Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий(магістерський)

Розробка моделі процесу керування вразливостями у складі комплексної системи захисту інформації
(тема)

Виконав:
студент 2 курсу, групи БДІРм-19-1
Поддубний В.О.
(прізвище, ініціали)

Спеціальності 125 Кібербезпека
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва освітньої програми)

Керівник доцент Сєвєрінов О.В.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Халімов Г.З.
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

Рівень вищої освіти другий(магістерський)

Спеціальність 125 Кібербезпека
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав кафедри _____
(підпис)
«___»_____ 20___р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові Поддубному Вадиму Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи *Розробка моделі процесу керування вразливостями у складі комплексної системи захисту інформації*
затверджена наказом по університету від "22" жовтня 2020 р. № 1413 СТ

2. Термін подання студентом роботи(проекту) 23.12. 2020 р.

3. Вихідні дані до роботи(проекту) серія міжнародних стандартів ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 27035

4. Зміст пояснювальної записки (перелік питань, що потрібно розробити)

4.1 Розглянути сучасну нормативну базу що надає рекомендації для керування вразливостями.

4.2 Розглянути систему оцінки ризику й прийняття рішень як складову частину процесу керування вразливостями в системах захисту інформації

4.3 Висунути вимоги до ситеми оцінки ризику й прийняття рішень

4.4 Розробити структуру й правила системи керування вразливостями.

4.5 Здійснити тестове використання створеної системи.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій *Презентаційний матеріал у вигляді слайдів*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів атестаційної роботи	Термін виконання етапів	Примітка
1	*Отримання завдання*	*09.09.20*	
2	*Аналіз літературних джерел за темою роботи*	*09.09.20 – 1.10.20*	
3.	*Аналіз сучасних моделей керування вразливостями*	*1.10.20 – 12.10.20*	
4.	*Розробка вимог до системи керування вразливостями*	*12.10.20 – 18.10.20*	
5.	*Розробка архітектури системи керування вразливостями*	*18.10.20 – 2.11.20*	
6.	*Розробка правил системи керування вразливостями*	*2.11.20 – 14.11.20*	
7.	*Тестове використання створеної системи*	*14.11.20 – 30.11.20*	
8.	*Усунення недоліків, що виявлені під час тесту*	*30.11.20 – 3.12.20*	
9.	*Оформлення пояснювальної записки*	*3.12.20 – 12.12.20*	
10.	*Представлення роботи на здачу*	*12.12.20 – 23.12.20*	

Дата видачі завдання ____. _____. 20__ р.

Студент _____
(підпис)

Керівник роботи (проекту) _____ доцент Сєвєрінов О.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до роботи містить 107 сторінок, 22 рисунків, 17 таблиць, 17 джерел.

ВРАЗЛИВІСТЬ, CVSS МЕНЕДЖМЕНТ ВРАЗЛИВОСТЕЙ, СУІБ, КСЗІ, ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 27035, РИЗИКИ.

Метою роботи є розробка моделі процесу керування вразливостями у складі комплексної системи захисту інформації.

Об’єкт дослідження – комлексна система захисту інформації.

Предмет дослідження – процеси керування вразливостями вразливостей у складі систем захисту інформації.

Відповідно до поставленої мети у роботі вирішуються наступні задачі:

1. Розгляд існуючої документації що надає рекомендації для керування вразливостями;

2. Розгляд процесу керування вразливостями у складі системи захисту інформації;

3. Розроблення архутектури системи оцінки ризику й прийняття рішень як складової частини процесу керування вразливостями у складі систем захисту інформації;

4. Розроблення правил для системи оцінки ризиків й прийняття рішень;

5. Тестове використання створеної системи оцінкуи ризиків й прийняття рішень.

ABSTRACT

The explanatory note contains: 107 pages, 22 figures, 17 tables, 17 references.

VULNERABILITY, CVSS VULNERABILITY MANAGEMENT, SWIB, KSZI, ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 27035, RISKS.

The purpose of the work is to develop a model of the vulnerability management process as part of a comprehensive information security system.

The object of research is a complex information protection system.

The subject of research – vulnerability management processes of vulnerabilities in information security systems.

In accordance with the goal in the work the following tasks are solved:

1. Review of existing documentation providing recommendations for vulnerability management;

2. Consideration of the process of vulnerability management as part of the information security system;

3. Development of the architecture of the risk assessment and decision-making system as part of the vulnerability management process in information security systems;

4. Development of rules for the risk assessment and decision-making system;

5. Test use of the created system of assessment of risks and decision-making.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

ІТС	–	Інформаційно-телекомунікаційна система
КСЗІ	–	Комплексна система захисту інформації
ПЕОМ	–	Персональна електронна обчислювальна машина
ПЗ	–	Програмне забезпечення
ПТК	–	Програмно-технічний комплекс
РМ	–	Робоче місце
СУІБ	–	Система управління інформаційною безпекою
CVSS	–	Common Vulnerability Scoring System
NVD	–	National Vulnerability Database

ВСТУП

Програмне забезпечення – це складова частина інформаційно-телекомунікаційної системи, проте під час розробки програмного забезпеченя виникають помилки, деякі помилки не несуть в собі небезпеки, а деякі становлять серйозну загрозу ІТС. Тому для забезпечення безпеки та працездатності ІТС важливо вести контроль за виявленням, усуненням та супроводженням вразливостей в програмному забезпечені.

Тому необхідно під час розробки та експлуатації системи здійснювати менеджмент вразливостей, який регламентує яким чином виявляти вразливості, реагувати на тих та встановлює відповідальність за процеси менеджменту.

Однією із частин менеджменту вразливостей є оцінка ризиків, така оцінка необхідна для вибору рішень щодо реакції на певну вразливість. Такими рішеннями може бути: оновлення програмного забезпечення, прийняття ризику, здійснення додаткових налаштувань, ручне усунення або виправлення, зменшення бізнес процесу тощо.

Проте слід зауважити, що хоча це досить важливий і необхідний процес, в Україні не існує вимог чи настанов які зобов’язують чи допомагають організаціям в веденні такого менеджменту. Наслідки такого відношення можуть сприяти різноманітним кіберінцидентам, що несуть збитки бізнес процесам компаній.

Тому управління вразливостями є необхідним процесом, що не виключить вразливості в ПЗ, проте пом’якшить або усуне наслідки від їх наявності.

Слід зауважити що в останні роки кількість знайдених вразливостей невпинно зростає, підставляючи під більшу небезпеку все більше програмних засобів та систем в цілому.

Обробку інформації, та прийняття рішень покладено на адміністраторів, які хоч і використовують сканери для виявлення цих вразливостей проте вимушені здійснювати оцінювання ситуації виходячи зі своїх знань та досвіду.

Такий підхід збільшує кількість помилок та створює неоднозначність трактування результатів. Також це підвищує вимоги до персоналу, та час адаптації, адже новим адміністраторам необхідно знати добре структуру, склад особливості функціонування системи.

В даний час існують лише гармонізовані стандарти (такі як ISO/IEC 27035 [1], ISO/IEC 27005 [2], ISO/IEC 27001 [3] та інші), які надають вказівки щодо контролю вразливостей у СУІБ. Також існують додаткові методики такі як «Implementing a Vulnerability Management Process. SANS Institute Information Security Reading Room» [4] проте ні вони, ні гармонізовані стандарти не надають чітких інструкцій щодо оцінювання ризиків. Ці стандарти та методики мають загальний рекомендований характер. В то час Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 269 "Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації" [5] встановлює як вимогу наявність у кваліфікованого надавача електронних довірчих послуг процедур з управління ризиками, персоналом, операційною безпекою, інцидентами. Процес гармонізації та внесення коректив в законодавчу базу показує рух України в даному напрямку. Розроблення, інтеграція, перехід та введення в дію нових вимог, стандартів, правил займе деякий час, проте вже зараз можна сказати, що даний процес вже запущений. Тому менеджмент вразливостей через деякий час стане не додатковим інструментом, а важливою необхідністю.

Однією із форм такого менеджменту є введення його в політику безпеки. Така політика повинна відповідати на ряд питань, а саме: яким чином виявляти вразливості, яким чином оцінювати ризики, як реагувати на

вразливості, які дії повинні виконати адміністратор безпеки та аудиту, системний адміністратор, управління [6].

Метою роботи є розробка моделі процесу керування вразливостями у складі комплексної системи захисту інформації.

Об’єкт дослідження – комлексна система захисту інформації.

Предмет дослідження – процеси керування вразливостями вразливостей у складі систем захисту інформації.

1. ВРАЗЛИВОСТІ

1.1 Походження та розповсюдження

Під час розробки програмного забезпечення жодний розробник не може гарантувати відсутність вразливостей в його продукті. Неважливо який це продукт, це може бути браузер (як приклад вразливість CVE-2020-6557), BIOS (як приклад вразливість CVE-2020-5388), чи програма інсталювання (як приклад вразливість CVE-2020-12304). Також вразливості можуть виникнути в наслідок ненадійних паролів, алгоритмів, непродуманості архітектури ПЗ, або в наслідок спеціальної взаємодії (шкідливих програм, SQL-ін’єкцій, тощо).

Проте слід зауважити що не завжди помилки в програмному коді виникають випадково, іноді розробники ПЗ (або окремі працівники) залишають спеціальні люки (trap door) – недокументовані функції, використання яких дозволяє обминути механізми захисту.

Деякі вразливості можливі лише теоретично, деякі обгрунтовані концептуально а інші мають код шкідливої програми яка може використати дану вразливість для атаки. Такі програми називають експлойтами (англ.-exploit).

Незважаючи на використання нових технологій розробки, автоматизації, контролю (таких як аналізатори програмного коду) кількість вразливостей щорічно збільшується.

Вразливості використовують для кібератак різним чином так наприклад одні з найбільших кібератак в Україні (WannaCry і Petya) були здійснені через використання вразливостей протоколу SMB [7].

Для контролю вразливостей необхідно збирати, обробляти, розповсюджувати інформацію про вразливості, що виникли. Для таких цілей існує безліч баз данних вразливостей, які містять необхідну інформацію. Найбільш розповсюдженні й авторитетні бази данних це: CVE [8], CERT

Vulnerability Notes Database [9], National Vulnerability Database [10]. В подальшому будуть приведені данні в більшості з бази данних National Vulnerability Database(або NVD).

NVD – це база данних уряду США стандартизованих даних управління вразливістю, представлених за допомогою протоколу автоматизації вмісту безпеки (SCAP). Ці дані дозволяють автоматизувати управління уразливістю, безпекою та відповідність вимогам. NVD включає бази даних посилань на контрольний список безпеки, недоліки програмного забезпечення, пов'язані з безпекою, неправильні конфігурації, назви продуктів та показники впливу.

Спочатку створена у 2000 році (як інструментарій категоризації атак або ICAT), NVD пройшла безліч ітерацій та вдосконалень, і надалі буде робити це для надання своїх послуг. NVD є продуктом відділу комп'ютерної безпеки NIST, лабораторії інформаційних технологій, і фінансується агентством безпеки кібербезпеки та інфраструктури.

NVD виконує аналіз CVE, які були опубліковані у словнику CVE. Співробітникам NVD доручається аналіз CVE шляхом агрегування точок даних з опису, наданих посилань та будь-яких додаткових даних, які на той час можуть бути загальнодоступними. Цей аналіз призводить до метрик впливу вразливості (з використанням Common Vulnerability Scoring System яка описана нижче), типів вразливості (Common Weakness Enumeration та заяв про використання (Common Platform Enumeration), а також інших відповідних метаданих.

NVD не проводить активного тестування на вразливість, покладаючись на постачальників, сторонніх дослідників безпеки та координаторів вразливості, щоб надати інформацію, яка потім використовується для призначення цих атрибутів. Коли додаткова інформація стає доступною, оцінки CVSS, CWE та заяви про застосовність можуть бути змінені. NVD намагається повторно проаналізувати CVE, до яких було внесено зміни, оскільки час і ресурси дозволяють забезпечити актуальність запропонованої інформації.

Згідно базою вразливостей NVD в останні роки кількість виявлених вразливостей в два-три рази перевищує аналогічні показники 2013-2016х років (Рис. 1.1).

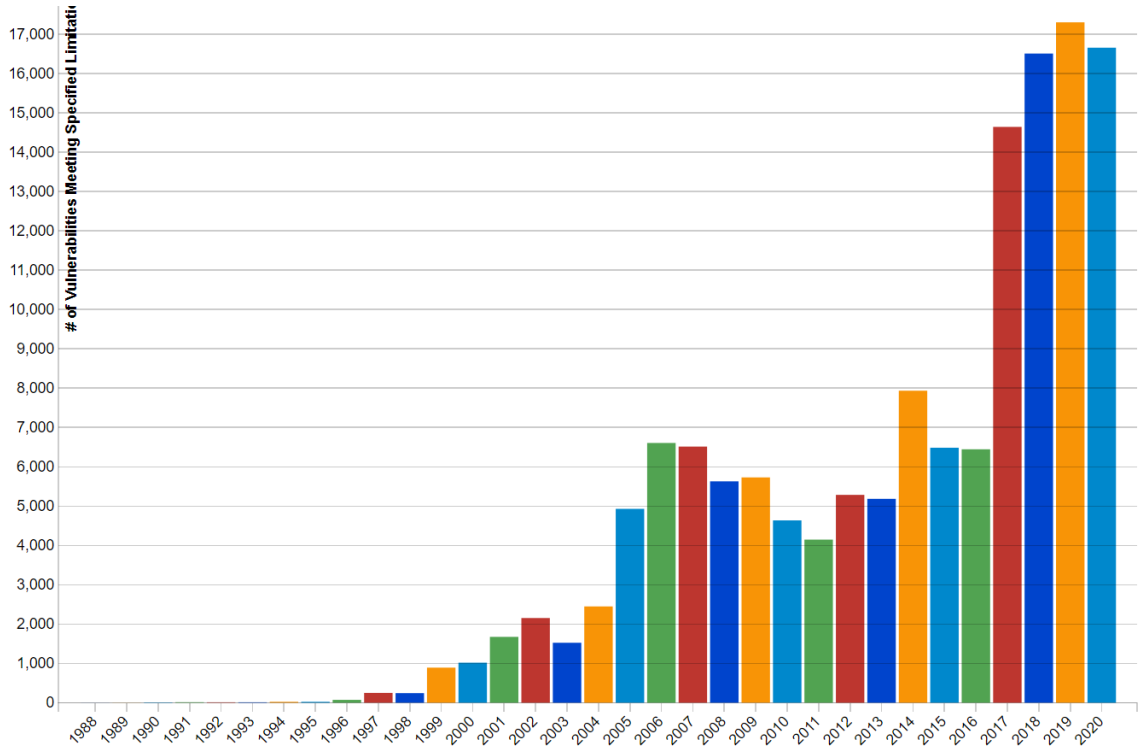

Рисунок 1.1 – Кількість вразливостей бази NVD щорічно

Такий ріст пов’язаний з розповсюдженням інформаційних технологій в все більші сфери життя, ускладненням програмних засобів, підтримкою застарілих архітектур, підтримкою зворотної сувмістимості програм та систем, створенням нових архітектур, протоколів, тощо.

Найбільш підвержені вразливостям складні системи, підтримка, модернізація та оновлення яких здійснюється протягом багатьох років. Згідно звіту AlienVault [11] про інтернет загрози за 2017 рік в топ-10 експлойтів переважають експлойти орієнтовані на вразливості в Windows и Microsoft Office.

Лише за 2019й рік для Windows (Рис. 1.2) та Microsoft Office (Рис. 1.3.) було виявлено 935 та 46 нових вразливостей відповідно.

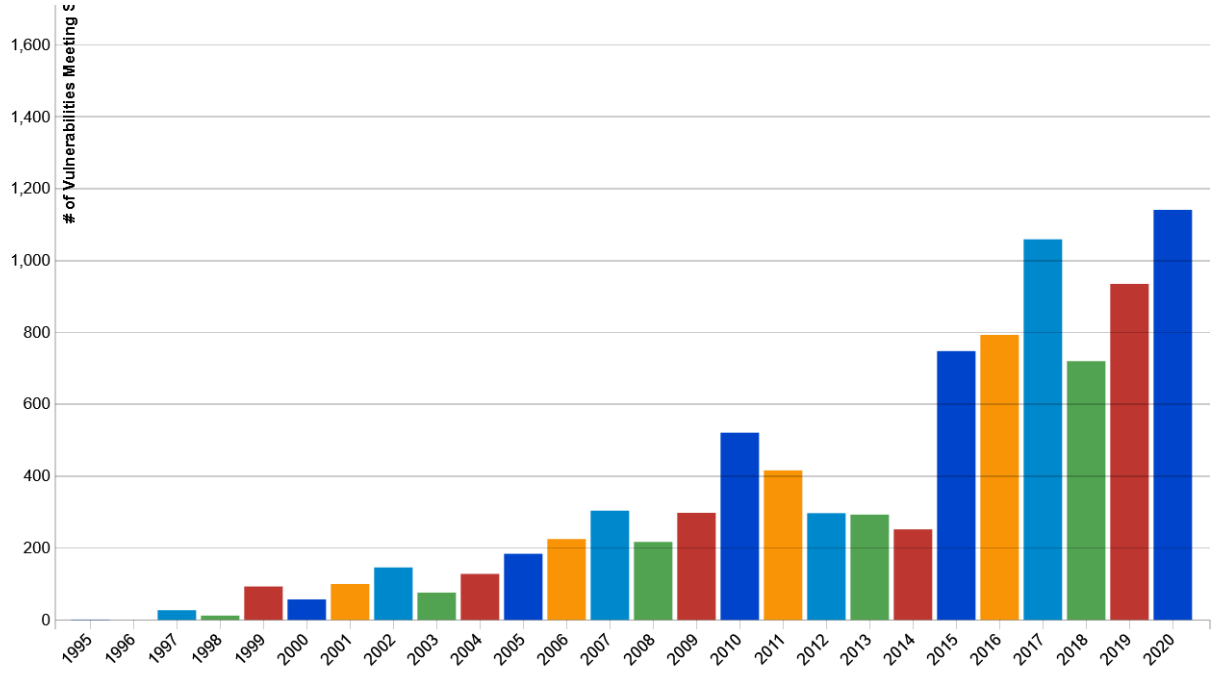

Рисунок 1.2 – Кількість виявлених вразливостей Windows відповідно до років

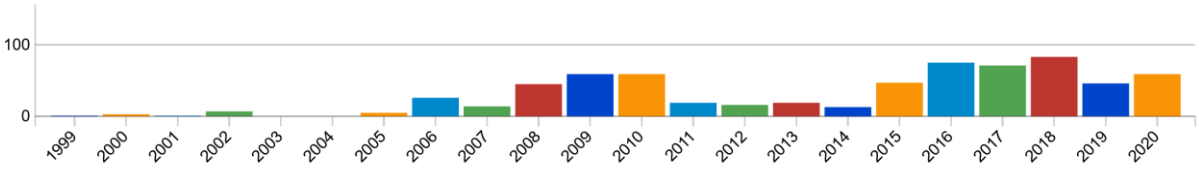

Рисунок 1.3 – Кількість виявлених вразливостей Microsoft Office відповідно до років

Такий результат закономірний зважаючи на розповсюдженість даних ПЗ, складність, та значний «багаж» модулів коду старіших версій ПЗ.

Вразливостям підвернені також open-source програми. Так наприклад за 2019 рік в операційній системі Linux виявили 459 нових вразливостей (Рис. 1.4). Під ОС Linux мається на увазі ядро ОС, кількість вразливостей для різних дистрибутивів ще більша, так наприклад, для одного з найпопулярніших дистрибутивів Ubuntu за 2019 рік було виявлено 992 вразливості (Рис. 1.5)

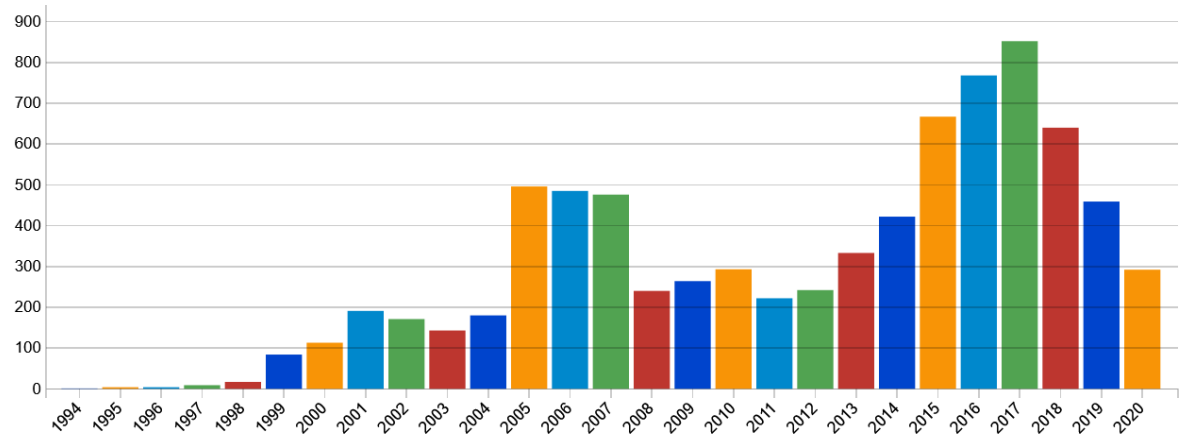

Рисунок. 1.4 – Кількість виявлених вразливостей Linux відповідно до років

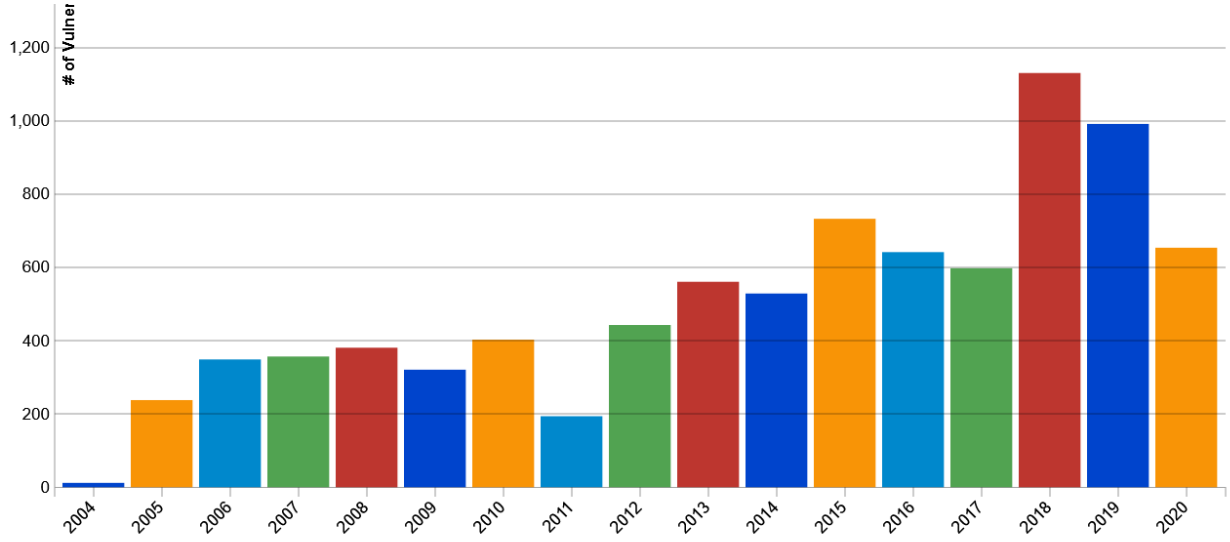

Рисунок 1.5 – Кількість виявлених вразливостей Ubuntu відповідно до років

Як помітно з графіків, за останні роки кількість виявлених вразливостей значно виросла, й навіть в добре вивченому та дослідженому ядрі Linux знаходять нові й нові вразливості.

Але слід зауважити що кількість нових атак не прямо пропорційна кількості виявлених вразливостей, серед вразливостей що часто експлуатуються можуть бути вразливості, виявлені в 2015, 2013, або навіть в 2010 році.

Однією з категорій вразливостей є так звані вразливості нульового дня.

Вразливість нульового дня (англ. Zero-day або 0day) — вразливість програмного забезпечення, яка ще невідома користувачам чи розробникам програмного забезпечення та проти якої ще не розроблені механізми захисту [12]. Сам термін означає, що у розробників було 0 днів на виправлення дефекту: уразливість або атака стає публічно відомою до моменту випуску виробником ПО для виправлення помилок (тобто потенційно уразливість може експлуатуватися на робочих копіях програми без можливості захищатися від неї).

Так наприклад згідно Cybersecurity Help s.r.o. за період з 6.11.2020 по 12.11.2020 знайдено 401 нова вразливість, із 27 все ще не мають виправлень(Рис. 1.6) [13].

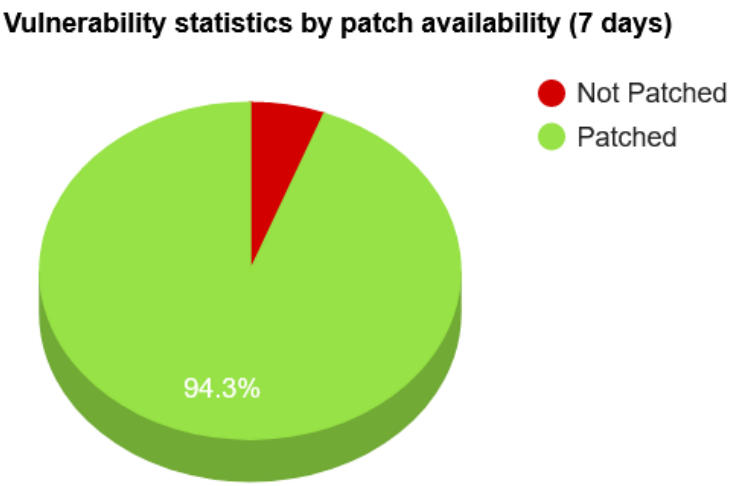

Рисунок 1.6 – Кількість вразливостей за період з 6.11.2020 по 12.11.2020 що все ще не мають виправлення

Такі вразливості потребують відповідних дій для пом’якшення або усунення результатів теоретичної атаки з використанням експлойту вразливості.

1.2 Якісне оцінювання вразливостей за допомогою CVSS

Як можна помітити, не всі вразливості однаково небезпечні для системи, також кожна вразливість може мати виправлення або ні, взаємодіяти на різні компоненти, нести шкоду різними шляхами, тощо. Для оцінювання вразливостей використовують декілька систем оцінки, наприклад однією із найрозповсюдженіших є вже згадувана загальна система оцінки вразливостей (CVSS).

Загальна система оцінювання вразливості фіксує основні технічні характеристики програмних, технічних та програмно-технічних вразливостей. Результати включають числові показники, які показують серйозність вразливості відносно інших вразливостей.

CVSS складається з трьох основних метричних груп, це: базов, часова, та метрика середовища.

Базовий показник відображає якость вразливості відповідно до її внутрішніх характеристик, які є постійними в часі, під час оцінювання передбачається найгірший вплив у різних розгорнутих середовищах

Часові метрики регулюють базовий показник вразливості на основі факторів, які змінюються з часом, наприклад, наявності експлойтів які використовують дану вразливість.

Показники середовища змінюють базові та часові показники для конкретного обчислювального середовища. Вони розглядають такі фактори, як наявність пом'якшення наслідків у цьому середовищі.

Базові оцінки зазвичай виробляються організацією, що підтримує продукт з вразливістю, або третьою стороною від її імені.

Це типово для публікації лише базових оцінок, оскільки вони не змінюються з часом і є загальними для всіх середовищ

Споживачі CVSS повинні доповнити базовий показник часовими та показниками оточення, характерними для використання вразливого продукту, щоб створити точнішу оцінку для їх середовища.

Споживачі можуть використовувати інформацію CVSS як вклад у процес управління організаційною вразливістю, який також враховує фактори, які не є частиною CVSS, щоб класифікувати загрози для їх технологічної інфраструктури та приймати обґрунтовані рішення.

Такими факторами можуть бути: кількість клієнтів на товарній лінійці, грошові втрати через порушення, загроза життю чи майну, або громадські настрої щодо вразливих місць. Вони виходять за рамки CVSS. На рисунку 1.7 наведено набір показників для кожної метричної групи CVSS.

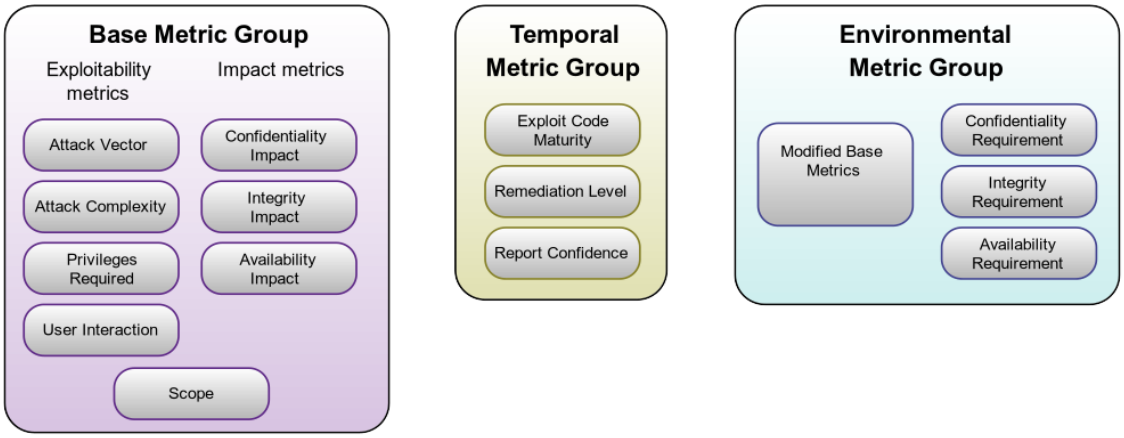

Рисунок 1.7 – Метричні групи CVSS

Коли аналітиком призначаються бали базовим показникам, базове рівняння обчислює бал, що становить від 0,0 до 10,0, як показано на рисунку 1.8.

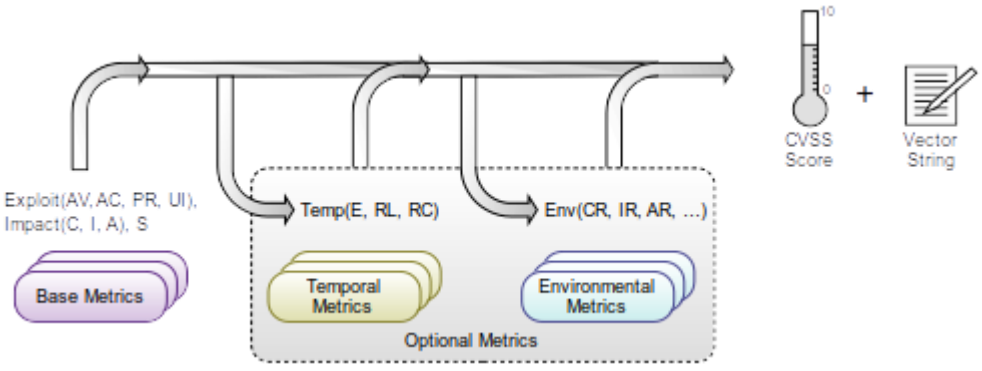

Рис. 1.8 – Метрики та рівняння CVSS

Зокрема, рівняння базової метрики виводиться з двох підрівнянь: підрівнювання підрахунку експлуатаційної здатності та рівняння підрахунку впливу.

Базовий показник може бути уточнений шляхом огляду тимчасових та метрик середовища, щоб більш точно відобразити відносну шкоду, спричинену вразливістю для оточуючого середовища в конкретний момент часу. Оцінювання часових та показників середовища не потрібно, але рекомендується для більш точних оцінок.

Як правило, базові та часові показники визначаються аналітиками бюлетенів уразливості, постачальниками продуктів безпеки або постачальниками додатків, оскільки вони, як правило, мають найбільш точну інформацію про характеристики вразливості.

Показники середовища визначені організаціями кінцевих споживачів, оскільки вони найкраще можуть оцінити потенційний вплив вразливості в їхньому власному обчислювальному середовищі.

Оцінювання показників CVSS також включає створення векторного рядка, текстового подання значень метрики, використаних для оцінки вразливості. Цей векторний рядок - це спеціально відформатований текстовий рядок, який містить кожне значення, присвоєне кожній метриці, і завжди повинен відображатися разом із оцінкою вразливості.

Слід зауважити, що всі показники повинні бути оцінені з урахуванням того, що зловмисник вже виявив і визначив уразливість. Тобто аналітику не потрібно враховувати засоби, за допомогою яких була виявлена вразливість. Крім того, цілком ймовірно, що багато різних типів людей будуть оцінювати вразливості (наприклад, постачальники програмного забезпечення, аналітики бюлетенів уразливості, постачальники продуктів безпеки), оцінка балів уразливості повинна бути незалежною для особистості та їх організації.

Як вже було сказано раніше, метрики експлуатації відображають характеристики вразливої речі, формально називають вразливим

компонентом. Тому кожен із перелічених нижче показників експлуатації повинен бути оцінений щодо вразливого компонента та відображати якості вразливості, що призводять до успішної атаки.

Оцінюючи базові показники, слід вважати, що зловмисник досконало знає слабкі сторони цільової системи, включаючи загальну конфігурацію та механізми захисту за замовчуванням (наприклад, вбудовані брандмауери, обмеження трафіку, правила маршрутизації). Наприклад, використання вразливості, що призводить до повторюваного, детермінованого успіху, слід вважати низьким значенням для складності атаки, незалежно від знань та можливостей зловмисника. Крім того, цільове зменшення атаки (наприклад, спеціальні фільтри брандмауера, списки доступу) повинно відображатись у групі оцінок показників середовища.

Конкретні конфігурації не повинні впливати на будь-який атрибут, що сприяє базовій шкалі CVSS, тобто, якщо для успішної атаки потрібна певна конфігурація, вразливий компонент повинен припускається, що вразлива річ знаходиться в цій конфігурації.

До переваг CVSS можна віднести стандартизовану методологію оцінювання вразливості для постачальників та платформ. Це відкрита структура, що забезпечує прозорість індивідуальних характеристик та методології, використовуваної для отримання оцінки.

На виході оцінювання CVSS отримується вектор вразливості, що описує вразливість згідно метрики CVSS та якісний бал від 0,0 до 10,0. В деяких випадках використовують ступінь враженості вразливості (Таблиця 1).

Таблиця 1.1 – Відповідність балам CVSS та ступеням враженості вразливості.

Серйозність	CVSS бал
Відсутня	0,0

Продовження таблиці 1.1

Низька	0,1-3,9
Середня	4,0-6,9
Висока	7,0-8,9
Критична	9,0-10

Наприклад, базовий показник CVSS 4,0 має відповідний ступінь вираженості середнього рівня. Використання цих якісних оцінок суворості не є обов'язковим, і немає необхідності включати їх при публікації балів CVSS. Вони покликані допомогти організаціям належним чином оцінити та визначити пріоритетними процеси управління ними [14].

Приклад використання CVSS показано на рисунку 1.8.

Рисунок 1.8 – Приклад використання CVSS

В даному випадку вразливість CVE-2019-3689, в ПЗ SUSE Linux Enterprise Server 12 має оцінку 9.8(Критична). Слід зауважити що аналітики NVD використовують загальнодоступну інформацію для асоціювання векторних рядків та оцінок CVSS. NVD також відображає будь-яку інформацію CVSS, надану в списку CVE від CNA.

Тому як можливо помітити, оцінка NVD CVSS не збігається з CNA(CVE Numbering Authorities). Найбільш поширеною причиною таких розходжень є те, що загальнодоступна інформація не забезпечує достатньої

деталізації або що інформація просто не була доступною на момент присвоєння векторного рядка CVSS.

Також слід зауважити, що опис вище актуальний для останньої версії CVSS 3.1, проте в деяких системах інколи все ще використовують CVSS версії 2.0.

1.3 Метрики експлуатації CVSS

Як вже було сказано раніше, метрики експлуатації відображають характеристики вразливої речі, формально називають вразливим компонентом. Тому кожен із перелічених нижче показників експлуатації повинен бути оцінений щодо вразливого компонента та відображати якості вразливості, що призводять до успішної атаки.

Оцінюючи базові показники, слід вважати, що зловмисник досконало знає слабкі сторони цільової системи, включаючи загальну конфігурацію та механізми захисту за замовчуванням (наприклад, вбудовані брандмауери, обмеження трафіку, правила маршрутизації). Наприклад, використання вразливості, що призводить до повторюваного, детермінованого успіху, слід вважати низьким значенням для складності атаки, незалежно від знань та можливостей зловмисника. Крім того, цільове зменшення атаки (наприклад, спеціальні фільтри брандмауера, списки доступу) повинно відображатись у групі оцінок показників середовища.

Конкретні конфігурації не повинні впливати на будь-який атрибут, що сприяє базовій шкалі CVSS, тобто, якщо для успішної атаки потрібна певна конфігурація, вразливий компонент повинен припускається, що вразлива річ знаходиться в цій конфігурації.

1.3.1 Вектор Атаки (AV)

Цей показник відображає контекст, за допомогою якого можлива експлуатація вразливості. Це метричне значення (а отже, і базовий показник)

більше , якщо зловмисник кий має можливість використовувати вразливий компонент буде більш віддалений (логічно та фізично).

Припущення полягає в тому, що кількість потенційних зловмисників на вразливість, яку можна використовувати з усієї мережі, більше, ніж кількість потенційних зловмисників, які могли б використати вразливість, що вимагає фізичного доступу до пристрою. Тому віддалене використання вразливості має більшу бальну оцінку. Перелік можливих значень представлений у таблиці 1.2.

Таблиця 1.2 – Вектор атаки

Значення показника	Опис
Мережевий (N)	Вразливий компонент пов'язаний з мережевим стеком, набір можливих зловмисників виходить за межі інших перелічених нижче варіантів, аж до всього Інтернету. Таку вразливість часто називають "віддаленою експлуатацією", і її можна розглядати як атаку, яка може бути використана на рівні протоколуза один або більше мережевих переходів (наприклад, через один або кілька маршрутизаторів). Прикладом мережевої атаки є зловмисник, який викликає відмову в обслуговуванні(DoS), надсилаючи спеціально створений пакет TCP по всій мережі мережі (наприклад, CVE-2004-0230).
Сусідній (A)	Вразливий компонент пов'язаний з мережевим стеком, але атака на рівні протоколу обмежена логічно сусідньою топологією. Це може означати, що атаку потрібно запускати з тієї самої загальної фізичної або логічної або зсередини захищеного або обмеженого адміністративним доменом. Одним із прикладів сусідньої атаки може бути потоп ARP (IP4) або відкриття сусіда (IP6), що призводить до відмови в обслуговуванні в локальному сегменті локальної мережі.

Продовження таблиці 1.2

Локальний (L)	Уразливий компонент не пов'язаний з мережевим стеком, і шлях зловмисника здійснюється за допомогою функції читання / запису / виконання. Або: зловмисник використовує вразливість, отримуючи доступ до цільової системи локально (наприклад, клавіатура, консоль) або віддалено (наприклад, SSH); або зловмисник покладається на взаємодію користувачів з іншою особою, щоб виконувати дії, необхідні для використання вразливості (наприклад, використовуючи методи соціальної інженерії, щоб обманути законного користувача на відкриття шкідливого документа).
Фізичний (P)	Напад вимагає від зловмисника фізично взаємодіяти або маніпулювати вразливим компонентом. Фізична взаємодія може бути короткою (наприклад, напад покоївки (напад на пристосований без нагляду пристрій, в якому зловмисник із фізичним доступом змінює його якимось невиразним способом, щоб згодом отримати доступ до пристрою чи даних на ньому)) або постійною. Прикладом такої атаки є атака холодного завантаження, при якій зловмисник отримує доступ до ключів шифрування диска після фізичного доступу до цільової системи. Інші приклади включають периферійні атаки через доступ до FireWire / USB Direct Memory (DMA).

Посібник з підрахунку балів: Мережу слід використовувати, навіть якщо зловмисник зобов'язаний знаходитися в одній інтрамережі для використання вразливої системи (наприклад, зловмисник може використовувати вразливість лише з внутрішньої корпоративної мережі).

1.3.2 Складність атаки (AC)

Цей показник описує умови поза контролем зловмисника, які повинні існувати, щоб використовувати вразливість. Як описано нижче, такі умови можуть вимагати збору більше інформації про ціль або обчислень. Важливо, що оцінка цього показника виключає будь-які вимоги щодо взаємодії користувачів з метою використання вразливості (такі умови відображаються в метриці взаємодії користувача). Якщо для успіху атаки потрібна певна конфігурація, слід брати показники Бази, припускаючи, що вразливий компонент в даній конфігурації. Базова оцінка найбільша для найменш складних атак. Перелік можливих значень представлений у таблиці 1.3.

Таблиця 1.3 – Складність атаки

Значення показника	Опис
Низький (L)	Спеціалізованих умов доступу чи пом'якшуючих обставин не існує. Зловмисник може очікувати повторного успіху при нападі на вразливий компонент.
Високий (H)	Вдалий напад залежить від умов, що не знаходяться під контролем нападника. Тобто, успішна атака не може бути здійснена за власним бажанням, але вимагає, щоб зловмисник вклав певну кількість вимірюваних зусиль для підготовки або виконання атаки вразливого компонента, перш ніж можна очікувати успішної атаки. Наприклад, успішна атака може залежати від того, чи подолає зловмисник будь-яку з наступних умов: - зловмисник повинен зібрати знання про середовище, в якому існує вразлива річ. Наприклад, збирати деталі про цільові налаштування конфігурації, порядкові номери або загальні секрети.

Продовження таблиці 1.3

Високий (H)	- зловмисник повинен підготувати цільове середовище для підвищення надійності експлуатації. Наприклад, неодноразова експлуатація для перемоги в умовах гонки або подолання передових методів пом'якшення експлуатації. - зловмисник повинен підключати себе в логічний мережевий шлях між ціллю та ресурсом, який взаємодіє з річчю що атакується , щоб прочитати та / або змінити мережеві комунікації (наприклад, людина, що знаходиться в середній атаці).

1.3.3 Потрібні привілеї (PR)

Цей показник описує рівень привілеїв, яким повинен володіти зловмисник, перш ніж успішно використовувати вразливість. Базова оцінка найкраща, якщо привілеї не потрібні. Перелік можливих значень представлений у таблиці 1.4.

Таблиця 1.4 – Потрібні привілеї

Значення показника	Опис
Відсутній (N)	Перед атакою зловмисник несанкціонований, тому не потребує доступу до налаштувань або файлів вразливої системи для здійснення атаки.
Низький (L)	Зловмиснику потрібні привілеї, які надають основні можливості користувача(можливий вплив лише на налаштування та файли, що належать користувачеві). Крім того, зловмисник з низькими привілеями має можливість отримувати доступ лише до нечутливих ресурсів.

Продовження таблиці 1.4

Високий (H)	Зловмиснику потрібні привілеї, які забезпечують значний (наприклад, адміністративний) контроль над вразливим компонентом, що дозволяє отримати доступ до налаштувань і файлів, що мають загальний компонент.

Посібник з підрахунку балів: Потрібні привілеї, як правило, відсутні для жорстко кодованих уразливих даних або вразливостей, що потребують соціальної інженерії (наприклад, відбиття сценаріїв на різних веб-сайтах, підроблення запиту на веб-сайті або вразливість розбору файлів у читачі PDF).

1.3.4 Взаємодія користувача (UI)

Цей показник фіксує вимогу до участі користувача, який не є зловмисником, в успішній атаці вразливого компонента. Цей показник визначає, чи може вразливість експлуатуватися виключно за бажанням зловмисника, чи в ньому повинен якось брати участь окремий користувач (або ініційований користувачем процес). Базова оцінка найкраща, коли взаємодія з користувачем не потрібна. Перелік можливих значень представлений у таблиці 1.5

Таблиця 1.5 – Взаємодія користувача

Значення показника	Опис
Відсутній (N)	Уразлива система може бути атакована без взаємодії з будь-яким користувачем.

Продовження таблиці 1.5

Необхідний (R)	Успішна експлуатація цієї вразливості вимагає від користувача певних дій перед тим, як вразливість може бути використана. Наприклад, успішна експлуатація може бути можливою лише під час встановлення програми системним адміністратором.

1.3.5 Масштабність (S)

В метриці масштабності відображається, чи впливає вразливість одного вразливого компонента на ресурси компонентів, що не входять до сфери його безпеки.

Формально орган безпеки (*security authority*) – це механізм (наприклад, додаток, операційна система, вбудоване програмне забезпечення, середовище з пісочницею), який визначає та застосовує контроль доступу з точки зору того, як певні суб'єкти / учасники (наприклад, користувачі, процеси) можуть отримати доступ до певних обмежених об'єктів / ресурсів (наприклад, файли, час процесору, пам'ять) контрольованим чином. Усі суб'єкти та об'єкти, що знаходяться під юрисдикцією одного органу безпеки, вважаються такими, що належать до однієї сфери безпеки. Якщо вразливість компонента може вплинути на компонент, який знаходиться в іншому обсязі безпеки, ніж вразливий компонент, відбувається зміна сфери застосування. Коли вплив вразливості порушує межу безпеки / довіри та впливає на компоненти поза сферою безпеки, в якій знаходиться вразливий компонент, відбувається зміна сфери застосування.

Область безпеки компонента охоплює інші компоненти, які забезпечують функціональність виключно цього компонента, навіть якщо ці інші компоненти мають власні повноваження щодо безпеки. Наприклад, база даних, що використовується виключно однією програмою, вважається частиною сфери безпеки цього додатка, навіть якщо база даних має власні

органи безпеки, наприклад, механізм контролю доступу до записів бази даних на основі користувачів бази даних та пов'язаних з ними привілеїв.

Базова оцінка найбільша, коли відбувається зміна обсягу. Перелік можливих значень представлений у таблиці 1.6.

Таблиця 1.6 – Масштабність

Значення показника	Опис
Без змін (U)	Експлуатована вразливість може впливати лише на ресурси, якими керує той самий орган безпеки. У цьому випадку вразливий компонент та компонент, що зазнає впливу, або є однаковими, або управляються одним і тим же органом безпеки
Зі змінами (C)	Експлуатована вразливість може вплинути на ресурси, що перевищують сферу безпеки, якою керує орган безпеки вразливого компонента. У цьому випадку вразливий компонент та компонент, на який впливає вплив, різні органи управління та керуються ними

1.4 Метрики випливу CVSS

Показники впливу фіксують наслідки успішно експлуатованої вразливості на компонент, який страждає від найгіршого результату, найбільш безпосередньо і передбачувано пов'язаний з атакою. Аналітики повинні стримувати вплив до розумного, остаточного результату, в якому вони впевнені, що нападник здатний його досягти.

При оцінці показників впливу вразливості слід враховувати лише збільшення доступу, отриманих привілеїв чи інших негативних результатів в результаті успішної експлуатації. Наприклад, розглянемо вразливість, яка вимагає дозволу лише для читання, перш ніж мати можливість

використовувати вразливість. Після успішної експлуатації зловмисник підтримує той самий рівень доступу для читання і отримує доступ до запису. У цьому випадку слід оцінювати лише показник впливу цілісності, а показники конфіденційності та доступності повинні бути встановлені як Ні.

Слід зауважити, що при оцінці зміни дельти удару слід використовувати остаточний вплив. Наприклад, якщо зловмисник починає частковий доступ до інформації з обмеженим доступом (конфіденційність низька) і успішна експлуатація вразливості призводить до повної втрати конфіденційності (конфіденційність висока), то отриманий базовий показник CVSS повинен посилатися на метричне значення "кінцевої гри". (Висока конфіденційність).

Якщо зміни масштабу не відбулися, показники впливу повинні відображати вплив конфіденційності, цілісності та доступності для вразливого компонента. Однак якщо відбулася зміна сфери дії, то показники впливу повинні відображати вплив конфіденційності, цілісності та доступності як на вразливий компонент, так і на компонент, який впливає, залежно від того, який страждає від найважчого результату.

1.4.1 Конфіденційність (C)

Ця метрика вимірює вплив на конфіденційність інформаційних ресурсів, якими керує програмний компонент через успішно використану вразливість. Конфіденційність стосується обмеження доступу та розкриття інформації лише авторизованим користувачам, а також запобігання доступу або розголошення їх несанкціонованим. Базовий показник найбільший, коли втрати на уражений компонент найбільші. Перелік можливих значень представлений у таблиці 1.7.

Таблиця 1.7 – Конфіденційність

Значення показника	Опис
Високий(H)	Існує повна втрата конфіденційності, внаслідок чого всі ресурси в межах ураженого компонента передаються зловмиснику. Як альтернатива, отримується доступ лише до деякої інформації з обмеженим доступом, проте розкрита інформація надає прямий, серйозний вплив. Наприклад, зловмисник викрадає пароль адміністратора або приватні ключі шифрування веб-сервера
Низький(L)	Є певна втрата конфіденційності. Отримано доступ до деякої інформації з обмеженим доступом, але зловмисник не має контролю над тим, яка інформація отримана, або сума чи вид збитків обмежені. Розкриття інформації не спричиняє прямих, серйозних втрат для пошкодженого компонента
Відсутній(N)	Внутрішній компонент не втрачає конфіденційності

1.4.2 Цілісність (I)

Цей показник вимірює вплив на цілісність під час успішного використання вразливості. Цілісність відноситься до достовірності та правдивості інформації. Базовий показник найбільший, коли наслідки для ураженої складової найвищі. Перелік можливих значень представлений у таблиці 1.8.

Таблиця 1.8 – Цілісність

Значення показника	Опис
Високий(H)	Є повна втрата цілісності або повна втрата захисту. Наприклад, зловмисник здатний змінювати будь-які / всі файли, захищені компонентом який атакований. Або лише деякі файли можуть бути змінені, але шкідливі зміни можуть мати прямий, серйозний наслідок для ураженого компонента.
Низький(L)	Модифікація даних можлива, але зловмисник не має контролю над наслідком модифікації або кількість модифікацій обмежена. Модифікація даних не має прямого, серйозного впливу на компонент, що впливає.
Відсутній(N)	Внутрішній компонент не втрачає цілісності

1.4.3 Доступність (A)

Цей показник вимірює вплив на доступність компонента, внаслідок успішної експлуатації вразливості. В той час коли показники впливу конфіденційності та цілісності застосовуються до втрати конфіденційності або цілісності даних (наприклад, інформації, файлів), що використовуються компонентом впливу, цей показник стосується втрати доступності самого впливового компонента, наприклад, мережевої послуги (наприклад, веб, база даних, електронна пошта). Оскільки доступність стосується доступності інформаційних ресурсів, атаки, які споживають пропускну здатність мережі, цикли процесора або дисковий простір, впливають на доступність компонента, на який здійснюється вплив. Базовий показник найбільший, коли наслідки для ураженої складової найвищі. Перелік можливих значень представлений у таблиці 1.9.

Таблиця 1.9 – Доступність

Значення показника	Опис
Високий(H)	Відбувається повна втрата доступності, внаслідок чого зловмисник зможе повністю відмовити в доступі до ресурсів, на які впливає атакований компонент; ця втрата є або стійкою (поки зловмисник продовжує здійснювати атаку), або постійною (зберігається навіть після завершення атаки). Або зловмисник має можливість заперечувати деяку доступність, але втрата доступності є прямим, серйозним наслідком для ураженого компонента
Високий(H)	(наприклад, зловмисник не може порушити існуючі з'єднання, але може запобігти новим з'єднанням; зловмисник може неодноразово використовувати вразливість при цьому в кожному випадку успішної атаки просочується лише невеликий об'єм пам'яті, але після багаторазової експлуатації служба стає абсолютно недоступною).
Низький(L)	Продуктивність знижується або виникають перебої в наявності ресурсів. Навіть якщо можлива повторна експлуатація вразливості, зловмисник не має можливості повністю відмовити в наданні послуг законним користувачам. Ресурси в ураженому компоненті або частково доступні весь час, або повністю доступні лише деякий час, але в цілому немає прямих, серйозних наслідків для ураженого компонента.
Відсутній(N)	Внутрішній компонент не втрачає доступності

1.5 Часові метрики CVSS

Часові метрики вимірюють поточний стан методів експлуатації або доступності коду, наявність будь-яких виправлень або обхідних шляхів або впевненість в описі вразливості.

1.5.1 Наявність коду експлойту (E)

Цей показник вимірює ймовірність атаки вразливості і, як правило, ґрунтується на поточному стані експлуатаційних методів, наявності коду експлуатації або активній експлуатації "в дикому вигляді". Загальнодоступність простого у користуванні коду експлуатації збільшує кількість потенційних зловмисників, включаючи некваліфікованих, тим самим збільшуючи ступінь вираженості вразливості. Спочатку експлуатація в реальному світі може бути лише теоретичною. Публікація коду перевірки концепції, функціонального коду експлуатації або достатніх технічних деталей, необхідних для використання вразливості. Крім того, наявний код експлуатації може переходити від демонстрації підтвердження концепції до використання коду, який успішно використовує вразливість. У важких випадках він може доставлятись як корисне навантаження хробака чи вірусу на основі мережі або інших автоматизованих засобів атаки.

Перелік можливих значень представлений у таблиці 1.10. Чим легше можна використовувати вразливість, тим вище показник вразливості.

Таблиця 1.10 – Наявність коду експлойту

Значення показника	Опис
Не визначений (X)	Призначення цього значення вказує на недостатню інформацію для вибору одного з інших значень і не впливає на загальний часовий бал, тобто воно має такий же ефект на бал як присвоєння Високого

Продовження таблиці 1.10

Високий(H)	Функціональний автономний код існує або не потребує експлуатування (ручний тригер), деталі широко доступні. Код експлойту працює в будь-якій ситуації або активно доставляється за допомогою автономного агента (наприклад, хробака чи вірусу). Підключені до мережі системи, ймовірно, можуть зіткнутися з спробами сканування або експлуатації. Розробка експлуатування досягла рівня надійних, широко доступних, простих у використанні автоматизованих інструментів.
Функціональний (F)	Доступний функціональний код експлойту. Код працює в більшості ситуацій, коли існує вразливість
Доведена концепція (P)	Доступна концепція коду експлойту, або демонстрація атаки не є практичною для більшості систем. Код або техніка не функціонують у всіх ситуаціях і можуть потребувати значних змін з боку кваліфікованого зловмисника.
Недоведений (U)	Немає кодуексплойту, або експлуатація теоретична.

1.5.2 Рівень виправлення (RL)

Рівень виправлення вразливості є важливим фактором пріоритетності. Типова вразливість не виправлена при первинному опублікуванні. Обхідні шляхи вирішення або виправлення можуть запропонувати тимчасове виправлення до отримання офіційного виправлення або оновлення. Кожен з цих відповідних етапів підганяє тимчасовій оцінці, відображаючи зменшення терміновості, до моменту коли виправлення стає остаточним. Перелік можливих значень представлений у таблиці 1.11. Чим менше офіційних та постійних виправлень, тим вище показник вразливості.

Таблиця 1.11 – Рівень виправлення

Значення показника	Опис
Не визначений (X)	Призначення цього значення вказує на недостатню інформацію для вибору одного з інших значень і не впливає на загальну часову оцінку, тобто воно має такий же ефект на оцінку, як і при призначенні Відсутній.
Відсутній (U)	Рішення відсутнє або його застосування неможливо.
Обхідний шлях (W)	Існує неофіційне рішення, що не є наданим постачальником. У деяких випадках постраждалі користувачі можуть створити власне виправлення або здійснять кроки для подолання чи іншим чином зменшення вразливості.
Тимчасове виправлення (T)	Існує офіційне, але тимчасове виправлення. Сюди відносять випадки, коли постачальник видає тимчасове виправлення, інструмент чи спосіб вирішення.
Офіційне виправлення (O)	Доступне повне рішення постачальника. Або постачальник надав офіційний патч, або оновлення.

1.5.3 Наявність вразливості(RC)

Цей показник вимірює ступінь впевненості у існуванні вразливості та достовірності відомих технічних деталей. Іноді оприлюднюється лише наявність уразливих місць, але без конкретних деталей. Наприклад, вплив може бути визнано небажаним, але першопричина може бути невідома. Пізніше вразливість може бути підтверджена дослідженнями, які підказують, де може знаходитися вразливість, хоча дослідження може бути непевним. Нарешті, вразливість може бути підтверджена через підтвердження автором

або продавцем технологій. Актуальність вразливості вище, коли відомо, що вразливість існує з певністю. Цей показник також підказує рівень технічних знань, доступних потенційним нападникам. Перелік можливих значень представлений у таблиці 1.12. Чим більше вразливість підтверджується продавцем або іншими авторитетними джерелами, тим вище бал.

Таблиця 1.12 – Наявність вразливості

Значення показника	Опис
Не визначений Not Defined (X)	Присвоєння цього значення вказує на недостатню інформацію для вибору одного з інших значень і не впливає на загальну часову оцінку, тобто воно має такий же ефект на оцінку, як і присвоєння підтверджений
Підтверджений Confirmed (C)	Детальні звіти існують, або можливе функціональне відтворення (функціональні експлойти можуть це забезпечити). Вихідний код доступний для незалежної перевірки тверджень дослідження, або автор або постачальник компоненту що атакується підтвердили наявність вразливості.
Обгрунтований Reasonable (R)	Опубліковані значні подробиці, але дослідники або не мають повної довіри до першопричини, або не мають доступу до вихідного коду, щоб повністю підтвердити всі взаємодії, які можуть призвести до результату. Однак існує обґрунтована впевненість у тому, що помилка відтворюється і принаймні один вплив може бути перевірений. Приклад - детальне написання дослідження вразливості з поясненням (можливо, затуманеним або «залишеним читачем»), що дає гарантії щодо відтворення результатів.

Продовження таблиці 1.12

Невідомий Unknown(U)	Є повідомлення про наслідки, які вказують на наявність вразливості. Звіти вказують на те, що причина вразливості невідома або звіти можуть відрізнятись від причини чи наслідків уразливості. Журналісти не впевнені в справжньому характері вразливості, і мало впевненості в обґрунтованості звітів або в тому, чи можна застосовувати статичний базовий показник з огляду на описані відмінності. Прикладом може слугувати звіт про помилку, в якому зазначається, що трапляється невпинна, але не відтворювана аварія, із свідченнями пошкодження пам’яті, що дозволяє припустити, що відмова в обслуговуванні чи можливі більш серйозні наслідки.

2. МЕНЕДЖМЕНТ ВРАЗЛИВОСТЕЙ

2.1 Принципи менеджменту вразливостей

Менеджмент вразливостей – це організаційний процес що існує як частина інформаційної безпеки, процесу контролю інцидентами інформаційної безпеки. Менеджмент вразливостей може бути складовою частиною системи управління інформаційною безпекою(далі – СУІБ), або комплексної безпеки захисту інформації(далі – КСЗІ). Основними задачами менеджменту є створення чітких правил, інструкцій, дій, щодо процесів виявлення, реагування, усунення, вразливостей.

Менеджмент створюється з метою зм’якшення або повного усунення впливу вразливості. Як складовою процесу є оцінка ризиків що виникають при наявності вразливості в інформаційній системі. Така оцінка необхідна для правильного розставлення пріоритетів та вибору дій(так наприклад оновлення ПЗ іноді підставляє систему під більший ризик ніж наявна вразливість).

Загалом менеджмент вразливостей повинен відповідати на такі питання:

- яким чином і якими засобами виявляти вразливості;
- яким чином реагувати на наявність конкретної вразливості в системі;
- чи є вразливість такою що потребує реакції чи вона створює такий ризик що може бути прийнятий;
- чи вартий ризик вразливості ризику оновлення;
- яким чином й кому здійснювати звіт щодо наявної вразливості, тощо.

2.2 Сучасна нормативна база

В даний момент існує декілька міжнародних стандартів, зводу практик, які допомагають в визначенні структури та параметрів менеджменту вразливостей.

Так в ISO/IEC 27001:2013 менеджмент вразливостей є невід'ємною частиною задачі управління інцидентами інформаційної безпеки і покращення. Метою даної задачі є гарантування поступового й більш результативного підходу до управління інцидентами інформаційної безпеки, включаючи інформування про події пов'язані з безпекою та вразливостями.

ISO/IEC 27001:2013 встановлює вимоги в кожній категорії процесу.

Обов'язки та процедури. Повинні бути встановлені обов'язки керівництва і процедури, щоб гарантувати швидку, результативну і належну відповідь на інциденти інформаційної безпеки.

Оповіщення про події, пов'язані з інформаційною безпекою. Оповіщення про події інформаційної безпеки повинно здійснюватися по відповідним каналам, як можна швидше.

Оповіщення про вразливості в інформаційній безпеці. Від працівників і найманих за контрактом працівників, які використовують інформаційну систему і сервіси організації, необхідно вимагати фіксування і доповідей про будь-які виявлені або вірогідні вразливості в інформаційній безпеці і сервісів.

Оцінка й вирішення подій інформаційної безпеки. Події інформаційної безпеки повинні спочатку бути оціненими, а після необхідно цього приймати рішення чи варто їх класифікувати як інцидент інформаційної безпеки.

Відповідні дії на інциденти інформаційної безпеки. Реагування на інциденти інформаційної безпеки повинно виконуватися в відповідності з задокументованими процедурами.

Винесення уроків із інцидентів інформаційної безпеки. Знання, отримані із аналізу і вирішення інцидентів інформаційної безпеки, повинні використовуватися в подальшому.

Збір свідоцтв. Організація повинна виділити і виконувати процедури для ідентифікації, збору, комплектування і збереження інформації, яка може бути використана в якості свідоцтв [3].

Як можна помітити ISO/IEC 27001 не встановлює чітких та суворих правил для процесу управління інцидентами, а сам менеджмент вразливостей не описаний окремим компонентом.

Більш детально принципи управління інцидентами встановлює стандарт ISO/IEC 27035. Даний стандарт формує архітектуру менеджменту, а саме розбиває його на частини: планування й підготовка, виявлення й звітність, оцінка й прийняття рішень, реагування та винесення уроків з даного інциденту(Рис. 2.1).

Також цей стандарт регламентує відповідальність різних працівників та підрозділів організації, надає приклади звітів, рекомедації щодо виявлення, тощо. Проте різні частини архітектури зачіпають інші стандарти. В самому документі є посилання на серії 27037, 27038, 27040, 27041, 27042, 27043, 27050, 30121 [2].

Аналогічно ISO/IEC 27035 звід практик «Implementing a Vulnerability Management Process. SANS Institute Information Security Reading Room» встановлює етапи й відповідальність за різні частини процесу менеджменту вразливостей. Крім того цей документ наводить приклади ПЗ (наприклад Nessus) які можуть використовуватися при здійснені менеджменту варазливостей.

Рисунок 2.1 – Етапи менеджменту вразливостей

Даний звіт практик також визначає етапи керування вразливістю в ІТС, проте він більш направлений на технічну частину менеджменту. Основними етапами згідно «Implementing a Vulnerability Management Process. SANS Institute Information Security Reading Room» є:

- підготовка;
- сканування на наявність вразливостей;
- визначення дій щодо виправлення;
- здійснення виправлення;

– повторне сканування.

Схематично ці етапи зображені на рисунку 2.2.

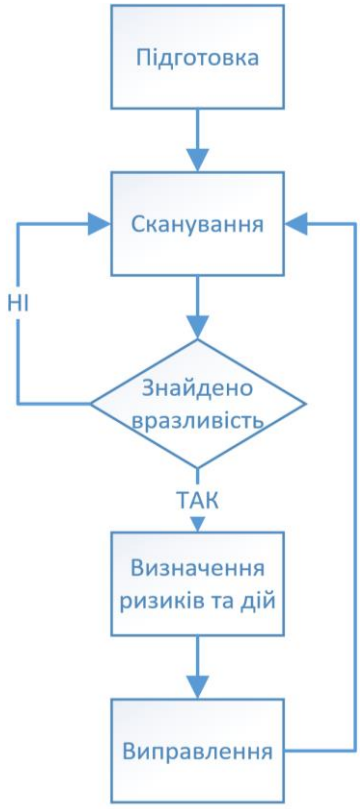

Рисунок 2.2 – Основні етапи менеджменту вразливостями згідно «Implementing a Vulnerability Management Process. SANS Institute Information Security Reading Room»

Крім того для менеджменту вразливостей можна використовувати й інші загальні стандарти в сфері інформаційної безпеки.

Так наприклад, як вже було сказано, одним із етапів управління вразливістю є оцінка ризиків пов’язаних з вразливостями. Даний етап майже не розкривається в ISO/IEC 27035, проте ISO/IEC-27005 встановлює методи та засоби менеджменту ризиками в інформаційній безпеці. В самому стандарті поняття вразливість використовується не лише для визначення вразливостей в ПЗ, це може бути вразливість технічного компоненту, організації робіт, налаштувань, фізичного середовища, тощо. Це пов’язано з однаковою природою різни вразливостей зі сторони оцінки ризику, адже

наявна вразливість не завдає шкоди сама по собі, так як необхідна наявність загрози, яка скористається нею. Вразливість, яка не має відповідної загрози, може не вимагати впровадження засобів контролю, але повинна усвідомлюватися і піддаватися моніторингу на предмет вимірювань.

Слід зазначити, що невірно реалізований або неправильно функціонуючий засіб контролю або засіб контролю, який неправильно використовується, сам може бути вразливістю.

Засіб контролю може бути ефективним чи неефективним в залежності від середовища, в якому воно функціонує. І навпаки, загроза, яка не має відповідної вразливості, може не призводити до ризику. Вразливості можуть бути пов'язані з властивостями активу, які можуть використовуватися способом і з метою, що відрізняються від тих, які планувалися під час придбання або створення активу. Вразливості, що виникають з різних джерел, підлягають розгляду, наприклад, ті які є зовнішніми або внутрішніми по відношенню до активу.

Основною задачею для менеджменту вразливостей під час оцінки ризику є: необхідність ідентифікувати вразливості, які можуть бути використані загрозами, щоб завдати шкоди активів або організації.

Як можна помітити стандарт ISO/IEC-27005 наголошує на необхідності правильної оцінки ризику кожної конкретної вразливості. Після такої оцінки, можна вибрати відповідні дії: зниження ризику, збереження ризику, уникнення ризику, перенос ризику.

Також існує стандарт ISO/IEC-27002, який є зводом норм та правилів менеджменту інформаційної безпеки. В даному стандарті є розділ посвячений вразливостям. Даний стандарт рекомендує постійно оновлювати та здійснювати повний опис активів, дані дії є передумовою ефективного менеджменту технічних вразливостей. Спеціальна інформація, що необхідна для підтримки менеджменту вразливостей, включає в себе інформацію про постачальника програмного забезпечення, номера версій, поточний стан розгортання (наприклад яке програмне забезпечення встановлено на яких

системах) і фахівцях, що відповідають в організації за програмне забезпечення.

Для створення ефективного процесу менеджменту щодо вразливостей необхідно виконувати наступні рекомендації:

1) в організації необхідно визначати і встановлювати ролі і обов'язки, пов'язані з менеджментом вразливостей, включаючи моніторинг вразливостей, оцінку ризику прояви вразливостей, виправлення програм (патчінга), стеження за активами і будь-які інші координуючі функції;

2) інформаційні ресурси, які будуть використовуватися для виявлення значимих вразливостей і забезпечення обізнаності про них, слід визначати для програмного забезпечення за іншою технологією на основі списку інвентаризації активів; ці інформаційні ресурси повинні оновлюватися слідом за змінами, що вносяться до опису, або коли знайдені інші нові або корисні ресурси;

3) необхідно визначити часові параметри реагування на повідомлення про потенційно значущі вразливості;

4) після виявлення потенційної вразливості організація повинна визначити пов'язані з нею ризики і дії, які необхідно зробити; такі дії можуть включати внесення виправлень в уразливі системи і (або) застосування інших заходів і засобів контролю та управління;

5) в залежності від того, наскільки терміново необхідно розглянути вразливість, дію слід здійснювати відповідно до заходів та засобів контролю і управління, пов'язаними з менеджментом змін, або слідуючи процедурам реагування на інциденти інформаційної безпеки;

6) якщо є можливість установки патчу, слід оцінити ризики, пов'язані з його встановленням (ризики, що створюються вразливістю, необхідно порівняти з ризиком установки патчу);

7) перед установкою патчі слід тестувати і оцінювати для забезпечення впевненості в тому, що вони є ефективними і не призводять до побічних

ефектів, які не можна допускати; якщо немає можливості встановити патч, слід розглянути інші заходи і засоби контролю і управління, наприклад:

– відключення сервісів, пов'язаних з уразливістю;

– адаптацію або додавання коштів управління доступом, наприклад міжмережевих екранів;

– посилений моніторинг для виявлення або запобігання реальних атак;

– підвищення обізнаності про уразливість;

8) в контрольний журнал слід вносити інформацію про всі зроблені процедури;

9) слід регулярно проводити моніторинг і оцінку процесу менеджменту вразливостей в цілях забезпечення впевненості в його ефективності та дієвості;

10) в першу чергу слід звертати увагу на системи з високим рівнем ризику [15].

Менеджмент вразливостей зачіпає безліч методик та стандартів, так як це досить складний процес і деякі його компоненти можуть бути описані в інших стандартах.

В результаті розгляду документації, стандартів, методик описаних вище, можна сказати що всі вони є загальними рекомендаціями, які встановлюють загальні вимоги щодо архітектури й реалізації процесів, проте не дають чітких настанов щодо дій після виявлення вразливості.

Створювана модель керування вразливостями повинна деталізувати процес оцінки ризику. Така система займає місце оцінки й прийняття рішень згідно ISO/IEC 27035.

3. ЗАГАЛЬНИЙ ОПИС СИСТЕМИ ОЦІНКИ РИЗИКУ Й ПРИЙНЯТТЯ РІШЕНЬ

3.1 Необхідність створення системи оцінки ризику

Система оцінки й прийняття рішень необхідна, так як сучасні стандарти не регламентують модель за якою повинно здійснюватися оцінювання конкретної вразливості, її вплив на систему, та відповідно і дії що необхідно приймати для конкретної вразливості. Як вже було сказано при розгляді нормативної бази (розділ 2.2) такі стандарти є збіркою рекомендацій, практик, й не межуть слугувати посібниками щодо встановлення дій або чітких архітектур.

В даний час оцінку ризиків, та вибір дій покладено на адміністраторів, які хоч і використовують сканери для виявлення вразливостей проте вимушені здійснювати оцінювання ситуації виходячи зі своїх знань та досвіду [16].

Такий підхід збільшує кількість помилок при прийнятті рішень щодо реагуваннння із-за суб’єктивізації результатів та створює неоднозначність трактування результатів. Також це підвищує вимоги до персоналу, та час адаптації, адже новим адміністраторам необхідно знати добре структуру, склад особливості функціонування системи [6].

3.2 Загальний опис системи

Однією із форм менеджменту є введення його в політику безпеки. Така політика повинна відповідати на ряд питань, а саме: яким чином виявляти вразливості, яким чином оцінювати ризики, як реагувати на вразливості, які дії повинне виконати адміністратор безпеки та аудиту, системний адміністратор, правління, де знаходиться межа прийняття ризику. Для того

щоб дати відповіді на ці питання необхідно правильно оцінювати кожну конкретну вразливість, що виникає при експлуатації ІТС.

Тому під час розробки такої політики не обійтися від системи оцінки вразливостей, яка буде здійснювати оцінку впливу як на всю ІТС та на окремі компоненти. Така система повинна сформувати якісні оцінки впливу а при додаванні критичності компонентів системи отримаємо сформовану оцінку ризику конкретної вразливості. Вже описана CVSS, якраз надає якісний бал та вектор впливу, який можна використовувати при реалізації системи менеджменту вразливостей. Цей вектор надає інформацію про вплив на конфіденційність, цілісність, доступність, вектор атаки, наявність виправлень, наявність програмної реалізації експлойту, тощо. Політика безпеки в даному випадку, встановлюватиме лише дії які необхідно виконати при конкретному значенні ризику.

Для такої системи необхідно правильно оцінювати компоненти та взаємозв'язки компонентів, так як вплив вразливостей може виходити за границі одного об'єкту чи процесу, або вплив вразливості на різні компоненти сколюватиметься й призводитиме до більш значних наслідків.

Схематично така модель матиме вигляд як показано на рисунку 3.1.

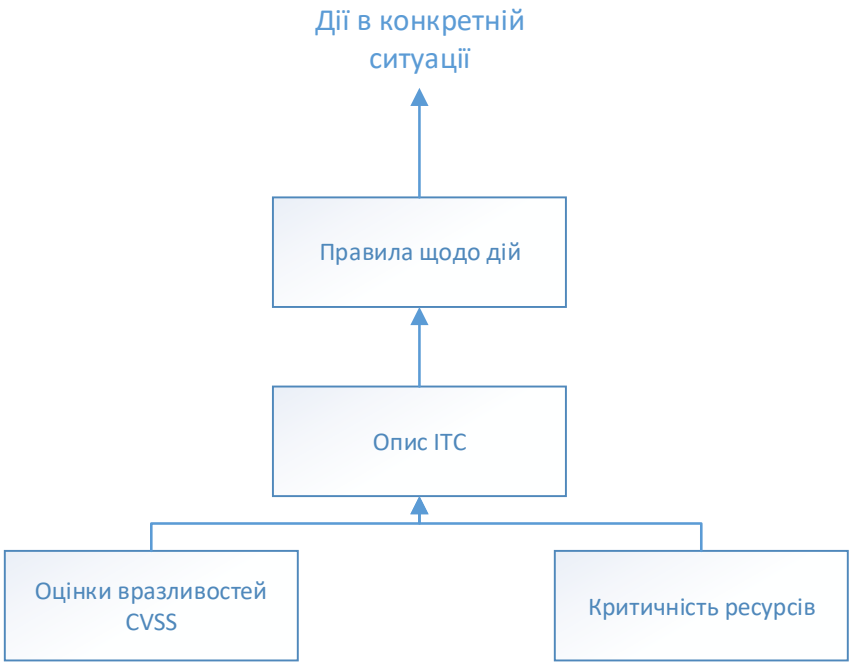

Рисунок 3.1 – Приклад моделі керування вразливостями в СУІБ

В такій системі вхід подається опис критичності ресурсів в числовому представленні (такі показники формуються заздалегідь під час створення політики безпеки ІТС), та конкретні оцінки вразливостей зі сканерів вразливостей. Ці данні накладаються на опис системи для визначення впливу вразливості на конкретні компоненти, взаємозв'язки між компонентами та загалом на систему. Після цього отримана якісна оцінка впливу слугує вказівником щодо оцінки ризику та вибору конкретних дій. Різні показники матимуть різну методику, щодо виправлень, або прийняття вразливості, якщо вона не є критичною або не впливає на роботу системи.

Правила реагування на конкретну оцінку повинні бути сформовані заздалегідь, погоджені з керівництвом та адміністраторами. З набору правил вибирається оптимальний варіант щодо дії виходячи з якісної оцінки впливу. Після цього адміністратор здійснює необхідні дії щодо усунення або прийняття ризику пов’язаним з наявністю вразливості.

В даній системі етап оцінки ризику повністю знятий з адміністратора, це означає можливість автоматизації процесів контролю вразливостями , усунення суб'єктивизації небезпеки, однозначність результатів.

Проте незважаючи на переваги такої системи менеджменту вона має один суттєвий недолік, а саме: в даний час не існує правил чи методик які б слугували правилами щодо опису ІТС. Тобто на даний момент сучасний опис ІТС не підходить для реалізації вказаної системи керування вразливостями, такий опис не показує належним чином взаємозв'язки компонентів, процесів, ресурсів, та не може бути використаний для реалізації системи керування вразливостями в СУІБ.

Тому для реалізації даної концепції необхідна система опису ІТС, яка б допомогла в встановлені взаємозв’язків компонентів.

3.3 Формалізований й неформалізований опис ІТС

Під час опису інформаційної системи та системи захисту інформації зазвичай використовують неформалізований опис, тому, на перший погляд, створювана система оцінювання та прийняття рішень повинна також бути неформалізованою, але це не найкращий варіант, адже неформалізований опис створює безліч проблем, а саме: складність розуміння системи новим персоналом, громіздкість опису систем, відсутність єдиного структурованого опису, погіршення опису взаємозв'язків процесів, знецінення важливої інформації, погану гнучкість.

Відсутність структурованого опису походить від того, що при неформалізованому описі системи розробник не має чітких вимог до структури та форми опису системи, тому зазвичай розробники ІТС під час опису керуються власними нормами або узгоджують їх з клієнтом. Тому опис різних ІТС може відрізнятися якщо вони були створені різними розробниками, навіть якщо ці системи створені однією фірмою, то вони можуть відрізнятися в залежності від типу ІТС, замовника, працівників, що займалися розробкою [15].

Громіздкість опису системи походить від того що вся інформація при неформалізованому описі зазвичай подається у вигляді тексту та відсутності структурованого опису. Чим більша система, чим більше процесів та об'єктів, тим більший опис з'являється на виході. Ситуація погіршується, якщо описувана система має обширні або специфічні зв'язки між об'єктами.

Гнучкість опису системи проявляється при її модернізації. Під час модернізації неформалізованого опису необхідне редагування безлічі частин опису, які можуть бути пов'язані або залежати одна від одної. Тому внесення навіть мінімальних правок в систему призводить до перегляду всього опису в цілому, не кажучи вже про додавання або виключення компонентів системи.

Під час такого опису погіршується відображення взаємозв'язків процесів, адже чим довше та складніше дерево об'єктів або процесів, тим

складніше його описати та тим більше буде опис системи. Також під час такого опису неможливо чітко дати оцінку впливу вразливості в одному об’єкті ІТС на інший, оскільки не існує метрик, формул та правил взаємодії. Ці правила встановлюються емпіричним методом на базі знань адміністратора.

З цих проблем виникає складність розуміння новим персоналом специфіки роботи системи. Такому персоналу слід обробити безліч інформації в текстовому представленні, яка структурно може відрізнятися від тієї з якою персонал працював раніше.

Під час такої обробки складно виділяти та концентрувати увагу, відслідковувати взаємозв’язки процесів та об’єктів, структурно та логічно класифікувати її, тому можливе погіршення обробки інформації та її знецінення.

Ці проблеми переходять на створювану систему оцінки вразливостей та посилюються там. Така система буде нечіткою, вузькоспеціалізованою, не враховуватиме всіх взаємозв’язків процесів та матиме вигляд зводу практик (аналогічно ISO/IEC 27035). Такі практики не надають методів обчислення ризиків чи впливу вразливості на різні компоненти ІТС. Весь тягар оцінки впливу вразливостей, оцінки ризику, прийняття рішень, покладено на адміністратора безпеки. При різних адміністраторах одна і та ж ситуація може трактуватися по-різному, відповідно і рішення будуть прийняті різні в залежності від досвіду, темпераменту адміністратора. В додаток до цих проблем неформалізований опис не може гарантувати рівень гарантій вище ніж Г-2 [7]. Для рівнів Г-3, Г-4, Г-5 стиль опису ІТС повинен бути частково-формалізований, для Г-6 та Г-3 формалізований.

На відміну від неформалізованого опису системи формалізований має чітку структуру та форму опису, відображає взаємозв’язки процесів, є гнучким та універсальним. В такій системі вплив вразливості легко відслідкувати від точки контакту до всіх об’єктів інформаційної системи. Формалізація дає змогу виявити загальну структуру системи, сформулювати

на цій основі загальні закони і правила, за якими відбувається визначення впливу вразливостей на ІТС. Така система зводить до мінімуму вплив адміністратора безпеки, покладаючи оцінку впливу та ризиків на чіткі та закріплені методики, забезпечуючи однозначність та відтворюваність результатів. Тому розроблена система оцінювання ризиків повинна бути формалізованою та побудованою над формалізованим описом ІТС.

Варіантом формалізованого опису ІТС може бути опис послуг безпеки в ІТС. Під час такого опису об’єкти та процеси інформаційної системи представляються в описі зі сторони послуг безпеки, які вони надають або обробляють. Ці послуги передаються від об’єкта до об’єкта, посилюються або взаємодіють з ними. Під час такої реалізації, вразливості будуть розцінюватися як небезпека для конкретної послуги безпеки.

Суміщення формалізованого опису та менеджменту вразливостей допоможе виявляти слабкі місця в ІТС, відслідковувати вплив окремої вразливості на компоненти, масштабувати вразливості, відслідковувати їх взаємозв’язок. При додаванні якісного оцінювання вразливостей можливе створення методик та інструкцій щодо оцінки ризиків. Такі методики можуть надати числову оцінку загрози як системи в цілому, її окремим компонентам, а оцінка ризиків допоможе адміністратору в виборі дій. Так як значення ризику мають числове представлення, то можливе створення чітких інструкцій щодо дій адміністратору. Також така система буде досить гнучкою і універсальною, адже будуватиметься над структурованим описом системи.

3.4 UML

Для формалізованого опису було вибрано мову моделювання Unified Modeling Language (UML), так як дана мова є універсальною, легко піддається змінам, та досить розповсюджена та наглядна.

UML— уніфікована мова моделювання, використовується у парадигмі об'єктно-орієнтованого програмування. Є невід'ємною частиною уніфікованого процесу розробки програмного забезпечення. UML є мовою широкого профілю, це відкритий стандарт, що використовує графічні позначення для створення абстрактної моделі системи, яка називається UML-моделлю. UML був створений для визначення, візуалізації, проектування й документування в основному програмних систем. UML не є мовою програмування, але в засобах виконання UML-моделей як інтерпретованого коду можлива кодогенерація.

Перша версія (1.0) UML вийшла 13 січня 1997, вона була створена консорціумом UML Partners за запитом Object Management Group (OMG) — організації, відповідальної за прийняття стандартів в галузі об'єктних технологій і баз даних. Після обговорення, у вересні 1997 року, версія 1.1 UML була представлена на голосування в OMG. Розробку UML підтримали і вже тоді використовували як стандарт такі гранди ринку інформаційних технологій, як Microsoft, IBM, Hewlett-Packard, Oracle, DEC, Sybase, Logic Works й інші. Поточна версія — 2.0.

UML може бути застосовано на всіх етапах життєвого циклу аналізу бізнес-систем і розробки прикладних програм. Різні види діаграм які підтримуються UML, і найбагатший набір можливостей представлення певних аспектів системи робить UML універсальним засобом опису як програмних, так і ділових систем.

Діаграми дають можливість представити систему (як ділову, так і програмну) у такому вигляді, щоб її можна було легко перевести в програмний код.

Крім того, UML спеціально створювалася для оптимізації процесу розробки програмних систем, що дозволяє збільшити ефективність їх реалізації у кілька разів і помітно поліпшити якість кінцевого продукту.

UML чудово зарекомендувала себе в багатьох успішних програмних проектах. Засоби автоматичної генерації кодів дозволяють перетворювати

моделі мовою UML у вихідний код об’єктно-орієнтованих мов програмування, що ще більш прискорює процес розробки.

Практично усі CASE-засоби (програми автоматизації процесу аналізу і проектування) мають підтримку UML. Моделі розроблені в UML, дозволяють значно спростити процес кодування і направити зусилля програмістів безпосередньо на реалізацію системи.

Діаграми підвищують супроводжуваність проекту і полегшують розробку документації.

При модифікації системи об'єктний підхід дозволяє легко включати в систему нові об'єкти і виключати застарілі без істотної зміни її життєздатності. Використання побудованої моделі при модифікаціях системи дає можливість усунути небажані наслідки змін, оскільки вони не ламають структури системи, а тільки змінюють поведінку об'єктів [14].

4. СИСТЕМА ОЦІНКИ РИЗИКУ Й ПРИЙНЯТТЯ РІШЕНЬ, ОПИС МОДЕЛІ

4.1 Етапи системи оцінки й прийняття рішень

В загальному вигляді система була описана в р.3.2.

Створювана система оцінки регламентує та встановлює порядок дій менеджменту вразливостей, всі дії в системі повинні виконуватися згідно єтапів.

Основними етапами використання даної системи є:

1) Опис ІТС згідно правил описаних в п.4.2.
2) Розроблення політики безпеки, якщо така не була створена, або її модернізація згідно п. 4.3;
3) Суміщення опису ІТС з політикою безпеки(п.4.4);
4) Розподіл обов’язків та створення інструкцій щодо дій(п. 4.5);
5) Введення в дію та модернізація(п. 4.6)

4.2 Опис ІТС згідно системи оцінки ризику й прийняття рішень

Для опису ІТС слід використовувати UML. В подальшому для опису використовувалось ПЗ Umbrello UML Modeller [17], це open source проект що дозволяє створювати UML діаграми. Проте для опису системи можна використовувати інші ПЗ.

В якості об’єктів ІТС використовуються класи UML. У якості атрибутів використовуються категорії ПЗ(ОС, браузер, тощо), у якості значень атрибутів назва та версія ПЗ.

В якості операцій описуються процеси що відбуваються на об’єкті, в якості параметрів потоки процесу(наприклад: Робота з браузером(Пошук сторінок, Завантаження файлів)).

Тобто об’єкт – це окремий модуль ІТС, атрибут – це характеристика об’єкту, операція – процеси що відбуваються на об’єкті.

Для атрибутів та операцій встановлюються ступені взаємодії з іншими компонентами.

Private – атрибут або операція виконується виключно в об’єкті ІТС та не взаємодіє з іншими об’єктами (в подальшому на схемах позначається символом «-»). Як прикладом може бути текстовий редактор.

Protected – атрибут або операція взаємодіє з іншими компонентами, але виступає в якості клієнту (в подальшому на схемах позначається символом «#»). Як прикладом може бути браузер.

Public – атрибут або операція взаємодіє з іншими компонентами, виступає в якості серверу (в подальшому на схемах позначається символом «+»). Як приклад може бути веб сервер.

Implementation – атрибут або операція взаємодіє з іншими компонентами й надає їм частковий доступ до ресурсів (в подальшому на схемах позначається символом «~»). Як прикладом може бути сервер особистого кабінету.

Приклад опису робочого місця користувача показано на рисунку 4.1.

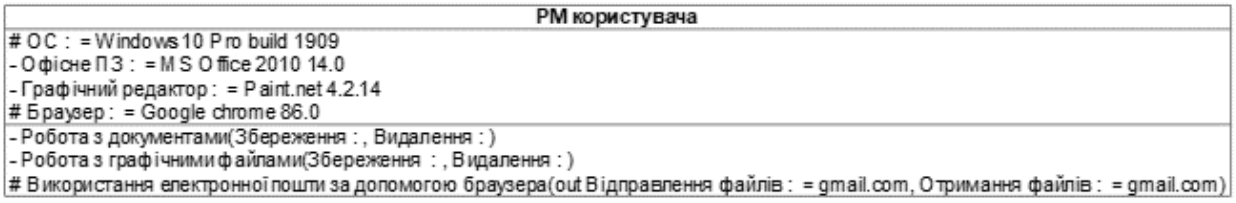

Рисунок 4.1 – Опис РМ користувача

В даному випадку РМ складається з ОС Windows, Офісного ПЗ MS Office, графічного редактора Paint.net, браузера Google chrome. На даному РМ здійснюються процеси роботи з текстовими та графічними файлами й відправка файлів засобами електронної пошти з використанням почтового сервісу gmail.com.

Взаємозв’язки між об’єтами існують 2х типів:

1) Передача інформації. Позначається як суцільна стрілка з підписом типу інформації та її представленням в середовищі(Рис. 4.2).

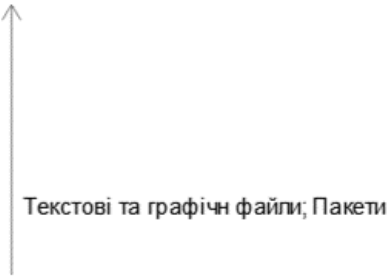

Рисунок 4.2 – Умовне позначення передачі інформації

2) Надання одним об’єктом ресурсів іншому. Позначається як пунктирна стрілка(Рис. 4.3).

Рисунок 4.3 – Умовне позначення використання ресурсів

Дозволяється різні рівні деталізації ІТС, рівень деталізації залежить від розробника. Проте повинні виконуватися наступні вимоги:

– повинні відображені всі компоненти системи;

– повинно бути відображено встановлене ПЗ, функції якого використовуються в ІТС(дозволяється пропускати стандартне ПЗ ОС);

– повинно бути описано апаратне забезпечення;

– повинні бути відображенні рівні віртуалізації;

– повинні бути відображені основні процеси на об’єктах;

– повинні бути відображені потоки інформації між об’єктими.

Така схема дозволить краще розуміти взаємозв’язки процесів та візуально відобразити точки входу вразливостей.

4.3 Політика безпеки

Перед початком використання системи оцінки ризику й прийняття рішень в ІТС повинна бути створена політика безпеки інформації відповідно до чинного законодавства України. Крім того як частиною такої політики повинно бути виконано оцінювання критичності кожного об’єкту ІТС(активу).

Внаслідок різноманітності активів, що зустрічаються в більшості організацій, ймовірно, що деякі активи, що мають відому грошову цінність, будуть оцінені в одиницях місцевої валюти, тоді як інші, володіють більш якісною цінністю, яким може бути присвоєна цінність, що коливається, наприклад, в межах від «дуже низька» до «дуже висока». Рішення про те, яку шкалу використовувати, кількісну або якісну, в дійсності є питанням переваги організації, але вона повинна бути доречна для оцінюваних активів. Обидва види визначення цінності можуть бути використані для одного і того самого активу.

Після встановлення критеріїв для розгляду організації слід узгодити шкалу, яка буде використовуватися в масштабах організації. Першим кроком є ухвалення рішення про кількість використовуваних рівнів. Не існує правил, що визначають найбільш доречне число рівнів. Більше число рівнів забезпечує більший рівень деталізації, але іноді занадто дрібна диференціація ускладнює привласнення узгоджених оцінок в масштабі організації. Зазвичай може використовуватися будь-яке число рівнів від 3 (наприклад низький, середній і високий) до 10 відповідно до підходу організації для всього процесу оцінки ризику. Організація може встановити власні межі цінності активів. Ці межі повинні оцінюватися відповідно до обраних критеріїв, (так, для можливих фінансових втрат межі повинні бути вказані в грошовому вираженні, але при розгляді, наприклад загрози особистої безпеки, визначити їх грошову цінність може бути важко і неприйнятно для всіх організацій).

Рішення про те, що вважати незначними або серйозними наслідками, повністю залежить від організації. Наслідки, катастрофічні для невеликої організації, можуть бути незначними або навіть тими що можна знехтувати для дуже великої організації [2].

Необхідно здійснити ранжування кожного компонента за його критичністю. Рекомендується здійснити оцінку від 0 до 5 для конфіденційності, цілісності та доступності (далі – К/Ц/Д). Приклад оцінювання приведено в таблиці 4.1.

Таблиця 4.1 – Приклад ступенів ранжування цінності активів

Числовий рівень	Опис рівня
0	Повна втрата К/Ц/Д об’єкту не призводить до наслідків, або вони є незначними чи локальними
1	Повна втрата Ц/К/Д об’єкту призводить до погіршення послуг які надає організація
2	Повна втрата Ц/К/Д об’єкту призводить до ситуації межах форс-мажорної ситуації
3	Повна втрата Ц/К/Д, призводить до ситуації в якій організація може відшкодувати збитки за рахунок внутрішніх активів, або утрата не призводить до серйозних наслідків репутації
4	Повна втрата Ц/К/Д, призводить до ситуації в якій організація може відшкодувати збитки за рахунок зовнішніх активів, або утрата призводить до серйозних наслідків репутації
5	Повна втрата Ц/К/Д, призводить до ситуації в якій існування організаціє постає під загрозу

4.4 Суміщення опису ІТС з політикою безпеки й підрахунок балів

Після оцінювання активів, кожний об’єкт системи повинний мати оцінку К/Ц/Д, яку необхідно внести в діаграму UML. Окремо створюються статичні атрибути «Конфіденційність», «Цілісність», «Доступність» так об’єкт РМ адміністратора з попереднього прикладу зі здійсненою оцінкою показано на рисунку 4.4.

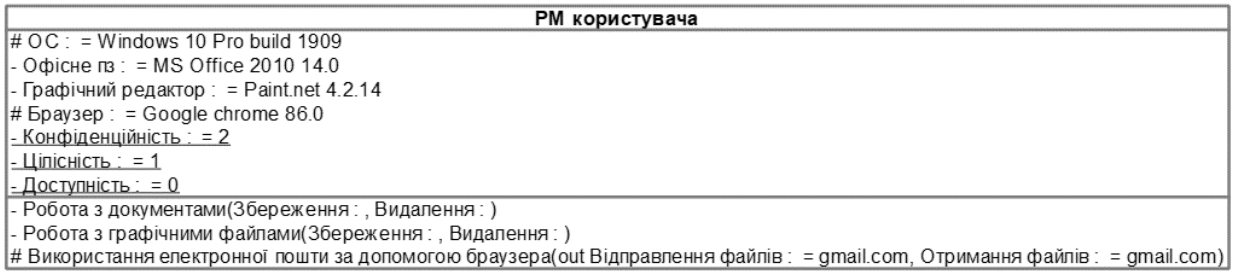

Рисунок 4.4 – суміщення діаграми UML з оцінками критичності

Після додавання кожної оцінки для кожного об’єкту необхідно здійснювати підрахунок кожної вразливості згідно правилу:
загальний бал впливу = оцінка вразливості згідно CVSS * бал конфіденційності ресурсу * коефіцієнт впливу вразливості на конфіденційність + оцінка вразливості згідно CVSS * бал цілісності ресурсу * коефіцієнт впливу вразливості на цілісність + оцінка вразливості згідно CVSS * бал доступності ресурсу * коефіцієнт впливу вразливості на доступність.

Якщо конфіденційність або доступність вразливості висока(High) то бали К/Ц підвищуються до половини максимального значення(округлення йде в більшу сторону). Тобто якщо К/Ц/Д – 1/1/5, то при вразливості з високим впливом на конфіденційність параметри К/Ц/Д розраховуються як 3/1/5.

Коефіцієнт впливу вразливості визначається з вектору вразливості і становить 0 для None, 0.5 для Low, 1 для High.

Таким чином якщо використовувати оцінку критичності від 0 до 5, то максимальний загальний бал становить 150.

Проте дана оцінка становитиме вплив компоненту ІТС на всю систему загалом. Тобто для всіх компонентів максимальний бал становитиме 150. Ця оцінка є абсолютним максимумом.

Для розуміння ситуації для конкретного об’єкту, для кожного об’єкту необхідно вивести відносну оцінку за формулою:

відносна оцінка на об’єкт = 10* бал конфіденційності ресурсу * коефіцієнт впливу вразливості на конфіденційність + 10* бал цілісності ресурсу * коефіцієнт впливу вразливості на цілісність + 10* бал доступності ресурсу * коефіцієнт впливу вразливості на доступність.

Тобто для попереднього прикладу відносна оцінка становить: 10*2+10*1+10*0=30. Ця оцінка є максимальною, якщо під час обчислення для вразливості з високою К/Ц вирахувано більший бал то він заміняється на максимальний.

Розділення на загальну та відносну оцінку необхідно для кращого ранжування пріоритетів. Це надає розуміння того на скільки вразливість критична для окремого компоненту, чи системи, який компонент потребує першочергової участі тощо. В першу чергу слід здійснювати дії над компонентом що має більший бал. Якщо вразливості мають однаковий бал, то слід вибирати вразливість об’єкту що має більше залежностей та взаємозв’язків.

Таким чином абсолютний бал слугує для визначення черговості виправлень компонентів, а відносний для дій щодо виправлення окремого об’єкту.

Для зручності розуміння рекомендується приводити відносний бал до десятибальної шкали. Так наприклад для відносного балу 30 кожний бал становить 0.33 балу десятибальної оцінки

4.5 Розподіл обов’язків та створення інструкцій щодо дій

Перед початком використання системи організація повинна розподілити обов’язки щодо контролю, дій та реагування. Рекомендується створення таких ролей як:

1) Адміністратор безпеки – особа яка відповідальна за виконання політик безпеки та менеджмент вразливостей. Адміністратор безпеки здійснює контроль та нагляд за процесами та працівниками. Адміністратор безпеки може на свій розсуд змінити дії щодо виправлення.

2) Системний адміністратор – особа яка відповідальна за налаштування сканерів вразливостей та планування сканування, здійснення виправлень.

Адміністратори безпеки повинні розробити інструкції щодо дій та погодити їх с керівництвом. За можливості при розробці рекомендується консультації з фахівцями, що розробляли ПЗ, компоненти, систему, тощо.

Приклад такої інструкції для прикладу з РМ користувача приведено приведено в таблиці 4.2.

Таблиця 4.2 – приклад інструкції щодо дій для РМ адміністратора

Бал для об’єкту Відносний бал. 30	Дії щодо виправлення
0-5	Прийняття ризику
5-7	Поселення контролю за об’єктором
7-8	Здійснення оновлення, якщо таке відсутнє, то посилений контроль за об’єктом
9	Здійснення оновлення, якщо таке відсутнє то обмеження роботи даного компоненту
10	Здійснення оновлення, якщо таке відсутнє то зупинка роботи до отримання оновлення від розробника

4.6 Введення в дію та модернізація

Після здійснення всіх дій система може бути введена в дію. Рекомендується під час роботи використовувати базу вразливостей NVD. Під час роботи системи забороняється змінювати базу вразливостей на іншу, так як CVSS бали вразливостей можуть відрізнятися.

Під час виявлення вразливості слід відображати знайдену вразливість на схемі ІТС й писати поруч вектор й бал CVSS. Рекомендується використовувати кольори відповідно до оцінки CVSS вразливості(0.1-3.9 зелений, 4.0-6.9 жовтий, 7.0-8.9 помаранчевий, 9.0-10.0 червоний).Це необхідно для покращення розуміння положення вразливості в ІТС.

Приклад використання кольорів та векторів наведено на рисунку 4.5.

Система повинна бути переглянута з інтервалом раз в рік або в наступних випадках;

– при зміні структури ІТС;
– при переоцінці активів;
– після інцидентів в якості процесу винесення уроків;
– за бажанням адміністратора безпеки;
– за бажанням керівництва.

Модернізована система повинна бути переузгодженна керівництвом організації.

3.9 AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:L

PM керівника
ОС : = Windows 10 build 1909 - Офісне ПЗ : = MS Oficce 2010 14.0 # Браузер : = Google Chrome 86 - ПЗ для перегляду PDF файлів : = PDF Reader 15.0 # Антивірусне ПЗ : = ESET Endpoint 7.1 - Конфіденційність : = 3 - Цілісність : = 2 - Доступність : = 1
- Робота з документами(Створення : , Видалення : , Модифікація :) # Робота в інтернеті(out Відправка запитів сторінок : , Отримання сторінок :) # Оновлення ОС (Отримання пакетів :) - Робота з PDF файлами(читання :)

5.3 AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:H/A:L

PM керівника_2
ОС : = Windows 10 build 1909 - Офісне ПЗ : = MS Oficce 2010 14.0 # Браузер : = Google Chrome 86 - ПЗ для перегляду PDF файлів : = PDF Reader 15.0 # Антивірусне ПЗ : = ESET Endpoint 7.1 - Конфіденційність : = 3 - Цілісність : = 2 - Доступність : = 1
- Робота з документами(Створення : , Видалення : , Модифікація :) # Робота в інтернеті(out Відправка запитів сторінок : , Отримання сторінок :) # Оновлення ОС (Отримання пакетів :) - Робота з PDF файлами(читання :)

7.6 AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H

PM керівника_3
ОС : = Windows 10 build 1909 - Офісне ПЗ : = MS Oficce 2010 14.0 # Браузер : = Google Chrome 86 - ПЗ для перегляду PDF файлів : = PDF Reader 15.0 # Антивірусне ПЗ : = ESET Endpoint 7.1 - Конфіденційність : = 3 - Цілісність : = 2 - Доступність : = 1
- Робота з документами(Створення : , Видалення : , Модифікація :) # Робота в інтернеті(out Відправка запитів сторінок : , Отримання сторінок :) # Оновлення ОС (Отримання пакетів :) - Робота з PDF файлами(читання :)

9.0 AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H

PM керівника_2_1
ОС : = Windows 10 build 1909 - Офісне ПЗ : = MS Oficce 2010 14.0 # Браузер : = Google Chrome 86 - ПЗ для перегляду PDF файлів : = PDF Reader 15.0 # Антивірусне ПЗ : = ESET Endpoint 7.1 - Конфіденційність : = 3 - Цілісність : = 2 - Доступність : = 1
- Робота з документами(Створення : , Видалення : , Модифікація :) # Робота в інтернеті(out Відправка запитів сторінок : , Отримання сторінок :) # Оновлення ОС (Отримання пакетів :) - Робота з PDF файлами(читання :)

Рисунок 4.5 – Маркування виявлених вразливостей

5. ВИКОРИСТАННЯ СИСТЕМИ ОЦІНКИ РИЗИКУ Й ПРИНЯТТЯ РІШЕНЬ

5.1 Загальна інфомація

Для демонстрації відтворимо використання системи оцінки ризику й прийняття рішень на прикладі.

Нехай існує фірма ПАТ «ФІРМА», дана фірма має сайт на якому можна дізнатися поточний час. Інші бізнес процеси в ПАТ «ФІРМА» відсутні. Всі послуги надаються однією ІТС.

Далі виконаємо почергово всі етапи.

5.2 Створення опису ІТС

Спочатку здійснюється опис ІТС, нехай ПАТ «Фірма» складається з наступних компонентів:

– ПТК адміністратора;

– ПТК керівника;

– ПТК веб серверу;

– комунікаційне обладнання.

ПТК адміністратора призначено для здійснення налаштувань веб серверу та редагування документів. ПТК адміністратора підключається до веб-серверу через локальну мережу, виходу в мережу інтернет РМ адміністратора не має.

ПТК керівника призначено для редагування документів та перегляду веб-сторінок.

Веб-сервер містить сторінку ПАТ «Фірма» та надає доступ до неї зовнішнім користувачам.

Комунікаційне обладнання призначено для створення локальної мережі, комутації пакетів в середині локальної мережі та прокидування порту веб-серверу.

Побудована модель ІТС за правилами системи оцінки та прийняття рішень показана на рисунку 5.1.

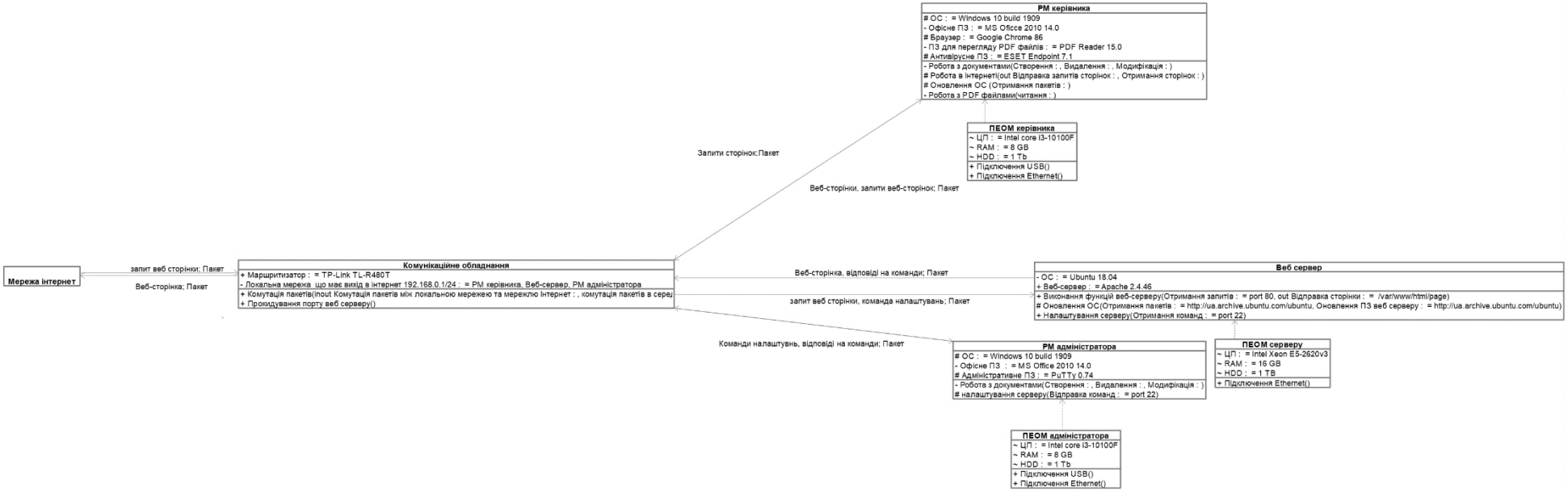

Рисунок 5.1 – Схематична модель ІТС

5.3 Створення політики безпеки, суміщення з описом ІСТ та підрахунок балів

Під час створення політики безпеки ПАТ «Фірма» в політиці безпеки було виділено активи відносно таблиці 2:

– ПТК адміністратора – 2/2/2;

– ПТК керівника – 3/2/1;

– ПТК веб серверу – 0/4/4;

– Комунікаційне обладнання – 0/2/4.

Максимальний бал для кожного активу:

– ПТК адміністратора – 60;

– ПТК керівника – 60;

– ПТК веб серверу – 80;

– Комунікаційне обладнання – 60.

Інформацію про активи внесено до загального опису ІТС (Рис. 5.2).

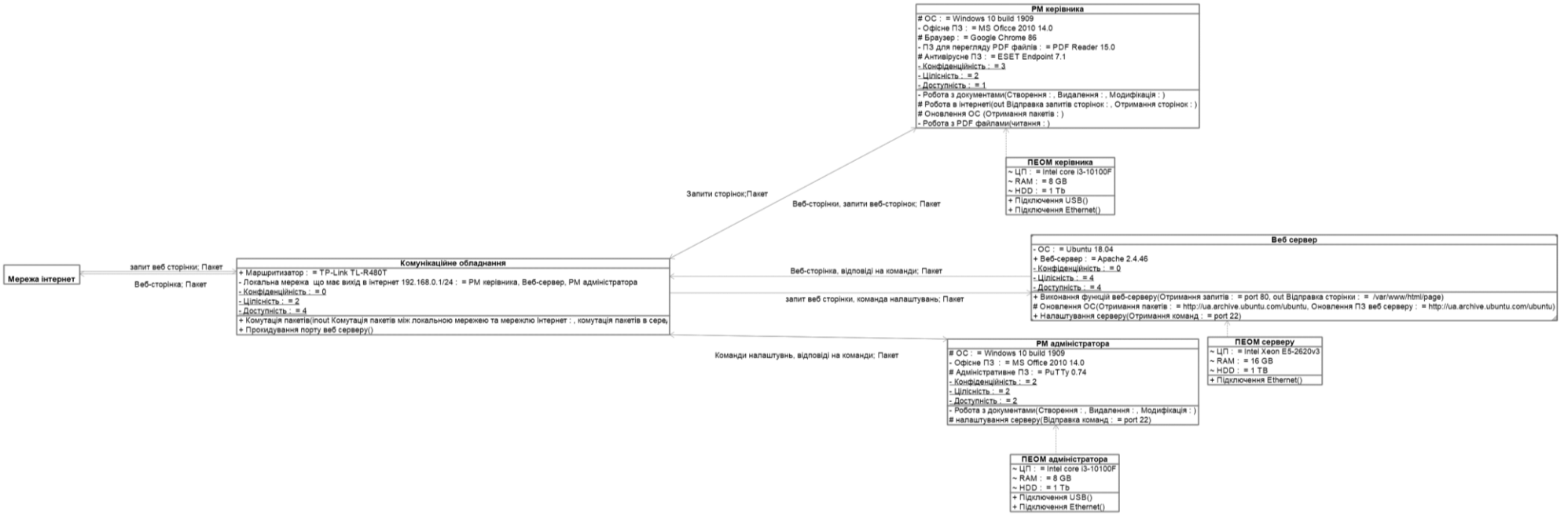

Рисунок 5.2 – Схематична модель ІТС з суміщенням політики безпеки

5.4 Створення інструкцій

Як можна помітити з підрахунку максимальних балів, першочергову важливість має веб сервер, так як порушення цілісності може призвести до підміни веб-сторінки й пошкодити репутацію, а недоступність об’єкту несе прямі збитки бізнес-процесу ПАТ «Фірма».

ПТК адміністратора, ПТК керівника, комунікаційне обладнання мають однаковий бал – 60. Проте як показано на схемі з комунікаційним обладнанням взаємодіють всі компоненти ІТС, тому воно являється важливішим чим ПТК адміністратора та ПТК керівника.

Керівництво вирішило ПТК адміністратора та ПТК мають одинаковий пріоритет дій.

Коефіцієнти для переводу балів в десятибальну шкалу:

– ПТК адміністратора – 0.166;

– ПТК керівника – 0.166;

– ПТК веб серверу 0.125;

– Комунікаційне обладнання 0.166.

Керівництво затвердило інструкції щодо дій адміністратору (Табл. 5.1, 5.2, 5.3, 5.4).

Таблиця 5.1 – Дії адміністратора для ПТК адміністратора

Бал для об’єкту Відносний бал. 60	Дії щодо виправлення
0-6	Прийняття ризику
7	Здійснення оновлення, якщо таке відсутнє, то обмеження чи відключеня роботи компоненту
7-10	Відключення від мережі та здійснення автономного оновлення

Таблиця 5.2 – Дії адміністратора для ПТК керівника

Бал для об’єкту Відносний бал. 60	Дії щодо виправлення
0-6	Прийняття ризику
6-9	Використання додаткових функцій шифрування та перевірки цілісності, відключення компонентів, якщо це можливо
10	Відключення від мережі та здійснення автономного оновлення

Таблиця 5.3 – Дії адміністратора для комунікаційного обладнання

Бал для об’єкту Відносний бал. 60	Дії щодо виправлення
0-7	Прийняття ризику
7-9	Здійснення оновлення/підготовка варіанту резервного маршрутизатора
10	Заміна резервним комутатором

Таблиця 5.4 – Дії адміністратора для ПТК веб-серверу.

Бал для об’єкту Відносний бал. 80	Дії щодо виправлення
0-5	Прийняття ризику
6	Здійснення оновлення, якщо таке відсутнє то прийняття ризику

Продовження таблиці 5.4

7	Здійснення оновлення, якщо таке відсутнє то здійснювати перевірку робото спроможності й аудит подій кожні 12 год.
8-10	Здійснення оновлення, якщо таке відсутнє то здійснювати перевірку робото спроможності кожні 6 год, змінити адміністративні паролі на складніші, підготуватися до можливої переінсталяції системи(якщо вразливість відсутня на нижчий версії ПЗ то вибрати його).

Наказом керівництва назначається адміністратор безпеки та системний адміністратор, якими доручено виконання системи оцінки й прийняття рішень.

5.5 Приклад реагування на вразливість

Після виконання попередніх етапів система приступає в промислову експлуатацію. Нехай під час експлуатації системи з’явилась вразливість CVE-2019-12881 для ОС Ubuntu 18.04 (Рис. 5.3) та Windows 10(Рис. 5.4).

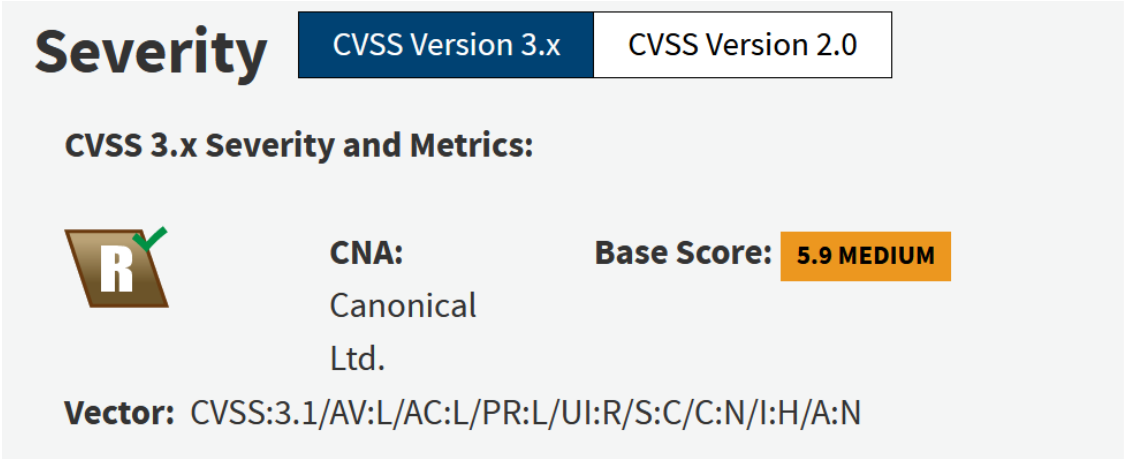

Рисунок 5.3 – Вразливість CVE-2019-12881 для ОС Ubuntu

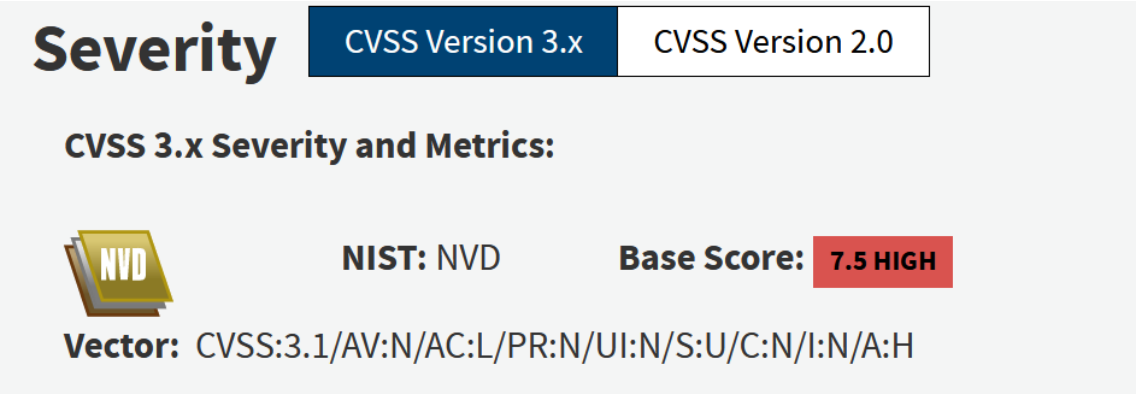

Рисунок 5.4 – Вразливість CVE-2020-16899 для ОС Windows 10

Для кращого розуміння відобразимо вразливості на схемі ІТС (Рис. 5.5).

Для вразливості CVE-2019-12881 та CVE-2020-16899 значення К/Ц/Д згідно вектору CVSS становлять 0/1/0 та 0/0/1 відповідно.

Вплив вразливості CVE-2019-12881 на ПТК веб серверу становить:

5,9 * 0 * 0 + 5,9 * 4 * 1 + 5,9 * 4 * 0= 23.6

Відносний бал становить 23,6*0.125 =2,95.

Вплив вразливості CVE- 2020-16899 на ПТК адміністратора становить:

7,5 * 2* 0 + 7,5 * 2* 0 + 7,5 * 2* 1 = 15

Відносний бал становить 15*0.166 =2,5.

Вплив вразливості CVE-2020-16899 на ПТК керівника:

7,5 * 3* 0 + 7,5 * 2* 0 + 7,5 * 1* 1 = 7,5

Відносний бал становить 7,5*0.166 =1,245.

З цього прикладу можна побачити що вплив вразливості CVE-2019-12881 на ІТС значно більший ніж CVE-2020-16899(23,6 бали відносно 15 та 7,4), хоч вона і має меншу оцінку CVSS (5,9 відносно 7,5).

З цього значить в першу чергу слід приймати рішення відносно дій для вразливості CVE-2019-12881 для веб серверу, потім для ПТК адміністратора і в останню чергу для ПТК керівника.

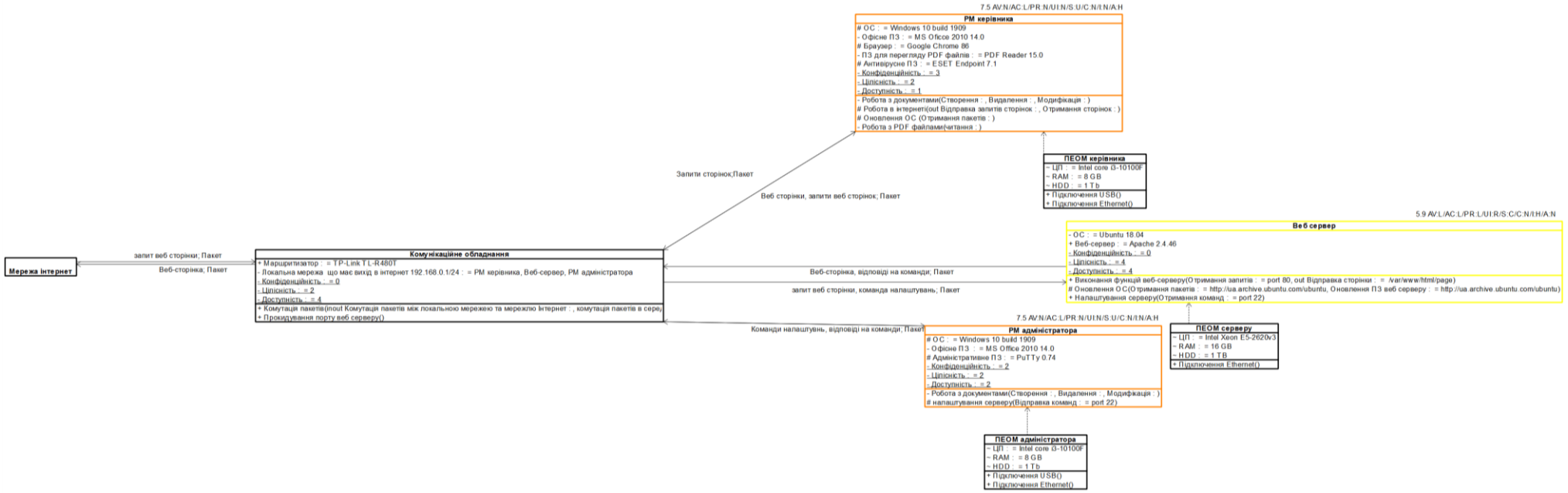

Рисунок 5.5 – Відображення вразливостей на схемі ІТС

Керуючись системою, були вибрані наступні дії щодо реагування:

– ПТК веб серверу – прийняття ризику;
– ПТК адміністратора – прийняття ризику;
– ПТК керівника – прийняття ризику.

ВИСНОВКИ

Під час виконання атестаційної роботи було розглянуто природу й походження вразливостей, проаналізовано й досліджено сучасну нормативну базу у сфері менеджменту вразливостей. Було встановлено, що існуюча документація, є загальними рекомендаціями, які встановлюють загальні вимоги щодо архітектури й реалізації процесів, проте не дає чітких настанов щодо дій після виявлення вразливості. Для усунення прогалини в області оцінки й прийняття рішень необхідна система оцінки й прийняття рішень, яка б домопогла адміністраторам у виборі дій щодо виправлення.

У якості варіанту була розроблена система оцінки ризику й прийняття рішень що інтегрована з політикою безпеки системи інформаційної безпеки. Ця система включає в себе наступні етапи: опис ІТС, розроблення політики безпеки, суміщення опису ІТС з політикою безпеки, розподіл обов’язків та створення інструкцій щодо дій, введення в дію та модернізація. Для кожного етапу існує звід правил які повинна виконати організація для використання даної системи. Розроблена система повинна покращити оцінку й прийняття рішень, зменшити суб’єктивний вплив адміністратора, гарантувати однозначність результатів. В межах прикладу продемонстровано роботоспроможність даної системи.

Результати досліджень, що викладені у магістерській роботі, було оприлюднено на Харківському Безпековому Форумі 2020 під патронатом Урядового офісу координації європейської та євроатлантичної інтеграції Секретаріату Кабінету Міністрів України та за сприяння Харківської обласної державної адміністрації.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. ISO/IEC 27035:2016. Information technology — Security techniques — Information security incident management, 2016. (Міжнародний стандарт)

2. ISO/IEC 27005 Information technology — Security techniques — Information security risk management, 2018. (Міжнародний стандарт)

3. ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements, 2013. (Міжнародний стандарт)

4. Tom Palmaers, Dennis Distler, Implementing a Vulnerability Management Process //SANS Institute Information Security Reading Room, 2013. 24 с.

5. Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації: затв. Адміністрацією Державної служби спеціального зв'язку та захисту інформації України від 14.05.2020 №269.

6. Поддубний В.О., Сєвєрінов О.В., Пустомельник О.С. Менеджмент вразливостей як складова частина політики безпеки ІТС // Системи управління, навігації та зв'язку. – Полтава: ПНТУ. - 2020. – Вип. 4(62). – С. 55-58.

7. Кіберполіція [Електроний ресурс]:[запис в Facebook від 27.06.2017]-Режим доступу: https://www.facebook.com/cyberpoliceua/posts/536947343096100

8. Common Vulnerabilities and Exposures [Електроний ресурс]:[Веб-сайт]-Режим доступу: https://cve.mitre.org

9. Software Engineering Institute. CERT Coordination Center [Електроний ресурс]:[Веб-сайт]-Режим доступу: https://www.kb.cert.org/vuls/

10. National Vulnerability Database [Електроний ресурс]:[Веб-сайт]-Режим доступу: https://nvd.nist.gov

11. AlienVault ранжировала эксплойты по итогам 2017 года – [Електроний ресурс]:[Веб-сайт]-Режим доступу: \WWW/http://dfir.pro/index.php?link_id=80860

12. Вразливість нульового дня [Електроний ресурс]:[Веб-сайт]-Режим доступу: https://uk.wikipedia.org/wiki/Вразливість_нульового_дня

13. Cybersecurity Help s.r.o. [Електроний ресурс]:[Веб-сайт]-Режим доступу: https://www.cybersecurity-help.cz/

14. CVSS Specification Document [Електроний ресурс]:[Веб-сайт]-Режим доступу: https://www.first.org/cvss/specification-document

15. Поддубний В.О., Сєвєрінов О.В., Менеджмент вразливостей з використанням формалізованого опису// Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 72 – 77.

16. Поддубний В.О., Сєвєрінов О.В., Менеджмент вразливостей як складова частина системи управління інформаційної безпеки // Проблеми інформатизації: восьма міжнародна науково-технічна конференція. 2020 Том 1: секції 1-3 с. 98

17. Umbrello Project [Електроний ресурс]:[Веб-сайт]-Режим доступу: https://umbrello.kde.org