МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

КОВАЛЬЧУК АНАСТАСІЯ ОЛЕГІВНА

Допускається до захисту:
Завідувач кафедри
інформаційних технологій,
к.т.н., доцент,
_____Нескородєва Т. В.
«__»_____20__р.

АНАЛІЗ МЕТОДІВ ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ У ВІРТУАЛЬНИХ СЕРЕДОВИЩАХ ТА ХМАРНИХ ПЛАТФОРМАХ

Спеціальність 125 Кібербезпека

Кваліфікаційна (бакалаврська) робота

Керівник:
Загоруйко Л. В.,
доцент кафедри інформаційних
технологій, к.т.н.
_____
(підпис)

Оцінка : _____ / _____ / _____
(бали/за шкалою ЄКТС/за національною шкалою)

Голова ЕК: _____
(підпис)

Вінниця - 2021

АНОТАЦІЯ

Ковальчук А. О. Аналіз методів проектування систем захисту інформації у віртуальних середовищах і хмарних платформах. Спеціальність 125 «Кібербезпека», Донецький національний університет імені Василя Стуса, Вінниця, 2021.

У кваліфікаційній (бакалаврській) роботі досліджено методи проектування систем захисту інформації та формальне представлення семантики інформаційних описів механізмів захисту та загроз безпеки інформації.

Ключові слова: система захисту інформації, методи проектування систем, віртуальні середовища, хмарні платформи.

Табл. 3. Рис. 3. Бібліограф.: 26 найм.

ABSTRACT

Kovalchuk A. Analysis of methods for designing information security systems in virtual environments and cloud platforms. Specialty 125 “Cybersecurity”. Vasyl` Stus Donetsk National University, Vinnytsia, 2021.

In the qualification (bachelor's) work the methods of designing information protection systems and formal representation of semantics of information descriptions of protection mechanisms and information security threats are investigated.

Keywords: information security system, system design methods, virtual environments, cloud platforms.

Tab. 3. Fig. 3. Bibliography: 26 items.

ЗМІСТ

ВСТУП

Інформаційна безпека відноситься до політик, процедур та технічних заходів, що використовуються для запобігання несанкціонованому доступу, зміні, крадіжці чи фізичному пошкодженню інформаційних систем. Найбільші загрози для організацій від інсайдерів, в результаті крадіжок чи зломів або ж від недостатності знань. Іноді зловмисники можуть обманом змусити співробітників розкрити паролі та дані доступу за допомогою соціальної інженерії. Співробітники також можуть вводити неправильні дані чи неправильно обробляти дані. Щоб виявити терміновість та пріоритет реагування на вразливості, організаціям потрібні моделі, які б відображали серйозність вразливостей.

Безпека інформаційних систем – серйозна проблема, оскільки зловживання комп'ютерами поширюється. Тому важливо, щоб системні аналітики та проектувальники мали досвід в методах проектування систем захисту інформації. Характеристики трьох поколінь загальних методів проектування інформаційних систем забезпечують основу для порівняння та розуміння сучасних методів проектування безпеки. Ці методи включають підходи, які використовують контрольні списки елементів управління, розділяють функціональні вимоги на інженерні розділи та створюють абстрактні моделі рішень.

Для підвищення ефективності систем захисту інформації необхідно забезпечити адекватність застосовуваних моделей та методів шляхом переходу від статистичної (ймовірнісної) концепції до концепції створення методичного базису на основі методів теорії нечітких множин, теорії можливостей та математичної інформатики, які краще підходять для опису та рішення задач з високим степенем невизначеності.

Метою бакалаврської роботи є аналіз існуючих методів проектування систем захисту інформації, що розміщені у віртуальних середовищах або хмарних платформах.

Завдання бакалаврської роботи: узагальнити, що таке система захисту, віртуальне середовище та хмарна платформа; проаналізувати методи проектування систем захисту та дослідити методи їх побудови.

Об’єктом дослідження є система захисту інформації у віртуальному середовищі та хмарній платформі.

РОЗДІЛ 1. СИСТЕМИ ЗАХИСТУ У ВІРТУАЛЬНИХ СЕРЕДОВИЩАХ ТА МЕТОДИ ЇХ ПРОЕКТУВАННЯ

1.1. Що таке система захисту

Комітет по системам національної безпеки (*Committee on National Security Systems*) визначає інформаційну безпеку як захист інформації та її найважливіших елементів, виключаючи системи та обладнання, які використовують, зберігають та передають цю інформацію. На рис 1.1. зображено, що інформаційна безпека включає в себе 3 основні області, які є досить широкими, це управління інформаційною безпекою, комп'ютерна безпека та безпека даних, а також мережева безпека[1].

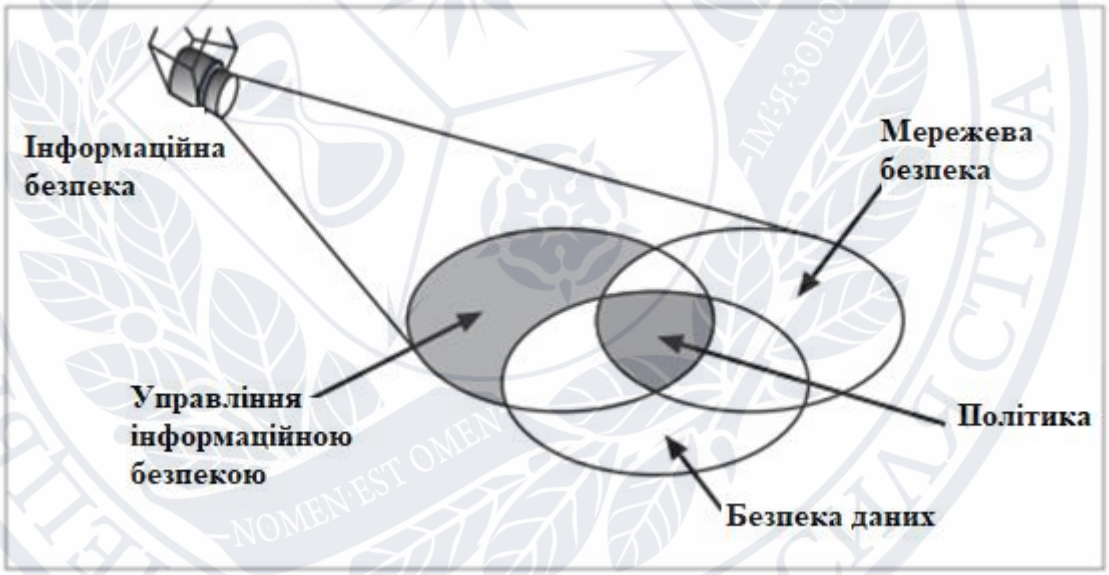

Рисунок 1.1. Інформаційна безпека

Першочергово така концепція була розроблена індустрією комп'ютерної безпеки та була названа трикутником *CIA*. Основа трикутнику - три характеристики інформації, які і роблять її цінною для будь-якої організації: цілісність, доступність та конфіденційність.

Для того, щоб дати визначення системі захисту, потрібно знати що таке система в цілому. В різних джерелах можна знайти різні визначення, узагальнивши які, можна сказати, що система – це набір взаємопов'язаних компонентів, які разом володіють такими властивостями, які не притаманні їм окремо. В цьому аспекті систему безпеки можна визначити як набір взаємопов'язаних компонентів, які створюють та підтримують безпеку, яка не може бути згенерована та підтримана компонентами, які розглядаються окремо.

Тип компонентів системи захисту залежить від рівня та характеру безпеки системи. В системі має гарантуватися гармонійне та послідовне з'єднання компонентів в цілях досягнення максимального рівня безпеки та створення умов для швидкого реагування на загрози. Надзвичайно важливим є розуміння того, що як і в будь-якій системі, в систему захисту не можна додавати чи видаляти з неї компоненти, не впливаючи негативно на її роботу.

1.1.1. Принципи системи захисту. Баланс інформаційної безпеки та доступу до системи

Принципи побудови та роботи системи захисту є фундаментальними питаннями, їх можна поділити та загальні та специфічні. До загальних відносяться:

- Принцип «функціональної лінії», який вимагає, щоб система безпеки була спроектована, структурована та використана відповідно конкретним очікуванням.
- Принцип «структурної збалансованості», який підтверджується вимогою включати в систему захисту лише необхідні компоненти, які будуть взаємопов'язаними.

Специфічні принципи системи відображають особливість продукту системи. До таких відносяться:

- Централізація, яка означає, що система захисту підпорядковується тому, чиїм інструментом вона є.
- Контроль системи, який виражається в обмежені автономії системи захисту тим, хто її створив та хто нею користується.
- Система захисту залежить від цінностей, тобто, змінна цінностей призводить до перегляду системи захисту та можливої її модифікації.

Досягти ідеального захисту інформації неможливо, навіть при найкращому плануванні та реалізації, оскільки інформаційна безпека це процес, а не ціль[2]. Баланс безпеки та доступу є необхідною складовою ефективного захисту, оскільки необмежений доступ для всіх це одна з найбільших загроз, а з іншого боку, повністю безпечна система не дозволить нікому отримати доступ.

Для того, щоб система задовільнила свого користувача та спеціаліста з безпеки, тобто досягла балансу, рівень безпеки повинен захищати від загроз і при цьому забезпечувати розумний доступ .

Якщо потребам кінцевого користувача перешкоджає надмірна увага до захисту інформаційних систем, то може виникнути дисбаланс. І спеціалісти з інформаційної безпеки і користувачі повинні пам’ятати, що вони хочуть досягти спільних цілей організації, тобто забезпечити доступність саме тих даних, які потрібні в цей момент, з мінімальними затримками та перешкодами. В ідеальному варіанті цей рівень доступності може бути досягнутий навіть після того, коли будуть усунені побоювання щодо втрати, пошкодження чи захоплення інформації.

1.1.2. Життєвий цикл розробки системи захисту

Перший етап – дослідження. Ця фаза розпочинається з директиви вищого керівництва, що визначає процес, результати та цілі проекту та інші обмеження[3]. Організовуються команди з співробітників, підрядників та

менеджерів, які аналізують об’єм проекту, його проблеми, а також конкретні цілі та задачі. В кінці виконується організаційний аналіз здійсненності, щоб визначити, чи є у організації ресурси та обов’язки, необхідні для проведення успішного аналізу та проектування безпеки.

Другий етап – аналіз. На цьому етапі вивчаються документи етапу дослідження. Команда розробників проводить попередній аналіз існуючих політик чи програм безпеки, а також аналіз задокументованих поточних загроз та пов’язаних з ними засобів захисту. Цей етап також включає аналіз відповідних юридичних питань, які можуть вплинути на розробку рішення безпеки. Все частіше закони про конфіденційність стають важливим фактором при прийнятті рішень щодо інформаційних систем, які управляють особистою інформацією. На даному етапі починається управління ризиками - процес виявлення, оцінки та оцінювання рівнів ризику, з якими зіштовхується організація, особливо загроз безпеки інформації, що зберігається та обробляється в організації.

Третій етап – логічний дизайн. На етапі логічного проектування створюються та розробляються схеми інформаційної безпеки, а також вивчаються та реалізуються ключові політики, які впливають на наступні рішення. Також на даному етапі команда планує дії по реагуванню на інциденти, які будуть прийняті у випадку часткової або катастрофічної втрати. Планування відповідає на наступні питання:

- Планування неперервності: як буде продовжуватися бізнес у випадку збитку?
- Реагування на інцидент: які кроки застосовуються при атаці?
- Аварійне відновлення: що потрібно зробити, щоб відновити інформацію та життєво важливі системи відразу після катастрофічного збою?

Потім аналіз здійсненності визначає, потрібно продовжувати проект чи передати його на аутсорсинг.

Четвертий етап – фізичний дизайн. На етапі фізичного проектування оцінюється технологія інформаційної безпеки, генеруються альтернативні рішення та визначається кінцевий проект. План інформаційної безпеки може бути переглянутий, щоб привести його у відповідність з змінами, які потрібні будуть після закінчення фізичного проектування. На цьому етапі також підготовлюються критерії для визначення успішних рішень.

П'ятий етап – виконання. На етапі реалізації виготовляються або купуються рішення безпеки, потім тестуються, впроваджуються та знову тестуються. Оцінюються кадрові питання, проводяться спеціальні програми навчання. Як результат, весь протестований пакет представляється вищому керівництву для кінцевого утвердження.

Шостий етап – обслуговування та зміни. Цей останній етап, можливо, є найважливішим, враховуючи постійно змінне середовище загроз. Сучасні системи інформаційної безпеки потребують постійного моніторингу, тестування, модифікації, оновлення та ремонту. Часто усунення пошкоджень та відновлення інформації – це постійні зусилля проти невидимого противника. По мірі виникнення нових та розвитку старих загроз профіль інформаційної безпеки організації повинен постійно адаптуватися, щоб протидіяти успішному проникненню загроз в конфіденційні дані. Цю постійну увагу та безпеку можна порівняти з фортецею, де загрози зовні та зсередини повинні постійно відслідковуватись та контролюватись за допомогою постійно нових та більш інноваційних технологій.

1.2. Методи проектування систем захисту інформації

1.2.1. Підхід Фішера

Безпека інформаційних систем Фішера – один з перших всеосяжних методів, що орієнтується на вимоги для розробки захисту даних. Він в значній

мірі опирається на досвід *IBM*, розширюючи аналіз ризиків Кортні до повного механічного інженерного підходу до інформаційної безпеки.

Фішер визначає п’яти етапний метод проектування в стилі водоспаду, який слідує за створенням організаційної політики безпеки/захисту активів. Адміністратор безпеки реалізує план, який включає в себе план реєстрації даних, план управління доступом, план реагування на надзвичайні ситуації, проміжний план обробки, план зберігання та програму класифікації безпеки даних.

Робота Фішера втілює концептуальний прогрес у використані сітки контрольних точок експозиції в якості засобу початкового аналізу. Деталі реалізації існуючої системи, а не контрольний список засобів контролю, тепер є основним засобом аналізу безпеки[4]. Між іншим, Фішер використовує більш повний цикл безпеки, який називається *Span*, в додатку, який присвячений методам планування безпеки. Цей процес планування включає в себе всі фази життєвого циклу атипової системи: визначення заходів безпеки (аналіз та проектування), реалізація заходів безпеки (реалізація) та моніторинг засобів управління і операцій (операції та технічне обслуговування)[5].

1.2.2. Програма комп’ютерної безпеки Паркера

Паркер розробив цей метод для Інституту комп’ютерної безпеки та протестував його в *SRI International*. Як і Фішер, Паркер підкреслює необхідність створення середовища управління для забезпечення безпеки інформаційних систем. Проте, Паркер розглядає, що певна оперативна група може приймати рішення про масштаби та проведення перевірки безпеки. Його метод складається з п’яти етапів: ідентифікація та оцінка активів, ідентифікація загроз, оцінка ризиків, виявлення, вибір та реалізація захисних заходів, впровадження.

Паркер визначає важливість соціальних аспектів безпеки та урівноважує ці аспекти з технічними проблемами. На основі свого більш раннього досліду комп'ютерних злочинів, Паркер концентрується на «мотивах», «діях» та людях як «джерелах» для виявлення загроз. Нарешті, програма Паркер – одна з перших, яка включає якісний альтернативний аналіз ризиків. Проте, зазначається, що в рамках цього методу може бути використаний і традиційний аналіз ризику.

1.2.3. CRAMM метод

«*CCCTA`s Risk Analysis and Management Methodology*» важливий тому що Центральне обчислювальне та телекомунікаційне агентство Великобританії (CCTA) застосовує цей метод в якості загальнодержавного стандартного підходу до аналізу ризиків та управління безпекою. Метод складається з трьох етапів.

Етап 1. На цьому етапі аналітики встановлюють об'єм та межі дослідження. Точний набір фізичних активів (та пов'язаних даних чи програмних активів) не вказується. Потім аналітики проводять структуровані інтерв'ю з кожним власником даних. Коли власники визначені, вони приступають до якісної оцінки кожного з активів. Оцінюються не тільки вартість активів, але і вплив проблем по 10-бальній шкалі.

Етап 2. Він розпочинається з групування активів. Групи активів стають основою для подальшого аналізу. Використовуючи базу із загальних загроз, програмне забезпечення вибірково генерує до 32 анкет про загрози та вразливості для кожної групи активів. Потім власники оцінюють вразливість кожного активу по відношенню до конкретної загрози. Програмне забезпечення *CRAMM* використовує ці дані для розрахунку рівня ризику кожної групи активів за 5-бальною шкалою. До того, як перейти до третього

етапу, команда виконує етап раціоналізації, на якому якісно переглядаються рівні ризику.

Етап 3. На третьому етапі існуючі системні контрзаходи (засоби контролю) вводяться в програмне забезпечення *CRAMM*. Потім, на основі груп активів, рівнів ризику, існуючих засобів контролю та внутрішньої бази даних складається список рекомендованих додаткових контрзаходів.

Після завершення процесу *CRAMM* та реалізації контрзаходів організація переходить в цикл обслуговування бази даних. Цей цикл включає різні перевірки, кожна з яких являє собою меншу ітерацію всього процесу *CRAMM*. Відгуки використовуються для оновлення бази даних. Після оновлень аналітики повинні перекомпілювати рекомендації по контрзаходам. Потім вносяться зміни в рекомендовані контрзаходи.

1.2.4. RISKPAC метод

Дві основні цілі RISKPAC – це простота використання та легкість інтерпретації результатів. Таким чином, цей метод може використовуватись аналітиками системної безпеки тільки з середнім рівнем підготовки та досвіду. Цей «аналізатор профілю ризику» забезпечує різні інтерактивні сеанси питань. Розробники систем безпеки, системні спеціалісти та користувачі інформаційних систем можуть напряму взаємодіяти з програмою. Схема анкети орієнтована на якісні оцінки користувачів з використанням лінгвістичних змінних.

1.2.5. BDSS метод

Байсівська система підтримки прийняття рішень (*The Bayesian Decision Support System*) – це повний комп’ютерний метод проектування інформаційної безпеки[6], який виник безпосередньо з методів кількісного аналізу ризиків

(*Ozier* 1989). В той час, як інші методи зменшили аналіз ризиків за допомогою більш м'яких якісних оцінок, *BDSS* примітний тим, що його розробники поступово підвищували формальну та статистичну строгість свого методу. Процес проектування безпеки *BDSS* складається з дев'яти дій, які підтримуються програмним забезпеченням. Ці дії згруповані в 4 етапи чи фази, які повторюються.

Збір даних. Цей етап складається з трьох дій. Перша, модуль визначення розміру проекту. Друга, модуль оцінки активів, матеріальних цінностей, збитків, використовує екрани вводу для інвентаризації та оцінки елементів інформаційної системи. Третя, модуль картографії загроз та вразливостей, використовує серію інтерактивних анкет для збору якісних та кількісних даних про кожну вразливість.

Машинний аналіз ризику. Цей етап складається з двох дій обчислювальної машини, які можуть ітеративно запускатися як фоновий процес. Аналізатор складає кількісну модель ризику, а потім застосовує визначений набір статистичних алгоритмів до цієї моделі та будує ризики для кожної загрози.

Інтерактивний аналіз гарантій. Цей процес включає три ітеративні комп'ютерні дії. Перша, аналізатор відображає загрози, виявлені на попередніх етапах. Друга, модуль затрат збирає інформацію про вартість захисних мір для подальшого використання при визначені найбільш економічно привабливого набору засобів контролю для реалізації. Остання, модуль оцінки та повторного аналізу збирає частотні розподіли, дані про взаємодії та ефект від обраних заходів. Ця оцінка дозволяє проаналізувати загальний профіль загроз організації, а також окремі загрози та міри захисту.

Звітність. BDSS представляє генератор звітів, який створює три основні типи документації, кожен з яких включає відповідні графіки. Короткий зміст являє собою високорівневий звіт про процес проектування з акцентом на

існуючі вразливості. Технічний аналіз включає повний комплект детальної документації, розробленої для аналізу безпеки та дизайн-проекту.

1.3. Забезпечення безпеки у віртуальних середовищах

Віртуалізація за дуже короткий термін досить суттєво вплинула на IT та мережі і вже призвела до великої економії коштів та окупності інвестицій корпоративним центрам обробки даних та постачальникам хмарних послуг[7]. Як правило, драйверами віртуалізації машин є більш ефективне використання серверів, консолідація центрів обробки даних, а також відносна простота та швидкість виділення ресурсів. Організації можуть використовувати віртуалізацію для скорочення капітальних затрат на серверне обладнання, а також для підвищення операційної ефективності.

Віртуалізовані середовища, в деякій мірі, є більш безпечними ніж традиційні, за наступними причинами:

- Ізоляція між віртуальними машинами, яку забезпечує гіпервізор;
- Немає відомих успішних атак на гіпервізори, за виключенням теоретичних, які потребують доступу до вихідного коду гіпервізору та можливості його реалізації;
- Можливість представлення базової інфраструктури та технологій безпеки у вигляді віртуальних приладів, такі як мережеві комутатори та брандмауери;
- Можливість ізоляції та швидкого відновлення після інцидентів.

По мірі того, як організації починають свій шлях віртуалізації, критично важливо аналізувати існуючі процеси та розробляти стратегії для усунення ризиків безпеки в фізичних та віртуальних середовищах, щоб забезпечити відповідність та прозорість безпеки в центрі обробки даних.

У звіті *CSA* «Основні загрози хмарних обчислень»[8] за 2013 рік експерти визначили наступні 9 критичних загроз хмарної безпеки (розташовані в порядку їх серйозності):

1. Витік даних
2. Втрата даних
3. Злом акаунту чи службового трафіку
4. Небезпечні інтерфейси та *API*
5. Відмова в обслуговувані
6. Шкідливі інсайдери
7. Зловживання хмарними послугами
8. Недостатня обачність
9. Вразливості загальних технологій

Коли організація приступає до реалізації ініціативи по віртуалізації серверів, вона повинна переконатись, що її структура управління інформаційною безпекою також придатна до її віртуалізованих IT-систем та послуг. Всі дії по управлінню інформаційною безпекою повинні підвищувати цінність бізнесу.

Ризики та проблеми безпеки, пов’язані з віртуальними IT-системами, можна умовно поділити на типи:

1. Архітектура. Рівень абстракції між фізичним обладнанням та віртуалізованими системами, на яких працюють IT-сервіси, є потенційною ціллю для атаки. Віртуальна машина або група віртуальних машин, які підключені до однієї мережі, можуть бути ціллю атаки з боку інших віртуальних машин.
2. Програмне забезпечення гіпервізору. Гіпервізор – це найважливіше програмне забезпечення у віртуальній IT-системі. Піддати ризику віртуальну машину може будь-яка вразливість системи безпеки в гіпервізорі та пов’язаної з ним інфраструктури.

3. Конфігурація. Нову інфраструктуру можна дуже легко розгорнути, завдяки простоті клонування та копіювання образів у віртуальному середовищі. В результаті, контроль та звіт стають критично важливими задачами для середовищ, що швидко розгортаються.

Організації, які обирають віртуалізацію, повинні виявити та оцінити ці ризики та проблеми безпеки та встановити відповідні засоби контролю для їх усунення до впровадження. *ISO/IEC* 27001:2013 та *ISO/IEC* 27005:2011 надають більш детальну інформацію про процес, який може бути використаний чи адаптований організаціями різного масштабу та складності

Забезпечення цінності для зацікавлених сторін підприємства за допомогою ініціатив віртуалізації потребують хорошого управління інформаційними та технологічними активами. Для віртуалізації потрібно також обрати комплексну структуру, яка дозволить їм досягати своїх технологічних цілей та приносити користь. Організації слід встановити політики та процедури, які включають програму аудиту, орієнтовану на віртуальні ІТ-системи. Повинні бути чітко визначені та задокументовані ролі і обов'язки системних адміністраторів та користувачів. ІТ-менеджери повинні гарантувати, що їх команди дотримуються політик та процедур віртуалізації, а організація повинна оцінювати, направляти та відслідковувати кожен етап процесу.

Організація, надавши загальне бачення того, як рішення віртуалізації будуть підтримувати її місію, повинна визначати потреби в самій віртуалізації.

На етапі планування та проектування організація повинна надати необхідну інструкцію для визначення та оцінки технічних характеристик рішення віртуалізації та пов'язаних компонентів, включаючи методи аутентифікації та криптографічні механізми для захисту зв'язку. Основні міркування включають вибір програмного забезпечення для віртуалізації, системи зберігання, топології мережі, доступності смуги пропускання та неперервності бізнесу. При проектуванні слід також враховувати логічний

розподіл екземплярів, що містять конфіденційні дані. Для забезпечення різних рівнів безпеки та захисту слід встановити окремо аутентифікацію для додатків і серверу, гостьової операційної системи, гіпервізору та хостової операційної системи. Організація також повинна визначати та документувати процеси обробки інцидентів, пов’язаних з рішенням віртуалізації.

Під час впровадження організація повинна забезпечити надійні методи безпеки шляхом оцінки вразливостей компонентів віртуалізації. Базова платформа віртуалізації повинна бути підсилена за допомогою рекомендацій постачальника або сторонніх інструментів. У віртуалізованому середовищі надійне управління ключами необхідне для контролю доступу та підтвердження прав власності як на дані, так і на ключі. Слід забезпечити дотримання політик доступу на основі ролей, щоб забезпечити розподіл обов’язків. Такі заходи управління даними необхідні для виявлення, відслідковування та контролю місцезнаходження екземплярів даних, що містять конфіденційні активи, в будь-який момент часу. Правильне шифрування віртуальної машини необхідне для значного зниження ризику, пов’язаного з доступом користувачів до фізичних серверів та сховищ, що містять конфіденційні дані.

Процес виведення віртуальних машин з експлуатації повинен відповідати законодавчим та нормативним вимогам, щоб запобігти витоку даних та порушень, включаючи знищення ключів, пов’язаних з зашифрованими віртуальними машинами.

Періодичні внутрішні та зовнішні аудити віртуалізованого середовища дозволять виявити та пом’якшити слабкі місця та вразливості, а також зроблять можливим дотримання юридичних та нормативних вимог.

1.4. Що таке хмарні платформи. Архітектура хмарних платформ

Хмарна платформа відноситься до операційної системи та обладнання серверу в інтернет-центрі обробки даних. Це дозволяє програмним та апаратним продуктам існувати віддалено та в більшому масштабі.

Хмарні платформи працюють наступним чином – організації орендують доступ до обчислювальних сервісів, таких як бази даних, сховища, аналітика, мережі, програмне забезпечення. Таким чином, підприємствам не потрібно створювати центри обробки даних чи обчислювальну інфраструктуру та володіти ними. Вони просто платять кошти за те, що використовують.

Хмарні платформи мають 5 ключових атрибутів, які дають їм переваги, порівняно з аналогічними технологіями, вони включають:

- Багатокористувацький режим;
- Велика масштабованість;
- Еластичність: користувачі можуть швидко збільшувати та зменшувати свої обчислювальні ресурси по мірі необхідності;
- Плати тільки коли користуєшся;
- Самозабезпечення ресурсів.

Архітектура хмарних платформ складається з трьох сервісів, відомі як програмне забезпечення як послуга (*SaaS*), платформа як послуга (*PaaS*) та інфраструктура як послуга (*IaaS*). Програмне забезпечення як послуга дозволяє користувачам використовувати різні додатки з хмари замість того, щоб використовувати додатки на своєму власному комп’ютері. Постачальник хмарних послуг зазвичай надає свого роду середовище розробки програмного забезпечення, що дозволяє розробляти додатки для використання в хмарі[9]. Інтерфейс прикладного програмування (*API*), який користувачі використовують для доступу до програмного забезпечення та взаємодії з ним, дозволяє користувачу використовувати це програмне забезпечення, не

турбуючись про те, як і де зберігаються дані чи скільки дискового простору доступно.

Платформа як послуга працює на більш низькому рівні ніж *SaaS*. Вона відповідає за управління простором збереження, виділення смуги пропускання та обчислювальні ресурси, доступні для додатку. Вона бере ресурси, необхідні для запуску програмного забезпечення та динамічно масштабує ці ресурси, коли потрібно. Також вона може масштабувати виділення смуги пропускання та серверних ресурсів, що дозволяє хмарі працювати в ситуаціях з високим трафіком чи вимогами, оскільки ресурси динамічно збільшуються по мірі необхідності.

Існує три основні типи моделей розгортання хмари – публічні, приватні та гібридні хмари.

Публічні хмари – найбільш розповсюджений тип. Тут декілька клієнтів можуть отримати доступ до веб-додатків та служб через Інтернет. У кожного окремого клієнта є свої власні ресурси, які динамічно надаються стороннім постачальником. Цей сторонній постачальник розміщує хмару для декількох клієнтів з декількох центрів обробки даних, управляє своєю безпекою та надає обладнання та інфраструктуру для роботи хмари. Замовник не може контролювати чи розуміти, як управляється хмара чи яка інфраструктура доступна.

Приватні хмари імітують концепцію хмарних обчислень в приватній мережі. Вони дозволяють користуватися перевагами хмарних обчислень без деяких підводних каменів. Приватні хмари надають повний контроль над управлінням даними та прийняттям заходів безпеки. Основна проблема з цією моделлю розгортання полягає в тому, що користувачі несуть великі витрати, оскільки вони повинні купувати інфраструктуру для запуску хмари, а також повинні самі управляти хмарою.

Гібридні хмари об’єднують публічні та приватні хмари в одній мережі. Це дозволяє організаціям використовувати обидві моделі розгортання.

Наприклад, організація може зберігати конфіденціальну інформацію в своїй приватній хмарі та використовувати публічну хмару для обробки великого трафіку та різних складних ситуацій.

1.4.1. Безпека хмарних платформ

Можна вважати, що хмарні платформи все ще знаходяться в зародковому стані, але існує ряд організацій та стандартних органів, що розробляють хмарні стандарти та *API*. В суспільстві є занепокоєння на рахунок безпеки обчислювальних даних. Один з ризиків, який бачать люди, полягає в тому, що провайдерам доводиться управляти мільйонами користувачів, і це являє собою проблему[10]. Це свідчить про те, що багато людей занепокоєні тим, що постачальники хмарних послуг не зможуть справитись з великими масштабами чи що інфраструктура не зможе правильно масштабуватися при великих об’ємах використання. Конфіденційність важлива для організації, особливо коли зберігається особиста чи конфіденційна інформація, але ще до кінця не зрозуміло, чи зможе інфраструктура хмарних платформ підтримувати зберігання конфіденційної інформації, не створюючи для організації відповідальності за порушення правил конфіденційності. Оскільки в багатьох приватних хмарах імена користувачів можуть бути дуже схожими, це ще більше погіршує заходи авторизації. Клієнту рекомендується надавати свої особисті дані чи використовувати систему хмарних провайдерів лише в тому випадку, коли він їм довіряє.

Постачальники хмарних послуг вважають, що шифрування є ключем безпеки та може допомогти з багатьма її проблемами[11]. Проте, все, що пов’язано з шифруванням – це «підводні камені», оскільки шифрування може вимагати багато ресурсів процесору. Шифрування не завжди є повним доказом захисту даних, іноді виникають невеликі збої, і дані не можуть бути розшифровані, що призводить до пошкодження даних та їх непридатності для

клієнтів та постачальних послуг. Також провайдери перезначають IP-адреси. Тобто, коли IP-адреса більше не потрібна одному клієнту по завершенню визначеного періоду часу, вона стає доступною для використанням іншим клієнтом. Постачальники хмарних послуг економлять гроші і не потребують такої великої кількості адрес, повторно використовуючи їх. Надто велика кількість таких невикористовуваних адрес може зробити хмарного провайдера вразливими до зловживання своїми ресурсами. Існує період між зміною IP-адреси в *DNS* та очищенням кешу *DNS*, в якому зберігається IP-адреса. Якщо ці старі IP-адреси зберігаються в кеші, тоді до них можна отримати доступ, що надасть користувачу доступ і до ресурсів, доступних для цієї IP-адреси. Крім того, інший клієнт того ж постачальника послуг може потенційно отримати доступ до ресурсів іншого клієнта, переміщаючись по мережам постачальника хмарних послуг, якщо не будуть прийняті заходи безпеки або їх буде недостатньо.

API хмар та програмне забезпечення як послуга все ще розвиваються, що означає, що оновлення можуть бути частими, але деякі хмари не інформують своїх клієнтів про внесення цих змін. Внесення змін в *API* означає зміну конфігурації хмари, яка впливає на всі її екземпляри. Зміни можуть вплинути на безпеку системи, оскільки зміна може виправити одну помилку, і в той же час створити іншу. Клієнти повинні дізнаватися, чи є якісь оновлення і запитати, які реалізації безпеки були впровадженні для захисту їх даних і що саме змінилось в системі. Один з способів перевірити, чи підходить компанія для розміщення та збереження вашої інформації – це запитати, чи є третя сторона, яка проводить аудит хмари та чи має вона сертифікати безпеки.

Якщо кіберзлочинець зламує хмарного провайдера та копіює дані, що належать клієнту, з серверу, клієнт може і не дізнатись про це. Оскільки, провайдер має доступ до журналів серверу, а клієнт – ні. Декілька клієнтів можуть разом використовувати ресурси одних і тих же серверів та один клієнт може використовувати декілька хостів кожен день. Тому, якщо хмарний

провайдер не розробив програмне забезпечення для моніторингу, яке може групувати та сортувати процеси, які відбуваються для кожного користувача, то це може бути великим ризиком для безпеки та зробити ці хмари ще більш привабливими для кіберзлочинців.

Більшість клієнтів не будуть знати, де їх дані зберігаються постачальником. Це створює ряд проблем, особливо якщо інформація важлива та цінна. Замовники, які турбуються про безпеку, повинні запитати свого постачальника, де знаходяться фізичні сервери, як часто вони обслуговуються та які заходи фізичної безпеки були прийняті (наприклад, біометричні дані чи доступ по PIN-коду) для обмеження доступу до ресурсів серверу. Існує ймовірність, що дані будуть зберігатися в іншій країні, це означає, що місцеве законодавство та юрисдикція будуть відрізнятися та можуть створити інший ризик безпеки, оскільки дані, які можуть бути захищені в одній країні, можуть бути небезпечними в іншій. Якщо розглянути різні погляди на конфіденційність В США та ЄС, то ця загроза безпеки стає більш очевидною, оскільки США дуже відкрито відносяться до конфіденційності даних.

РОЗДІЛ 2. МОДЕЛІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ У ВІРТУАЛЬНИХ СЕРЕДОВИЩАХ ТА ХМАРНИХ ПЛАТФОРМАХ

Перспективи розвитку інформаційних систем пов’язані з реалізацією віртуальних середовищ та хмарних платформ, що надають користувачам можливість доступу до інформаційних ресурсів з мережі Інтернет, більші порівняно з традиційними системами послуг в плані багатокористувацької структури, яка забезпечує легкість та зручність в роботі. Важливим аспектом є економічність хмарних обчислень та доступність електронних інформаційних ресурсів для різних інтересів населення.

Система захисту інформації таких систем повинна забезпечувати захист від актуальних загроз безпеки інформації як традиційних засобів обчислювальної техніки, нейтралізація яких здійснюється також на декількох рівнях захисту: *BIOS* (*Basicinput-outputsystem* – базова система введення-виведення), апаратний, операційна система, мережевий, система управління базами даних, функціональне (прикладне) програмне забезпечення, так і актуальних загроз безпеки інформації, характерних для конкретної хмарної платформи.

Практика застосування засобів віртуалізації та хмарних платформ в інформаційних системах показує, що для захисту інформації недостатньо існуючих механізмів захисту, які розраховані для використання в традиційних засобах обчислювальної техніки, і тому в наш час активно розробляються нові, особливо криптографічні.

Методика проектування систем захисту інформації у віртуальних середовищах та хмарних платформах передбачає використання вже існуючих механізмів захисту та включає в себе метод вибору механізмів захисту, які найбільш ефективно нейтралізують актуальні загрози інформаційної безпеки на рівнях захисту. Методика повинна враховувати теоретико-семантичні аспекти організації комплексної системи захисту інформації.

Система захисту інформації являє собою складну організаційно-технічну систему, поведінка якої відображає динаміку слабо структурованих процесів[12] та характеризується високою степеню невизначеності внаслідок не стаціонарності, неточності та недостатності спостережень, нечіткості та нестабільності тенденцій. Якість, що розглядається, не має статистичної природи: неможливо отримати вибірки статистично однорідних подій з їх генеральної сукупності, що спостерігається в незмінних зовнішніх умовах спостереження. Тобто, класично зрозумілої статистики не існує.

Робота з випадковими величинами доказує, що ймовірнісні методи застосовуються обмежено при моделюванні складних недетермінованих процесів, до того ж до цих процесів можна віднести і дії по несанкціонованому доступу до хмарних сервісів. В працях [13, 14] показано, що теорія ймовірностей є окремим випадком теорії можливостей. В свою чергу, математичною основою останньої є інтервальний аналіз та теорія нечітких множин. В якості підходу до вирішення проблеми високої невизначеності в процесі розробки методики проектування систем захисту інформації у віртуальних середовищах та хмарних платформах буде використовуватись теорія нечітких множин[15, 16], теорії можливостей[17] та теоретичної інформатики[18].

Відповідно стандарту міжнародного союзу електрозв'язку *ITU-T E*.408 кількісна оцінка ризику загрози інформаційної безпеки в мережі зв'язку, визначається двома характеристиками – ймовірністю загрози та наслідком від реалізації цієї загрози. Що стосується першої характеристики, то тут доцільно оцінювати не ймовірність, а можливість реалізації загроз безпеки інформації з існуючими механізмами захисту та з використанням експертних оцінок. Експертні оцінки частково стосуються визначення рейтингів потенціалу нападу та стійкості механізмів захисту, співвідношення яких і визначає можливість реалізації загрози чи можливість її нейтралізації. Вважається, що потенціал нападу залежить від рівня мотивації зловмисника, його кваліфікації

та ресурсів, які вже є. Мотивація впливає на час, виділений для атаки, і, ймовірно, на ресурси, які приваблюють зловмисника.

Невизначеність обумовлена також оцінками параметрів ефективності механізмів захисту, таких як вартість цих механізмів, середня кількість загроз, які нейтралізуються цими механізмами, величина ризику, степінь довіри та сумісність засобів захисту, можливість застосування механізмів захисту у віртуальних середовищах та хмарних платформах.

2.1. Аналіз моделі системи захисту інформації

В рамках методики проектування систем захисту інформації у віртуальних середовищах та хмарних платформах проаналізуємо модель системи захисту інформації з розподіленням механізмів захисту по загрозам, які нейтралізуються на рівнях захисту, запропоновану в роботі [19] та уточнюючу більш загальну модель захисту. При побудові даної моделі в якості вихідної взятий сенс, який полягає в тому, що в системах захисту інформації як для традиційних засобів обчислювальної техніки, так і для віртуальних середовищ та хмарних платформ повинен бути хоча б один механізм захисту для нейтралізації будь-якої потенційно можливої загрози безпеки інформації.

Представимо модель системи захисту інформації у вигляді кортежу.

$$MOD_{\text{СЗІ}} =< \{UR\}, \{UG\}, \{MZ\}, \{PR\}. \{TR\}$$

Тут $ur_u \in$ UR – рівні захисту в СЗІ, $u = \overline{1, U}$, U – кількість рівні захисту;

$ug_u \in$ UG – множина актуальних загроз, $n = \overline{1, U}$, N – кількість загроз;

MZ $= \{mz_k\} = \cup_{u=} MZ_u = \{mz_{k \in K,u}\}$, де MZ – підмножина механізмів захисту рівня $ur_u \in UR, k \in K_u$- підмножина індексів $k = \overline{1, K}$ механізми захисту на цьому рівні, $\cup K_u = K, \cap K_u = \emptyset$;

$pr_j \in PR, j = \overline{1, J}$, множина параметрів оцінки ефективності механізмів захисту;

$tr_{mz} \in TR$ – множина вимог до механізмів захисту;

$tr_{mz} = \{rsk_{mz}, st_{mz}^{max}\}$, де rsk_{mz} - допустимий рівень ризику від реалізації загрози, st_{mz} – максимально допустимі затрати на засоби захисту (для класу функціонально-однотипних механізмів захисту).

Загрозу ug_n представимо у вигляді вектору $ug_n = \{p^{ug_n}, uch^{ug_n}, rsk^{ug_n} = p^{ug_n} * uch^{ug_n}$, де p^{ug_n} – оцінка можливості реалізації загрози ug_n, uch^{ug_n} – збиток від реалізації загрози ug_n, p^{ug_n} – ризик від реалізації загрози ug_n.

Слід сформувати структуру системи захисту інформації шляхом розподілу $mz_{ku} \in MZ$ по множині актуальних загроз $ug_n \in UG$ на рівнях захисту $ur_u \in UR$:

$$\mathrm{M_{CSI}} = \bigcup_n M_n = \{mz_{k1} | \max poss(mz_{k1}, ug_n); \dots, \max poss(mz_{ku}, ug_n)\}$$

Тут $mz_{ku} | \max poss(mz_{ku}, ug_n)$ – механізм захисту, обраний на рівні захисту $ur_u \in UR$, що забезпечує максимальну можливість нейтралізації актуальної загрози $ug_n \in UG$.

Обмеження моделі системи захисту інформації, яка розглядається, полягає в точкових оцінках можливостей нейтралізації актуальної загрози безпеки інформації визначеним механізмом захисту і в точкових оцінках у вигляді значень відповідних функцій приналежності параметрів ефективності механізмів захисту.

Потенціал нападу оцінюється в загальному по тій же схемі, що і степінь ризику від наявності вразливостей, але з деякими відмінностями (наприклад, з декількох сценаріїв нападу вибирається найгірший, з найбільшим потенціалом). Вважається, що він є функцією рівня мотивації зловмисника, його кваліфікації та наявних ресурсів. Мотивація впливає на час, виділений для атаки та ресурси, які потрібні зловмиснику[20].

Тоді можливість $poss(mz_k, ug_i)=\mu_{ugi}(mz_k)$ нейтралізації загрози ug_i функцією захисту mz_k можна визначити наступним чином:

$$m_{ugi}(mz_k) = \begin{cases} 1, \text{якщо } r_c \geq r_н; \\ \dfrac{r_c}{r_н}, \text{якщо } r_c < r_н \end{cases}$$

Тут $r_н$ – рейтинг потенціалу нападу, r_c – рейтинг стійкості функції захисту. Розуміємо, що для будь-якої загрози існує функція захисту така, що $r_c \geq r_н$: $\forall ug_i \; \exists mz_k \; | r_c \geq r_н$ будь-яка загроза нейтралізується хоча б однією функцією захисту. Величина $\mu_{ugi}(mz_k)$ являє собою точкову оцінку. Подолати вказане вище обмеження можна шляхом оцінки рейтингів нападу та стійкості механізмів захисту з використанням нечітких чисел. Таке рішення аргументується тією обставиною, що діапазони рейтингів, що характеризуються стійкість механізмів захисту та потенціал нападу, представлені лінгвістичними значеннями[20]: діапазони рейтингів стійкості механізмів захисту – базова (діапазон 10-17), середня (діапазон 18-24), висока (діапазон > 24) та потенціал нападу – низький (діапазон < 10), помірний (діапазон 10-17), високий (діапазон 18-24) та нереально високий (діапазон > 24). Лінгвістичні значення можна інтерпретувати як нечітке число, визначене на заданому інтервалі.

Набір операцій над нечіткими числами зводиться до алгебраїчних операцій зі звичайними числами при задані інтервалу достовірності (рівня приналежності), що називаються м’якими обчисленнями[21, 22].

2.2. Представлення якісних оцінок *S*-нечіткими множинами

Важливим для практичних додатків в плані представлення якісних виразів та оцінок людини в процесі рішення задач є випадок *S* нечітких множин[23], що задаються парою (X, μ), де $(\mu : X \rightarrow S)$ відображення з X в лінійно впорядковану множину *S*.

В тому випадку, коли набір нечітких множин $\widehat{A_i}, i = \overline{1, I}$, в X відповідає I властивостям об'єкту, що розглядається, кожен елемент $x \in X$ характеризується вектором значень приналежності $((\mu_1(x), \ldots, \mu_I(x))$, що виражає степінь задоволення цією властивістю. Таким чином, будується функція $\mu : X \to S_1 \times \ldots \times S_I$, де S_I – обмежені лінійно впорядковані множини. Приклади кінцевої лінійної впорядкованої множини – набір лінгвістичних значень змінної «Рейтинг нападу» = {низький, помірний, високий, нереально високий}, «Рейтинг стійкості механізмів захисту» = {базовий, середній, високий}

2.3. Операції над нечіткими числами

Для практичних обчислень зручно працювати з нечіткими числами спеціального виду: трикутними та трапецієподібними. Трапецієподібне число має функцію приналежності, що задається формулою:

$$\mu_A(x) = \begin{cases} 0, x < a_1 \text{ або } x > a_1, \\ \frac{x-a_1}{a_2-a_1}, a_1 \le x < a_2, \\ 1, a_2 \le x \le a_3, \\ \frac{a_1-x}{a_4-a_3}, a_3 < x \le a_4, \end{cases} \quad (1)$$

де $a_1 \le a_2 \le a_3 \le a_4$.

Воно зазвичай позначається як $\tilde{A} = (a_1, a_2, a_3, a_4)$. У випадку $a_2 = a_3$ виходить трикутне число $\tilde{A} = (a_1, a_2, a_4)$.

Маючи на увазі принцип розширення нечітких множин та застосовуючи його до арифметичних операцій та трапецієподібних нечітких чисел отримаємо наступні правила додавання та віднімання:

$$(a_1, a_2, a_3, a_4) + (b_1, b_2, b_3, b_4) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4), \quad (2)$$

$$(a_1, a_2, a_3, a_4) - (b_1, b_2, b_3, b_4) = (a_1 - b_4, a_2 - b_3, a_3 + b_2, a_4 + b_1), \quad (3)$$

Добуток та частка від ділення трапецієподібних чисел вже не будуть трапецієподібними, але будуть криволінійно трапецієподібними. В даному випадку можна написати наближені рівності:

$$(a_1, a_2, a_3, a_4) * (b_1, b_2, b_3, b_4) \approx (a_1 * b_1, a_2 * b_2, a_3 * b_3, a_4 * b_4), \quad (4)$$

$$(a_1, a_2, a_3, a_4)/(b_1, b_2, b_3, b_4) \approx (a_1/b_4, a_2/b_3, a_3/b_2, a_4/b_1), \quad (5)$$

Розуміється, що нечіткі числа додатні, тобто $a_1 > 0$ та $b_1 > 0$. Точність обчислень за формулами (2-5) залежить від кількості α-зрізів.

Зниження об'єму обчислень при операціях над нечіткими числами досягається застосуванням чисел (*L-R*)-типу. Функції приналежності нечітких чисел (*L-R*)-типу задаються за допомогою незростаючих на множині невід'ємних дійсних чисел функцій дійсного змінного *L(x)* та *R(x)*[24].

З нечітким трапецієвидним числом $\tilde{A} = (a_1, a_2, a_3, a_4)$ пов'язують дві числові характеристики: середнє значення та дисперсію, що обчислюються за формулами[24]:

$$E(\tilde{A}) = \frac{a_1 + 2a_2 + 2a_3 + a_4}{6}$$

$$Var(\tilde{A}) = \frac{(a_4 - a_1)^2 + 2(a_4 - a_1)(a_3 - a_2) + 3(a_3 - a_2)^2}{24}$$

2.4. Семантика інформаційних описів механізмів захисту

Відповідно основним положенням теоретичної інформатики під інформаційними описом $\Delta(mz)$ будь-якого механізму захисту мається на увазі структуровану сукупність даних типу $(p)A(mz)$: $\Delta(mz) = \{(p_i)A_i\}(mz), i = \overline{1, N}$.

Тут дані $\{(p_i)A_i\}(mz)$ інтерпретуються як «механізм захисту *mz* з *MZ* характеризується можливістю (семантичною достовірністю) p_i нейтралізації загрози $ug_n \in A_i$», A_i – підмножина загроз безпеки інформації ug_n з *UG*, які можуть бути нейтралізовані механізмом mz, $A_i \subset UG$. Іншими словами,

можливість нейтралізації механізмів захисту mz_k загрози ug_n можна записати у вигляді $poss(mz_k, ug_n) = \mu_{ug_i}(mz_k) = \widetilde{p_{kn}}$, $\widetilde{P_{kn}}$ являє собою нечітке число, значення якого показує правдоподібність того, що дійсне значення величини $\widetilde{ug_i}$ дорівнює $\mu_{u\tilde{g}_i}(mz_k)$.

Формальне визначення інформаційного опису $\Delta(mz)$ механізмів захисту дозволяє зробити висновок про те, що параметри оцінки ефективності застосовуються і до оцінки нейтралізуючих загроз безпеки інформації. Відповідно, застосовуючи до нейтралізуючих загроз можна оцінити вартість нейтралізації цих загроз, середню кількість механізмів захисту, нейтралізуючу загрозу, величину ризику, степінь довіри та сумісність засобів захисту при нейтралізації загрози, степінь застосовуваності механізмів захисту при нейтралізації конкретної загрози у віртуальних середовищах та хмарних платформах.

2.5. Параметри ефективності механізмів захисту

На багатьох актуальних загрозах $ug_n \in UG$ та механізмах захисту $mz_k \in MZ$ визначено нечітке відношення $M\widetilde{U}$. В нашому випадку $poss(mz_k, ug_n) = \widetilde{p_{kn}}$ – оцінка можливості нейтралізації функцією захисту mz_k актуальної загрози ug_n. В класичному випадку $\mu_{MU}(ug_n, mz_k) = x_{MU}(ug_n, mz_k) = 1$, якщо загроза ug_n однаначно нейтралізується засобом захисту mz_k та $\mu_{MU}(ug_n, mz_k) = x_{MU}(ug_n, mz_k) = 0$ – якщо загроза не нейтралізується.

Оцінку ефективності механізму захисту будем обчислювати з використанням параметрів, що представлені нижче. Розуміється, що кількісні оцінки значень параметрів представлені нечіткими числами, визначені на відповідних шкалах (універсальних множинах). Значення параметрів зафіксовані на момент часу оцінки механізму захисту.

1. Параметр pr_1

Вартість механізмів захисту. Кількісну оцінку параметру можна визначити у вигляді нечіткого числа $mz_{ku}(p\tilde{r}_1)$ на універсальній шкалі вартостей.

Вартість нейтралізації актуальної загрози. Позначимо через $mz_{ku}(p\tilde{r}_1)$ значення параметру $p\tilde{r}_1$ для засобу захисту mz_{ku}. Тоді значення $ug_n(p\tilde{r}_1)$ параметру $p\tilde{r}_1$для загрози ug_n можна визначити наступним чином:

$$ug_n(p\tilde{r}_1) = \max\{\min\{mz_{ku}(p\tilde{r}_1)|p_{ku,u} > 0\}\}$$

Тут $\min\{mz_{ku}(p\tilde{r}_1)|p_{ku,u} > 0\}$ – мінімальне значення параметру $p\tilde{r}_1$ для mz_{ku}, що нейтралізують загрозу ug_n на рівні $ur_u \in UR$, $ug_n(p\tilde{r}_1)$ – максимальна вартість нейтралізації актуальної загрози існуючими функціями захисту. На кожному рівні захисту вибираються механізми з мінімальною вартістю, а для нейтралізації загрози по всім рівням системи захисту обирається найгірший варіант – застосовується функція захисту з максимальною вартістю.

2. Параметр pr_2.

Оцінка середньої кількості загроз, що нейтралізуються функцією mz_{ku}.

$$p\tilde{r}_2 = (\frac{|UG_k| - sm^{mz_{ku}}}{\max(|UG_k| - sm^{mz_{ku}})})$$

де $UG_k = \{ug_n|\tilde{p}_{ku,u} > 0\}$ – множина загроз, що нейтралізуються функцією захисту mz_{ku}, $sm^{mz_{ku}} = \sum_{n=1}^{N} \widetilde{P_{ku,u}}$ – сума оцінок можливостей нейтралізації загроз засобом захисту mz_{ku}, $\max(|UG_k| - sm^{mz_{ku}})$ – максимальна різниця між кількістю загроз та сумою оцінок можливостей нейтралізації загроз засобами захисту mz_{ku} на u-ному рівні.

Оцінка середньої кількості механізмів захисту, що нейтралізують актуальну загрозу ug_n.

$$ug_n(p\tilde{r}_2) = \min\{\max\{mz_{ku}(p\tilde{r}_2)|\tilde{p}_{ku,u} > 0\}\}$$

По рівням захисту обираються механізми захисту з максимальною оцінкою середньої кількості загроз, що нейтралізуються. Для оцінки

нейтралізації загрози на всіх рівнях захисту розглядається варіант застосування функції захисту з мінімальною середньою оцінкою кількості нейтралізуючих загроз.

3. Параметр $p\tilde{r}_3$.

Величина ризику, якому перешкоджає функція захисту mz_{ku} від реалізації актуальних загроз.

Ризик від реалізації загрози раніше був визначений як $rsk^{ug_n} = p^{ug_x} \times uch^{ug_n}$. Тоді $rsk_{mz_{ku}}^{max} = max_{n=1}^{N} rsk^{ug_n} \times (1 - p_{ku,u})$ – максимальний ризик від реалізації загроз, які не були нейтралізовані функцією захисту mz_{ku} на рівні захисту u та значення параметру $p\tilde{r}_3$ для mz_{ku} можна визначити наступним чином:

$$p\tilde{r}_3 = \left(\left| \frac{rsk_{mz_{ku}}^{max}}{rsk_{mz_{ku}}^{\text{доп}}} \right| \right).$$

Розуміється, що актуальна загроза нейтралізується хоча б одним механізмом захисту.

Величину ризику від реалізації загрози оцінимо наступним чином $ug_n(p\tilde{r}_3) = \min\{\max\{mz_{ku}(p\tilde{r}_3) \big| \tilde{p}_{ku,u} > 0\}\}$.

По рівнях захисту обирається функція захисту, яка може допустити максимальний збиток від реалізації загрози. В цілому по рівнях захисту приймається варіант спричинення мінімального збитку від реалізації загрози.

4. Параметр $p\tilde{r}_4$.

Степінь довіри до механізмів захисту.

Степінь довіри $p\tilde{r}_4 = sd_{mz_k}$ до функції захисту можна визначити по методиці, представленій в роботі [25].

Відповідно [25] кількісна оцінка степеню довіри функції захисту обчислюється з використанням п’яти критеріїв: kr_1^{sd} – оцінка компанії-розробника; kr_2^{sd} – об’єм вихідних кодів, що надаються; kr_3^{sd} – оцінка досліджень засобу захисту за вимогами безпеки інформації; kr_4^{sd} – оцінка технології виробництва засобу захисту; kr_5^{sd} – оцінка технічної підтримки

засобу захисту. Критерії kr_2^{sd} та kr_3^{sd} дозволяють оцінити виконання вимог безпеки інформації розробником, а критерії kr_4^{sd} та kr_5^{sd} характеризують степінь технологічної незалежності механізмів захисту, що виготовляються.

Степінь довіри до механізмів захисту по відношенню до загроз, що нейтралізуються обчислюється як $ug_n(p\tilde{r}_4) = \min\{\max\{mz_{ku}(p\tilde{r}_4)|\widetilde{p_{ku,u}} > 0\}\}$.

На рівнях захисту оцінка здійснюється по механізмам захисту з максимальною оцінкою степеню довіри.

5. Параметр $p\tilde{r}_5$.

Степінь сумісності механізмів захисту.

На множині $mz_{ku} \epsilon\, MZ$ визначимо відношення SV наступним чином: $\mu_{SV}(mz, mz_j) = \tilde{p}_{kj}$ – степінь сумісності mz_k з mz_j , $\tilde{p}_{kj}$ – нечітке число. Обернене може бути не вірним: mz_j може бути несумісним з mz_k. В класичному випадку $\mu_{SV}(mz_k, mz_j) = X_{SV}(mz_k, mz_j) = 1$, якщо mz_k повністю сумісне з mz_j та $\mu_{SV}(mz_k, mz_j) = X_{SV}(mz_k, mz_j) = 0$ – якщо несумісні.

Степінь сумісності mz_k з іншими засобами захисту по периметру $p\tilde{r}_5$ визначимо наступним чином: $p\tilde{r}_5 = \left(\frac{\left(|SV_k| - sm_{mz_k}^{SV}\right)}{|SV_k|}|\right)$, де $SV_k = \{mz_j|\tilde{p}_{kj} > 0\}$ – множина функцій захисту, сумісних з mz_k, $sm_{mz_k}^{SV} = \sum_{j=1}^{K} \tilde{p}_{kj}$ – сума степенів сумісності mz_k з mz_j.

Оцінка степені сумісності механізмів захисту по відношенню до загроз, що нейтралізуються: $ug_n(p\tilde{r}_5) = \min\{\max\{mz_{ku}(p\tilde{r}_5)|\widetilde{p_{kJ,u}} > 0\}\}$.

На рівнях захисту застосовуються механізми з максимальною оцінкою степені сумісності. Структура системи захисту інформації при нейтралізації загрози характеризується найменш сумісними механізмами захисту.

6. Параметр $p\tilde{r}_6$.

Застосовність в хмарних платформах. Кількісну оцінку параметру можна визначити у вигляді нечіткого числа $mz_{ku}(p\tilde{r}_6)$ на універсальній шкалі.

Застосовність по відношенню до загроз інформаційної безпеки. Позначимо через $mz_{ku}(p\tilde{r}_6)$ значення параметру $p\tilde{r}_6$ для механізму захисту mz_{ku}. Тоді значення $ug_n(p\tilde{r}_6)$ параметру $p\tilde{r}_6$ для загрози ug_n визначимо наступним чином $ug_n(p\tilde{r}_6) = min\{mz_{ku}(p\tilde{r}_6)|\tilde{p}_{kn,u} > 0\}$. Тут $min\{mz_{ku}(p\tilde{r}_6)|\tilde{p}_{kn,u} > 0\}$ – мінімальне значення параметру $p\tilde{r}_6$ для mz_{ku}, що нейтралізують загрозу ug_n на рівні $ur_u \in UR$, $ug_n(p\tilde{r}_6)$ – максимальна можливість застосування функції захисту для нейтралізації актуальної загрози безпеки інформації. На кожному рівні захисту обираються механізми захисту з мінімальною можливістю застосування, а по всім рівням системи захисту – функція захисту з максимальною можливістю застосування.

2.6. Метод вибору бажаних механізмів захисту в структурі системи безпеки інформації

Формування структури системи захисту інформації шляхом збору бажаних механізмів захисту $mz_{ku} \in MZ$ здійснюється на рівнях захисту $ur_u \in UR$ шляхом їх розподілу по множині нейтралізуючих загроз безпеки інформації $ug_n \in UG$, що забезпечує максимальну можливість нейтралізації цих загроз. Для реалізації такого розподілу необхідно визначити правило вибору бажаних механізмів, яке пов’язане з формуванням семантичного порогу бажань при розподілі механізмів по нейтралізуючим загрозам[26].

Раніше ми визначили, що можливість нейтралізації механізмом захисту mz_k загрози ug_n представляється нечітким числом $\tilde{p}_{kn}$. Це визначення можна представити у вигляді відношення $M\tilde{U}$:

$$M\tilde{U} = \begin{matrix} \\ mz_1 \\ mz_2 \\ . \\ . \\ . \\ mz_k \end{matrix} \begin{matrix} [ug_1 & \dots & ug_N] \\ \begin{bmatrix} \tilde{p}_{11} & \tilde{p}_{12} & \tilde{p}_{1N} \\ . & . & . \\ \tilde{p}_{k1} & \tilde{p}_{k2} & \tilde{p}_{kN} \end{bmatrix} \end{matrix}$$

В нечітких множинах $\tilde{A}_1, \tilde{A}_2, \dots, \tilde{A}_N$ представлені можливості $\tilde{p}_{kn}$ нейтралізації загроз $\tilde{A}_1, \tilde{A}_2, \dots, \tilde{A}_N$, $n = \overline{1, N}$,функціями захисту mz_{ku}: $\mu_{\tilde{A}_1}(\tilde{p}_{k1})$, $\mu_{\tilde{A}_2}(\tilde{p}_{k2}), \dots, \mu_{\tilde{A}_N}(\tilde{p}_{kN})$. Обчислимо значення $p\tilde{g}'$ наступним чином:

$p\tilde{g}' = \min(\max(\tilde{A}_1(\tilde{p}_{k1}) \min \tilde{A}_2(\tilde{p}_{k2}), (\tilde{A}_1(\tilde{p}_{k1}) \min \tilde{A}_3(\tilde{p}_{k3})), \dots,$
$(\tilde{A}_1(\tilde{p}_{k1}) \min \tilde{A}_N(\tilde{p}_{kN}), (\tilde{A}_2(\tilde{p}_{k2}) \min \tilde{A}_3(\tilde{p}_{k3})), \dots, ((\tilde{A}_{N-1} \min \tilde{A}_N)))$.

В цьому випадку поріг бажань $p\tilde{g}$ при виборі механізму захисту полягає в пошуку у відношенні $M\tilde{U}$ такого найбільшого значення, як менше $p\tilde{g}'$:

$p\tilde{g} = \min\{p_{kn}\} | p_{kn} > p\tilde{g}'\}$.

На множинах *MZ* та параметрах ефективності *PR* визначимо відношення $M\tilde{R} - \mu_{MR}: MZ \times PR \to [m\tilde{r}_{rj}]$. Тут $m\tilde{r}_{rj}$ - нечітке число, що відображає оцінку можливого значення параметру ефективності $pr_j \in PR$ для $mz_k \in MZ$.

Відношення $M\tilde{R}$ представимо в матричній формі:

$$M\tilde{R} = \begin{matrix} \\ mz_1 \\ mz_2 \\ . \\ . \\ . \\ mz_k \end{matrix} \begin{matrix} [pr_1 & \dots & pr_J] \\ \begin{bmatrix} m\tilde{r}_{11} & m\tilde{r}_{12} & m\tilde{r}_{1J} \\ . & . & . \\ mr_{k1} & m\tilde{r}_{k2} & m\tilde{r}_{kJ} \end{bmatrix} \end{matrix}$$

На множинах параметрів *PR* та актуальних загроз *UG* формуємо відношення $K\tilde{G} - \mu_{K\tilde{G}}: PR \times UG \to [k\tilde{g}_{jn}]$. Для всіх $pr_j \in PR$ та всіх $ug_n \in UG$ $k\tilde{g}_{jn}$ – оцінка загрози ug_n по параметру pr_j , що визначається необхідністю нейтралізації загрози ug_n механізмами захисту mz_k. Оцінки $k\tilde{g}_{jn}$ у вигляді нечітких чисел обраховуються в порядку, який представлений в розділі 2.5.

В матричній формі відношення набуває вигляду

$$K\tilde{G} = \begin{bmatrix} pr_1 \\ \dots \\ pr_J \end{bmatrix} \begin{matrix} [ug_1 & \dots & ug_N] \\ \begin{bmatrix} k\tilde{g}_{11} & \dots & k\tilde{g}_{1N} \\ \dots & \dots & \dots \\ k\tilde{g}_{J1} & \dots & k\tilde{g}_{JN} \end{bmatrix} \end{matrix}$$

Тоді на базі відношень $M\tilde{R}$ та $K\tilde{G}$ можна сформувати відношення $M\tilde{G}$, представлене нижче:

$$M\tilde{G} = \begin{bmatrix} mz_1 \\ \dots \\ mz_K \end{bmatrix} \begin{matrix} [ug_1 & \dots & ug_N] \\ \begin{bmatrix} \mu_{\tilde{A}_1}(m\tilde{g}_{11}) & \dots & \mu_{\tilde{A}_N}(m\tilde{g}_{1N}) \\ \dots & \dots & \dots \\ \mu_{\tilde{A}_1}(m\tilde{g}_{K1}) & \dots & \mu_{\tilde{A}_N}(m\tilde{g}_{KN}) \end{bmatrix} \end{matrix}$$

Елементи в матриці визначимо наступним чином:

$\mu_{\tilde{A}_n}(m\tilde{g}_{Kn}) = \frac{\sum_j m\tilde{r}_{kj} \times k\tilde{g}_{jn}}{\sum_j m\tilde{r}_{kj}}$, для всіх $mz_k \in MZ, pr_j \in KR, ug_n \in UG$.

Сума $\sum_j m\tilde{r}_{kj}$ інтерпретується як кількість значимих параметрів *pr*, які характеризують *mz*, а $\mu_{\tilde{A}_n}(m\tilde{g}_{Kn})$ являє собою зважену оцінку можливості нейтралізації актуальної загрози ug_n механізмом захисту mz_k (степінь надання переваги при виборі механізму захисту mz_k для нейтралізації актуальної загрози ug_n).

Відмітимо, що раніше визначені значення $\mu_{\tilde{A}_1}(\tilde{p}_{k1}), \mu_{\tilde{A}_2}(\tilde{p}_{k2}), \dots, \mu_{\tilde{A}_N}(\tilde{p}_{kN})$ $\mu_{\tilde{A}_1}(mz_k)$ (відношення $M\tilde{U}$) та обчислені значення $\mu_{\tilde{A}_1}(m\tilde{g}_{K1}), \mu_{\tilde{A}_2}(m\tilde{g}_{K2}), \mu_{\tilde{A}_N}(m\tilde{g}_{KN})$ відображають оцінки можливостей та нейтралізації загрози ug_i функцією захисту mz_k. Але при визначені $\mu_{\tilde{A}_1}(\tilde{p}_{k1})$ не робляться припущення відносно коректності реалізації механізму захисту, або простіше кажучи, не враховуються їх параметри ефективності: степінь довіри, параметри вартості, середня кількість нейтралізуючих загроз і тому подібні. Значення критеріїв ефективності функцій захисту враховані в обчислених значеннях $\mu_{\tilde{A}_N}(m\tilde{g}_{KN})$.

Відповідно прийнятому підходу формується матриця $\widetilde{W}$.

$$\widetilde{W}=\begin{bmatrix}\mu_{\tilde{A}_1}(m\tilde{g}_{11})\min\mu_{\tilde{A}_2}(m\tilde{g}_{12}), & \dots, & \mu_{\tilde{A}_{N-1}}(m\tilde{g}_{1N-1})\min\mu_{\tilde{A}_N}(m\tilde{g}_{1N})\\ \mu_{\tilde{A}_2}(m\tilde{g}_{21})\min\mu_{\tilde{A}_2}(m\tilde{g}_{22}), & \dots, & \mu_{\tilde{A}_{N-1}}(m\tilde{g}_{2N-1})\min\mu_{\tilde{A}_N}(m\tilde{g}_{2N}),\\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots.. \\ \mu_{\tilde{A}_1}(m\tilde{g}_{k1})\min\mu_{\tilde{A}_2}(m\tilde{g}_{k2}), & \dots, & \mu_{\tilde{A}_{N-1}}(m\tilde{g}_{kN-1})\cap\mu_{\tilde{A}_N}(m\tilde{g}_{N})\end{bmatrix}$$

Семантичний поріг надання переваги застосовується для вибору механізму захисту, який найбільш ефективно нейтралізує загрози $ug_n \in UG$ по рівнях захисту та в структурі системи захисту інформації в цілому.

$M_n = \{mz_{ku} | \mu_{\tilde{A}_n}(mz_{ku}, ug_n) \geq p\tilde{g}\}$ - множина механізмів захисту mz_{ku}, які нейтралізуються загрозу ug_n на рівнях захисту $ur_u \in UR$ з можливістю, що перевищує обчислювальний семантичний поріг переваги.

РОЗДІЛ 3. ОПТИМІЗАЦІЯ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ НА ПЛАТФОРМІ

AI Platform Notebooks – це сервіс, що надає інтегроване та безпечне середовище *JupyterLab* для спеціалістів по даним та розробників машинного навчання для експериментів, розробки та розгортання моделей у виробничому середовищі.

В цьому розділі під конфіденційними даними мається на увазі конфіденційна інформація, для доступу до якої будь-кому у вашій організації потрібні більш високі рівні привілеїв.

Застосування політик управління даними та безпеки на платформі *AI* з конфіденційними даними часто потребує досягнення балансу між наступними цілями:

- Допомога в захисті даних, що використовуються екземплярами портативних комп'ютерів, за рахунок використання тих же методів управління даними та безпеки, які ви застосовуєте в своїй організації.
- Забезпечення того, щоб спеціалісти по даним у вашій організації мали доступ до даних, які їм необхідні для отримання змістовної інформації.

Периметр в архітектурі платформи *AI* називається верхньою межею довіри. Це допомагає захистити конфіденційні дані, що використовуються у віртуальній приватній хмарі (*VPC*). Спеціалісти з обробки даних повинні отримувати доступ до даних через більш високу межу довіри. Більш висока межа довіри включає кожен хмарний ресурс, який взаємодіє з конфіденційними даними.

Архітектура також створює елементи управління безпекою, які допомагають в наступному:

- Знижувати ризик крадіжки даних на пристрій, який використовується спеціалістами по обробці даних в організації.

- Захищати ноутбуки від зовнішнього мережевого трафіку.
- Обмежувати доступ до віртуальної машини, на якій розміщені екземпляри конфіденційних документів.

Для структурування організації потрібно логічно згрупувати ресурси по проектам та папкам. У виробничій папці потрібно створити нову папку, яка буде представляти довірене середовище. В цю папку додаються політики організації.

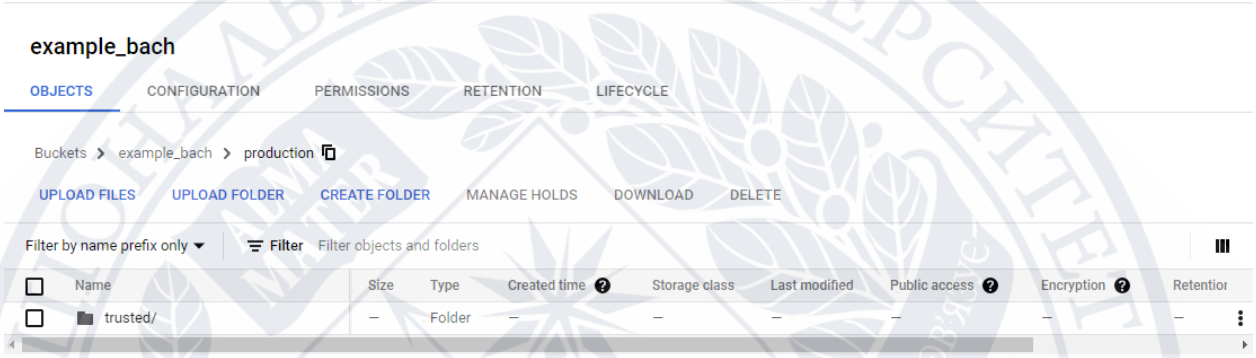

Рисунок 3.1. Головна папка та підпапки

Схема допомагає ізолювати дані, вводячи нову підпапку у виробничу папку для блокнотів *AI Platform* та будь-яких даних. Відношення папок всередині організації описані в табл. 1.

Таблиця 1. Відношення папок.

Папка	Опис
production	Містить проекти з протестованими та готовими до використання хмарними ресурсами
trusted	Містить проекти та ресурси для екземплярів записних книжок з конфіденційними даними. Ця папка є дочірньою по відношенню до папки production.

Для ізоляції середовища за допомогою проектів необхідно створити явні прив'язки політик для відповідних груп. В табл. 2 описано, де потрібно створити проекти, необхідні для організації.

Таблиця 2. Створення проектів

Проект	Батьківська папка	Опис
trusted-kms	*trusted*	Містить служби, що керують ключем шифрування, який захищає ваші дані.
trusted-data	*trusted*	Містить служби, що обробляють конфіденційні дані
trusted-analytics	*trusted*	Містить записи на платформі, які використовують спеціалісти з аналізу даних.

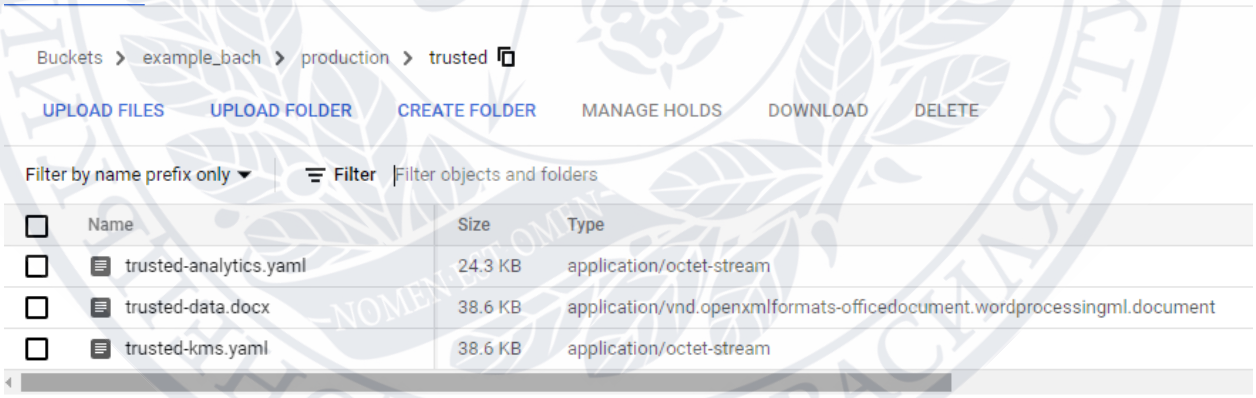

Рисунок 3.2. Створення проектів

Далі потрібно налаштувати обмеження, що застосовуються до папки *trusted*.

Таблиця 3. Обмеження для папки *trusted*

Обмеження політики	Опис	Рекомендоване значення
gcp.resourceLocations	Обмеження на те, які ресурси розгортаються у визначених областях.	"*in:us-locations", "in:eu-locations"*
iam.disableServiceAccountCreation	Якщо значення *true*, забороняє створення облікового запису	*true*
iam.disableServiceAccountKeyCreation	Якщо значення *true*, забороняє створення ключів облікового запису служби	*true*
iam.automaticIamGrantsForDefaultServiceAccounts	Якщо значення *true*, забороняє представлення облікових записів служб	*true*
compute.requireOsLogin	Якщо значення *true*, дозволяє вхід в ОС	*true*
constraints/compute.restrictProtocolForwardingCreationForTypes	Створює нові правила переадесації	*["is:INTERNAL"]*
compute.restrictSharedVpcSubnetworks	Визначає набір загальних підмереж *VPC*, які можуть використовувати відповідні ресурси	["under:projects/VPC_SUBNET"]
compute.vmExternalIpAccess	Визначає набір екземплярів, в яких є дозвіл на	*deny all=true*

	використання зовнішніх *IP*-адрес	
compute.skipDefaultNetworkCreation	Якщо значення *true*, дозволяє створення мережі за замовчуванням	*true*
compute.disableSerialPortAccess	Якщо значення *true*, забороняє доступ через послідовний порт до віртуальних машин	*true*
compute.disableSerialPortLogging	Якщо значення *true*, забороняє ведення журналу послідовного порту з віртуальних машин	*true*

Привілейований доступ. Користувачі з вказаної групи спеціалістів по обробці даних з більш високим рівнем довіри *trusted-data-scientists@example.com* мають привілейований доступ. Цей рівень доступу означає, що у цих користувачів є посвідчення, які можуть отримати доступ до конфіденційних даних. Разом з групою ідентифікації потрібно надати апаратні ключі безпеки з внутрішньою двоетапною аутентифікацією для цих ідентифікаційних даних спеціалістів.

Для захисту даних потрібно використовувати ключі шифрування. Ключі мають підтримуватися хмарним *HSM FIPS 140-2* рівня 3. Такі ключі допоможуть захистити дані наступним чином:

- Доступність ключа налаштовується залежно від області та інформації, яка в ній може міститись.
- Налаштовується ротація ключів.
- Обмежений доступ до ключа.

Поряд з елементами управління безпекою, які встановлюються, потрібно налаштувати наступні операційні політики безпеки, щоб забезпечити постійний захист даних в портативних комп’ютерах, що використовуються в організації:

- Конфігурація реєстрації та моніторингу.
- Політика управління вразливостями.
- Видимість активів.

Після створення ієрархії організації потрібно налаштувати елементи управління ведення журналу.

ВИСНОВКИ

Безпека – важливий компонент інформаційних систем. Методи аналізу та проектування безпеки розвивались аналогічно загальним методам розробки інформаційної безпеки. В них є такі спільні риси як цілі, засоби, проблеми та основні концепції. Перші методи забезпечення безпеки були зосереджені на контрольних списках та простому аналізі ризиків для підтримання прийняття рішень. Більш пізні методи зосереджені на механічному розподілі складності в бажаній системі. Вони тягнуть за собою пошук тих важливих елементів управління, які забезпечують мінімальний необхідний захист для всієї інформаційної системи. Останнім часом зростає інтерес до методів, які фокусуються на абстрактних моделях як засобі розуміння різних потреб безпеки в інформаційній системі. Після багатьох років інтелектуального прогресу методи безпеки, можливо, досягли важливого стику з більш загальними методами розробки інформаційної безпеки. Схоже, що методи забезпечення безпеки не можуть досягти значного прогресу за межами цього моменту без їх інтеграції в ці більш загальні методи. Насправді, загальні методи можуть бути нездатними досягти практичного успіху без надання таких спеціальних засобів для аналізу та розробки заходів безпеки. Важливий результат – взаємодія двох потоків дослідження.

В даній роботі була досліджена формальна модель багаторівневої системи захисту інформації в якій якісне вираження та оцінки представлені *S*-нечіткими множинами, де значеннями функцій є нечіткі числа. Кількісні оцінки значень параметрів представлені нечіткими числами, які визначені на відповідних шкалах. Також досліджено формальне представлення семантики інформаційних описів механізмів захисту та загроз безпеки інформації.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. National Security Telecommunications and Information Systems Security. National Training Standard for Information Systems Security (Infosec) Professionals. 20 June 1994.
2. Microsoft. “C2 Evaluation and Certification for Windows NT (Q93362).” URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;93362. (Дата звернення: 10.03.2021)
3. Grance, T., Hash, J., and Stevens, M. Security Considerations in the Information System Development Life Cycle. NIST Special Publication 800-64, rev. 1. 15p.
4. В. Бондарев "Введение в информационную безопасность автоматизированных систем", 2016. 89 с.
5. Хорошко В. О. та ін. «Проєктування комплексних систем захисту інформації». 75 с.
6. Sean Smith. «The Internet of Risky Things: Trusting the Devices That Surround Us 1st Edition». 153 p.
7. John Rhoton. Cloud Computing Explained: Implementation Handbook for Enterprises Paperback, 2009. 67 p.
8. Cloud Computing. URL: https://cloudsecurityalliance.org/research/top-threats/ (дата звернення: 16.03.2021)
9. Thomas Erl. Cloud Computing: Concepts, Technology & Architecture (The Pearson Service Technology Series from Thomas Erl) 1st Edition. 114-135 p.
10. Kief Morris. Infrastructure as Code: Managing Servers in the Cloud. 73p.
11. Бурачок Р. А. «Телекомунікаційні системи передавання інформації. Методи кодування.» 56 p.
12. Simon H. The Structure of Ill-structured Problems.1973. 181-202 p.

13. Yager R. A foundation for a theory of possibility // J. of Cybernetics, 1980. Vol. 10. №. 1−3. P. 177−209.
14. Пытьев Ю. П. Возможность. Элементы теории и применения, Эдиториал УРСС, 2000. 237 с.
15. Zadeh L.A. Fuzzy Sets. Information and Control. 8 (1965). pp. 338-353.
16. Zadeh L.A. PRUF - A Meaning Representation Language for Natural Language // Intern J. of Man-Machine Studies, 1978. Vol.10. N4. P.395-399,451-460.
17. Дюбуа Д. Теория возможностей: приложения к представлению знаний в информатике, 1990. 237 с.
18. Чечкин А.В. Математическая информатика. М.: Наука. Гл. ред. физ.-мат. лит. 1991. 416 с.
19. Мурзин А.П., Бутусов И.В., Романов А.А. Адаптация системы защиты информации автоматизированных систем управления к нейтрализуемым угрозам // Приборы и системы. Управление, контроль, диагностика. Автоматизированные системы управления, 2017. №10. С. 1-7.
20. Комплексная защита информации. Анализ уязвимостей и оценка стойкости функций безопасности. URL: http://rpcnix.blogspot.ru/2012/04/1999.html. (Дата звернення 25.03.2021).
21. Сапкина Н. В. Свойства операций над нечеткими числами // Вестник ВГУ, серия: системный анализ и информационные технологии, 2013. № 1. С. 23-28.
22. Аньшин В.М., Демкин И.В., Царьков И.Н., Никонов И.М. Применение теории нечётких множеств к задаче формирования портфеля проектов (теория возможностей). 73 с.
23. Нечеткие множества в моделях управления и искусственного интеллекта / Под ред. Д. А. Поспелова. М.: Наука. Гл. ред. физ.-мат. лит., 1986. 312 с.

24. Сапкина Н. В. Свойства операций над нечеткими числами // Вестник ВГУ, серия: системный анализ и информационные технологии, 2013. № 1. С. 23-28.
25. Оладько В.С. Модель выбора рационального состава средств защиты в системе электронной коммерции. 47 с.
26. Нащекин П.А. Перспективы информатизации основных видов деятельности в государственной системе правовой информации //Приборы и системы. Управление, контроль, диагностика. Автоматизированные системы управления. 2020. № 5. с. 1-6.