березень 2018 року підтримкою і адмініструванням реєстру вразливостей CVE займається група з 84 організацій по всьому світу, в число яких входять провідні виробники програмного забезпечення, телекомунікаційного обладнання та інтернет-сервісів, такі як Apple, Cisco, Facebook, Google, IBM, Intel, Microsoft, Oracle.

В рамках підтримки проекту MITRE CVE основними завданнями цих організацій є:

- Пошук та збір інформації про вразливості програмного забезпечення.
- Класифікація знайдених вразливостей.
- Резервування CVE-ідентифікаторів для знайдених вразливостей.
- Актуалізація відповідної інформації в двох офіційних каталогах - реєстрі вразливостей CVE List Mitre Corporation та базі даних вразливостей NVD (National Vulnerability Database), підтримуваної NIST[52].

Ідентифікатори CVE мають формат CVE-YYYY-NNNN, відображаючи в перших чотирьох цифрах рік реєстрації вразливості і в наступних чотирьох/шести цифрах - унікальний в рамках цього року номер вразливості. Ідентифікатор CVE присвоюється дефектам, які відповідають певному набору критеріїв, а саме:

- Незалежно фіксується. Цей недолік може бути виправлений незалежно від будь-яких інших помилок.
- Підтверджено відповідним постачальником або задокументовано. Постачальник програмного або апаратного забезпечення визнає помилку і те, що вона робить негативний вплив на безпеку. Або репортер повинен був поділитися звітом про вразливість, який демонструє негативний вплив помилки і те, що вона порушує політику безпеки системи.
- Вплив на одну кодову базу. Недоліки, які впливають на більш ніж один продукт, отримують окремі CVE. У разі спільних бібліотек, протоколів або стандартів недолік отримує один CVE тільки в тому випадку, якщо немає можливості використовувати загальний код, не будучи вразливим. В іншому випадку кожна порушена кодова база або продукт отримує унікальний CVE.

Для кожної з виявлених вразливостей запис в базі містить короткий опис типу і причин виникнення вразливості, вразливі версії ПЗ, оцінку критичності вразливості відповідно до стандарту Common Vulnerability Scoring System (CVSS) та посилання на зовнішні джерела з інформацією про вразливість - найчастіше, такими виступають інформаційні бюлетені на сайтах виробників програмного забезпечення або дослідницьких організацій[53].

Перевагою баз даних MITRE CVE-List і NVD є щоденне оновлення реєстрів відомих вразливостей. При виявленні нової вразливості виробником ПЗ або дослідницькою організацією (або підтвердженні наявності вразливості вендором ПЗ у відповідь на повідомлення від приватних дослідників або організацій, що не входять в CVE Numbering Authorities) під неї оперативно реєструється новий CVE-ідентифікатор і створюється запис в базі, після чого відбувається періодичне оновлення інформації. Деяким обмеженням баз даних CVE List і NVD є відсутність в записах про вразливості будь-якої інформації про точне місце локалізації вразливості в коді вразливого ПЗ і можливих векторах атак, за допомогою яких можлива експлуатація даної вразливості.

4.1.2 NVD

Національна база даних вразливостей (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 записів вразливостей. 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. 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. Однак у даного формату представлення записів продуктів є ряд недоліків, а саме: неоднозначність значень різних полів формату; недостатнє використання записів даного словника базою NVD.

4.1.3 CVSS

Переваги CVSS включають надання стандартизованої методології оцінки вразливостей. Це відкрита структура, що забезпечує прозорість індивідуальних характеристик і методології, що використовуються для отримання оцінки. CVSS складається з трьох метричних груп: базової, тимчасової та контекстної[53]. Базова оцінка відображає серйозність вразливості відповідно до її внутрішніх характеристик, які є постійними з плином часу, і передбачає розумний вплив найгіршого випадку в різних розгорнутих середовищах. Тимчасові метрики коригують базову серйозність вразливості на основі факторів, які змінюються з плином часу, таких як доступність коду експлойта. Показники контекстної групи коригують базову і тимчасову строгість відповідно до конкретного обчислювального середовища. Вони враховують такі фактори, як наявність заходів щодо пом'якшення наслідків у цьому середовищі.

Базові оцінки зазвичай проводяться організацією, що підтримує вразливий продукт, або ж третьою стороною. Зазвичай публікуються тільки базові метрики, оскільки вони не змінюються з часом і є загальними для всіх середовищ. Споживачі CVSS повинні доповнити базову оцінку тимчасовими та контекстними оцінками, специфічними для їх використання вразливого продукту, щоб отримати більш точну оцінку серйозності для їх організаційного середовища. Споживачі можуть використовувати інформацію CVSS як вхідні дані для процесу управління вразливостями організації, який також враховує фактори, що не є частиною CVSS, для ранжирування загроз їх технологічній інфраструктурі та прийняття обґрунтованих рішень щодо усунення загроз. До таких факторів можуть відноситися: кількість клієнтів, грошові втрати через порушення, загроза життю, майну або громадська думка з приводу широко освітлюваних вразливостей.

Базова група метрик представляє внутрішні характеристики вразливості, які є постійними в часі і в різних призначених для користувача середовищах. Група тимчасових метрик відображає характеристики вразливості, які можуть змінюватися з плином часу, але не в різних призначених для користувача середовищах. Наприклад, наявність простого у використанні набору експлойтів збільшить оцінку CVSS, в той час як створення офіційного патча зменшить її. Група контекстних показників представляє характеристики уразливості, які є релевантними і унікальними для середовища конкретного користувача. Включають наявність засобів контролю безпеки, які можуть пом'якшити деякі або всі наслідки успішної атаки, а також відносну важливість вразливою системи в технологічній інфраструктурі. Коли аналітик присвоює значення базовим метрикам, базове рівняння обчислює оцінку в діапазоні від 0,0 до 10,0. Чим простіше вразливість експлуатується і чим більше шкідливого впливу вона надає, тим вище оцінка. Якщо вплив не надається ні на конфіденційність, ні на цілісність, ні на доступність, то числова оцінка базової групи метрик дорівнює нулю.

Розглянемо оцінку базової групи метрик на прикладі вразливості Heartbleed (CVE-2014-0160)[54]. Ця вразливість є наслідком помилки в пакеті OpenSSL, дозволяє витягти довільні дані з оперативної пам'яті сервера. Для проведення атаки

зловмиснику потрібно відправити спеціальним чином сформований запит на атакований сервер. Тобто, зловмиснику достатньо доступу з глобальної мережі (Access Vector: Network). Складність атаки зводиться до запуску готового експлойта (Access Complexity: Low). Аутентифікація при цьому не потрібна (Authentication: None). Отримання приватного ключа сервера означає часткову втрату конфіденційності (Confidentiality Impact: Partial). Так як прочитати не завантажені в оперативну пам'ять дані не вийде, на цілісності та доступності втрата конфіденційності ніяк не позначиться (Integrity Impact: None, Availability Impact: None). Такий результат публікується у вигляді скороченого вектора (AV: N/AC: L/Au: N/C: P/I: N/A: N). Підставивши значення з цього вектора в базове рівняння, отримуємо числову оцінку 5.0 для досліджуваної вразливості.

4.1.4 OSVDB

База даних вразливостей з відкритим кодом (OSVDB) була незалежною базою даних вразливостей. Метою проекту було надати точну, детальну, актуальну та об'єктивну технічну інформацію про вразливості безпеки. Проект сприяв більш широкому та відкритому співробітництву між компаніями та приватними особами. База OSVDB була запущена в 2004 році, за результатами конференцій з комп'ютерної безпеки Blackhat і DEF CON і будувалася навколо ключової ідеї: організувати такий реєстр вразливостей, який містив би повну і детальну інформацію про всі виявлені вразливості, і підтримка якого не була б під впливом виробників програмного забезпечення. Спочатку повідомлення про вразливість, опубліковані в різних списках безпеки та на веб-сайтах, були введені в базу даних як новий запис у черзі нового обробника даних. Новий запис містив лише заголовок та посилання на розкриття інформації. На цьому етапі сторінка нового запису не містила детального опису вразливості або будь-яких пов'язаних метаданих. По мірі можливості нові записи аналізувались та вдосконалювались, додаючи опис вразливості, а також рішення, якщо воно доступне. Автори OSVDB прийняли рішення про закриття бази даних, яке відбулося в 2016 році. В даний час триває епізодична підтримка блогу проекту, а співпраця організації Open Security Foundation та комерційної компанії Risk Based Security призвела до створення

каталогу вразливостей VulnDB, як комерційної реінкарнації OSVDB. База VulnDB станом на дані 2018 року містить інформацію про 176 тис. виявлених вразливостей, включаючи майже 60 тис. записів про вразливості, відсутніх в базах CVE List і NVD. Одним з можливих призначень пропонованого сервісу може бути ризик-менеджмент і оцінка рівня захищеності комп'ютерних мереж організацій.

4.1.5 VND

Прикладом іншого підходу до організації бази вразливостей є база Vulnerability Notes Database (VND), підтримувана центром реагування CERT/CC. Кожен запис в базі VND агрегує інформацію про безліч подібних вразливостей для будь-якого конкретного ПЗ, посилаючись на безліч відповідних CVE-ідентифікаторів. Дана агрегація є характерною відмінністю бази VND від баз CVE List і NVD, дозволяючи перевірити безліч вразливостей схожої природи в конкретному вразливому ПЗ або його компоненті. Крім цього, записи в базі VND часто містять докладний і детальний посібник з усунення вразливостей та запобігання їх експлуатації зловмисником, а також огляд поточної ситуації з наявністю або успішним закриттям виявленої вразливості різними вендорами. Дані характеристики бази VND відносяться до числа її сильних сторін і доповнюються дозволом на безкоштовне використання всіх матеріалів бази для будь-яких цілей і можливістю повного скачування всіх записів бази в форматі JSON за допомогою спеціального безкоштовно програмного забезпечення. Недоліками бази VND є рідкісні оновлення раз на місяць і слабке охоплення всіх існуючих вразливостей, що істотно обмежують корисність даного каталогу вразливостей для оперативного реагування на нові вразливості ПЗ.

4.2 Постановка комбінаторної задачі

Порушені в дослідженні питання оцінки рівня захищеності системи можуть бути зведені до постановки комбінаторних задач. Розглянемо класичне формулювання задачі про покриття множини. Задача про покриття множини широко відома в дискретній оптимізації і має численні додатки. Дана задача узагальнює NP-повну задачу про вершинне покриття і тому також є NP-складною. До задачі про покриття можна звести багато завдань дискретної оптимізації:

стандартизації, упаковки і розбиття множини, побудови розкладів. Відома також і зворотна зводимість задачі до цих завдань. На практиці задачі про покриття виникають при розміщенні пунктів обслуговування, в системах інформаційного пошуку, при призначенні екіпажів на транспорті, проектуванні інтегральних схем, конвеєрних ліній і т. д. Постановка задачі полягає в наступному[55]. Для скінченної множини $M = \{m_1, m_2, \dots, m_m\}$ і деякого скінченного сімейства її підмножин S_j, $j = 1, 2, \dots, n$ потрібно знайти підсімейство $S_j^{`} \subseteq S_j$ з мінімальним набором підмножин $S_j$ таке, що кожен елемент вихідної множини M належить, принаймні, одній із цих підмножин. Знайдені підмножини $S_j^{`}$ зазвичай називають покривними, а сімейство $S_j^{`}$ – найменшим покриттям M. У тому випадку, коли покривним елементам приписана деяка вага, розглядають зважену задачу про покриття, яка передбачає пошук найменшого зваженого покриття M. Коли ж покривні підмножини попарно не перетинаються, задача про найменше покриття трактується як задача про розбиття множини M на найменшу кількість класів. Також задача про покриття формулюється в термінах цілочисельного лінійного програмування. Нехай $A = (a_{ij})$ – довільна матриця розміру $m \times n$ з елементами $a_{ij} \in \{0, 1\}$ без нульових рядків і стовпців. Стверджуємо, що в матриці A рядок i покривається стовпцем j, якщо $a_{ij} = 1$. Підмножина стовпців називається покриттям, якщо в сукупності вони покривають всі рядки матриці A. Нехай кожному стовпцю поставлено у відповідність позитивне число c_j, зване вагою стовпця. Потрібно знайти покриття мінімальної сумарної ваги. Вводячи змінні x_j, рівні 1, якщо стовпець j входить в шукане покриття, і рівні 0 в іншому випадку, приходимо до наступного формулювання задачі про покриття:

$$\sum_{j=1}^{n} c_j x_j \to min \qquad (4.1)$$

При обмеженнях:

$$\sum_{j=1}^{n} a_{ij} x_j \geq 1, i = 1, \dots, m, x_j \in \{0, 1\}, j = 1, \dots, n \qquad (4.2)$$

4.3 Математична модель задачі вибору оптимального плану усунення вразливостей

Вибір засобів захисту інформації це складне завдання в зв'язку з тим, що для кожного об'єкта захисту і виконуваної функції можливе застосування різних програмних і технічних засобів, представлених на ринку. Отже, можна побудувати безліч варіантів комплексів засобів захисту в конкретній інформаційній системі, що відрізняються структурою, складом, вартістю. Для економічного обґрунтування витрат на захист інформації необхідно розглянути питання вибору економічно ефективних стратегій захисту, а саме вибір з безлічі наявних засобів захисту інформації таких, які забезпечують досягнення необхідних значень параметрів системи при мінімальному витрачанні ресурсів. Такий вибір конкретного комплексу засобів захисту на основі принципу «необхідної достатності» ставить за мету вирішення оптимізаційних завдань. Більшість сучасних методик побудови моделі загроз базуються або на статистичних методах, або на експертному оцінюванні. Прогнозувати загрози можна, виходячи з власної статистики порушень безпеки або сторонніх статистичних звітів. При відсутності статистичної інформації оцінка загроз може бути проведена експертним шляхом. Експерти ранжують загрози за їх значимістю і ймовірністю реалізації, керуючись своїм досвідом і знаннями аналізованої системи. Для побудови шкали експертних оцінок можна використовувати механізм оцінювання загроз на основі нечіткої логіки. Він вимагає формування оцінок ключових параметрів і подання їх у вигляді лінгвістичних змінних. На основі моделі загроз вибираються технології, які можуть ефективно протидіяти загрозам безпеці. Кожна загроза повинна бути перекрита відповідним засобом захисту, що відносяться до рекомендованого обладнання.

Для вирішення завдання раціонального побудови структури і вибору складу засобів захисту інформації необхідно мати безліч критеріїв, що відображають найбільш істотні аспекти створюваного комплексу засобів захисту. Для кожного засобу захисту найбільш доцільно застосовувати наступні групи критеріїв:

- відносні показники ефективності (захищеності) засобів захисту при впливі кожної із загроз безпеці;

- економічні, що враховують різні види і складові витрат (вартість засобу захисту інформації і витрати на установку, експлуатацію, обслуговування);
- додаткові критерії (швидкодія, показники простоти і зручності використання).

Отже, кожен із засобів захисту описується набором параметрів: $M_i = C_i, \{P_{ij}\}, W_i, V_i, ...$, де c_i - витрати засобів захисту; $\{P_{ij}\}$ - безліч відносних показників ефективності (захищеності) засобів захисту для кожної із загроз безпеці; W_i - час на здійснення елементарної операції; V_i - необхідний обсяг оперативної пам'яті. За необхідністю проектувальники системи захисту можуть додати нові критерії для оцінки механізмів захисту. Відносний показник ефективності засобу захисту для однієї із загроз безпеці P_{ij} - кількісна характеристика оцінки рівня забезпечуваного інформаційного захисту, якою володіють засоби захисту при здійсненні даної загрози. Значення цього показника лежить в межах від 0 до 1. Чим він більший, тим ефективніше використання даного засобу захисту для протидії загрозі. При відсутності перекриття механізмом захисту M_i певної загрози A_i показник ефективності P_{ij} засобів захисту для загрози безпеці приймається рівним 0.

Розглянемо математичну постановку задачі оптимального вибору складу способів і засобів захисту в формі, яка дозволить звести її до стандартних задач математичного програмування. Вибір необхідних засобів M_i з усього безлічі доступних (сертифікованих) для побудови системи захисту інформації, що забезпечують перекриття виявлених вразливостей і мінімізацію витрат на захист інформації, сформулюємо у вигляді комбінаторної задачі про найменше покриття. Перейдемо до детального розгляду моделі задачі дослідження. Маємо множину засобів нейтралізації вразливостей $M = \{m_1, m_2, \dots, m_m\}$. Сукупність її підмножин $\{M_j\}$ - покриття множини M. Кожному M_j приписано вагу c_j - витрати обчислювальних або матеріальних ресурсів. Потрібно знайти покриття, що має мінімальну сумарну вагу c_j. Введемо змінну $x_j, j = 1, \dots, m$. Змінна $x_j = 1$, якщо

засіб захисту входить в покриття, інакше $x_j = 0$. Визначимо матрицю $A = \{a_{ij}\}, i = 1, \dots, n, j = 1, \dots m$:

$$a_{i,j} = \begin{cases} 1, \text{якщо засіб j нейтралізує вразливість i;} \\ 0, \text{в протилежному випадку.} \end{cases}$$

Задача полягає в знаходженні вектора цілочисельних варійованих змінних $X = \{x_i\}, j = 1, \dots m$, мінімізуючи лінійну цільову функцію:

$$F(X) = \sum_{j=1}^{m} c_j x_j \to min \tag{4.3}$$

При обмеженнях:

$$\sum_{j=1}^{m} a_{ij} x_j \geq 1, \quad i = \overline{1, n} \tag{4.4}$$

$$\sum_{j=1}^{n} a_{ij} x_j \geq 0, \quad j = \overline{1, m}, \tag{4.5}$$

де x_i приймає значення 0 або 1; m - число засобів нейтралізації вразливостей; n - кількість виявлених вразливостей; c_j – сумарні витрати. Умова (4.4) виражає вимогу забезпечення протидії будь-якій вразливості за допомогою хоча б одного з використовуваних засобів захисту.

Процедуру обґрунтування плану нейтралізації виявлених вразливостей на основі застосування наявних у розпорядженні адміністратора інформаційної безпеки механізмів захисту інформації можна звести до задачі про призначення. Задача призначення - це задача розподілу, де для виконання кожної роботи потрібен один і лише один ресурс. Кожен ресурс може бути використаний на одній і тільки одній роботі. Іншими словами, в класичному варіанті приймається, що ресурси неподільні між роботами, а роботи неподільні між ресурсами. Нехай задані: m - кількість наявних ресурсів; n - кількість робіт; $a_i = 1$ - одинична кількість ресурсу, $A_i, i = 1, \dots, m$; $b_j = 1$ - одинична кількість роботи, $B_j, j = 1, \dots, n$; $r_{i,j}$ -

характеристика якості (позитивний ефект), обумовлений виконанням роботи B_j за допомогою ресурсу A_i. Шукані параметри: $x_{i,j}$ - індикатор призначення ресурсу A_i на роботу B_j.

$$x_{i,j} = \begin{cases} 0, \text{якщо ресурс } i \text{ не призначений на работу } j; \\ 1, \text{якщо ресурс } i \text{ призначений на работу } j. \end{cases}$$

Математична модель задачі про призначення має наступний вигляд:

$$f(X) = \sum_{i=1}^{m} \sum_{j=1}^{n} (r_{i,j} \cdot x_{i,j}) \to max, \tag{4.6}$$

$$\sum_{i=1}^{m} x_{i,j} = 1, \;\; j = 1, \dots, n, \tag{4.7}$$

$$\sum_{j=1}^{n} x_{i,j} = 1, \;\; i = 1, \dots, m, \tag{4.8}$$

де $x_{i,j} = \{0,1\}, \; i = 1, \dots, m, \; j = 1, \dots, n.$

У поточній інтерпретації задачі в області інформаційної безпеки модель задачі має наступні особливості:

1) Потрібно в результаті вирішення задачі запропонувати такий план $X^* = (x_1^*, x_2^*, \dots, x_n^*)$ захисту, який дозволить нейтралізувати виявлені вразливості і домогтися мінімального середнього збитку при здійсненні атак зловмисника з найменшими витратами обчислювальних (або матеріальних) ресурсів. Окремі засоби захисту можуть бути використані для інтегрованого захисту ресурсів, що проявляється в можливості одночасної нейтралізації декількох корельованих вразливостей. Допустима нейтралізація одночасно двох різних вразливостей за допомогою одного засобу захисту.
2) Реалізація плану захисту ресурсів полягає в активізації m $(m \leq N)$ наявних механізмів захисту.

3) Оцінка реалізованого механізму нейтралізації характеризується витратами ресурсів, вираженими у вартісному еквіваленті, і середнім відверненим збитком, зумовленим успішною нейтралізацією ймовірної атаки зловмисника.

З урахуванням зазначених зауважень визначимо узагальнений показник оптимальності комплексу заходів захисту наступним чином:

$$F(X) = \frac{F_1(X)}{F_2(X)}, \tag{4.9}$$

де $F_1(X)$ - величина сукупного запобігання збитку в вартісному еквіваленті; $F_2(X)$ - величина сукупних витрат на реалізацію активованого механізму захисту, що реалізує оптимальний план нейтралізації вразливостей у вартісному еквіваленті. Вираз (4.9) являє собою показник, сформований відповідно до узагальненого критерію «ефективність/вартість».

4.4 Огляд алгоритмів вирішення задачі

Для вирішення задачі покриття множин розроблено безліч алгоритмів, які можна розділити на наступні класи: наближені алгоритми з апріорною оцінкою, евристичні алгоритми, точні алгоритми. Одним з перших наближених алгоритмів є жадібний алгоритм. Оскільки евристики мають імовірнісний характер, їх складність неможливо оцінити апріорно. До них можна віднести методи лагранжевої релаксації, генетичні алгоритми, пошук із заборонами, алгоритми мурашиної колонії, нейронні мережі. Прикладом точних алгоритмів служить метод гілок і меж[52].

У 1979 році Вацлав Хватал вивчив зважену версію задачі про покриття множин і довів, що жадібний алгоритм забезпечує хороші наближення до оптимального рішення[56]. Жадібний алгоритм розв'язання задачі про зважене покриття множини будує покриття шляхом послідовного вибору множини S, що мінімізує відношення ваги c_j до кількості елементів у S, ще не покритих вибраними множинами. Алгоритм зупиняє роботу і повертає вибрані множини, як тільки вони утворюють покриття:

1) Ініціалізувати $S_j^{`} \leftarrow \emptyset$. Визначити $f(S_j^{`}) \doteq \left|U_{S_j \in S_j^{`}} S\right|$.
2) Повторювати, поки не буде досягнуто $f(S_j^{`}) = f(S_j)$:
3) Вибрати елемент $s \in S$, мінімізуючий вартість на елемент $c_j / [f(S_j^{`} \cup \{s\}) - f(S_j^{`})]$.
4) Поклавши $S_j^{`} \leftarrow S_j^{`} \cup \{s\}$.
5) Повернути $S_j^{`}$

На кожній ітерації вибираємо найефективнішу множину, видаляємо покриті елементи і продовжуємо до тих пір, поки не будуть покриті всі елементи.

Генетичний алгоритм є евристичним методом випадкового пошуку, заснованим на імітації еволюції біологічної популяції. Для проблеми покриття, при роботі багатьох варіантів генетичного алгоритму відбувається послідовна зміна популяцій, кожна з яких є сімейством покриттів, які називаються особинами популяції.

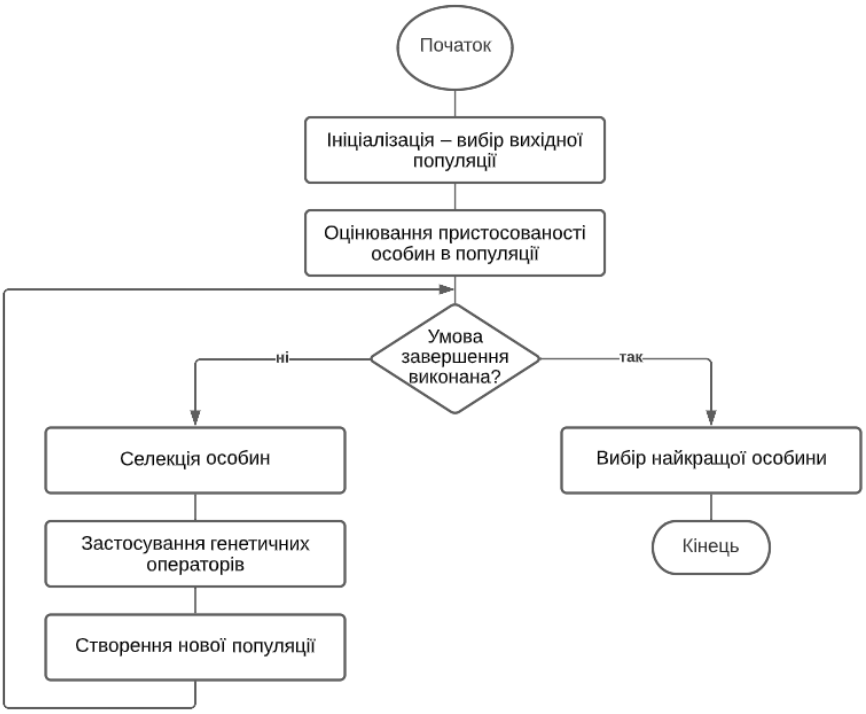

Рисунок 4.1 - Загальна схема роботи генетичного алгоритму

Алгоритм повного перебору. Повний перебір (brute force) – метод вирішення математичних задач. Відноситься до класу методів пошуку рішення вичерпуванням всіляких варіантів. Складність повного перебору залежить від кількості всіх

можливих рішень задачі. Будь-яке завдання з класу NP може бути вирішена повним перебором. При цьому, навіть якщо обчислення цільової функції від кожного конкретного можливого рішення задачі може бути здійснено за поліноміальний час, в залежності від кількості всіх можливих рішень повний перебір може вимагати експоненціального часу роботи. Суть алгоритму повного перебору для вирішення задачі покриття полягає в переборі всіх можливих поєднань різної довжини підмножин вихідного безлічі і, якщо чергове поєднання є покриттям і його вага мінімальна, необхідно зберегти його. З теорії множин відомо, що число всіх підмножин множини з n елементів дорівнює 2^n. Тобто:

$$\sum_{k=0}^{n} c_n^k = 2^n. \tag{4.10}$$

4.5 Задача класифікації вразливостей

Розглянемо оптимізаційний підхід подання задачі класифікації вразливостей. У загальному випадку задача класифікації полягає в розбитті деякого числа n об'єктів на ω класів так, щоб мінімізувати деякий критерій взаємної неузгодженості їх властивостей. Припустимо, що задані N об'єктів і для кожної пари об'єктів i і j відомо деяке число $\lambda_{i,j} \geq 0$, якщо ці об'єкти розглядаються як елементи евклідового простору або в загальному випадку індекс неузгодженості. Завдання полягає в розбитті множини N цих об'єктів на ω класів та у виборі в кожному класі спеціального опорного об'єкта, званого представником цього класу, таким чином, щоб сума відстаней від конкретних об'єктів до їх представників у класах була мінімальною. Позначимо через $M = (1,2, \dots, j, \dots, n)$ – множину вразливостей, а $S = (1,2 \dots, i, \dots, m)$ як множину класів. Також введемо змінну $x_{i,j} = \{0,1\}$, яка має наступну властивість:

$$\mathrm{x_{i,j}} = \begin{cases} 1, \text{якщо об}'\text{єкт j відноситься до класу i;} \\ 0, \text{в протилежному випадку.} \end{cases}$$

Представимо модель задачі класифікації в наступному вигляді:

$$\sum_{i \in I} \sum_{j \in J} \lambda_{i,j} \cdot x_{i,j} \to min, \tag{4.11}$$

$$x_{i,j} \le y_i \qquad \forall\, i \in I, \qquad \forall\, j \in J, \tag{4.12}$$

$$\sum_{i \in I} x_{i,j} = 1 \quad \forall\, j \in J, \tag{4.13}$$

$$\sum_{i \in I} y_i = \omega, \tag{4.14}$$

де $y_i = \{0; 1\}\ \forall\, i \in I$ та $y_j = \{0; 1\}\ \forall\, j \in J$.

Обмеження (4.11) виражає той факт, що об'єкт j може бути пов'язаний з представником i лише тоді, коли представник класу i обраний $(y_i = 1)$. Обмеження (4.11) у поєднанні з вимогою бінарності змінних $x_{i,j}$ відтворюють той факт, що кожен об'єкт (вразливість) повинен бути пов'язаний з одним і лише одним представником, тобто належати одному класу. Співвідношення (4.14) визначає число класів.

4.6 Метод класифікації рівня небезпеки вразливостей

Для оцінки вразливостей безпеки розподілених систем розглянемо метод на основі ранжування. Вразливості мають різний ступінь небезпеки, який кількісно можна оцінити на основі ранжування, тобто розділивши на групи, методом експертної оцінки. Ступінь вразливостей для кожної групи можна визначити як відношення добутку показників кожної вразливості до максимального значення. Усі вразливості мають різний ступінь небезпеки W_l, який можливо кількісно оцінити, провівши їх ранжування. Як критерії порівняння і відокремлення пропонуються наступні показники[57]:

- Фатальність вразливості W_{1l}. Фатальність визначає ступінь впливу вразливості та складність усування наслідків реалізації загрози.
- Доступність вразливості W_{2l}. Доступність визначає можливість використання вразливості джерелом загроз, наприклад: складність, вартість необхідних засобів, можливість використання неспеціалізованої апаратури.
- Кількість вразливості W_{3l}. Цей показник визначає кількість елементів об’єкта, для яких характерна та або інша вразливість.

Кожен показник оцінюється експертно-аналітичним методом за п’ятибальною системою. Оцінка 1 відповідає мінімальному ступеню впливу оцінюваного показника на небезпеку використання вразливості, а оцінка 5 - максимальному. W_l для окремої вразливості можна визначити як відношення добутку вищенаведених показників до максимального значення (125):

$$W_l = \frac{W_{1l} W_{2l} W_{3l}}{125} \tag{4.15}$$

Для підгрупи вразливостей W_l визначається як середнє арифметичне коефіцієнтів окремих вразливостей у підгрупі. Для зручності аналізу середній показник для групи W_l нормується щодо сукупності всіх коефіцієнтів підгруп у своїй групі, а середній показник для класу W_l визначається як сукупність коефіцієнтів груп класу.

Крім того, всі вразливості мають різний рівень небезпеки. Відповідно, за рівнем небезпеки доцільним поділити вразливості на[58]:

- Критичні. Критичними вразливостями об’єкта інформаційної безпеки є такі вразливості, наявність яких знижує здатність об’єкта до самозахисту до такого рівня, коли потенційна загроза при виникненні створює небезпеку настання негативних наслідків із відсутністю можливості їх запобігти або така можливість потребує значних затрат організаційних, технічних та людських ресурсів.
- Середній ступень небезпеки. Вразливостями середнього ступеня небезпеки можна вважати такі недоліки об’єкта інформаційної безпеки, наявність яких знижує здатність об’єкта до самозахисту до такого рівня, коли потенційна загроза при виникненні створює небезпеку настання негативних наслідків із ускладненням можливості їх запобігти.
- Низький ступень небезпеки. Вразливостями низького ступеня небезпеки можна вважати такі недоліки об’єкта інформаційної безпеки, наявність яких майже не зачіпає здатність об’єкта до самозахисту або знижує його здатність до самозахисту до такого рівня, коли потенційна

загроза при виникненні створює небезпеку настання негативних наслідків, але існує реальна можливість їх запобігання.

Якщо позначити множину всіх вразливих функцій як $F = \{f_1, f_2, \dots, f_n\}$, а всі вразливості, до яких може привести використання цих зазначених функцій як $V = \{v_1, v_2, \dots, v_m\}$, то визначив множину ймовірностей, з якими функція f_i може привезти до появи вразливості v_j як $P = \{p_j^i\}$ $(i = 1, \dots, n,\ j = 1, \dots, m)$, можливо визначити рівень небезпеки того чи іншого застосунка як

$$D = \sum_{i=1}^{n} \left(K_i \sum_{j=1}^{m} p_j^i r_j \right), \tag{4.16}$$

де K_i - число функцій і-го виду в застосунку, а r_j - небезпека j-ї вразливості в балах, які визначаються методом експертних оцінок.

ВИСНОВКИ

В результаті проведеного дослідження слід зазначити, що розподілені обчислення мають ряд наступних переваг, таких як: підвищена продуктивність, спільний доступ до ресурсів, підвищена розширюваність, підвищена надійність, доступність і відмовостійкість. Безпека розподілених систем забезпечує цілісне уявлення про поточні проблеми, процеси та рішення. Безпека визначає майбутні напрямки в контексті сучасних розподілених систем.

Проведений аналіз кібератак показав, що у сценарії атак задіяні ряд етапів, а саме: підробка, розвідка, підготовка, впровадження, експлуатація, встановлення, контроль та дії спрямовані на досягнення остаточної мети. Кожен з етапів націлений на відключення або отримання доступу до цільової системи. Найбільш поширені кібератаки нового покоління включають Andromeda, AdvisorsBot, Cerber, Cnrih, Cryptoloot, Fireball, Hidden Miner, Iotroop, Nivdort, NotPetya, RubyMiner, Trackbot, WannaCry, WannaMine, Ransomware, adultSwine. Об'єктами атак виступають: комп'ютери, сервери, мережеве обладнання, веб-ресурси, люди, мобільні пристрої. До найбільш поширених методів атак відносяться: використання шкідливого програмного забезпечення, методи соціальної інженерії, підбір облікових даних, хакінг, експлуатація веб-вразливостей, розподілені атаки типу «відмова в обслуговуванні». Також проведений аналіз відомих баз даних вразливостей, таких як: CVE, NVD, OSVDB та VND. Вказані бази даних реєструють велику кількість нових вразливостей випускаючи оперативні оновлення щодо виявлення нових недоліків.

За підсумками проведеного дослідження відзначимо, що забезпечення надійного рівня захищеності вузлів системи прямо пов'язане з використанням раціонального плану нейтралізації виявлених вразливостей. В умовах використання обмежених ресурсів, виділених для завдань пошуку і нейтралізації недоліків доцільним є визначення оптимального шляху мінімізації ризиків. В дослідженні приведена математична модель задачі оптимального плану усунення вразливостей. Розглянуто класичне формулювання задачі про покриття множини

та ряд алгоритмів вирішення зазначеної задачі, таких як: жадібний алгоритм, генетичний алгоритм, алгоритм повного перебору. В кваліфікаційній роботі наведена модель задачі покриття в інтерпретації інформаційної безпеки. Для практичного використання запропонованого оптимізаційного підходу слід коректно визначити вагу покриваючих елементів та визначити найменше покриття. Таким чином, зазначені показники визначають оптимальне рішення задач забезпечення безпеки інформаційної системи. У запропонованому методі процедуру обґрунтування плану нейтралізації виявлених вразливостей на основі застосування наявних механізмів захисту зведено до задачі про призначення. Запропонований метод дозволяє розробити план захисту, який позволяє нейтралізувати виявленні вразливості з найменшими витратами ресурсів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cisco Annual Internet Report (2018–2023) *White Paper*: веб-сайт. URL: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annualinternet-report/white-paper-c11-741490.html (дата звернення: 15.08.2022).
2. Andrew S. Tanenbaum, Maarten Van Steen. Distributed systems: Principles and Paradigms: 2nd edition. London: Pearson, 2007. 704 p.
3. Distributed systems - Concepts and design: 5th edition / George Coulouris and others. London: Addison-Wesley, 2011. 1080 p.
4. Mohamed Firdhous. Implementation of security in distributed systems - A comparative study. *International Journal of Computer Information Systems*. 2011. Vol. 2, №. 2. P. 1-6.
5. K.G. Srinivasa, Anil Kumar Muppalla. Guide to High Performance Distributed Computing: textbook. Berlin: Springer, 2015. 304 p.
6. Kai Hwang, Geoffrey C. Fox, Jack J. Dongarra. Distributed and Cloud Computing. From Parallel Processing to the Internet of Things: book. Burlington, USA: Morgan Kaufmann, 2011. 672 p.
7. Gregory Pfister. In Search of Clusters: 2nd edition. London: Pearson, 2001. 575 p.
8. Per-Olov Östberg. Virtual Infrastructures for Computational Science: Software and Architectures for Distributed Job and Resource Management. *Department of Computing Science:* Print & Media, Umea University, 2011. 74 p.
9. Ghada Farouk Elkabbany. Mohamed Rasslan. Chapter 9. Security Issues in Distributed Computing System Models. *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications (3 Volumes)* / IGI Global, 2018. P. 381-418.
10. Grid Computing: The European Data Grid Project / B. Segal and others. *In Nuclear Science Symposium Conference Record*, 2000 IEEE, 2000.
11. SETI@ Home / D. P. Anderson and others. An Experiment in Public-Resource Computing Communications of the ACM: 2002.

12. R. Williams. Grids and the Virtual Observatory. *Grid Computing: Making the Global Infrastructure a Reality*, 2003.
13. Peter Mell. Timothy Grance. The NIST Definition of Cloud Computing. *NIST Special Publication 800-145*. 2011. 7 p.
14. KVM: The Linux Virtual Machine Monitor / Ani Kivity and others, volume 1. 2007. P. 225-230.
15. Amazon Web Services. Amazon Elastic Compute Cloud: User Guide for Linux Instances: user guide. 2022. 2016 p. URL: https://docs.aws.amazon.com/pdfs/AWSEC2/latest/UserGuide/ec2-ug.pdf (дата звернення: 25.08.2022).
16. Amazon Web Services. Amazon Simple Storage Service: user guide. 2022. 1642 p. URL: https://docs.aws.amazon.com/pdfs/AmazonS3/latest/userguide/s3-userguide.pdf (дата звернення: 10.09.2022).
17. Mitch Tulloch. Introducing Windows Azure: book. Redmond, Washington: Microsoft Press, 2013. 142 p.
18. Nimbus is cloud computing for science. *Nimbus:* веб-сайт. URL: https://www.nimbusproject.org (дата звернення: 11.09.2022).
19. The Open Source Cloud & Edge Computing Platform. OpenNebula: веб-сайт. URL: https://opennebula.io (дата звернення: 22.10.2022).
20. Security Issues in Cloud Environments - A Survey: manuscript. / Diogo A. B. Fernandes and others. International Journal of Information Security, 2013. 62 p.
21. Cloud Deployment Models. *GeeksforGeeks*: веб-сайт. URL: https://www.geeksforgeeks.org/cloud-deployment-models/ (дата звернення: 15.09.2022).
22. Amazon Web Services. Amazon Virtual Private Cloud: user guide. 2022. 373 p. URL: https://docs.aws.amazon.com/pdfs/vpc/latest/userguide/vpc-ug.pdf (дата звернення: 15.09.2022).
23. Cloud Deployment Models: Advantages and Disadvantages. *SaM Solutions*: веб-сайт. URL: https://sam-solutions.us/advantages-and-disadvantages-of-cloud-deployment-models/ (дата звернення: 16.09.2022).

24. Multi-Cloud Advantages and Disadvantages. *Cloud Institute*: веб-сайт. URL: https://www.cloudinstitute.io/blog/multi-cloud-advantages-and-disadvantages/ (дата звернення: 18.09.2022).
25. ISO. ISO/IEC Directives; ISO/IEC: Washington, DC, USA, 2009.
26. Cyber security breaches survey 2017 / Dr Rebecca Klahr and others. UK, 2017. 67 p.
27. Cyber Security Breaches Survey 2019 / Department for Digital, Culture, Media and Sport. London, 2019. 66 p.
28. Framework. *Collins Dictionary Online*: веб-сайт. URL: https://www.collinsdictionary.com/dictionary/english/analytical-framework (дата звернення: 26.09.2022).
29. ISO31000, “ISO 31000:2018(en) Risk management — Guidelines”. ISO Online Browsing Platform (OBP), 2018.
30. Hamed Taherdoost. Understanding Cybersecurity Frameworks and Information Security Standards: review. Electronics, 2022. 21 p.
31. IAPP and OneTrust map ISO 27001 to the GDPR. *IAPP*: веб-сайт. URL: https://iapp.org/news/a/iapp-and-onetrust-map-iso-27001-to-the-gdpr/ (дата звернення: 29.09.2022).
32. Securing the Future of Payments: PCI SSC Publishes PCI Data Security Standard v4.0. *PCI Security Standards Council:* веб-сайт. URL: https://www.pcisecuritystandards.org/about_us/press_releases/securing-the-future-of-payments-pci-ssc-publishes-pci-data-security-standard-v4-0/ (дата звернення: 02.10.2022).
33. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology, 2018. 55 p. URL: https://doi.org/10.6028/NIST.CSWP.04162018 (дата звернення: 03.10.2022).
34. Eric Lachapelle, Mustafe Bislimi. ISO 27001 Information Technology - Security Techniques Information Security - Management Systems – Requirements: whitepaper. 2015. 17 p.

35. ISSA Journal. Evolution of the Cybersecurity Framework. July 2018. Volume 16, Issue 7.
36. Ciza Thomas, Paula Fraga-Lamas, Tiago M. Fernández-Caramés. Introductory Chapter. Computer Security Threats: London, 2020. P. 3-13.
37. Saket Acharya, Namita Tiwari. Survey of DDoS Attacks Based On TCP/IP Protocol Vulnerabilities: IOSR Journal of Computer Engineering, 2016. P. 68-76.
38. Hybrid Botnet Detection Based on Host and Network Analysis / Suzan Almutairi and others. Journal of Computer Networks and Communications: 2020, 16 p.
39. Saravani A., S. Sathya Bama S. A Review on Cyber Security and the Fifth Generation Cyberattacks. Oriental Journal of Computer Science and Technology: 2019, P. 50-56.
40. Top 15 Malicious Spyware Actions - 2018. *SANS Institute*: веб-сайт. URL: https://www.sans.org/emea/ (дата звернення: 12.10.2022).
41. An overview of security issues in cluster interconnects in Cluster Computing and the Grid / M. Lee and others. Sixth IEEE International Symposium: 2006. 9 p.
42. Clusters and security: distributed security for distributed systems in Cluster Computing and the Grid / Pourzandi M. and others. IEEE International Symposium: 2005. P. 96-104.
43. What is an HPC cluster. *Iowa State University:* веб-сайт. URL: https://www.hpc.iastate.edu/guides/introduction-to-hpc-clusters/what-is-an-hpc-cluster (дата звернення: 15.10.2022).
44. Wei Li, Rayford B. Vaughn. Cluster Security Research Involving the Modeling of Network Exploitations Using Exploitation Graphs. Sixth IEEE International Symposium: Singapore, 2006. P. 26-36.
45. Survivability Evaluation of Cluster-Based Wireless Sensor Network under DoS Attack / Chang C. and others. Communications in Computer and Information Science: Berlin, 2012. P. 126-132.
46. Thalod, S., Niwas R. Security model for computer network based on cluster computing. International Journal of Engineering and Computer Science: 2013. P. 1920-1927.

47. Grid computing security mechanisms: State-of-the-art / Mohammad Essaaidi and others. Information and Telecommunication Systems Laboratory Faculty of Sciences: Morocco, 2009. 20 p.
48. Eleni Koutrouli, Aphrodite Tsalgatidou. Taxonomy of attacks and defense mechanisms in P2P reputation systems - Lessons for reputation system designers. Computer Science: review, 2012. P. 47-70.
49. Top Threats to Cloud Computing. Cloud Security Alliance: report. 2022. 47 p.
50. Worst AWS Data Breaches of 2021. *Sonrai Security:* веб-сайт. URL: https://sonraisecurity.com/blog/worst-aws-data-breaches-of-2021/ (дата звернення: 21.10.2022).
51. CVE Program. *MITRE Corporation*: веб-сайт. URL: http://cve.mitre.org/ (дата звернення: 21.10.2022).
52. CVE List Home. *MITRE Corporation*: веб-сайт. URL: https://cve.mitre.org/cve/ (дата звернення: 30.10.2022).
53. Common Vulnerability Scoring System SIG. *First*: веб-сайт. URL: https://www.first.org/cvss/ (дата звернення: 22.10.2022).
54. Heartbleed уязвимость. *Habr*: веб-сайт. URL: https://habr.com/ru/company/eset/blog/218907/ (дата звернення: 22.10.2022).
55. Алгоритм глобального рівноважного пошуку розв'язання задачі про покриття / Рощин В. О. та ін. Наукові записки: 2014. С. 25-32.
56. Chvatal V. A greedy heuristic for the set-covering problem. Math. Oper. Res. 4(3). 1979. P. 233-235.
57. Городиський Р., Басараб О. Аналіз оцінки загроз вразливостей мобільних автоматизованих робочих місць. Технічні науки: 2020. С. 276-290.
58. Юдкова К. В. Рівень інформаційного імунітету як складова частина правової моделі інформаційної безпеки. Правова інформатика: 2014. С. 58-63.

ДОДАТОК А. КОПІЇ ПУБЛІКАЦІЙ

НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
ІМ. М.Є. ЖУКОВСЬКОГО
„ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ"
Кафедра комп'ютерних систем, мереж і кібербезпеки

СТУДЕНТСЬКА КОНФЕРЕНЦІЯ ІНФОРМАЦІЙНА, ФУНКЦІЙНА І КІБЕРБЕЗПЕКА

СКІФіК

Матеріали другої науково-технічної конференції

30 листопада, 1 грудня 2022 року

ХАРКІВ - 2022

Секція 2

РОЗРОБКА МЕТОДУ КЛАСИФІКАЦІЇ РІВНЯ НЕБЕЗПЕКИ ВРАЗЛИВОСТЕЙ СУЧАСНИХ РОЗПОДІЛЕНИХ СИСТЕМ

Пономаренко В. В.
Харківський національний університет імені В. Н. Каразіна
Науковий керівник Олійников Р. В.

Актуальність. Забезпечення належної безпеки інформаційних ресурсів є актуальним завданням у кіберпросторі. Згідно зі звітом Cisco Annual Internet Report (AIR), до 2023 року користувачами Інтернету стануть 66% населення Землі. До глобальної мережі будуть підключені більше 28 мільярдів пристроїв [1]. Зазначимо той факт, що на фоні росту кількості інтернет користувачів і підключених пристроїв буде спостерігатися зростання кібератак. Щодня інформаційні ресурси піддаються зазіханням сторонніми особами. Тому, критично важливим є ефективна протидія та мінімізація можливих збитків від потенційних загроз. Одним із способів протидії загрозам є своєчасне виявлення існуючих вразливостей системи. Виникає потреба в обґрунтованому наданні пріоритету виправлення знайденим недолікам, для того щоб першочергово усунути найбільш критичні вразливості. Отже актуальною є розробка методу класифікації рівня небезпеки вразливостей.

Метою досліджень є підвищення безпеки сучасних розподілених систем. Підвищення безпеки системи вимагає використання обґрунтованих засобів та методів пошуку недоліків. Від оперативної ідентифікації загроз суттєво залежить надійність системи.

Основні положення. В роботі запропоновано метод класифікації вразливостей в межах сучасних розподілених систем. Запропонована модель задачі класифікації рівня небезпеки вразливостей та спосіб її реалізації на основі вирішення задачі дискретної оптимізації. Модель задачі вибору оптимального плану усунення найкритичніших серед виявлених вразливостей, яка зведена до формулювання задачі про покриття множини. Задача про покриття множини широко відома в дискретній оптимізації і має численні додатки. Дана задача узагальнює NP-повну задачу про вершинне покриття і тому також є NP-складною. До задачі про покриття можна звести багато завдань дискретної оптимізації: стандартизації, упаковки і розбиття множини, побудови розкладів. Відома також і зворотна зводимість задачі до цих завдань. Постановка задачі полягає в наступному. Для скінченної множини $M = \{m_1, m_2, \dots, m_m\}$ і

деякого скінченного сімейства її підмножин S_j, $j = 1, 2, \dots, n$ потрібно знайти підсімейство $S_j^{`} \subseteq S_j$ з мінімальним набором підмножин $S_j$ таке, що кожен елемент вихідної множини M належить, принаймні, одній із цих підмножин. Знайдені підмножини $S_j^{`}$ зазвичай називають покривними, а сімейство $S_j^{`}$ – найменшим покриттям M. У тому випадку, коли покривним елементам приписана деяка вага, розглядають зважену задачу про покриття, яка передбачає пошук найменшого зваженого покриття M. Коли ж покривні підмножини попарно не перетинаються, задача про найменше покриття трактується як задача про розбиття множини M на найменшу кількість класів [2]. Таким чином, коректне визначення ваги покривних елементів і найменшого покриття визначає оптимальне вирішення завдання забезпечення безпеки інформаційної системи.

Висновки. Запропонований метод дозволяє визначити оптимальний шлях мінімізації ризиків і потенційних збитків за рахунок попередження найбільш критичних вразливостей при використанні обмежених ресурсів, що виділені для цих задач.

Список літератури

1. Cisco Annual Internet Report (2018–2023) White Paper: веб-сайт. URL: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html;

2. Рощин В. О., Боярчук Д. О., Ляшко В. І., Шило П. В. Алгоритм глобального рівноважного пошуку розв'язання задачі про покриття. Наукові записки. Том 163. Комп'ютерні науки. 2014.

Відомості про авторів

Пономаренко Віталій Віталійович, магістрант кафедри безпеки інформаційних систем і технологій, м.т. 095-559-14-04, vponomarenko1712@gmail.com

Олійников Роман Васильович, професор кафедри безпеки інформаційних систем і технологій, д.т.н., доцент, roliynykov@gmail.com

СЕРТИФІКАТ

ЗА КРАЩУ ДОПОВІДЬ

видано

Пономаренку В. В.

за доповідь "Розробка методу класифікації рівня небезпеки вразливостей сучасних розподілених систем", у студентській конференції "Інформаційна, Функційна і Кібербезпека", СКІФіК, Харків, 30 листопада 2022 року.

Співголова організаційного комітету конференції
Лауреат Державної премії України в галузі науки і техніки,
заслужений винахідник, професор, д.т.н., завідувач кафедри
комп'ютерних систем, мереж і кібербезпеки.

ХАРЧЕНКО В.С.

УДК 004.056.57

МЕТОДИКА ПОШУКУ ВРАЗЛИВОСТЕЙ НА БАЗІ СКАНЕРА NESSUS

Пономаренко В.В., магістрант гр. КБ-51
Науковий керівник: професор Олійников Р.В.
Харківський національний університет ім. В.Н. Каразіна

Забезпечення належної безпеки інформаційних ресурсів є актуальним завданням у кіберпросторі. Пропонується один із способів пошуку загроз в системі безпеки, а саме застосування сканерів вразливостей.

Мета роботи полягає в розгляді засобів автоматизації пошуку вразливостей. Для досягнення поставленої мети необхідно розглянути сучасні програмні рішення виявлення вразливостей. Також вирішити задачу своєчасного виявлення потенційних загроз для мінімізації можливих збитків.

На світовому ринку сканерів вразливостей виділяються декілька програмних продуктів, таких як: сканер Nessus компанії Tenable, OpenVAS від Greenbone Networks, Flan Scan американської компанії CloudFlare. Зазначені продукти відповідають різним наборам критеріїв аналізу захищеності, але при цьому всі вони спрямовані на запобігання компрометації даних і систем.

Для підвищення ефективності протидії потенційним загрозам в ході роботи було детально розглянуто модель загроз інформаційної безпеки, а також модель порушника. Проведений аналіз показує, що використання сканерів вразливостей дозволяє отримати передове комерційне рішення щодо забезпечення інформаційної безпеки. Відмінною рисою таких рішень є всеосяжний звіт про результати сканування.

Таким чином, використання сканера вразливостей дозволяє якісно і швидко здійснити діагностику та моніторинг мережі. Слід додати, що своєчасне виявлення вразливостей прямо впливає на кількість інцидентів безпеки.

СЕРТИФІКАТ УЧАСНИКА

засвідчує, що

Пономаренко Віталій Віталійович

KHARKIV IT CLUSTER

є доповідачем 13-ї міжнародної студентської науково-технічної конференції

“Перспективні мережні та комп'ютерні технології”

ПерСиК 2022,

яка проводилася

кафедрою комп'ютерних систем, мереж і кібербезпеки

Національного аерокосмічного університету ім. М.Є. Жуковського “ХАІ”

Україна, Харків, ХАІ, 28 квітня 2022 р.

Лауреат Державної премії України у галузі науки і техніки,
Заслужений винахідник України
доктор технічних наук, професор В.С. Харченко,
завідувач кафедри комп'ютерних систем, мереж і кібербезпеки ХАІ