МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій,
обліку та фінансів
Кафедра комп'ютерних технологій
і моделювання систем

Кваліфікаційна робота
на правах рукопису

Острогляда Євгенія Андрійовича

УДК 004.056:366:71

КВАЛІФІКАЦІЙНА РОБОТА

Оцінка стану безпеки банку на основі SIEM-системи

125 - Кібербезпека

Подається на здобуття освітнього ступеня магістр

кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Острогляд Є. А.

Керівник роботи
Євсеєв Сергій Петрович
д.т.н., професор

Житомир – 2023

Висновок кафедри_____

за результатами попереднього захисту: _____

Протокол засідання кафедри_____

№___від «____» _____ 20___р.

Завідувач кафедри_____

_____ _____ _____

(науковий ступінь, вчене звання) (підпис) (прізвище, ім’я, по батькові)

«____»_____20_____р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти _____захистив (ла)

(прізвище, ім’я, по батькові)

кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою_____

за шкалою ECTS _____

за національною шкалою_____

Секретар ЕК

_____ _____ _____

(науковий ступінь, вчене звання) (підпис) (прізвище, ім’я, по батькові)

АНОТАЦІЯ

Острогляд Є.А. Оцінка стану безпеки банку на основі SIEM-системи – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня магістр за спеціальністю 125 – кібербезпека. – Поліський національний університет,

Житомир, 2024.

Магістерська робота присвячена оцінці стану безпеки банку на основі SIEM-системи. У роботі розглянуто сучасні системи для захисту інформаційних ресурсів банків у порівнянні, розглянуто їх функції, переваги та недоліки та завдання, які вони виконують, проведено класифікацію кібератак на основі моделі OSI.

Основною частиною є розробка методики методології комплексного підходу для оцінки рівня безпеки банківських інформаційних ресурсів. В методиці представлено, синергетична моделі загроз, удосконалений класифікатор загроз, модель зловмисника, модель оцінки захищеності банківських інформаційних ресурсів та модель інфраструктури автоматизованих банківських систем. Запропонована методика встановлює підхід до формування стратегій реагування на загрози інформаційної безпеки.

Окремою частиною роботи є процес випробування розробленої методики, підтверджуючи її ефективність в реальних умовах. Застосування методика на практиці дозволило отримати переконливі результати щодо оцінки рівня кібербезпеки інформації в банківських системах, тим самим дозволяє оптимізувати затрати на систему захисту інформації.

Ключові слова: безпека банківських інформаційних ресурсів, автоматизована банківська система, синергетична модель загроз безпеці БІР, класифікатор загроз безпеці БІР, інформаційна безпека, кібербезпека, безпека інформації.

SUMMARY

Ostroglyad E.A. Assessment of the state of bank security on the basis of the SIEM system - Qualification work on the rights of the manuscript.

Qualification work for obtaining a master's degree in the specialty 125 - cyber security. – Polis National University, Zhytomyr, 2024.

The master's thesis is devoted to the evaluation of the security state of the bank on the basis of the SIEM system. The paper examines modern systems for protecting information resources of banks in comparison, examines their functions, advantages and disadvantages and the tasks they perform, classifies cyber attacks based on the OSI model.

The main part is the development of a comprehensive approach methodology for assessing the level of security of banking information resources. The methodology presents a synergistic threat model, an improved threat classifier, an attacker model, a model for assessing the security of banking information resources, and a model of the infrastructure of automated banking systems. The proposed methodology establishes an approach to the formation of response strategies to information security threats.

A separate part of the work is the process of testing the developed methodology, confirming its effectiveness in real conditions. The application of the methods in practice made it possible to obtain convincing results regarding the assessment of the level of cyber security of information in banking systems, thereby allowing to optimize the costs of the information protection system.

Keywords: security of banking information resources, automated banking system, synergistic model of BIR security threats, BIR security threat classifier, information security, cyber security, information security.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ 6
ВСТУП 7
РОЗДІЛ 1. ФУНКЦІЇ ТА СФЕРА ЗАСТОСУВАННЯ. ПОРІВНЯЛЬНИЙ АНАЛІЗ ІСНУЮЧИХ СИСТЕМ 9
1.1 Призначення системи 9
1.2 Область використання SIEM 9
1.3. Аналіз сучасних загроз 11
1.4. Аналіз застосунків, які використовуються для створення системи захисту інформації 12
Висновок до 1 розділу 14
2 ДОСЛІДЖЕННЯ SIEM-СИСТЕМ: АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ ТА ОЦІНКА РИЗИКІВ 15
2.1. Аналіз SIEM-систем 15
2.2. Методи оцінки та виявлення аномалій 17
2.3 Класифікатори загроз та розроблення методу оцінки на основі класифікатора загроз 19
Висновок до 2 розділу 21
3 РЕАЛІЗАЦІЯ БЕЗПЕКИ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ 22
3.1 Методика комплексного підходу оцінки поточного стану інформаційної безпеки банку 23
3.2 Реалізація методології комплексного підходу для оцінки рівня безпеки банківських інформаційних ресурсів 29
Висновок до розділу 3 35
ЗАГАЛЬНІ ВИСНОВКИ 36
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 38
ДОДАТКИ 40

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ

АБС – автоматизована банківська система;

БІ – безпека інформації;

БІн – банківська інформація;

БД – база даних;

БІР – банківський інформаційний ресурс;

ЗЗІ – засоби захисту інформації;

ІБ – інформаційна безпека;

ІР – інформаційний ресурс;

ІС – інформаційна система;

ОБС – організація банківського сектору

КЗ – контрольована зона;

КС – комп’ютерна система;

КМ – комп’ютерна мережа

КТ – кінцева точка;

КСЗІ – комплексна система захисту інформації;

СПБШ – система протидії банківському шахрайству;

СППР – система підтримки прийняття рішень;

ТСЗІ – технічні засоби захисту інформації;

ВСТУП

Актуальність роботи: в наш час, важливу роль національної безпеки України та інформаційної безпеки банків відіграють сучасні механізми профілювання поведінки користувачів, які не завжди досягають повної ефективності, що може призводити до того, що протягом тривалого періоду порушники можуть функціонувати у внутрішній мережі, залишаючись непоміченими, через що, збитки від порушень безпеки приносять збитки як і для банків, так і для клієнтів банку.

Метою і завдання роботи: огляд та аналіз сучасних систем для захисту інформаційних ресурсів банків, ідентифікація переваг та недоліків цих систем. Розробка вдосконаленого класифікатора загроз на основі комплексного підходу, оцінка рівня небезпеки, що виходить від зловмисників, і ступеня ефективності захисних заходів, результати дослідження яких, дозволять вчасно реагувати події, формуючи превентивні заходи для запобігання реалізації загроз та розробляти плани інвестування в технічні засоби захисту інформації.

Завдання:

Об’єкт дослідження: процес удосконалення класифікації загроз та методів оцінки ризиків.

Предмет дослідження: методики оцінки ризиків банківської інформації.

Методи дослідження: прийоми індукції та дедукції, узагальнення, системний аналіз, математичний аналіз.

Апробація результатів:

1. Острогляд Є.А., Євсеєв С.П. Аналіз систем виявлення аномалій в об’єктах критичної інфраструктури. *Безпека, технології, інновації: нові горизонти* : збірник праць учасників між факультетської науково-практичної інтернет-конференції здобувачів вищої освіти і молодих вчених, 15 листопада 2023 р. Житомир : Поліський національний університет, 2023. 68 с.
2. Острогляд Є.А., Дрейс Ю. О. Аналіз комплексної системи санкціонованого доступу. *Інформаційні технології та моделювання систем* : збірник праць учасників Всеукраїнської науково-практичної конференції здобувачів вищої освіти і молодих вчених, 30 березня 2023 р. Житомир : Поліський національний університет, 2023. 140 с.
3. Острогляд Є.А. Роль інноваційних технологій у вдосконаленні заходів протидії кібератакам SIEM-систем. *Практичні та теоретичні питання розвитку науки та освіти*: матеріали XI Міжнародної науково-практичної конференції м. Львів, 9-10 лютого 2024 року. – Львів : Львівський науковий форум, 2024. – 57 с.

Практична цінність: розроблено методологію оцінки захищеності банківських установ.

Загальна характеристика кваліфікаційної роботи: 51 с., 8 табл., 22 рис., 2 дод., 15 джерел.

РОЗДІЛ 1. ФУНКЦІЇ ТА СФЕРА ЗАСТОСУВАННЯ. ПОРІВНЯЛЬНИЙ АНАЛІЗ ІСНУЮЧИХ СИСТЕМ

1.1 Призначення системи

У сучасних умовах одним із ключових викликів для організацій є комплексне забезпечення інформаційної безпеки, що є особливо важливим для плідної роботи підприємства. Потік інформації, що передається різними каналами, такими як лінії зв'язку та розподільчі інформаційні системи, може бути недостатньо захищеним і може призвести до втрати конфіденційної інформації компанії. Несанкціонований доступ до важливої конфіденційної інформації може зашкодити репутації компанії. Порушники можуть передати інформацію конкурентам, чинити тиск на керівництво організації або передати фінансову звітність чи іншу економічну інформацію зацікавленим особам з метою дискредитації організації.

Впровадження системи SIEM (Security information and event management) яка проводити збір, об'єднання та аналіз подій безпеки в реальному часі, отриманих від різних джерел, таких як: програми, пристрої, сервери, датчики систем безпеки, бази даних та користувачі організації. Виявляє нетипові дії та надає інформацію, у зручному вигляді, щоб фахівці з безпеки могли ефективно реагувати, виявляти та блокувати кібератаки.

Що призведе до підвищення рівня виявлення подій у всій корпоративній мережі, дозволяючи організаціям ефективно реагувати на можливі кібератаки та відповідати вимогам стандартів безпеки.

SIEM може бути представлений як додатками, пристроями або сервісами, а також використовується для журналювання даних та створення звітів для взаємодії з іншими бізнес-даними [2].

1.2 Область використання SIEM

SIEM система використовується:

1) Фінансовий сектор: банки та фінансові установи використовують SIEM для захисту фінансових транзакцій, виявлення шахрайства та дотримання регуляторних вимог.
2) IT-галузь: компанії з сфери інформаційних технологій використовують SIEM для захисту корпоративних мереж, виявлення атак та управління подіями в реальному часі.
3) Організації з важливою інформацією: установи, які обробляють конфіденційну інформацію, таку як лікарні та наукові установи, використовують SIEM для забезпечення конфіденційності та запобігання витокам даних.
4) Виробничий сектор: компанії, які виробляють товари або надають послуги, використовують SIEM для захисту виробничих систем та даних виробничого процесу.
5) Торгівля та роздрібна галузь: роздрібні компанії використовують SIEM для захисту від кіберзлочинців, виявлення крадіжок та оптимізації управління подіями в точках продажу.
6) Телекомунікації: компанії з галузі телекомунікацій використовують SIEM для захисту своїх мереж, виявлення атак і забезпечення якості обслуговування.
7) Державні установи: урядові та публічні організації використовують SIEM для забезпечення кібербезпеки та виявлення загроз національній безпеці.

А також, установи де є інформаційні потоки, які пересилаються через різноманітні канали, які можуть мати недостатній рівень захисту, що може призвести до витоку інформації.

1.3. Аналіз сучасних загроз

Загроза – умови або події, які можуть спричинити потенційні або реально існуючі порушення політики безпеки інформації і завдати шкоди автоматизованій системі [3].

Щоб проаналізувати основні види загроз можна використати модель тріади CIA (confidentiality, integrity, availability) [4]. В цій моделі безпека інформації БІР - процес забезпечення конфіденційності, цілісності та доступності інформації клієнтами представлено схемою на рис. Б.1.

Враховуючи особливості банківського сектора, основні загрози безпеці інформації на банківських інформаційних ресурсах представлені в таблиці А.1, за характером впливу зображені на рисунку Б.2.

Основними загрозами кібербезпеці АБС, які мають на меті порушити або контролювати процеси управління, є кібератаки, які поділяються на чотири основні класи, які зображені на рисунку Б.3.

Класифікація наочно свідчить, що кібератаки різних класів не залежно від функціонального призначення мають місце на різних рівнях моделі взаємодії відкритих систем OSI.

Вибір цілі зловмисника значною мірою залежить від його технічної підготовки, наявності необхідних інструментів та знань про внутрішні процеси банку, які є предметом інтересу злочинців. Одним з найбільш поширених та ефективних методів проникнення в інфраструктуру банку є розсилання фішингових листів на електронну пошту співробітників банку або розповсюдження шкідливого ПЗ через відвідувані веб-сайти.

Отримавши доступ до локальної мережі банку, зловмисник намагатиметься отримати права локального адміністратора на комп'ютерах співробітників і серверах. Після отримання максимальних привілеїв в системі вузла, зловмисники витягують облікові дані всіх користувачів з пам'яті системи, такі як ідентифікатори, паролі або геш-

суми паролів. Ці дані використовуються для підключення до інших комп'ютерів в мережі.

Зафіксувавшись в мережі та отримавши права адміністратора, зловмисник може витягти паролі до додатків або зашифрованих баз, а потім отримати відкритий доступ до всіх критично важливих систем банку, таких як АБС, SWIFT, автоматизоване робоче місце для управління банкоматами та інші.

1.4. Аналіз застосунків, які використовуються для створення системи захисту інформації

СПБШ (Системи протидії банківського шахрайства) виявляють і запобігають шахрайству, яке не має початкового, або кінцевого етапу і повинно здійснюватися безперервно і має такі підпроцеси: моніторинг, виявлення, прийняття рішень та навчання. Можливості СПБШ зображені на рисунку Б.4.

Endpoint Detection and Response (EDR) – це технологія, яка спрямована на виявлення та реагування на загрози на рівні кінцевих точок в мережі організації, захищаючи як від широкомасштабних відомих загроз, так і від багатьох невідомих, але в більшості випадків не є достатнім рішенням. Можливості EDR наведені на рисунку Б.5.

Система Check Point SandBlast Zero-Day Protection – рішення для захисту від атак "нульового дня" – атаки стосуються вразливостей в програмному забезпеченні, які ще не були відомі розробникам або виробникам, тому відсутні ефективні захисні заходи і має виконує наступні функції, що зображені на рисунку Б.6.

DLP-система – це система захисту від втрати даних, яка призначена для виявлення, моніторингу та запобігання витоку чутливої інформації з внутрішньої мережі організації. Основна мета DLP-систем - забезпечити контроль за рухом даних та попередження витоків інформації, часто спричинених недбалістю або зловживанням прав доступу користувачів.

DLP-системи використовують для:

1) Контролю використання співробітниками робочого часу і робочих ресурсів;
2) Моніторингу комунікацій співробітників для виявлення "таємної" діяльності;
3) Контролю законності поведінки співробітників.

Можливості DLP-систем:

1) Моніторинг: відвіданих веб-сайтів; фіксування натискань клавіш; змісту буфера обміну; електронної пошти.
2) Пошук: виявлення витоків за заданими шаблонами; моніторинг діяльності конкретного співробітника.
3) Запис: запис з веб-камер; запис з мікрофонів; зняття скріншотів.
4) Оформлення звітів: оцінка ризиків; історія активності; журналювання встановленого ПЗ; ведення контролю за обладнанням.

SIEM (Security information and event management) – технологія яка об'єднує:

1) SIM (управління інформаційною безпекою) – забезпечує довгострокове зберігання, аналіз і звітність збережених даних, журналів подій і надання аналітичній команді відповідних висновків.
2) SEM (управління подіями безпеки) – здійснює моніторинг у режимі реального часу, кореляцію подій, оповіщення та індикацію кінцевих точок (нові підключення, можливі проблеми, підозріла поведінка) [2].

Функції SIEM-систем зображені на рисунку Б.7 [2]:

Звісно, існує велика кількість різних підприємств, і кожне з них встановлює власні системи для досягнення своїх цілей. Однак загалом, перед SIEM-системою стоять дві основні задачі: SIEM обробляє находжену

інформацію відповідно до встановлених вбудованих правил. В результаті роботи SIEM генерує інформаційну панель, звіти та повідомлення про виявлені події.

Аналізуючи отриману інформацію, можна визначити переваги SIEM-систем: Підвищення рівня захищеності від потенційних загроз; Виявлення слабких місць в системі захисту; Створення надійної БД для проведення розслідувань інцидентів; Автоматизація обробки та управління інцидентами ІБ з різних джерел; Здійснення ретроспективного аналізу; Допомога в виявленні та реагуванні на несправності в роботі ІТ та систем інформаційної безпеки.

SIEM-система попереджає про початок атаки ще заздалегідь, виявляючи аномалії в поведінці користувачів, в серверах і в мережі, цим самим виявляючи приховані інциденти, які загрожуватимуть інфраструктурі. Завдяки цьому, експертам по ІБ надається точна інформація, яку можна використати для моніторингу і реагування на потенційні загрози для організації.

Таблиця А.2 містить порівняльний аналіз раніше розглянутих систем з метою визначення найбільш оптимального рішення.

Висновок до 1 розділу

Враховуючи популярні рішення в галузі інформаційної безпеки, можна зазначити, що SIEM видається найбільш повним і універсальним в контексті задоволення потреб користувачів. Воно може бути успішно впроваджене як у невеликі компанії, так і у великі підприємства з численними робочими станціями. Завдяки деталізованій та чітко структурованій звітності, графікам та динамічним таблицям у SIEM-системах, фахівці можуть приймати інформовані рішення щодо захисту комп'ютерної інфраструктури та отримувати своєчасні повідомлення про свіжі проникнення, які можуть призвести до серйозних наслідків.

2 ДОСЛІДЖЕННЯ SIEM-СИСТЕМ: АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ ТА ОЦІНКА РИЗИКІВ

2.1. Аналіз SIEM-систем

Успішні плани реагування та втручання повинні забезпечувати швидке і точне виконання заходів протидії для мінімізації можливих втрат від потенційних загроз. Для досягнення цієї мети SIEM-система повинна вирішувати завдання, які зображені на рисунку Б.8.

Тим самим, SIEM здатна відстежити небезпечні фактори, які зображені на рисунку Б.9.

Відстеживши загрози, SIEM-система генерує звіти на виході, формування звітності зображено на рисунку Б.10.

SIEM-системи не здатні самостійно запобігати інцидентам і не мають вбудованих функцій безпеки. Мета таких систем - визначити пріоритетність інцидентів і виявити першопричини на основі встановлених критеріїв, процес пріорітизації зображений на рисунку Б.11.

Деякі SIEM-системи збирають дані від джерел за допомогою агентів – програмний компонент, який аналізує і фільтрує записи системного журналу (logs) від цільової системи і передає SIEM [5]. Якщо не має необхідного джерела, події можуть бути передані у форматі Syslog. Також є можливість дистанційного збору даних, використовуючи з'єднання за протоколами NetBIOS, RPC, TFTP, FTP.

Окрім можливостей обробки обширних потоків різноманітних даних, SIEM-системи дозволяють проводити аналіз минулих подій безпеки та їх наслідків, визначати шляхи атак, створювати моделі та встановлювати нові правила для виявлення загроз, а також оцінювати рівень їх критичності.

Також, для подання результатів в SIEM використовуються панелі управління (dashboards), які визначають організацію інформації у графічному вигляді для зручного розуміння та вирішення завдань. Залежно від мети завдання можна виділити різновиди таких панелей управління.

Аналітичні: візуалізують уже готові результати аналізу обробки даних про події, які відбулися в ІС; Оперативні: відстежують події безпеки або переглядають дані датчиків безпеки в режимі реального часу, як правило, включаючи табличне представлення даних, у деяких випадках доповнене графічними моделями візуалізації, гістограмами та лінійними графіками.

У більшості випадків дослідження інцидентів безпеки проводиться за допомогою інтерактивних таблиць, де елементи часто представлені у вигляді гіперпосилань, які дозволяють перейти до інших даних, що значно спрощує пошук необхідної інформації [6].

SIEM, як і інші системи ІБ, не є комплексним вирішенням всіх проблеми в ІС. Впровадження даної системи є складним та дорогим процесом, а для її експлуатації необхідна наявність кваліфікованого фахівця, який забезпечить контроль безперервності збору подій, управління правилами кореляції, а також буде коригувати і оновлювати правила. Неправильний процес інтеграції SIEM, може призвести до:

- Неефективне управління ресурсами;
- Можлива втрата контролю за інцидентами;
- Можливі втрати в прибутку через несвоєчасне / неадекватного реагування на інциденти ІБ.

Однак грамотне впровадження системи дозволить:

- Здійснювати кореляцію і оцінку впливу ІБ-подій, так і ІТ-процесів на бізнес;
- Проводити аналіз ситуації в інфраструктурі в режимі реального часу;
- Впровадити автоматизацію процесів виявлення загроз та аномалій, а також процесів реєстрації та моніторингу інцидентів.
- Збирати доказову базу для розслідування інцидентів та аномалій, в тому числі відбулися давно.

2.2. Методи оцінки та виявлення аномалій

Хоча SIEM-системи проводять маніпуляції, в режимі реального часу, з великою кількістю подіями безпеки, більша частина із них це звичайна поведінка користувачів, яка не є шкідливою, а інша – інформація про події порушення безпеки. Аналізуючи це, пошук загроз в ІБ можна позиціонувати як виявлення аномалій або відхилень від нормального поведінки користувачів і системи.

Виявлення аномалій – це процес пошуку елементів, подій або спостережень, які не відповідають очікуваному шаблону або значно відрізняються від інших елементів у наборі даних, наприклад: відхилення, викиди або шум [7].

Розглянемо методи виявлення аномалій:

1. Кластеризація. це процес групування схожих об'єктів разом у кластери або групи, не маючи визначених класів. Виявлення аномалій може базуватися на припущенні, що нормальні дані утворюють великі та щільні кластери, а аномальні дані малі та розрізнені. Однією з найпростіших реалізацій методів на основі кластеризації є алгоритм k-середніх [8].
2. Алгоритм найближчого сусіда. Щоб використовувати цей метод, спочатку потрібно визначити поняття міри подібності між об’єктами. Два основні підходи ґрунтуються на наступних припущеннях, зображені на рисунку Б.12.
3. Спектральні методи. Ці методи використовують комбінацію атрибутів, які охоплюють більшу частину варіацій даних, щоб знайти наближення даних. Методика полягає в тому, щоб перетворити вхідні дані у відповідний спектральний простір, де вони можуть бути ефективно оброблені.
4. Класифікація. Цей метод реалізується на основі, що для визначення нормальної поведінки системи потрібно один або

декілька класів. Існує дві фази виявлення аномалій: навчання та ідентифікація. Після навчання класифікатор на масиві даних визначається його приналежність до відомого класу. Якщо не може бути визначеним він позначається, як аномалія. Найбільш поширеними механізмами реалізації ідентифікації аномалій за допомогою класифікації є: нейронні мережі, Баєсівська модель та метод опорних векторів, які зображені на рисунку Б.13.

5. Статистичний аналіз. Підхід передбачає аналіз процесу роботи ІС, створює його профіль та порівнює його з фактичною поведінкою. Коли різниця аномальності між фактичною і ймовірною поведінкою системи, що визначається функцією, вище певної міри, це свідчить про наявність відхилень. Цей метод вигідний тим, що не потребує спеціальних знань про тип аномалії. Є дві групи статистичного аналізу:
   - Параметричні: Вважається, що параметричний розподіл генерує не аномальні дані з параметром "θ" та функцією ймовірності P(x, θ), де "x" - це спостереження. В контексті аналізу аномалій, аномалія визначається через ймовірність того, що спостереження (значення x) буде меншим або рівним певному значенню в розподілі.
   - Не параметричні: Структура моделі не визначається заздалегідь, але формується на основі наявних даних. У базовому алгоритмі виявлення аномалії, використовуються два етапи. Перший – будується гістограма з використанням значень обраної характеристики для зразків навчальних даних. Другий – досліджується належність зразка до одного зі стовпчиків гістограми, якщо він не належить хоча б одному стовпчику він вважається аномалією.

Складемо порівняльну таблицю на основі наведених вище методів виявлення аномалій див. таблиці А.3.

2.3 Класифікатори загроз та розроблення методу оцінки на основі класифікатора загроз

Щоб створити метрику загроз використовуючи комплексний підхід, потрібно побудувати класифікатор загроз на основі моделі подвійних трійок [8], яка зображена на таблиці А.4. Самі компоненти класифікатора розділяються крапкою, а сам класифікатор має вигляд «XX.XX.XX.XX».

Крок 1. Для оцінки вірогідності потенційних впливів загроз на безпеку БІР потрібно:

Нехай класифікатор з чотирма послугами безпеки БІР, який має Т загроз і давали послуги N спеціалістів, має вигляд:

t = {Cn, It, Av, At}; *t* – послуга безпеки; *Cn* – послуга конфіденційності; *It* – послуга цілісності; *Av* – послуга доступності; *At* – послуга автентичності.

Нехай «*x*» – поточний номер загрози ($\{x\}_1^T$) і через «*n*» – поточний номер спеціаліста, котрий виконував оцінку ($\{n\}_1^N$).

Тоді середнє значення експертної оцінки всіх загроз одної послуги буде записане наступним чином [9]:

$$v^t = \frac{1}{N}\sum_{x=1}^{T}\sum_{n=1}^{N} v_{xn}^t\,, \qquad (1)$$

де v_{xn}^t – коефіцієнт, виставлений *n*-м спеціалістом для загрози під номером *x*, послуги *t*; *T* – кількість загроз; *N* – кількість спеціалістів.

Крок 1.2. Далі потрібно щоб спеціалісти сформували цифрове значення ідентифікатора загрози, відповідно до компонентів класифікатора.

Крок 1.3. Потрібно обрати вагові коефіцієнти b_t для розрахунку виникнення загрози *t* відповідно до таблиці А.5 [10, 11].

Крок 1.4. Оцінка виникнення кожної загрози, враховуючи вірогідність виникнення атаки.

Щоб визначити виникнення кожної загрози позначеної як *t*, враховуючи ймовірність виникнення атаки, можна використати формулу:

$$v_x^t P_x^t = \frac{1}{N} P_x^t \sum_{n=1}^{T} v_{xn}^t \,, \tag{2}$$

Для конкретної послуги забезпечення безпеки та *i*-ї загрози використовують формули:

$$\begin{gathered} v_x^{It} b_x^{It} = \frac{1}{N} b_x^{It} \sum_{n=1}^{N} v_{xn}^{It} \text{ – послуга цілісності,} \\ v_x^{Av} b_x^{Av} = \frac{1}{N} b_x^{Av} \sum_{n=1}^{N} v_{xn}^{Av} \text{ – послуга доступності,} \\ v_x^{Cn} b_x^{Cn} = \frac{1}{N} b_x^{Cn} \sum_{n=1}^{N} v_{xn}^{Cn} \text{ – послуга конфіденційності,} \\ v_x^{At} b_x^{At} = \frac{1}{N} b_x^{At} \sum_{n=1}^{N} v_{xn}^{At} \text{ – послуга автентичності,} \end{gathered} \tag{3}$$

де v_{xn}^{It} v_{xn}^{Av} v_{xn}^{Cn} v_{xn}^{At} – поставлені спеціалістами коефіцієнти послуг безпеки: цілісності, доступності, конфіденційності, автентичності;

b_x^{It} b_x^{Av} b_x^{Cn} b_x^{At} – вагові коефіцієнти послуг безпеки виникнення загрози *t*, відповідно до таблиці А.5 [10, 11].

Крок 1.5. Для визначення декількох загроз (синергії) певної послуги використовують вираз:

$$\begin{gathered} V_{syn}^{It} = \sum_{x=1}^{K} v_x^{It} b_x^{It} \text{ – послуга цілісності,} \\ V_{syn}^{Av} = \sum_{x=1}^{K} v_x^{Av} b_x^{Av} \text{ – послуга доступності,} \\ V_{syn}^{Cn} = \sum_{x=1}^{K} v_x^{Cn} b_x^{Cn} \text{ – послуга конфіденційності,} \\ V_{syn}^{At} = \sum_{x=1}^{K} v_x^{At} b_x^{At} \text{ – послуга автентичності,} \end{gathered} \tag{4}$$

де K – кількість загроз вибраних спеціалістом з безпеки банку з множини $\{x\}_x^K$ – підмножина всього набору множин загроз, іншими словами $K \leq T$.

Формуючи метричні коефіцієнти передбачається, що результати відносяться до незалежних загроз, якщо існує залежність, коли класифікатор вказує на збіг, потрібно використати вираз для визначення повної вірогідності залежних інцидентів [12]:

$$P(AB) = P(A) + P(B) - P(AB).$$

Загальна середня оцінка загрози t розраховується за кількості спеціалістів за формулою:

$$i_x = \frac{\sum_{n=1}^{N} i_n \times n_n}{N},$$

де – i_n оцінка впливу загрози x спеціалістом n; n_n – рівень знань спеціаліста; N – кількість спеціалістів.

Щоб оцінити погодженість думок спеціалістів, потрібно обчислити дисперсію за виразом:

$$\sigma_i^2 = \frac{1}{N}\sum_{n=1}^{N} n_n (i_n - i_x)^2,$$

Статистичне значення отриманого результату з ймовірністю $1-b_x$, дорівнює: $[i_x - \Delta, i_x + \Delta]$, де i_x є значенням, розподіленим за нормальним законом із центром у i_x та дисперсією σ_i^2. Величина Δ визначається згідно наступного виразу:

$$\Delta = j\sqrt{\sigma_i^2 / K},$$

де – j = 0,95, значення розподілу Стюдента для N – 1 ступенів; N – кількість спеціалістів [13].

Крок 1.6. Враховуючи формули (3) обчислення загальної комплексної загрози розраховується за формулою:

$$V_{syn}^{BI} = \sum_{x=1}^{T}(v_x^{Cn} \cap v_x^{It} \cap v_x^{Av} \cap v_x^{At})b_x,$$
$$V_{syn}^{KB} = \sum_{x=1}^{T}(v_x^{Cn} \cap v_x^{It} \cap v_x^{Av} \cap v_x^{At})b_x,$$
$$V_{syn}^{IB} = \sum_{x=1}^{T}(v_x^{Cn} \cap v_x^{It} \cap v_x^{Av} \cap v_x^{At})b_x. \quad (5)$$

Крок 1.7. Визначення загальної комплексної загрози в ресурсах АБС:

$$V_{syn}^{BI.KB,IB} = V_{syn}^{BI} \cup V_{syn}^{KB} \cup V_{syn}^{IB}. \quad (6)$$

Крок 1.8. Розрахунок з урахуванням гібридності, загальної комплексної загрози визначається за формулою:

$$V_{syn}^{hyb\ Cn,It,Av,At} = V_{syn}^{Cn} \cap V_{syn}^{It} \cap V_{syn}^{Av} \cap V_{syn}^{At}. \quad (7)$$

В результаті ми отримуємо вдосконалений класифікатор загроз безпеки БІР на основі синтетичної моделі загроз.

Висновок до 2 розділу

Було порівняно найбільш часто використовувані системи в SIEM, з урахуванням основних можливостей кожної системи та визначено основні можливості класифікації. Представлена ідея базується на комплексному

підході по рішенню найбільш оптимальних методів для досягнення задач по безпеки БІР в АБС, враховуючи рівень ризику на кожному рівні та забезпечуючи ефективний контроль, виконуючи функції, пов’язаними з системами управління інформаційною безпекою в ОБС.

Було використано і вдосконалено класифікатор загроз безпеки БІР для визначення оцінки рівня захищеності від загроз за видами послуг, рівнем ієрархії інфраструктури АБС, особливості інформації, характеру напряму атаки, враховуючи гібридність та вірогідності впливу.

3 РЕАЛІЗАЦІЯ БЕЗПЕКИ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

3.1 Методика комплексного підходу оцінки поточного стану інформаційної безпеки банку

Процес оцінювання результативності роботи комплексної системи захисту БІР в АБС при комплексному підході потребує провести наступні етапи:

1. Етап 1 – Оцінка вірогідності потенційних впливів загроз на безпеку БІР на основі вищезазначеного класифікатора загроз, який був розписаний відповідно розділу 2.3;
2. Етап 2 – Встановлення взаємозв'язків між об'єктами АБС, БІР та загрозами за допомогою вдосконаленої моделі АБС, синергетичної моделі загроз, удосконаленого класифікатора загроз і моделі порушника;
3. Етап 3 – Встановлення комплексного показника безпеки БІР [1, 14].

Етап №2. Встановлення взаємозв'язків між об'єктами АБС, БІР та загрозами за допомогою вдосконаленої моделі АБС, синергетичної моделі загроз, удосконаленого класифікатора загроз і моделі порушника.

Синергетична модель безпеки БІР базується на основі методів та комплексному підході безпеки БІР, оцінки рівня безпеки інформаційних ресурсів в БС в умовах гібридності загроз, а також моделей: синергетичної моделі, удосконалених інфраструктурної моделі АБС, моделі зловмисника та оцінки безпеки АБС.

Удосконалена інфраструктурна модель АБС має такий вигляд:

$$X^{ABS} = \{\{K^{ABS}\}, \{M^{ABS}\}, \{L_A\}\},$$

де K^{ABS}– множина об'єктів, що характеризують компоненти АБС та їх відношення до рівнів ієрархії АБС; M^{ABS}– множина взаємозв'язків між

компонентами, яка вираховується за допомогою матриці суміжності в наступному кроці; L_A – множина об'єктів інформаційних ресурсів банку.

Крок 2.1. Визначення взаємозв'язків між активами БІР $\{L_A\}$ та елементами АБС [14]:

$$A^{ABS} = \|a_{ij}^{ABS}\|.$$

Кожен компонент $L_{A_i} \in \{L_A\}$ можна уявити у вигляді вектора $L_{A_i} = (T, X^{Cn}, X^{It}, X^{Av}, X^{At}, C_T)$, де Т – тип активу, який описується множиною: $T = \{BS, PD, CD, CS, SR, PaI, MI, PD\}$, де BS – банківська таємниця; PD – платіжний документ; *CD* – кредитний документ; *CS* – комерційна таємниця; *SR* – статистичні звіти; *PaI* – доступна інформація; *MI* – керівна інформація; PD – персональні дані. X^{Cn}– конфіденційність; X^{It}– цілісність; X^{Av}– доступність; X^{At}– автентичність; C_T– властивість безперервності інформації, котру необхідно забезпечувати. Значення набувають «1» – якщо властивість потрібна, «0» – в інших випадках.

Крок 2.2. Визначення взаємозв'язків між активами БІР $\{L_A\}$ та об'єктами середовища $Obj_l \in \{Obj^{ABS}\}$ представляється у вигляді вектора $Obj_l = \{X^{ABS}, IObj\}$, де X^{ABS} – рівень ієрархії структури, яка визначається множиною $X^{ABS} = \{FL, NL, OSL, DBL, BL\}$, де FL фізичний рівень; NL –

мережевий рівень; OSL – рівень операційних систем; DBL – рівень управління БД; BL – рівень банківських технологій.

Щоб визначити тип зв'язку та співвідношення $IObj^R$ інформаційних активів і компонентами АБС використовують формулу:

$$IObj^R = \|IObj_{xt}^R\|,$$

де $IObj_{xt}^R$ – вказує характер зв'язку і його наявність між інформаційним активом *x* та компонентом середовища АБС *t*.

При цьому $\forall x \in \{L_a\}$, а $\forall t \in \{Obj^{ABS}\}$ свідчить що:

$$IObj_{xt}^{R} = \begin{cases} 0 - \text{зв}'\text{язок відсутній} \\ cs - \text{включає і зберігає} \\ pt - \text{обробляє або передає} \\ so - \text{підримує функціонування} \end{cases}$$

Вагові категорії призначаються кожному параметру, відповідно до правила Фішберна [15], яке базується на факті, що зміна вагових коефіцієнтів критеріїв слідує за спадною арифметичною прогресією. У цьому випадку найважливіший і найвищий ваговий коефіцієнт, це самий перший критерій (x = 1), розташований за важливістю у ранжованому ряду критерії x = 1,2,3, ..., k. Це правило виражається у вигляді формули:

$$W_x = \frac{2\,(K-k+1)}{K(K+1)},$$

де W_x – ваговий коефіцієнт Фішберна; K – сумарна кількість параметрів; k – номер, який визначає позицію параметра; x – кількість параметрів.

Згідно з формулою Фішберна, ми отримуємо:

$$W_1 = \frac{2 \times K}{K(K+1)}, W_N = \frac{2}{N(N+1)}, \gamma = \frac{W_1}{W_N} = K,$$

де γ – це кількість разів, на яку вагові коефіцієнти відрізняються один від одного.

Крок 2.3. Використання синергетичної моделі загроз і удосконаленої моделі зловмисника для визначення складності множин загроз.

Синергетична модель загроз має такий вигляд [1,15,16]:

$$STM^{ABS} = \left\{\{MT^{ABS}\}, \{X_{risk}\}, \{X_P\}, \{X_U\}, \{SD\}\right\}. \quad (8)$$

де MT^{ABS} – сукупність потенційних джерел загроз; $\{X_{risk}\}$ – показник ризику; $\{X_P\}$ – набір умов, що представляють ймовірність виникнення принаймні однієї загрози для активу t; $\{X_U\}$ – набір величин термінів, які формують збиток від реалізації загрози; $\{SD\}$ – набір руйнівних станів компонентів системи.

Удосконалена модель порушника записується формулою [15,17]:

$$D_{IX}^{ABS} = \{id_x, m_x, T_{IX}, PL_{max_x}, Pr_t, R_x^{ABS}\} \forall x \in k, \forall t \in a, \quad (9)$$

де id_x – унікальний номер, або категорія зловмисника; m_x – мета зловмисника; T_{IX} – час, який потрібно загрозі на реалізацію; PL_{max_x} – потенційний збиток системи; Pr_t – ймовірність, що загроза реалізується хоча б раз в активі *x*; R_x^{ABS} – рекомендації по виявленню, реагуванню ТСЗІ.

На основі моделей (7,8) можна визначити складність множин загроз:

$$G^{ABS} = \{A^{NS}\} \cup \{A^{AS}\}, \quad (10)$$

де $\{A^{AS}\} = \{A^{IB}\} \cap \{A^{KB}\} \cap \{A^{BI}\}$, де $\{A^{NS}\}$ – тип джерела природних загроз; $\{A^{AS}\}$ – тип антропогенних загроз; $\{A^{IB}\}$, $\{A^{KB}\}$, $\{A^{BI}\}$, – множини загроз ІБ, КБ, БІ.

Крок 2.4. Оцінка ціни ризику всіх об’єктів БІР.

Ціна ризику дорівнює сумі цін ризику всіх об’єктів БІР розраховується за формулою:

$$TRP = \sum_{i=1}^{n} RP_i ,$$

де RP_i – ціна ризику для кожного окремого компонента; *n* – загальна кількість об’єктів.

$$RP_i = pr_t \times q_t,$$

де pr_j – ймовірність реалізації хоча б однієї загрози активу t; q_t – збиток;

Крок 2.5. Оцінка вірогідності виникнення принаймні однієї загроза для кожного об’єкта БІР. Розрахунок цієї ймовірності виконується за формулою:

$$P_{rt} = 1 - \prod_{x=1}^{n}(1 - P_{xt}) ,$$

де P_{xt} – ймовірність реалізації загрози *x* для об’єкта *t*.

Крок 2.6. Оцінка взаємозв’язку між джерелами загроз та об’єктами АБС

$$M^{MT} = \left\| m_{ij}^{MT} \right\|,$$

Етап 3. Розрахунку комплексної оцінки захищеності БІР з використанням покращеної моделі оцінки безпеки.

Для розрахунок захищеності АБС від загроз ІБ, КБ, БІ на БІР пропонується використовувати модель [16]:

$$TL_{OZ}^{ABS} = \{\{L_A\}, \{K^{ABS}\}, \{MT^{ABS}\}, \{Rr^{ABS}\}, \{MPS^{ABS}\}, \{\text{SAR}^{ABS}\}, \{SL_r^{ABS}\}\},$$

де $\{L_A\}$ – множина об'єктів інформаційних ресурсів банку; $\{K^{ABS}\}$ – множина об'єктів рівнів ієрархії АБС; $\{MT^{ABS}\}$ – сукупність загроз безпеці АБС; $\{Rr^{ABS}\}$ – сукупність вимог безпеки регуляторів АБС; $\{MPS^{ABS}\}$ – множина можливих ТСЗІ; $\{\text{SAR}^{ABS}\}$ – інформація про безпеку АБС; $\{SL_r^{ABS}\}$ – рівень безпеки АБС.

Крок 3.1. Визначення взаємозв'язку між загрозами та технічними засобами захисту інформації.

Кожен захисний механізм банку $MPS_i \in \{MPS^{ABS}\}$ визначається вектором $MPS_i = (X_{MPS}, T_{imp}, V_{MPS})$, де X_{MPS} – вид захисту; T_{imp} – час для впровадження; V_{MPS} – вартість.

Згідно з формулою (22) формування взаємозв'язків між загрозами та ТСЗІ можна описати такою формулою:

$$M^{MTMPS} = \left\| m_{ij}^{MTMPS} \right\|,$$

враховуючи $\forall j \in \{L_A\}, \forall i \in \{MT_i\}$

$$\|M^{MT}\| = \begin{cases} 1, \text{якщо загроза } i \text{ існує для об'кту } j \\ 0, \text{якщо загроза } i \text{ відсутня для об'кту } j \end{cases}$$

де m_{ij}^{MTMPS} – вказує на присутність взаємозв'язків між i-ю загрозою $MT_i \in \{MT^{ABS}\}$ і j-м засобом захисту інформації $MPS_i \in \{MPS^{ABS}\}$.

Дана модель використовуються два типи зв'язку:

- MZ – має механізм захисту від деструктивного впливу $SD_i \in \{SD\}$;
- NMZ – немає механізму захисту від загрози i.

Елементи матриці визначаються за правилом:

$$\left\| m_{ij}^{MTMPS} \right\| = \begin{cases} MZ - \text{якщо загроза } i \text{ виявляється } j \text{ засобом} \\ NMZ - \text{якщо загроза } i \text{ не виявляється } j \text{ засобом} \end{cases}$$

При цьому, що всі $i = \left\| m_{ij}^{MTMPS} \right\| = NMZ$, вказує на те, що засоби захисту інформації банку не можуть захистити інформацію від загроз, а щоб покращити захист банку потрібно витратити додаткові кошти.

Крок 3.2. Формування вимог регуляторів.

Для формування вимог регуляторів використовується формула [16]:

$$\{Rr^{ABS}\} = \{r_{BIR}\} \cup \{PS\} \cup \{CR\},$$

де $\{r_{BIR}\}$ – вимоги до безпеки ресурсів банку; $\{PS\}$ – множина оцінок рівня виконання вимог; $\{CR\}$ – множина загальних рівнів відповідності до вимог безпеки.

Використовуючи вимоги з постанови НБУ [18] для оцінки вимог регуляторів можна зрозуміти, що показники поділяються на типи:

1) Приватні показники, що є обов'язковими для виконання;
2) Приватні показники, що є рекомендовані для виконання.

Для обов'язкових показників рекомендовані оцінки ступеня виконання вимог наведені в таблиці А.6.

Для рекомендованих показників рекомендовані оцінки ступеня виконання вимог наведені в таблиці А.7.

Крок 3.3. Формування загальної оцінки рівня захищеності банку.

Оцінка рівня захищеності банку, яка може визначити відповідність ТСЗІ до вимог регуляторів визначається за формулою:

$$GSI^{ABS} = \sum_{i=1}^{n} GSI_i ,$$

де n – кількість показників безпеки; GSI_i – показник що набуває значення показників: GSI_1 – наявність недопустимого ризику при формуванні моделей загроз, порушника і оцінки ризиків, GSI_1 = 0, якщо визначено ризик, GSI_1 = 1 – ризику немає; GSI_2– наявність загроз з якими не впораються засоби захисту інформації, GSI_2 = 0, якщо виявлені загрози з якими не впораються засоби захисту, GSI_2 = 1, якщо в системі є загрози, які нейтралізовані засобами захисту інформації; GSI_3 – відповідність безпеки

до вимог регуляторів, $GSI_3 = 1$, якщо відповідає вимогам, $GSI_3 = 0$, якщо не відповідає вимогам.

На основі зібраних даних система отримає один із трьох рівнів захисту: SL^{ABS} ={високий, середній, низький}, згідно з правилом:

$$SL^{ABS} = \begin{cases} \text{Високий, якщо } GSI^{ABS} = 3; \\ \text{Середній, якщо } 1 \leq GSI^{ABS} < 3; \\ \text{Низький, якщо } GSI^{ABS} = 0. \end{cases}$$

В результаті, отримана оцінка безпеки інформації дасть сформувати розуміння про найціннішу інформацію, яка циркулює в системі, продуктивність засобів захисту інформації, їх відповідність до вимог стандартів безпеки та ідентифікувати найбільш вразливі місця в системі і на основі цього це дозволяє розробити рекомендації для підвищення інформаційної безпеки в АБС.

3.2 Реалізація методології комплексного підходу для оцінки рівня безпеки банківських інформаційних ресурсів

Етап 1. Визначення вірогідності потенційних впливів загроз на безпеку БІР:

Крок 1.1. Формування оцінки загроз спеціалістами за послугами безпеки.

Використовуючи веб-застосунок [19] було відображено оцінки спеціалістів в формуванні даних для класифікатора загроз, які зображені на рисунку 3.1.

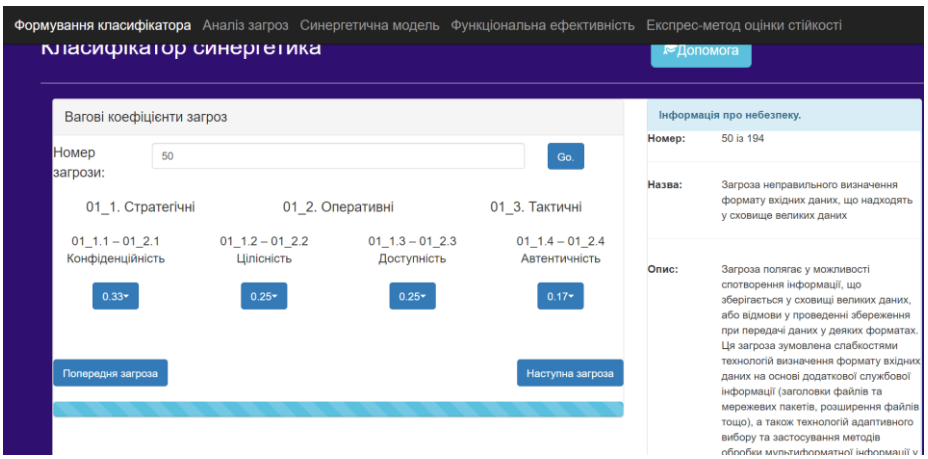


Рис. 3.1 – Формування оцінок загроз

Крок 1.2. Формування цифрових значень ідентифікатора загроз на основі компонентів класифікатора.

Відповідно до таблиці А.4 спеціалісти формую цифрове значення, результати зображені на рисунку 3.2.

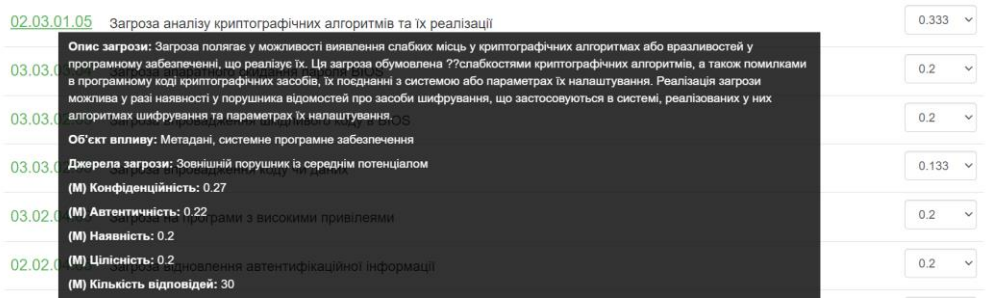


Рисунок 3.2 – Формування ідентифікатора загроз

Крок 1.3. Вибір вагових коефіцієнти b_t вірогідності виникнення загрози.

Згідно таблиці А.5 встановлені значення вагових коефіцієнтів b_t для розрахунку виникнення загрози t обчислюється на основі оцінок спеціалістів для кожної послуги безпеки, ранжуючи результат.

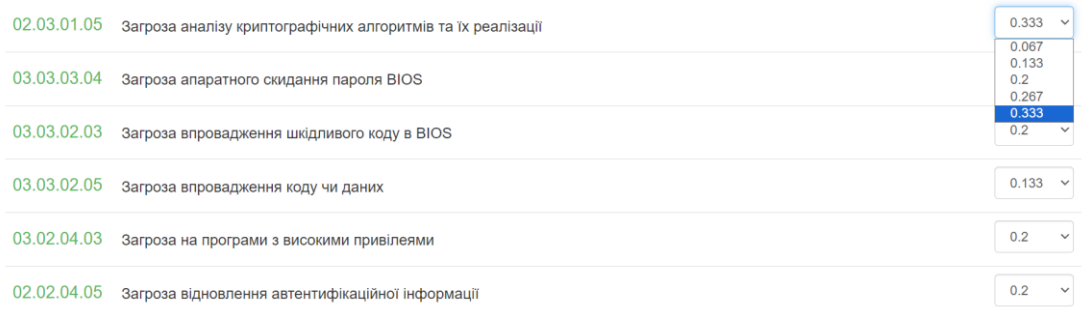


Рисунок 3.3 – Встановлення коефіцієнтів b_t для розрахунку виникнення загрози t.

Крок 1.4. Оцінка виникнення кожної загрози t, враховуючи вірогідність виникнення атаки.

Згідно з формулами (2-3) визначаємо результати виникнення кожної загрози t, враховуючи вірогідність виникнення атаки.

Номер загрози	Короткий опис загрози	μ[C]	μ[I]	μ[A]	μ[Au]	D[C]	D[I]	D[A]	D[Au]
02.03.01.05	Загроза аналізу криптографічних алгоритмів та їх реалізації	0.033	0.083	0.083	0.133	0.11	0.034	0.056	0.03
03.03.03.04	Загроза апаратного скидання пароля BIOS	0.02	0.02	0.132	0.028	0.068	0.07	0.07	0.062
03.03.02.03	• Загроза впровадження шкідливого коду в BIOS • Загроза деструктивного використання декларованого функціоналу BIOS • Загроза несанкціонованого доступу до віртуальних машин, що захищаються з віртуальної та (або) фізичної мережі • Загроза несанкціонованого керування буфером	0.238	0.128	0.116	0.128	0	0	0	0
03.03.02.05	• Загроза впровадження коду чи даних • Загроза заміни вмісту мережевих ресурсів	0.0939	0.0456	0.0755	0.0456	0	0	0	0
03.02.04.03	• Загроза на програми з високими привілеями • Загроза використання підроблених цифрових підписів BIOS • Загроза програмного скидання пароля BIOS	0.097	0.047	0.1669	0.157	0	0	0	0
02.02.04.05	Загроза відновлення автентифікаційної інформації	0.02	0.14	0.02	0.02	0.126	0.035	0.033	0.149
02.02.02.03	Загроза відновлення попередньої вразливої версії BIOS	0.02	0.094	0.066	0.02	0.052	0.078	0.198	0.082

Рисунок 3.4 – Результати оцінювання основних кожної загрози

Крок 1.5. Визначення виникнення декількох загроз для певної послуги розраховується згідно з формулами (3):

$$V_{syn}^{It} = \sum_{x=1}^{K} v_x^{It}\, b_x^{It} = 0.053 + 0.101 + 0.058 = 0{,}212,$$
$$V_{syn}^{Av} = \sum_{x=1}^{K} v_x^{Av}\, b_x^{Av} = 0.14 + 0.0113 + 0.076 = 0{,}329,$$
$$V_{syn}^{Cn} = \sum_{x=1}^{K} v_x^{Cn}\, b_x^{Cn} = 0.065 + 0.076 + 0.047 = 0{,}188,$$
$$V_{syn}^{At} = \sum_{x=1}^{K} v_x^{At}\, b_x^{At} = 0.093 + 0.02 + 0.083 = 0{,}196.$$

Крок 1.6. Обчислення загальної комплексної загрози за складовими безпеки розраховується за формулами (4):

$$V_{syn}^{BI} = 0.047 \times 0.058 \times 0.076 \times 0.083 = 0.0000172$$

$$V_{syn}^{KB} = 0.076 \times 0.101 \times 0.113 \times 0.02 = 0.0000173$$

$$V_{syn}^{IB} = 0.065 \times 0.053 \times 0.14 \times 0.93 = 0.0000449$$

Крок 1.7. Розрахунок загальної комплексної загрози в ресурсах АБС Згідно з формулою (5) визначимо загальну комплексну загрозу:

$$V_{syn}^{BI.KB,IB} = 0.0000172 + 0.0000173 + 0.0000449 = 0.000079.$$

Крок 1.8 Розрахунок з урахуванням гібридності, загальної комплексної загрози визначається за формулою:

Згідно з формулою (6) визначимо загальну комплексну загрозу, враховуючи гібридність:

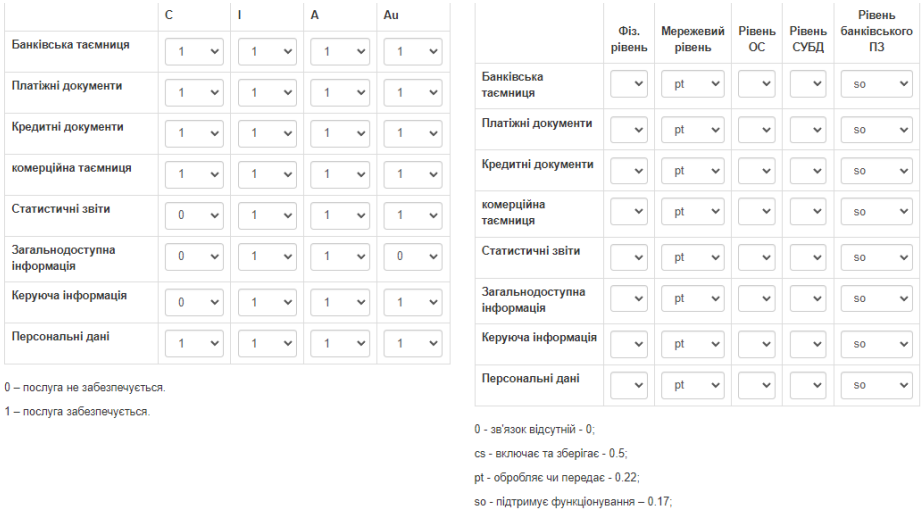
$$V_{syn}^{hyb\ Cn,It,Av,At} = 0.188 \times 0.212 \times 0.329 \times 0.196 = 0.002570.$$

Результати записані в таблицю А.8.

Етап 2. Встановлення взаємозв’язків між об’єктами АБС, БІР та загрозами за допомогою вдосконаленої моделі АБС, синергетичної моделі загроз, удосконаленого класифікатора загроз і моделі порушника.

Крок 2.1. Визначення взаємозв’язків між активами БІР $\{L_A\}$ та елементами АБС.

Крок 2.2. Визначення взаємозв’язків між активами БІР $\{L_A\}$ та об’єктами середовища.



	C	I	A	Au
Банківська таємниця	1	1	1	1
Платіжні документи	1	1	1	1
Кредитні документи	1	1	1	1
комерційна таємниця	1	1	1	1
Статистичні звіти	0	1	1	1
Загальнодоступна інформація	0	1	1	0
Керуюча інформація	0	1	1	1
Персональні дані	1	1	1	1

0 – послуга не забезпечується.

1 – послуга забезпечується.

	Фіз. рівень	Мережевий рівень	Рівень ОС	Рівень СУБД	Рівень банківського ПЗ
Банківська таємниця		pt			so
Платіжні документи		pt			so
Кредитні документи		pt			so
комерційна таємниця		pt			so
Статистичні звіти		pt			so
Загальнодоступна інформація		pt			so
Керуюча інформація		pt			so
Персональні дані		pt			so

0 - зв'язок відсутній - 0;

cs - включає та зберігає - 0.5;

pt - обробляє чи передає - 0.22;

so - підтримує функціонування – 0.17;

Рисунок 3.5 – Результати взаємозв’язків між активами БІР матриці елементами АБС і об’єктами середовища

Крок 2.3. Використання синергетичної моделі загроз і удосконаленої моделі зловмисника для визначення складності множин загроз.

Крок 2.4. Оцінка ціни ризику всіх об’єктів БІР.

Крок 2.5. Оцінка вірогідності виникнення принаймні однієї загроза для кожного об’єкта БІР.

Результати кроків 2.3–2.5 зображені на рисунку 3.6.

	Банківська таємниця	Платіжні документи	Кредитні документи	комерційна таємниця	Статистичні звіти	Загальнодоступна інформація	Керуюча інформація	Персональні дані
02.03.01.05	0.2	0.2	0.2	0.2	0.18	0.1	0.18	0.2
03.03.03.04	0.2	0.2	0.2	0.2	0.18	0.152	0.18	0.2
03.03.02.03	0.2	0.2	0.2	0.2	0.134	0.07	0.134	0.2
03.03.02.05	0.132	0.132	0.132	0.132	0.099	0.066	0.099	0.132
03.02.04.03	0.2	0.2	0.2	0.2	0.17	0.12	0.17	0.2
02.02.04.05	0.2	0.2	0.2	0.2	0.18	0.16	0.18	0.2
02.02.02.03	0.2	0.2	0.2	0.2	0.18	0.16	0.18	0.2
01.02.03.02	0.133	0.133	0.133	0.133	0.133	0.133	0.133	0.133
03.02.03.01	0.132	0.132	0.132	0.132	0.099	0.066	0.099	0.132
03.02.02.03	0.132	0.132	0.132	0.132	0.132	0.132	0.132	0.132
03.03.02.03	0.2	0.2	0.2	0.2	0.06	0.04	0.06	0.2
01.01.03.05	0.132	0.132	0.132	0.132	0.119	0.099	0.119	0.132
03.03.02.04	0.268	0.268	0.268	0.268	0.228	0.094	0.228	0.268
03.01.03.02	0.267	0.267	0.267	0.267	0.23	0.203	0.23	0.267
01.01.03.04	0.2	0.2	0.2	0.2	0.17	0.15	0.17	0.2
03.03.03.03	0.268	0.268	0.268	0.268	0.249	0.222	0.249	0.268
02.03.01.02	0.333	0.333	0.333	0.333	0.223	0.143	0.223	0.333
03.01.03.02	0.267	0.267	0.267	0.267	0.23	0.203	0.23	0.267
01.01.02.05	0.2	0.2	0.2	0.2	0.19	0.17	0.19	0.2
03.03.03.03	0.2	0.2	0.2	0.2	0.19	0.04	0.19	0.2
01.01.03.05	0.132	0.132	0.132	0.132	0.099	0.079	0.099	0.132

Рисунок 3.6 – Вірогідність виникнення і-ї загрози на інформаційних ресурсах

Крок 2.6. Оцінка взаємозв’язку між джерелами загроз та об’єктами АБС.

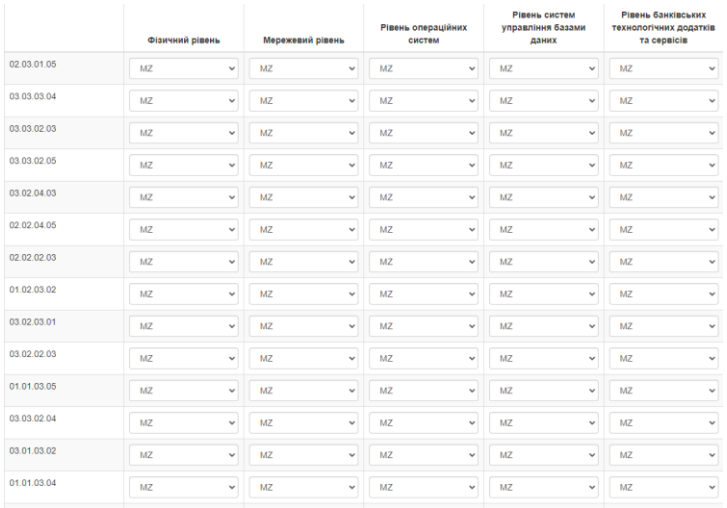
Результат зображений на рисунку 3.7.

	Фізичний рівень	Мережевий рівень	Рівень операційних систем	Рівень систем управління базами даних	Рівень банківських технологічних додатків та сервісів
02.03.01.05	0.3212	0.3212	0.2482	0.73	0.2482
03.03.03.04	0.33264	0.33264	0.25704	0.756	0.25704
03.03.02.03	0.29436	0.29436	0.22746	0.669	0.22746
03.03.02.05	0.20328	0.20328	0.15708	0.462	0.15708
03.02.04.03	0.3212	0.3212	0.2482	0.73	0.2482
02.02.04.05	0.3344	0.3344	0.2584	0.76	0.2584
02.02.02.03	0.3344	0.3344	0.2584	0.76	0.2584
01.02.03.02	0.23408	0.23408	0.18088	0.532	0.18088
03.02.03.01	0.20328	0.20328	0.15708	0.462	0.15708
03.02.02.03	0.23232	0.23232	0.17952	0.528	0.17952
03.03.02.03	0.2552	0.2552	0.1972	0.58	0.1972
01.01.03.05	0.21934	0.21934	0.16949	0.4985	0.16949
03.03.02.04	0.4158	0.4158	0.3213	0.945	0.3213
03.01.03.02	0.43956	0.43956	0.33966	0.999	0.33966
01.01.03.04	0.3278	0.3278	0.2533	0.745	0.2533
03.03.03.03	0.4532	0.4532	0.3502	1	0.3502
02.03.01.02	0.49588	0.49588	0.38318	1	0.38318
03.01.03.02	0.43956	0.43956	0.33966	0.999	0.33966

Рисунок 3.7 – Результат взаємозв’язку між джерелами загроз та об’єктами АБС

Етап 3. Розрахунку комплексної оцінки захищеності БІР з використанням покращеної моделі оцінки безпеки.

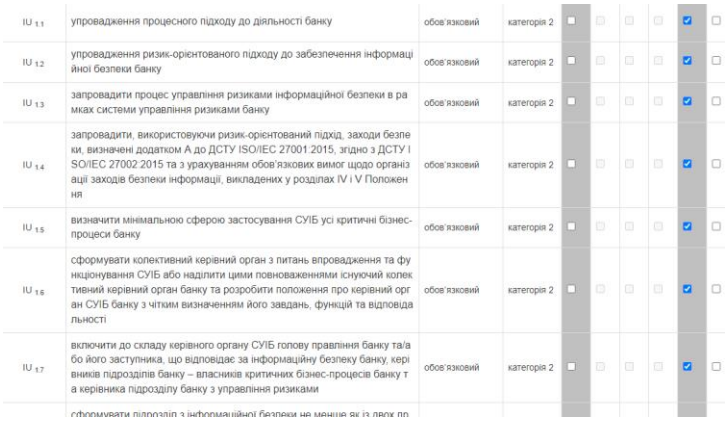
Крок 3.1. Визначення взаємозв'язку між загрозами та технічними засобами захисту інформації.



	Фізичний рівень	Мережевий рівень	Рівень операційних систем	Рівень систем управління базами даних	Рівень банківських технологічних додатків та сервісів
02.03.01.05	MZ	MZ	MZ	MZ	MZ
03.03.03.04	MZ	MZ	MZ	MZ	MZ
03.03.02.03	MZ	MZ	MZ	MZ	MZ
03.03.02.05	MZ	MZ	MZ	MZ	MZ
03.02.04.03	MZ	MZ	MZ	MZ	MZ
02.02.04.05	MZ	MZ	MZ	MZ	MZ
02.02.02.03	MZ	MZ	MZ	MZ	MZ
01.02.03.02	MZ	MZ	MZ	MZ	MZ
03.02.03.01	MZ	MZ	MZ	MZ	MZ
03.02.02.03	MZ	MZ	MZ	MZ	MZ
01.01.03.05	MZ	MZ	MZ	MZ	MZ
03.03.02.04	MZ	MZ	MZ	MZ	MZ
03.01.03.02	MZ	MZ	MZ	MZ	MZ
01.01.03.04	MZ	MZ	MZ	MZ	MZ

Рисунок 3.8 – Взаємозв’язок між загрозами і ТСЗІ

Крок 3.2. Формування вимог регуляторів.



IU 1.1	упровадження процесного підходу до діяльності банку	обов'язковий	категорія 2	☐	☐	☐	☐	☑	☐
IU 1.2	упровадження ризик-орієнтованого підходу до забезпечення інформаційної безпеки банку	обов'язковий	категорія 2	☐	☐	☐	☐	☑	☐
IU 1.3	запровадити процес управління ризиками інформаційної безпеки в рамках системи управління ризиками банку	обов'язковий	категорія 2	☐	☐	☐	☐	☑	☐
IU 1.4	запровадити, використовуючи ризик-орієнтований підхід, заходи безпеки, визначені додатком А до ДСТУ ISO/IEC 27001:2015, згідно з ДСТУ ISO/IEC 27002:2015 та з урахуванням обов'язкових вимог щодо організації заходів безпеки інформації, викладених у розділах IV і V Положення	обов'язковий	категорія 2	☐	☐	☐	☐	☑	☐
IU 1.5	визначити мінімальною сферою застосування СУІБ усі критичні бізнес-процеси банку	обов'язковий	категорія 2	☐	☐	☐	☐	☑	☐
IU 1.6	сформувати колективний керівний орган з питань впровадження та функціонування СУІБ або наділити цими повноваженнями існуючий колективний керівний орган банку та розробити положення про керівний орган СУІБ банку з чітким визначенням його завдань, функцій та відповідальності	обов'язковий	категорія 2	☐	☐	☐	☐	☑	☐
IU 1.7	включити до складу керівного органу СУІБ голову правління банку та/або його заступника, що відповідає за інформаційну безпеку банку, керівників підрозділів банку – власників критичних бізнес-процесів банку та керівника підрозділу банку з управління ризиками	обов'язковий	категорія 2	☐	☐	☐	☐	☑	☐
	сформувати підрозділ з інформаційної безпеки не менше як із двох пр								

Регулятори	поточне значення	Номінальне значення	% відповідності
RBBI2	0.77	0.85	90
RBBI3	0.75	0.85	88
ooБІн	0.79	0.85	93.33
ОVБІТП	0.82	0.85	96.32
БПТП	0.74	0.85	87.5
ozBin	0.84	0.85	98.75

Рисунки 3.9-3.10 – Формування вимог і оцінка регуляторів

Крок 3.3. Формування загальної оцінки рівня захищеності банку.

Показник	Номінальне значення	поточне значення
GSI_1	1	1
GSI_2	1	1
GSI_3	1	0

Загальний рівень безпеки: *Середній*

Рисунок 3.11 – Загальна оцінка захисту БІР

Висновок до розділу 3

Загальна оцінка захисту інформації в банку вказує на ефективність комплексної системи захисту. Вона безпосередньо відображає поточний рівень ІБ і є одним із ключових критеріїв при ухваленні рішень.

Розроблена методика дозволяє ідентифікувати найвірогідніші загрози безпеки інформаційних ресурсів, оцінити загальний показника рівня захищеності БІР на основі синергетичної моделі загроз, вдосконаленого класифікатора загроз та моделі порушника, що дозволить оптимізувати затрати коштів на систему захисту БІР, базуючись на комплексному підході по вибору оптимальних шляхів забезпечення безпеки, враховуючи ризики.

ЗАГАЛЬНІ ВИСНОВКИ

Проаналізовано сучасні системи для захисту інформаційних ресурсів банків у порівнянні, розглянуто їх функції, переваги та недоліки та завдання, які вони виконують. Виявлено основні загрози порушення безпеки інформаційних ресурсів банку на основі моделі CIA, також проведено класифікацію кібератак на основі моделі OSI.

Завдяки деталізованій та чітко структурованій звітності, графікам та динамічним таблицям у SIEM-системах, можна зазначити, що SIEM видається найбільш повним і універсальним функціоналом для надання інформації про події, через що фахівці можуть приймати інформовані рішення щодо захисту комп'ютерної інфраструктури та отримувати своєчасні повідомлення про свіжі проникнення, які можуть призвести до серйозних наслідків.

Проведено аналіз функціональних можливостей SIEM-систем, завдання, які вона виконує, небезпечних факторів, які SIEM-системи можуть ідентифікувати. Описано процес звітності і пріорітизації SIEM-систем та методи оцінки та виявлення аномалій. Було використано і вдосконалено класифікатор загроз безпеки БІР для визначення оцінки рівня захищеності від загроз за видами послуг, рівнем ієрархії інфраструктури АБС, особливості інформації, характеру напряму атаки, враховуючи гібридність та вірогідності впливу. Порівняно з іншими класифікатор загроз безпеці банківських інформаційних ресурсів, базується на синергетичній моделі загроз. Це дозволяє класифікувати загрози за складовими безпеки, видами послуг та рівнями ієрархії інфраструктури банківських систем, оцінювати комплексність та гібридність загроз, вірогідність впливу загроз на безпеку інформаційних ресурсів, що виходить від зловмисників, і ступеня ефективності захисних заходів, результати дослідження яких, дозволять вчасно реагувати події, формуючи превентивні заходи для

запобігання реалізації загроз та розробляти плани інвестування в технічні засоби захисту інформації.

Визначено взаємозв’язків між загрозами та засобами захисту інформації, сформовано до вимог регуляторів, критерії оцінки інформаційної безпеки, використовуючи постанову НБУ.

Розроблено методику комплексного підходу для оцінки загального рівня безпеки банківських інформаційних ресурсів на основі синергетичної моделі загроз, удосконалених класифікатора загроз та моделі зловмисника, моделі оцінки захищеності банківських інформаційних ресурсів та моделі інфраструктури автоматизованих банківських систем, що дозволяє своєчасно реагувати на загрози інформаційної безпеки, планувати інвестування в технічні засоби захисту інформації, формувати превентивні заходи для недопущення реалізації загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Євсєєв С. Оцінка забезпечення безперервності бізнес-процесів в організаціях банківського сектора на основі синергетичного підходу, ч. 2 : Сучасна спеціальна техніка. Науково-практичний журнал. 2017. 10–17 с.
2. SIEM. *Вікіпедія* : веб-сайт. URL: https://uk.wikipedia.org/wiki/SIEM (дата звернення: 20.12.2023)
3. Інформаційна загроза. *Вікіпедія* : веб-сайт. URL: https://uk.wikipedia.org/wiki/Інформаційна_загроза (дата звернення: 20.12.2023)
4. Common Criteria. *Вікіпедія* : веб-сайт. URL: https://uk.wikipedia.org/wiki/Common_Criteria (дата звернення: 20.12.2023)
5. Романець Ю. В. Захист інформації в комп'ютерних системах і мережах. 2001. 376 с.
6. Кирилов В. А. Система збору та кореляції подій (SIEM) як ядро системи інформаційної безпеки : вісник технологічного університету. 2016. 135 с.
7. С. С. Бучик,"Методика експертного оцінювання функціональних профілів загроз державних інформаційних ресурсів".2015. 271–280 с.
8. Домарєв Д., Домарєв В., Прокопенко С. Методика оцінювання захищеності інформаційних систем за допомогою СУІБ "Матриця", Захист інформації, том 15, 2013. 80 – 86 с.
9. С. В. Павленко, "Метод оцінки захищеності інформаційних систем", Системи озброєння і військова техніка, 2009. 149 – 154 с.
10. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень. Житомир: Рута, 2010.

11. Євсєєв С. П. Аналіз захисту в національній системі масових електронних платежів. Інформаційна безпека. 2014. 15 с.
12. Євсеєв С.П. Оцінка обміну даними в глобальних обчислювальних мережах на основі комплексного показника якості обслуговування мережі : науковий журнал: Радіоелектроніка, інформатика, управління : Запоріжжя, 2017. 115-128 с.
13. Грищук Р.В. Методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах : Науково-технічний журнал "Безпека інформації", 2017. 204-214 с.
14. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : Постанова НБУ 28.09.2017 № 95. URL : http://zakon2.rada.gov.ua/laws/show/en/v0095500-17/page (дата звернення: 10.10.2023)
15. Класифікатор синергетика : веб-сайт. URL: http://skl.hneu.edu.ua/Threat (дата звернення: 20.12.2023).

ДОДАТКИ

ДОДАТОК А

Таблиця А.1 – Основні загрози інформації БІР

Основні загрози інформації БІР		
Порушення конфіденційності включають: виявлення паролів користувачів через секретні активні підключення до мережі; неправдиві заяви про отримання платіжних документів; несанкціоноване введення даних; вилучення інформації зі статистичних БД; використання КМ як активного ретранслятора (фальсифікація платіжних документів), фішинг, претекстінг, несанкціонована передача конфіденційної інформації тощо.	Порушення цілісності включають: внесення змін або копіювання даних з носіїв інформації, залишених без нагляду або з файлів; викрадення ПЗ; внесення змін до даних програм для фальсіфікації та підробки фінансових документів під час несанкціонованих відвідувань; подолання системних засобів захисту за допомогою ПЗ; знищення обладнання чи носіїв інформації; дистанційне знищення інформації; зчитування або зміна фінансової інформації в БД.	Порушення доступності включають: несанкціоноване використання рівнів доступу до конфіденційної інформації; обхід механізмів захисту за допомогою несанкціонованого перевищення прав доступу; відмова клієнта від передачі або надання помилкових відомостей для зняття з себе відповідальності за виконання операцій; викрадення або виявлення паролів; зловживання повноваженнями.

Таблиця А.2 – Порівняння сучасних систем

Критерії	СПБШ	SIEM	CPSZDP	EDR	DLP
Реалізація	Організаційно-технічний	Програмний	Програмно-апаратний	Програмний	Програмний
Сповіщення	-	+	+	+	+
Моніторинг системних змін	+	+	+	+	+

Продовження таблиці

Критерії	СПБШ	SIEM	CPSZDP	EDR	DLP
Аналіз ризиків	-	+	-	-	+
Виявлення слабких місць в системі захисту	-	+	+	-	+
Швидке прийняття рішень	+	+	-	-	-
Ретроспективний аналіз	-	+	-	-	-
Блокування загроз	+	-	+	+	+
Візуалізація інформації	-	+	-	-	+
Генерація звітів	-	+	+	-	+

Таблиця А.3 – Порівняння методів визначення аномалій

Метод	Тип розпізнавання	Результат	Робота без попереднього класу аномалій	Визначення класу аномалії
Кластеризація	Неконтрольоване, контрольоване	Мітка	-	-
Класифікація	Контрольоване, напівконтрольоване	Мітка	-	+
Алгоритм найближчого сусіда	Напівконтрольоване	Ступінь	+	-
Спектральні методи	Неконтрольоване, напівконтрольоване	Мітка	+	-
Статистичний аналіз	Напівконтрольоване	Ступінь	-	-

Таблиця А.4 – Модель методу подвійних трійок

Компоненти	Класифікація
Перша компонента	Загроза класифікується відповідно до банківських інформаційних ресурсів в організації банківської системи: Інформаційна безпека – «01» Безпека інформації – «02» Кібербезпека – «03»
Друга компонента	Загроза класифікується залежно від характеру напряму: Нормативно-правовий – «01» Організаційний – «02» Інженерно-технічний – «03»
Третя компонента	Загроза класифікується залежно від особливості інформації: Конфіденційність – «01» Цілісність – «02» Доступність – «03» Автентичність – «04»
Четверта компонента	Загроза класифікується відповідно від ієрархії в інфраструктурі банківської системи: Фізичний рівень (FL) – «01» Мережевий рівень (NL) – «02» Рівень операційних систем (OSL) – «03» Рівень управління БД (DBL) – «04» Рівень банківських технологій (BL) – «05»

Таблиця А.5 – Таблиця вагових коефіцієнтів

Ваговий коефіцієнт	Частота виникнення загрози
0,067	Рідше, ніж раз на кожні 5 років
0,133	Рідше, ніж раз на рік
0,2	Рідше, ніж раз на місяць
0,267	Рідше, ніж раз на тиждень
0,333	Кожний день

Таблиця А.6 – Таблиця рекомендованих оцінок приватного показника обов’язкових вимог інформаційної безпеки

Оцінка показника обов’язкової вимоги безпеки	Критерій показника безпеки
«н/о»	Вимоги не є актуальними для організації
0	Вимоги до інформаційної безпеки не встановлені у документах аудиту
0,25	Вимоги до інформаційної безпеки встановлені у документах аудиту, але не виконуються
0,5	Вимоги до інформаційної безпеки встановлені у документах аудиту, але виконуються не повністю
0,75	Вимоги до інформаційної безпеки встановлені у документах аудиту, але виконуються майже повністю
1	Вимоги до інформаційної безпеки встановлені у документах аудиту і виконуються повністю

Таблиця А.7 – Таблиця рекомендованих оцінок приватного показника рекомендованих вимог інформаційної безпеки

Оцінка показника обов’язкової вимоги безпеки	Критерій показника безпеки
0 та/або «н/о»	Вимоги до інформаційної безпеки не встановлені у документах аудиту
1	Вимоги до інформаційної безпеки у документах аудиту встановлені і виконуються

Таблиця А.8 – Результати оцінки безпеки на основі комплексного підходу

Складові безпеки	Послуги безпеки				
	V_{syn}^{Cn}	V_{syn}^{It}	V_{syn}^{Av}	V_{syn}^{At}	Підсумок
V_{syn}^{IB}	0.065	0.053	0.14	0.093	0.0000449
V_{syn}^{KB}	0.076	0.101	0.113	0.02	0.0000173
V_{syn}^{BI}	0.047	0.058	0.076	0.083	0.0000172
Підсумок	0.188	0.212	0.329	0.196	
$V_{syn}^{BI.KB,IB} = 0.000079$			$V_{syn}^{hyb\ Cn,It,Av,At} = 0.002570$		

ДОДАТОК Б

Рисунок Б.1 – Модель тріади CIA

Економічні загрози	**Фізичні загрози**	**Інтелектуальні загрози**
Наслідки: збитки або втрати прибутків. Корупція, шахрайство, недобросовісна конкуренція та використання неефективних технологій.	Наслідки: збитків, пов'язані з втратою власності банку, або його відновлення. Пограбування, крадіжки банківського майна та коштів, поломки, виведення з ладу банківського обладнання, неефективне використання ресурсів.	Наслідки: шкода іміджу, соціальна та психологічна напруженість навколо банку та всередині колективу. Витік або зловживання банківською інформацією, дискредитація банку, соціальні конфлікти навколо або всередині банківських установ.

Рисунок Б.2 – Види загроз за характером впливу

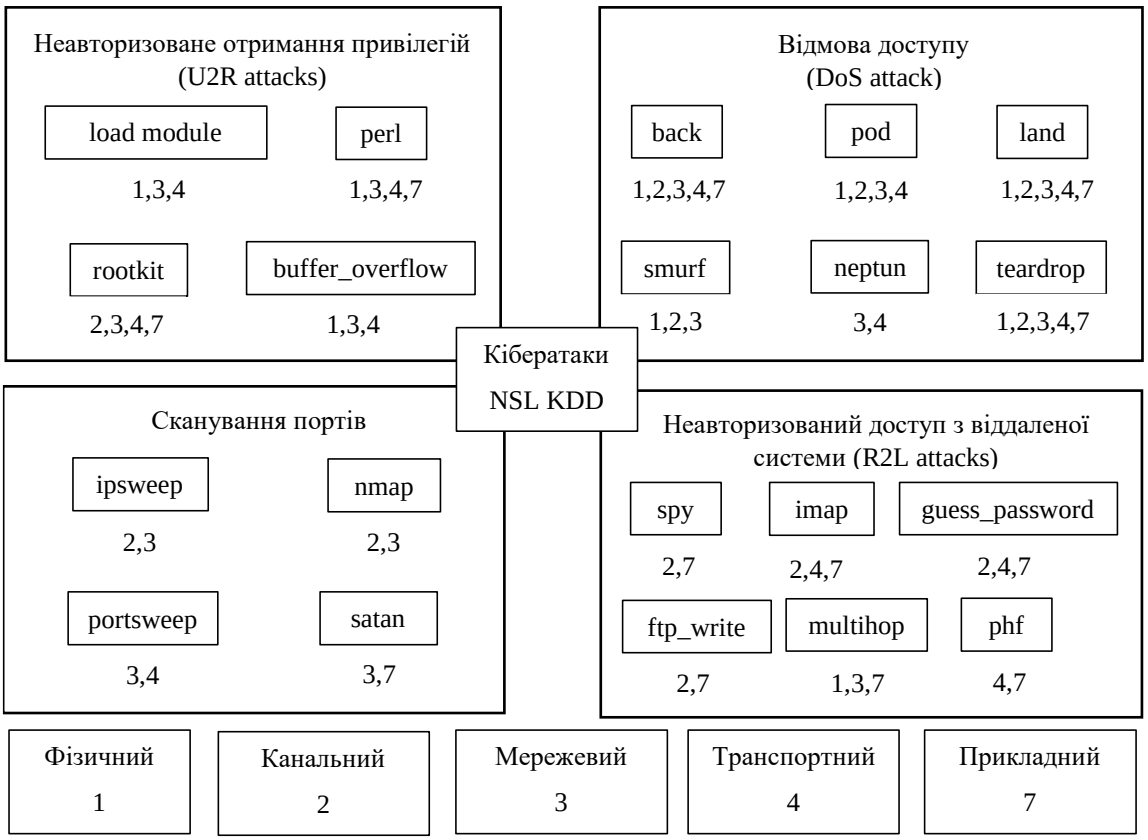


Рисунок Б.3 – Класифікація кібератак на АБС з посиланням на модель OSI.

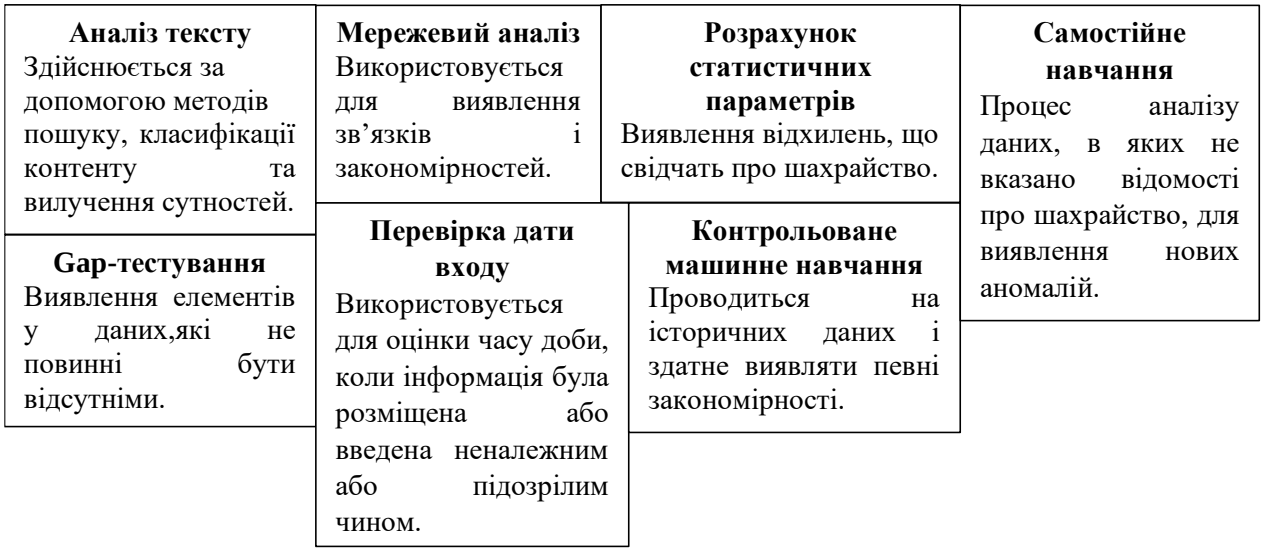


Рисунок Б.4 – Функціональні можливості СПБШ

Моніторинг	**Виявлення**	**Відстеження активності**	**Сповіщення**
Моніторинг кінцевих точок та активностей робочих станцій в режимі реального часу в підприємстві.	Виявлення та визначення пріорітетів подій в ІБ залежно від їх винекнення на кінцевих точках.	Запис та зберігання інформації про активність на кінцевих точках з метою аналізу в рамках розслідувань інцидентів.	Надання експертам з ІБ даних, необхідної для швидкого розслідування інцидентів.

Рисунок Б.5 – Функціонал EDR-систем

<table>
<tr><td colspan="2">Ізоляція пошкодженого пристрою, лікування та обробка інформації.
Заборона установлення зворотних зв'язків з серверами хакера, повне чи часткове обмеження доступу зі станції до корпоративної мережі. Переведення пристроїв до безпечного стану: ізоляція шкідливих файлів, зупинка процесів, що були активовані під час атаки, та очищення реєстру.</td><td rowspan="2">Реагуванняна інциденті розслідування
- Візуалізація та детальний розгляд усіх подій, які відбулися під час інциденту;
- Аналіз методів зловмисника на етапах атаки;
- Оцінка збитків, завданих атакою.</td></tr>
<tr><td>Уникнення атак
- Заборона доступу відомим шкідливим файлам;
- Перешкодження новим варіаціям відомих загроз через статичний аналіз та використання методів машинного навчання;
- Визначення, чи використовують користувачі корпоративні паролі на особистих веб-сайтах.</td><td>Зменшення зони атаки
- Перевірка наявності оновлень, патчів та функцій безпеки;
- Контроль зовнішніх носіїв, пристроїв та мережевих з'єднань;
- Шифрування жорстких дисків, трафіку (VPN), документів;
- Перевірка статусу станції при підключенні до мережі;</td></tr>
<tr><td colspan="2"></td><td>Виявлення та блокування атак
Визначення та зупинення небезпечної та підозрілої активності, за допомогою методів машинного навчання.</td></tr>
</table>

Рисунок Б.6 – Функції Check Point SandBlast Zero-Day Protection

Агрегація	Кореляція	Сумісність	Зберігання даних
Збір в журнали подій, даних, які отримуються з різних джерел, таких як мережеві пристрої, сервіси, датчики систем безпеки, сервери, бази даних і програми. Проводиться консолідація цих даних для виявлення критичних подій.	Пошук з агрегованих даних зв'язків між спільними значеннями, атрибутами та подіями. Таким чином, дані зводяться в єдине ціле для подальшого аналізу.	Використання програм для автоматизації процесу збору даних та генерації звітів з метою інтеграції агрегованої інформації у поточні процеси управління ІБ та аудиту.	Система зберігає отримані дані для аналізу та забезпечення можливості трансформації. Ці дані мають велике значення для проведення експертиз і розслідування інцидентів.

Інформаційна панель	Експертний аналіз	Сповіщення
Надає можливість візуалізації отриманої інформації у вигляді графіків і діаграм дозволяє легше сприйняти інформацію і визначити відхилення в поведінці, які розрізняються з типовою поведінкою різних систем.	Дозволяє здійснення пошуку по зафіксованим подіям, що дає можливість виконувати програмно-технічну експертизу безпеки мережі.	Система автоматично аналізує отримані дані про події і генерує сповіщення щодо поточних проблем. Сповіщення може відображатися на внутрішньому інтерфейсі додатка та надсилатися через зовнішні канали: електронна пошта, GSM-шлюх і т.д.

Рисунок Б.7 – Функції SIEM-систем

1) Здійснення збору, обробки та аналізу подій безпеки, що надходять в систему;	2) Виявлення атак та порушень критеріїв і політики безпеки в реальному часі;	3) Проведення аналізу та управління ризиками на підставі об'єктивних і експертних оцінок;	4) Оцінка оперативної захищеності критично важливих інформаційних ресурсів;
5) Реалізація розслідувань інцидентів;	6) Складання звітних документів;	7) Прийняття ефективних рішень щодо захисту інформації.	

Рисунок Б.8 – Завдання SIEM-системи

1) Недоліки, помилки та відмови в роботі ІС.	4) Спроби модифікувати інформацію та здійснювати обман.
2) Зараження вірусами, наявність невилучених вірусів, бекдорів і троянів.	5) Неправильна конфігурація інструментів безпеки та ІС
3) Спроби несанкціонованого доступу.	

Рисунок Б.9 – Небезпечні фактори які може виявити SIEM-система

Моніторонговий	Виявлення оповіщень	Досліднецький аналіз
Встановлення правил моніторингу безпеки для визначення за чим потрібно вести нагляд та реєструвати.	Система використовує встановлені правила кореляції для аналізу зібраних даних та виявлення можливих загроз чи аномалій. Класифікатори служать для групування виявлених оповіщень за різними категоріями або важливістю.	На цьому етапі проводиться детальний аналіз виявлених оповіщень, враховуючи контекст дослідження. Це може включати вивчення деталей подій, визначення їхнього потенційного впливу та встановлення подальших кроків.

SIEM

Формуючи звітність SIEM збирає, агрегує та аналізує дані, що надходять з усіх трьох етапів. Також відповідає за сповіщення управління операційними системами безпеки, управління інциндентами та виконання основних правил та політик безпеки.

Рисунок Б.10 – Створення звітності в системі SIEM

Рисунок Б.11 – Схема пріорітизації SIEM

Відстань до k-го найближчого сусіда. Щоб реалізувати цей підхід, відстань до найближчого об’єкта визначається для кожного тестового екземпляра класу. Аномальні екземпляри - це ті, які знаходяться найдальше від найближчого об’єкта.	Використання відносної щільності. Підхід заснований на оцінці щільності середовища кожного екземпляра даних. Екземпляр з низькою щільністю розцінюється як аномальний, і навпаки, з високою – нормальний. Для заданого екземпляра даних відстань до його k-го найближчого сусіда дорівнює радіусу гіперсфери з центром у цьому екземплярі, що містить інших k-екземпляри.

Рисунок Б.12 – Підходи по виявленню аномалій в алгоритмі найближчого сусіда

Метод нейронних мереж складається з двох етапів. Спочатку нейронну мережу навчають ідентифікувати клас нормальної поведінки на навчальній вибірці. Потім кожен екземпляр передається як вхідний сигнал нейронної мережі. Дана система, може ідентифікувати безліч класів нормальної поведінки. Для виявлення аномалій за допомогою одного класу використовуються реплікативні нейронні мережі.
Баєсівська модель – графічна модель, яка відображає ймовірність залежності між змінними, що дає можливість проводити ймовірнісний аналіз на основі цих змінних. Складається з двох частин: графічна – визначає набори залежностей і незалежностей в множинах випадкових величин, наданих як предмети предметної області, і набір – розподіл ймовірностей, що визначає силу їх залежностей. Отже, Байєсівська мережа використовується для виявлення аномалій шляхом оцінки ймовірності спостереження одного з нормальних або аномальних класів. Найпростішою реалізацією цього підходу є Наївний Байєсівський підхід (Naive Bayes Approach).
Метод опорних векторів (Support Vector Machine) використовується в системах, де лише один клас не має аномальної поведінки. Цей метод визначає межі області, де є нормальні екземпляри даних. Для кожного екземпляра метод визначає, чи лежить він у певній області та визначає його як ненормальний, якщо він лежить за межами області.

Рисунок Б.13 – механізмами класифікації для розпізнавання

аномалій