ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ФАКУЛЬТЕТ ЕКОНОМІЧНОЇ ІНФОРМАТИКИ
КАФЕДРА КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Пояснювальна записка

до дипломної роботи

бакалавра

на тему: “Аналіз оцінки поточного стану інформаційної безпеки на основі SIEM-систем”

Виконав: студент 4 року навчання,
за освітнім ступенем “бакалавр”
зі спеціальності 125 “Кібербезпека”
Макаренко А.О
Керівник: д.т.н., проф. Євсеєв С.П.

Рецензент: к.т.н., доц. Шматко О.В.

Харків – 2020 рік

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

АБС – автоматизована банківська система;

БІн – банківська інформація;

БІР – банківський інформаційний ресурс;

ЗЗІ – засоби захисту інформації;

ІБ – інформаційна безпека;

ІР – інформаційний ресурс;

ІС – інформаційна система;

КЗ – контрольована зона;

КС – комп’ютерна система;

КТ – кінцева точка;

КСЗІ – комплексна система захисту інформації;

СПБШ – система протидії банківському шахрайству;

СППР – система підтримки прийняття рішень;

ТЗЗІ – технічні засоби захисту інформації;

ЗМІСТ

ВСТУП

В умовах масової комп’ютеризації, доступності телекомунікацій, збільшення обсягу обороту електронного документообігу між банківськими установами та клієнтами, переходу на електронну комерцію проблеми безпеки БІР в силу природних і штучних чинників тільки загострюються. З цієї причини, збитки від порушення безпеки БІР приносять все більше фінансових витрат як для банкам, так і для їх клієнтів.

Порушники навчилися імітувати нормальну роботу системи, не виконує непередбачених системою дій, використовують тільки дозволені системні процеси і встановлене ПЗ, за рахунок чого можуть залишатися непоміченими тривалий період часу.

Цей фактор змушує переглянути механізми виявлення зловмисників у внутрішній мережі за допомогою аналізу поведінки користувачів і побудови профілю їх поведінки, тобто визначення аномалій.

Актуальність роботи полягає в тому, що сучасні механізми профілюванням поведінки користувачів не до кінця ефективні, через що в протягом тривалого часу порушники можуть знаходитися у внутрішній мережі непоміченими.

Метою даної роботи є огляд та аналіз сучасних систем захисту банківських інформаційних ресурсів, визначення їх переваг та недоліків, а також розробка вдосконаленого класифікатора загроз на основі синергетичного підходу і оцінки показників ступеня небезпеки зловмисників і ступеня реалізації захисних заходів, який надає можливість своєчасно коригувати керівні документи банку з інформаційної безпеки, планувати інвестування в технічні засоби захисту інформації, формувати превентивні заходи щодо недопущення реалізації загроз.

1 АНАЛІЗ КІБЕРНЕТИЧНИХ СИСТЕМ ТА СУЧАСНИХ ЗАГРОЗ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

1.1. Кібернетичні системи

Важливу роль під час процесу побудови систем безпеки інформаційних ресурсів (ІР) автоматизованих банківських систем (АБС) як складової національних інформаційних ресурсів держави відіграє теорія та практика, в якій науково-методологічна база є основою для прийняття обґрунтованих та ефективних управлінських рішень суб'єктами забезпечення ІБ держави на усіх рівнях [1]. Ієрархічна структура зображена на рис.1.1.

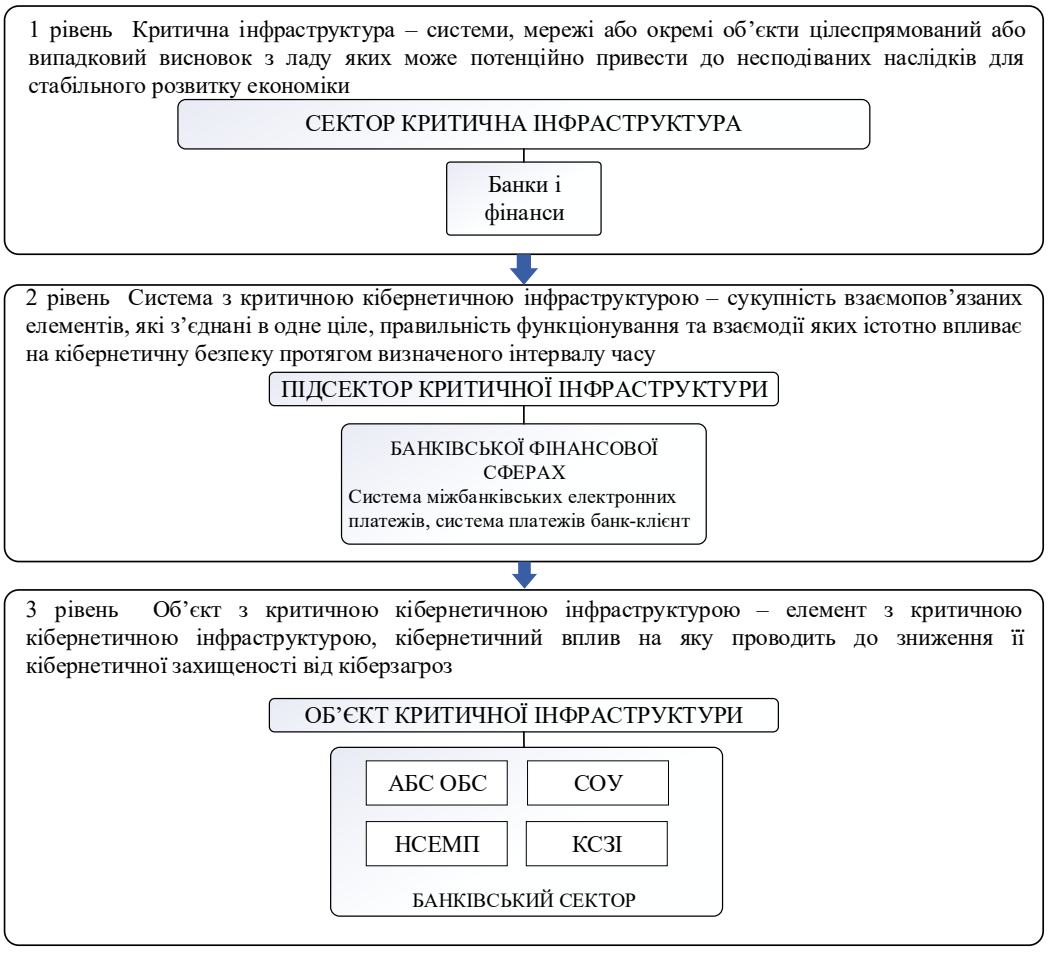


Рисунок 1.1 – Ієрархічна структура критичної інфраструктури метасистеми банківського сектор

Під терміном "метасистема критичної інфраструктури держави" (МКІД) розуміється система стратегічного масштабу, тобто являє собою сукупність

значної кількості різноманітних елементів, об’єднаних в рамках єдиної критичної кібернетичної архітектури в єдину систему, що володіє синергізмом і має загальне призначення та функцію [2].

На рис. 1.2 наведений взаємозв’язок між основними складовими інформаційної безпеки (ІБ) держави.

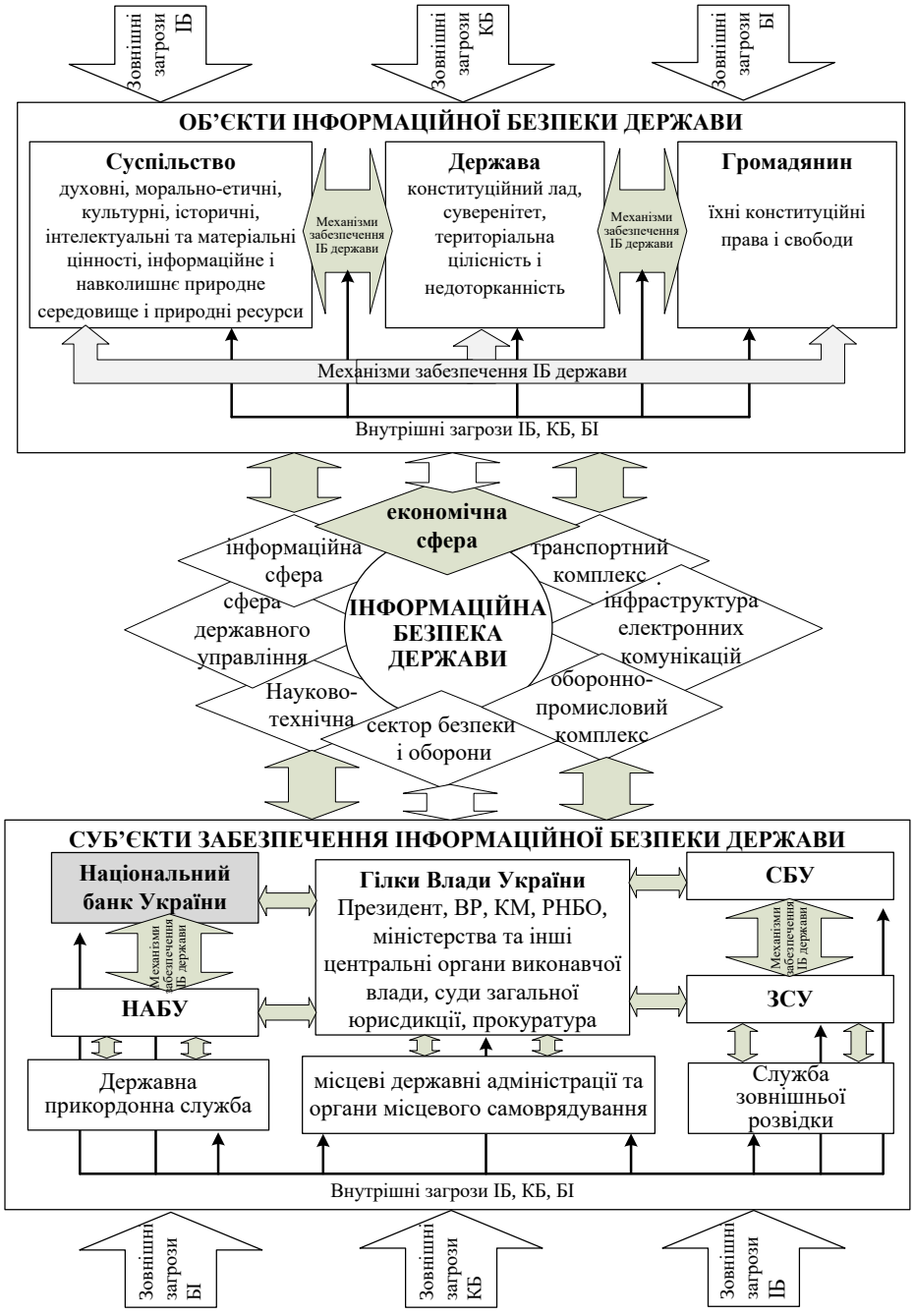


Рисунок 1.2 – Взаємозв’язок основних складових інформаційної безпеки держави

В сучасних умовах однією з головних проблем для організації є комплексне надання захисту інформації, даний напрямок є особливо важливим для здійснення плідної діяльності компанії.

Інформаційні потоки, що передаються по різних каналах, таким як лінії зв'язку або розподільні інформаційні системи можуть бути недостатньо серйозно захищені, що надалі може привести до втрати корпоративної конфіденційної інформації. При отриманні важливої службової інформації сторонніми особами може бути підірвана репутація компанії. Порушники можуть передати інформацію конкурентам, чинити тиск на керівний склад організації, дискредитувати авторитет організації шляхом передачі фінансових звітів та іншої економічної інформації зацікавленій стороні.

Важливу роль у забезпеченні національної безпеки України та особливо її економічної складової відіграють процеси забезпечення інформаційної безпеки (ІБ) держави в банківському секторі (БнС).

Ієрархічна структура критичної інфраструктури метасистеми держави приведена на рис.1.3.

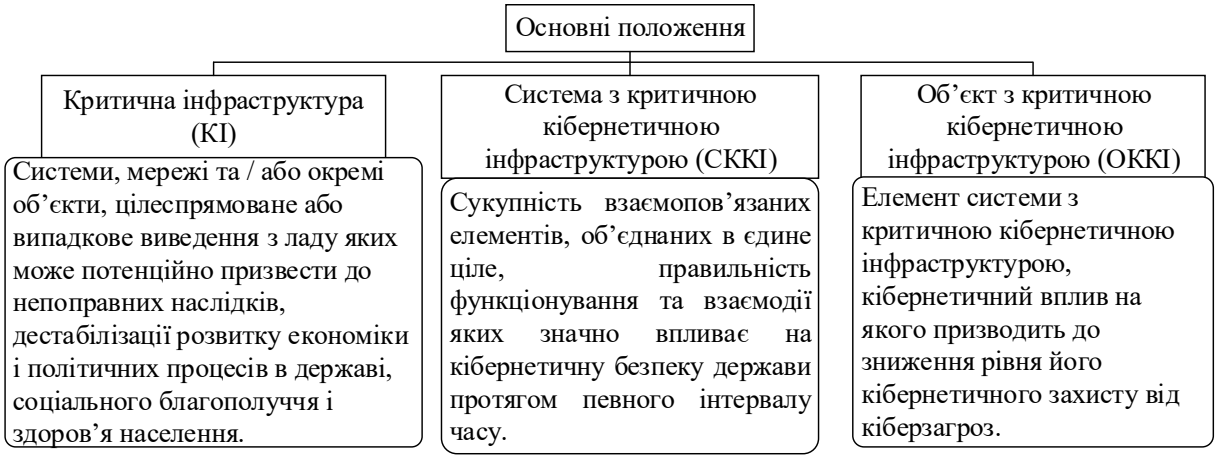


Рисунок 1.3 – Основні поняття ієрархічної структури критичної інфраструктури метасистеми держави

Автоматизована банківська система здійснює автоматичну побудову статистичної звітності, а також легко підлаштовується до різних змін та нововведень Національного Банку, що розширює функціональність системи без необхідності кардинальних програмних змін (рис.1.4).

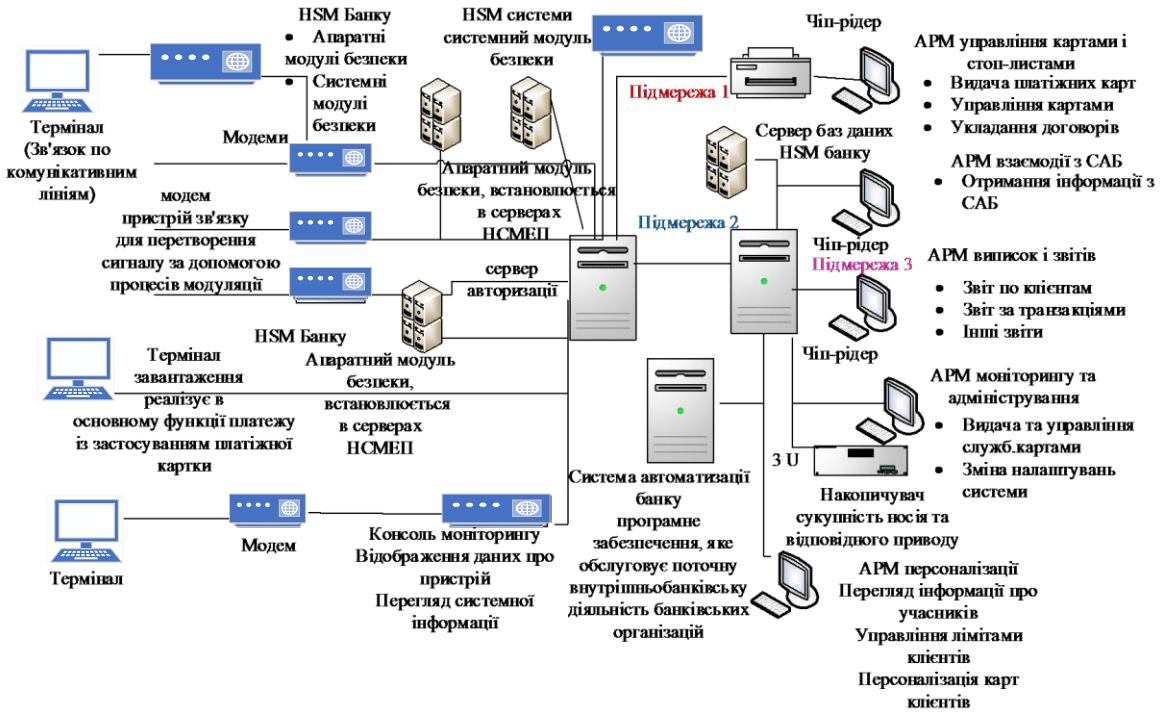


Рисунок 1.4 – Влаштування АБС

1.2. Сучасні загрози

Під загрозами безпеки інформаційної системи розуміється сукупність умов і факторів, що створюють потенційну або реально існуючу небезпеку, пов’язану з витоком інформації або несанкціонованими, ненавмисними впливами на неї. Таким чином, загрози безпеки інформації можуть бути пов’язані як з ненавмисними діями персоналу інформаційної системи, так і з спеціально здійснюваними неправомірними діями окремих організацій та громадян. Класифікація причин основних загроз для банківських систем зображена на рис.1.5.

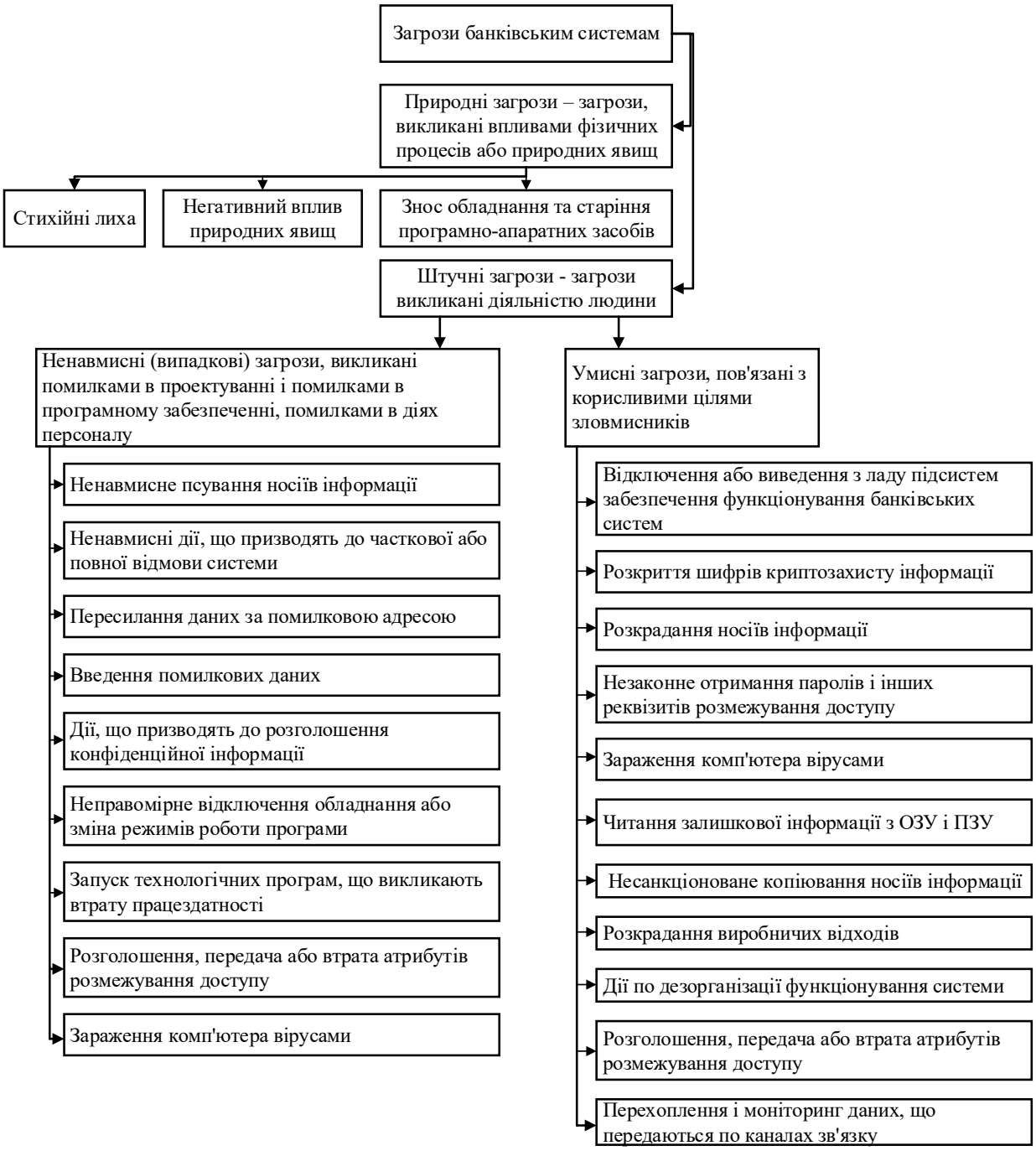


Рисунок 1.5 – Класифікація причин основних загроз для банківських систем

Для аналізу основних видів загроз безпеки інформації банківських інформаційних ресурсів може бути адаптована модель тріади *CIA* (*confidentiality, integrity, availability*) [3]. В цій моделі «безпека інформації БІР» - процес забезпечення конфіденційності, цілісності та доступності інформації клієнтами (рис.1.6).

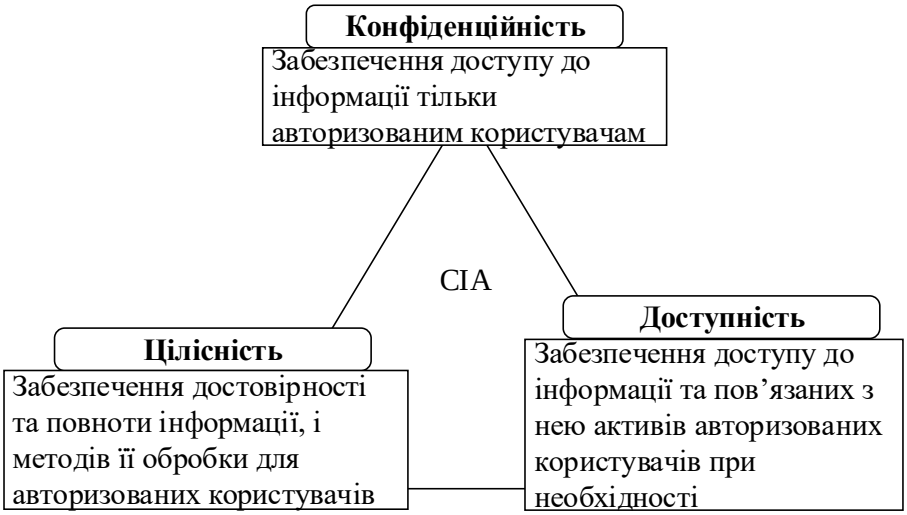


Рисунок 1.6 – Модель тріади CIA

З огляду на специфіку банківської сфери основними загрозами безпеці інформації БІР можна вважати такі загрози, які представлені на рис.1.7.

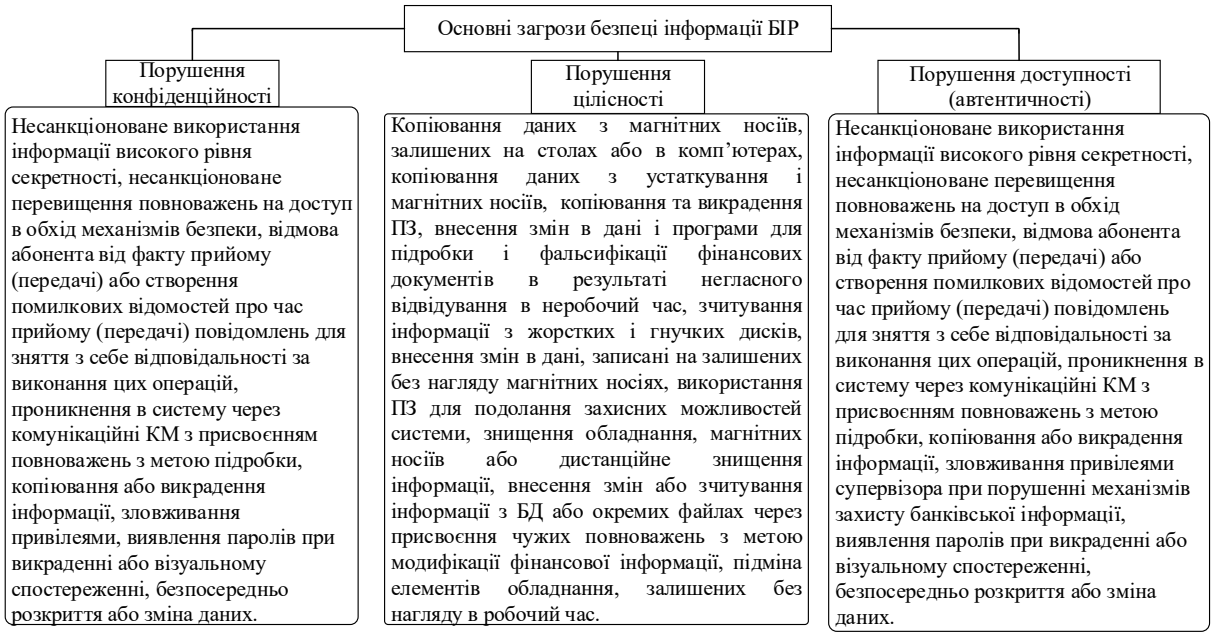


Рисунок 1.7 – Загрози безпеці інформації в банківській сфері

До числа загроз інформаційній безпеці БІР, що впливає на інформаційну систему, а також на економічну складову належать внутрішні і зовнішні загрози [4]. За спрямованістю і характером впливу на діяльність певних суб'єктів і об'єктів можуть бути економічними, фізичними та інтелектуальними (рис.1.8) [5].

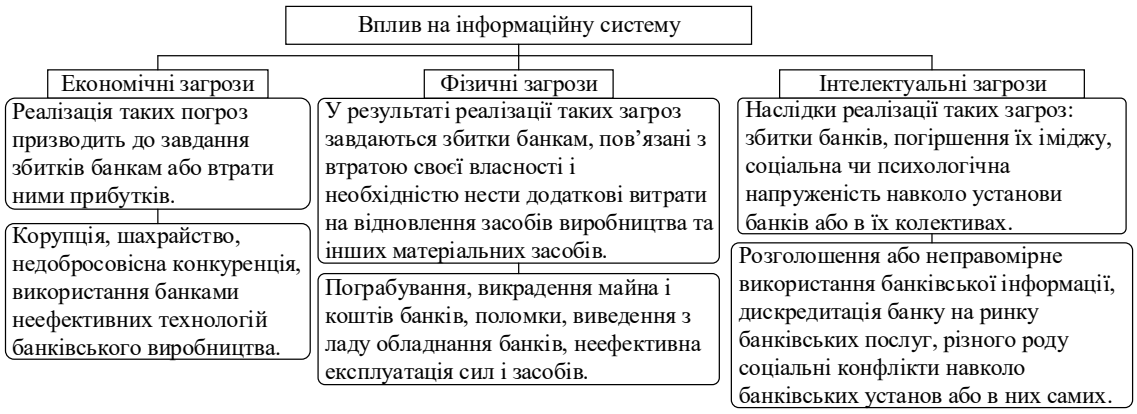


Рисунок 1.8 – Вплив на ІС та економічну складову

Необхідним профілем безпеки ІР пропонується вважати КБ. Кібербезпека – набір засобів, принципів забезпечення безпеки, гарантій безпеки, підходів до управління ризиками, дій і технологій, які використовуються для захисту кіберпростору, ресурсів організацій та користувачів [6]. Відповідно до стандарту *ISO/IEC 27032:2012 «Інформаційні технології. Методи забезпечення безпеки. Настанови щодо кібербезпеки»*, на кібербезпеку покладаються завдання щодо забезпечення умов, спрямованих на досягнення і збереження властивостей безпеки у ресурсах організації або користувачів, що покликані захистити від відповідних кіберзагроз (рис.1.9).

Рисунок 1.9 – Логічні взаємозв'язки кібербезпеки та інших доменів безпеки згідно зі стандартом *ISO/IEC 27032:2012*

Основними загрозами кібербезпеці АБС, спрямованими на зрив процесів управління або взяття їх під контроль, будуть кібератаки, які можна об'єднати в чотири основні класи, змістовна частина яких розкрита на рис.1.10.

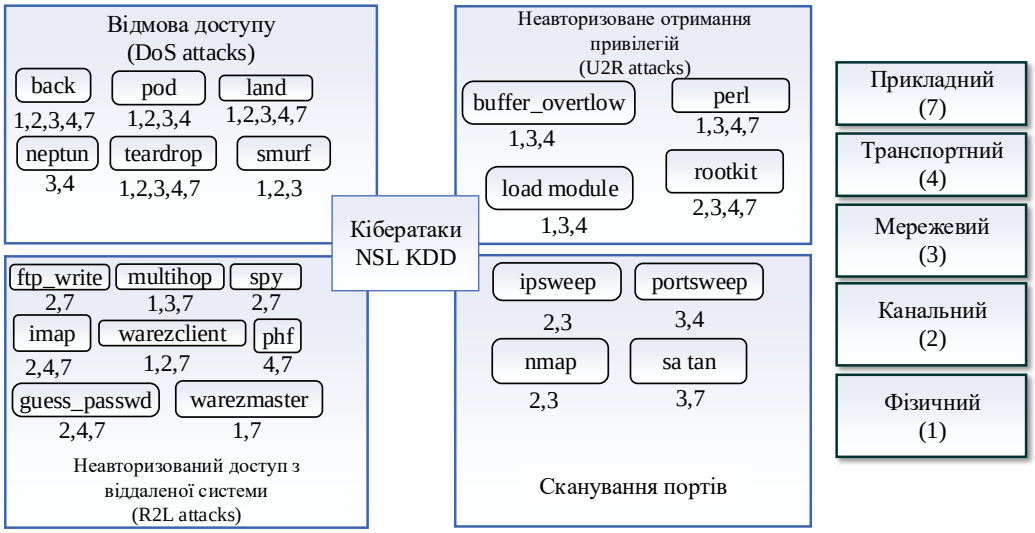


Рисунок 1.10 – Класифікація кібератак на АБС з прив’язкою до моделі OSI

Класифікація (рис.1.10) наочно свідчить, що кібератаки різних класів не залежно від функціонального призначення мають місце на різних рівнях моделі взаємодії відкритих систем OSI.

Описані вище загрози в силу різних суб’єктивних і об’єктивних причин мають місце для більшості відомих і проектованих АБС, спираючись на тісний взаємозв’язок між ними для різних профілів безпеки, і з метою розробки ефективних систем безпеки БІР, пропонується нова модель загроз безпеці БІР, в подальшому звана синергетичною.

Можна виділити дві основні групи методик оцінювання ризиків безпеки (рис.1.11).

Рисунок 1.11– Методик оцінювання ризиків безпеки

У будь-якій соціальній сфері інциденти безпеки, переривання роботи (*disruptive events*) і аварії (*disasters*) неминучі. Їх вплив на діяльність компанії має бути мінімізовано: дані повинні бути збережені, технічні засоби знаходиться в робочому стані, репутація врятована, люди – поза небезпекою. Рішення вказаних завдань можливо здійснити в рамках управління безперервністю бізнесу – цілісного процесу управління, в рамках якого ідентифікуються потенційні загрози діяльності організації, оцінюються можливі впливи на бізнес-операції в разі реалізації цих загроз (рис.1.12).

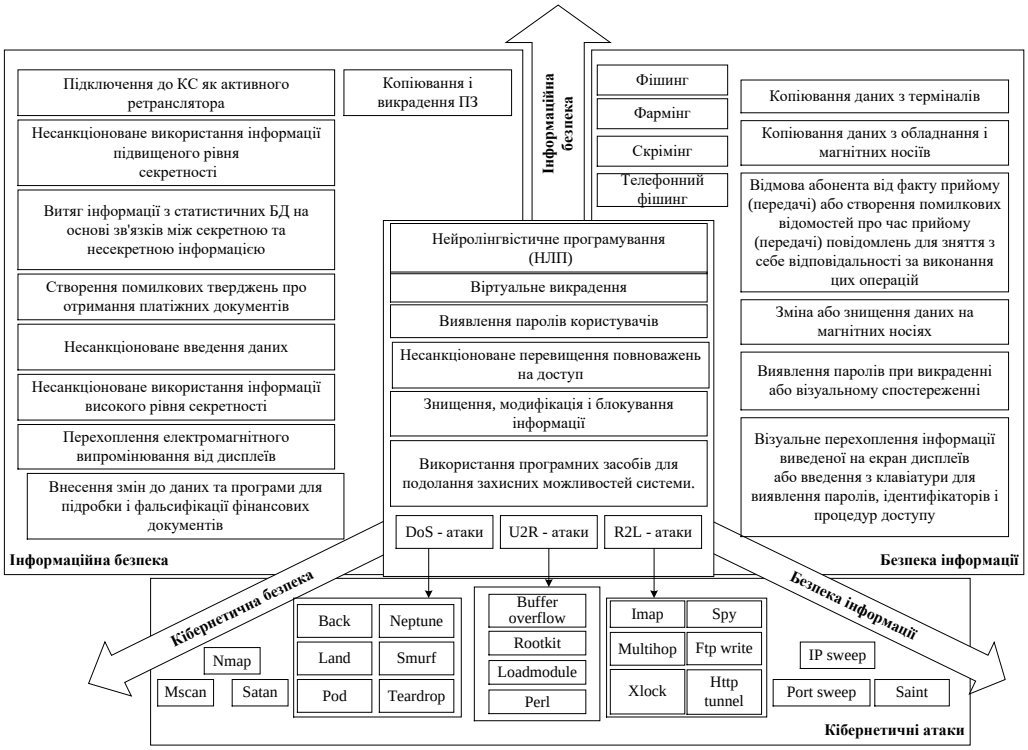


Рисунок 1.12 – Синергетична модель загроз безпеці БІР

Весь комплекс питань, пов’язаних із забезпеченням безпеки БІР України, а саме – ІБ, КБ, БІ в АБС повинен вирішуватися в комплексі і нерозривно один від іншого, гармонійно доповнюючи і заповнюючи, в разі необхідності, один одного.

Типова схема атаки на банківську систему. Вибір мети зловмисника багато в чому обумовлений технічною підготовкою, наявними інструментами і знаннями про внутрішні процеси банку, які мають злочинці. Зловмисники

діють за простими сценаріями, що складається з 5 основних етапів, представлених на рис.1.13.

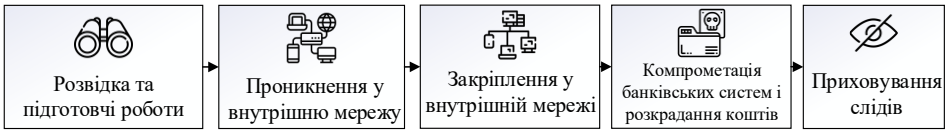


Рисунок 1.13 – Основні етапи на БІР

Перед порушниками стоїть завдання зібрати якомога більше інформації про банк, яка допоможе подолати системи захисту, і провести попередню організаційну роботу, з огляду на специфіку банку (рис.1.14).

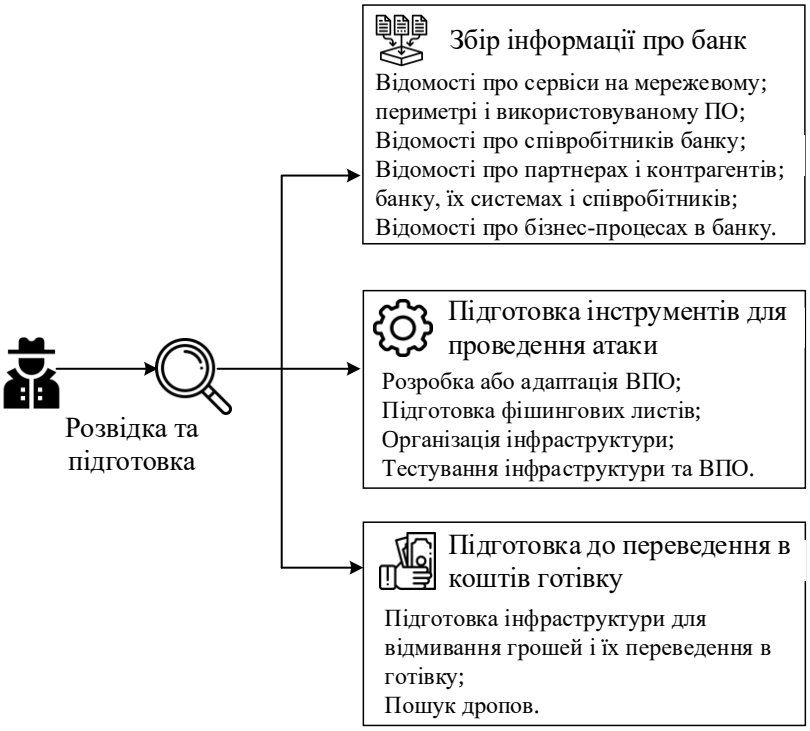


Рисунок 1.14 – Розвідка та підготовка до атаки

Найбільш поширеним і ефективним методом проникнення в інфраструктуру банку є фішингове розсилання електронних листів на адресу співробітників банку. Інший варіант початкового поширення шкідливого ПЗ - злом сторонніх компаній, які мають більш низький рівень безпеки, а також зараження сайтів, часто відвідуваних співробітниками цільового банку (рис.1.15).

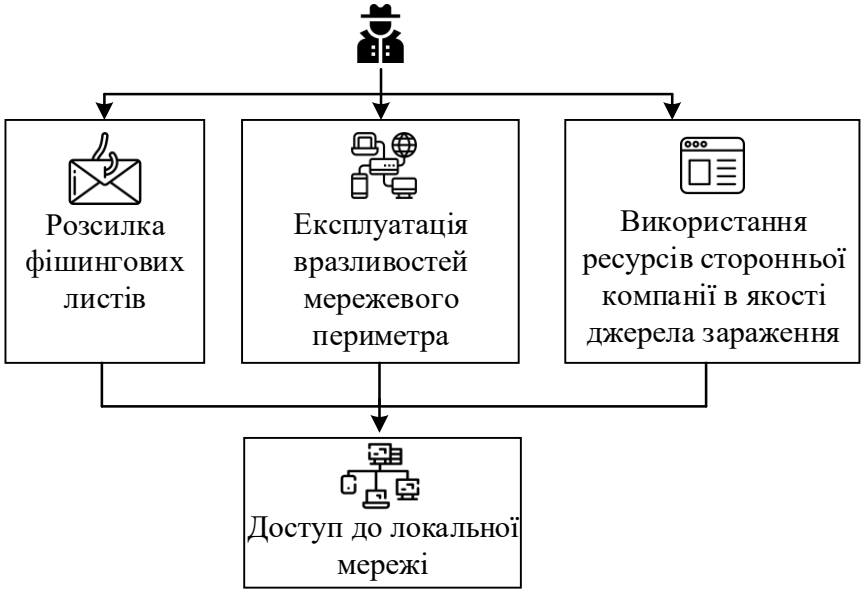


Рисунок 1.15 – Проникнення у внутрішню мережу

Після отримання доступу до локальної мережі банку, злочинець намагається отримати привілеї локального адміністратора на комп'ютерах співробітників і серверах.

Можна виділити поширені уразливості, що зображені на рис.1.16.

Рисунок 1.16 – Поширені уразливості локальних мереж банку

Після отримання максимальних привілеїв в ОС на вузлі злочинці отримують з пам'яті ОС облікові дані всіх користувачів, що підключаються до неї (ідентифікатори, паролі або геш-суми паролів). Ці дані використовуються для підключення до інших комп'ютерів в мережі (рис.1.17) [7].

Рисунок 1.17 – Розвиток атаки і закріплення в мережі

Закріпившись в мережі, порушники повинні зрозуміти, на яких вузлах знаходяться шукані банківські системи і як буде зручніше отримати до них доступ. Злочинець з привілеями локального адміністратора ОС може скопіювати дамп пам’яті цього процесу, витягти паролі для доступу до додатка або зашифрованим баз, а потім отримати у відкритому вигляді паролі для доступу до всіх критично важливих систем банку – АБС, SWIFT, автоматизованого робочого місця для управління банкоматами та ін . Такий сценарій атаки вельми ефективний і неодноразово застосовувався в ході тестування на проникнення (рис.1.18).

Рисунок 1.18 – Компрометація банківських систем і розкрадання грошей

Злочинці можуть перебувати в інфраструктурі банку довго, залишаючись непоміченими, збирати інформацію про інфраструктуру і процеси. Це означає, що крадіжку грошей можна запобігти, якщо вчасно виявити факт компрометації, застосувавши сучасні системи аналізу загроз та виявлення аномалій.

1.3. Аналіз систем виявлення аномалій в роботі (відхилень від нормальної роботи)

Розглянемо основні і найпопулярніші рішення, які змогли б допомогти нам отримати цілісну картину щодо не тільки окремо взятого комп’ютера, а й цілої інфраструктури (рис.1.19).

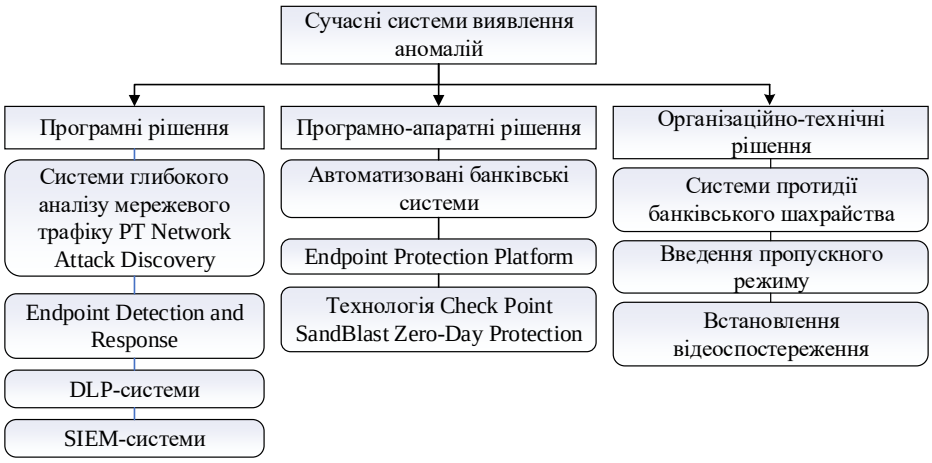


Рисунок 1.19 – Класифікація систем виявлення аномалій

Кожна з цих систем захисту генерує інформацію про події. Без комплексної картини неможливо зрозуміти, що відбувається в IT-інфраструктурі організації.

Автоматизовані банківські системи (АБС). Дана система розроблена для оптимізації діяльності банківського сектору і призначена для комплексного підходу до питання автоматизації банківської діяльності, що дозволяє найбільш ефективно управляти роботою банку.

Важливою характеристикою даного продукту є її трьохрівнева архітектура, яка дозволяє розподілити навантаження на систему, дає можливість використання термінального доступу, і як наслідок, зниження вимог до каналів зв'язку і потужностей робочих станцій.

Функції АБС реалізуються за допомогою застосування таких основних технологій і засобів забезпечення безпеки банківської інформації (рис.1.20).

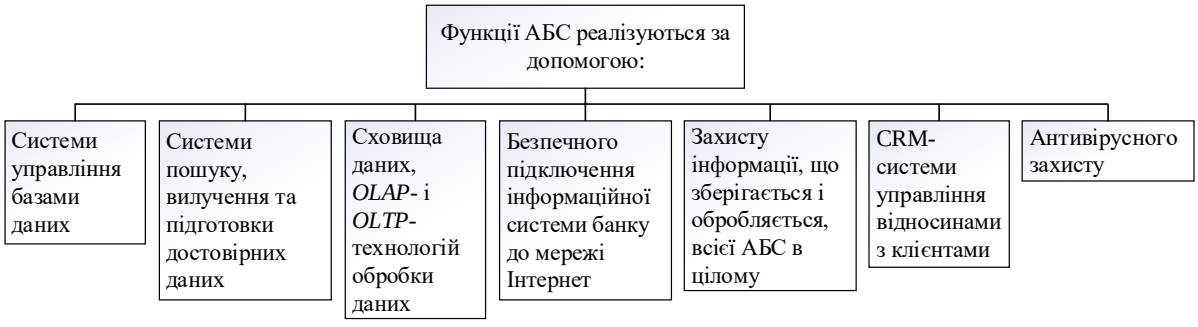


Рисунок 1.20 – Складові функцій АБС

Такі системи вирішують проблему взаємодії зарубіжних систем автоматизації банківської діяльності до законодавства України, що особливо актуально для філій міжнародних банків з впровадженими АБС західного зразка. Цей продукт також може здійснювати побудову і перегляд звітності за попередні періоди, що дозволяє зменшити навантаження на персонал банку при необхідності повторного надання звітів [8]. За своїми функціональними можливостями система може справлятися на високій швидкості з дуже великими обсягами даних, тим самим показуючи кращі результати при менших апаратних потужностях. А максимальне використання можливостей windows та web-інтерфейсів спрощує роботу з системою з точки зору розуміння, швидкості і зручності для користувача.

Системи глибокого аналізу мережевого трафіку PT Network Attack Discovery. PT NAD аналізує дані на рівнях моделі OSI від L2 (канальний рівень) до L7 (рівень додатків) з аналізом вмісту пакетів (рис.1.21).

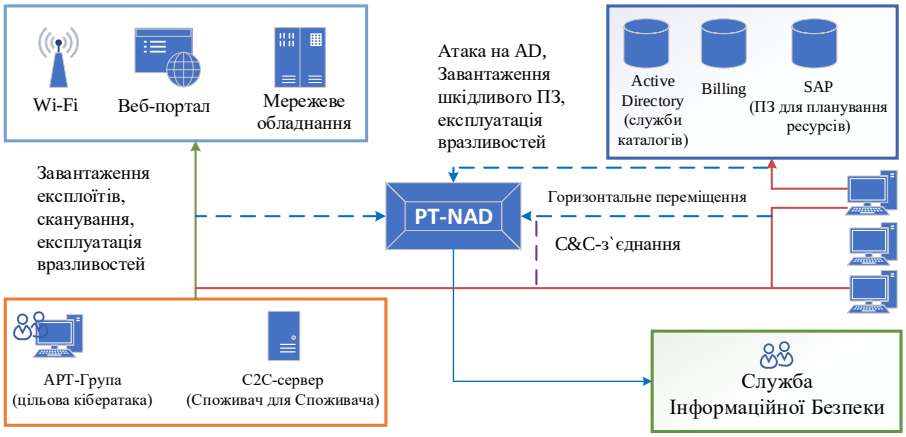


Рисунок 1.21 – Схема роботи PT NAD

Архітектурно продукт складається з ядра і сенсорів (рис.1.22).

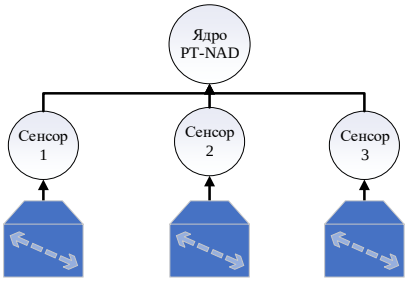


Рисунок 1.22 – Логічна архітектура PT NAD

Сенсори збирають мережеві протоколи та проводять аналіз трафіку за допомогою правил і виконують роль сховища «сирого» трафіку [9]. Аналіз трафіку на сенсорі відбувається за допомогою правил детектування. У базі знань PT NAD - більше 5000 правил. Продукт здатний виявляти горизонтальне переміщення зловмисника всередині периметра, активність шкідливих програм, спроби приховати їх дії від засобів захисту, експлуатацію вразливостей і використання хакерського інструментарію. «Сирий» трафік зберігається в файлах формату PCAP. Їх можна вивантажувати для більш детального аналізу в сторонніх системах і використовувати в якості доказової бази при розслідуванні інциденту. З сенсорів розібраний трафік передається в ядро. Після чого він досліджується із застосуванням машинного навчання, ретроспективного аналізу і індикаторів компрометації. Були визначені основні можливості PT NAD, шо наведені на рис.1.23.

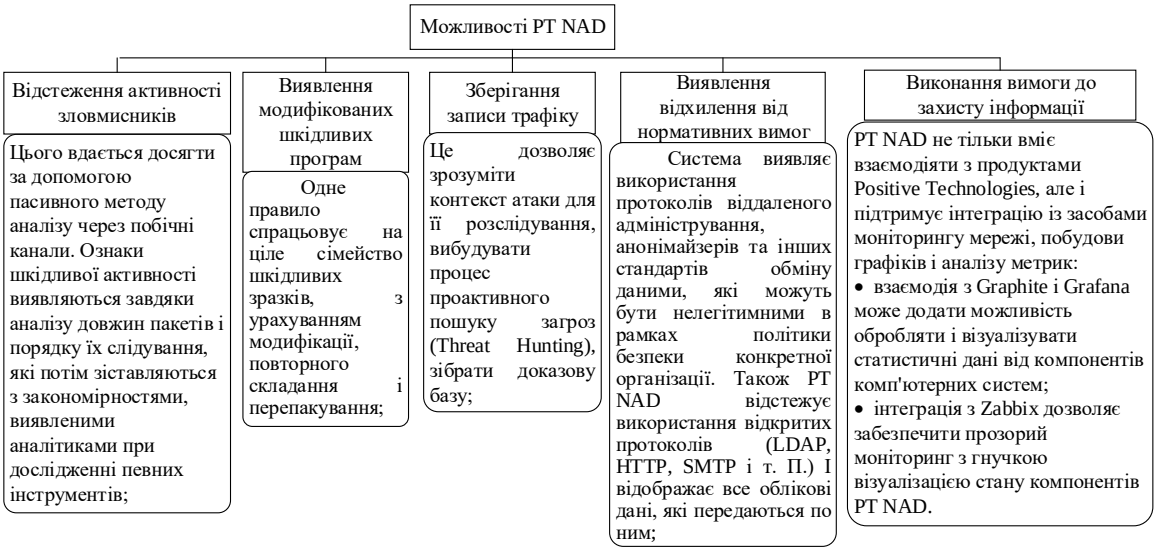


Рисунок 1.23 – Можливості PT NAD

Також були виявлені основні функції системи глибокого аналізу мережевого трафіку, які наведені на рис.1.24.

Рисунок 1.24 – Функціональні можливості PT NAD

Системи протидії банківського шахрайства. Функція антифрод-систем - виявляти і запобігати шахрайству. Процес виявлення та запобігання шахрайству не має початкової або кінцевої стадії, він повинен виконуватися безперервно і включати в себе наступні підпроцеси, що зображені на рис.1.25.

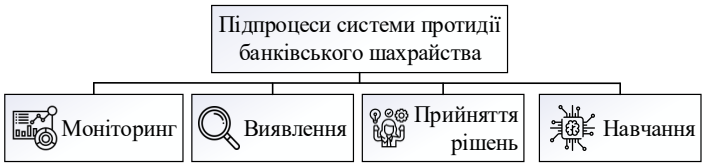


Рисунок 1.25 – Підпроцеси СПБШ

Системи протидії шахрайству можуть мати в своєму арсеналі наступні технології і можливості, наведені на рис 1.26.

Рисунок 1.26 – Функціональні можливості СПБШ

У загальному випадку система захисту від банківського фрода повинна відповідати таким вимогам методів безпеки, зображені на рис.1.27.

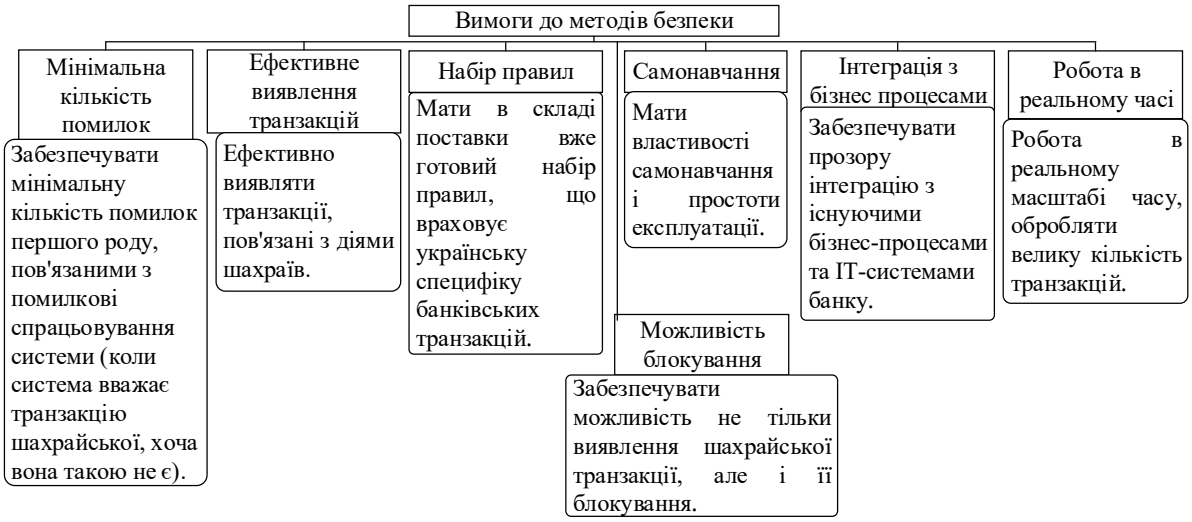


Рисунок 1.27 – Вимоги до методів безпеки системи захисту від банківського фроду

Можна виділити наступні можливі способи реалізації систем виявлення шахрайських операцій (рис.1.28).

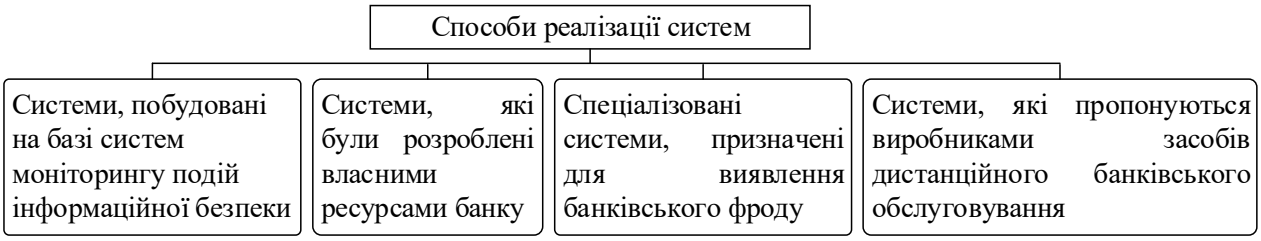


Рисунок 1.28 – Способи реалізації систем виявлення шахрайських операцій

Endpoint Protection Platform. В область визначення «кінцевої станції» входять як персональні комп'ютери користувачів і корпоративні сервера, так і мобільні пристрої і пристрої IoT (Internet of Things). З цієї причини значно збільшилася кількість векторів атак, як на корпоративні мережі, так і на простих користувачів.

Gartner в своєму аналітичному звіті Redefining Endpoint Protection за 2017 та 2018 дає визначення для Endpoint Protection Platform - це рішення, розгорнуте на кінцевих пристроях, для запобігання атак на основі файлів, виявлення шкідливих дій і забезпечення розслідування і відповідної реакції,

необхідних для реагування на динамічні інциденти безпеки і попередження про них. Таким чином, Gartner визначає, що EPP, як і класичний антивірус - це перш за все file-centric-система, яка відштовхується від припущення про те, що якщо не всі, то більшість атак на кінцеві станції проводяться саме через заражені файли. При цьому сучасної EPP відводиться і роль EDR-системи з класичними ознаками таких систем - розслідування інциденту і можливістю формування реакції на нього. Одночасно з цим, захист серверів переходить від класичних EPP-рішень до спеціалізованих, сфокусованим на гібридних центрах обробки даних [10]. Класичний підхід інтеграції безлічі функцій захисту кінцевих станцій в одному продукті не завжди є єдино можливим. Додатковими системами, що розширюють можливості класичних EPP-систем (1.29).

Рисунок 1.29 – Додаткові системи в EPP-системах

Endpoint Detection and Response. Платформи захисту КТ (Endpoint Protection Platform - EPP), які присутні у більшості організацій, можуть захищають від масових, відомих, а також і ряду невідомих загроз, але в більшості випадків, вважаються недостатнім рішенням. Організаціям необхідні додаткові інструменти, які допоможуть їм ефективно виявляти нові, більш складні загрози, з якими вже не в змозі впоратися традиційні засоби захисту. Ці засоби захисту виявляють інциденти на КТ, але зазвичай не здатні визначити, надходячі що попередження можуть бути складовими частинами

більш небезпечною і складної схеми, яка може спричинити за собою більш чутний для організації збиток.

Сучасний захист КТ потребує адаптації до сучасного ландшафту складних загроз і повинен включати функціональність виявлення комплексних атак, спрямованих на КТ, і бути здатною оперативно реагувати на виявлені інциденти.

Рішення EDR виступають самостійним продуктом, або складовою платформи Anti-APT, інтегруючись з пісочницями і забезпечуючи більш високий рівень детектування підозрілої активності.

Результатом від впровадження EDR-рішення щодо протидії складним загрозам буде організація передовий захисту кінцевих пристроїв, що призведе до помітного зменшення поверхні комплексних цільових атак і тим самим до скорочення загального числа кіберзагроз (рис.1.30).

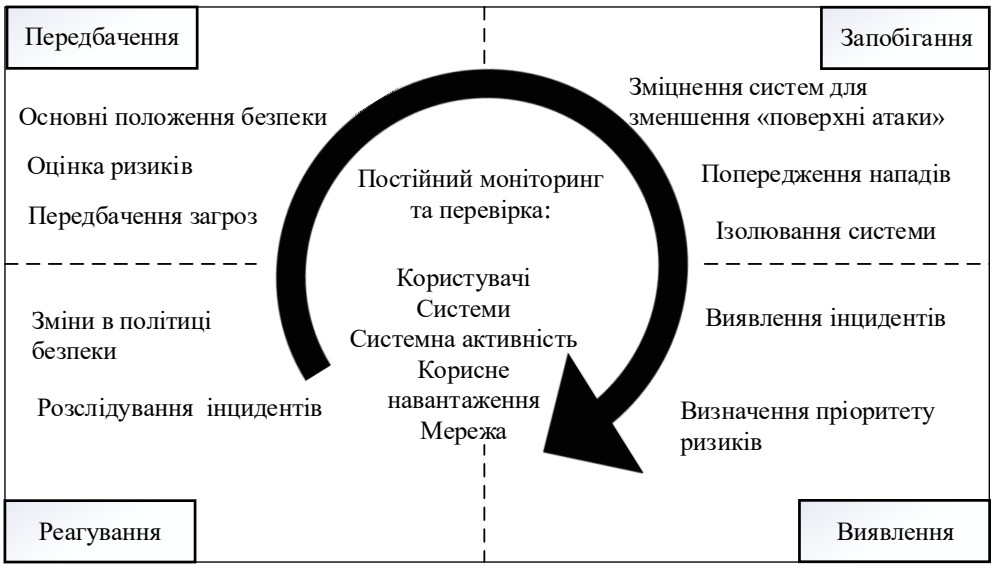


Рисунок 1.30 – Функціональність EDR

Сучасні рішення класу EDR дозволяють надавати можливості, що наведені на рис.1.31.

Рисунок 1.31 – Можливості сучасних EDR-систем

Рішення EDR дозволяє проводити спостереження за всіма діями КТ, таких як, встановлення нового ПЗ, скачування файлів, зміни в політиці безпеки, а також зміни в запущених процесах, в мережевій активності, в поведінці користувачів та ін.

У разі інциденту можна перевірити ці дані і зрозуміти, на яких користувачів була спрямована атака, які системи могли бути скомпрометовані і яка інформація могла постраждати. Рішення EDR відстежує запуск програм і дозволяє визначати місце розташування шкідливих об'єктів в корпоративній мережі. Коли файл потрапляє на КТ, EDR продовжує спостерігати, аналізувати і записувати всю активність файлу, незалежно від його розташування.

Були визначені наступні методи виявлення порушень в EDR системах (рис.1.32).

Рисунок 1.32 – Методи виявлення

Технологія Check Point SandBlast Zero-Day Protection для запобігання раніше невідомих і цільових атак

Check Point SandBlast Zero-Day Protection - технологія, яка складається з двох ключових компонентів (рис.1.33).

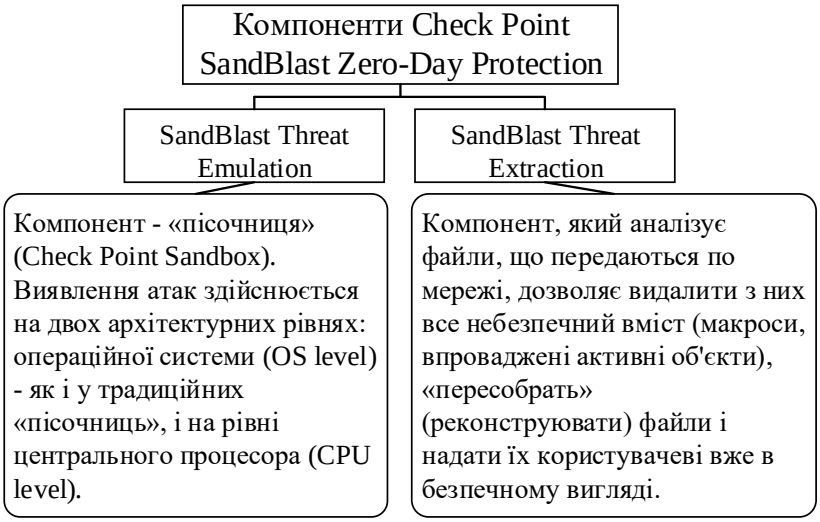


Рисунок 1.33 – Компоненти Check Point SandBlast Zero-Day Protection

Компоненти технології Check Point SandBlast мають різне призначення і реалізовані в рамках програмних продуктів (рис.1.34).

Рисунок 1.34 – Програмні продукти в рамках Check Point SandBlast Zero-Day Protection

Система Check Point SandBlast Zero-Day Protection використовується для вирішення наступного комплексу задач, що приведені на рис.1.35.

Рисунок 1.35 – Завдання просунутої захисту кінцевих точок

DLP-системи. DLP-система являє собою програмний продукт, який ставить задачу забезпечення ІБ. Суть її роботи заснований на створенні захисного периметра, який проводить аналіз будь-яких вхідних і вихідних даних. DLP-системи дозволяють керівництву організацій контролювати інформаційні потоки, відстежувати появу каналів витоку конфіденційної інформації.

Сучасні DLP-системи мають такий набор можливостей зображений на рис. 1.36:

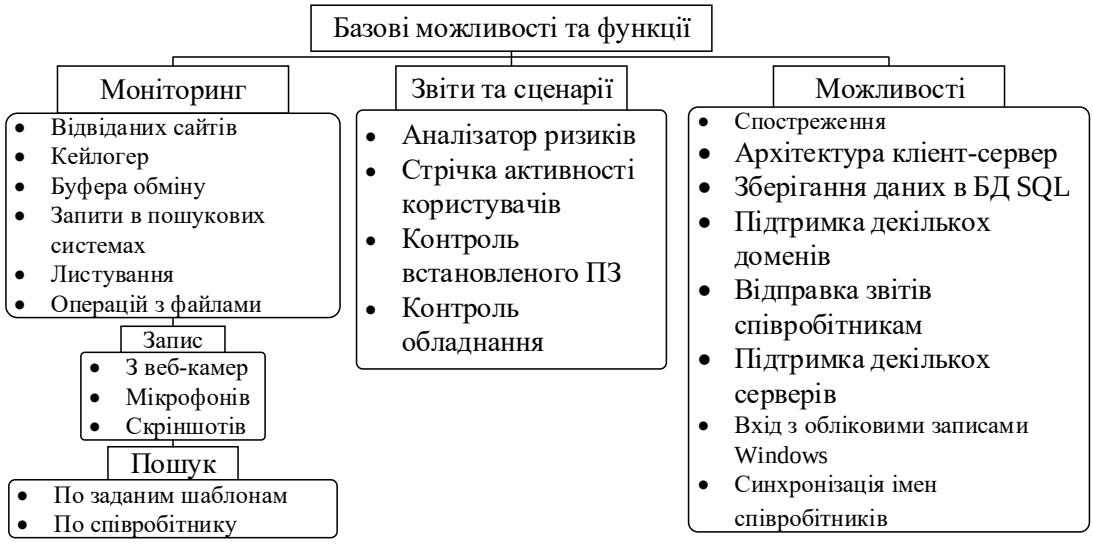


Рисунок 1.36 – Можливості та функції DLP

Найбільш часто DLP-системи застосовуються для вирішення наступних завдань (рис.1.37).

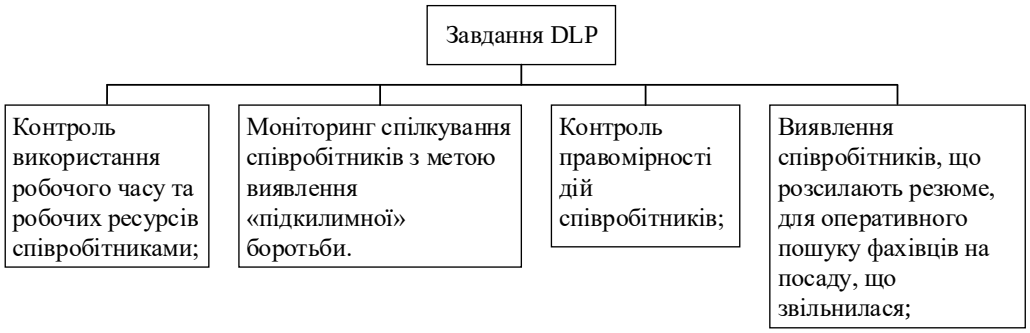


Рисунок 1.37 – Завдання DLP-систем

DLP-системи можуть розпізнавати критичні документи: за формальними ознаками - це надійно, але вимагає попередньої реєстрації документів в системі; з аналізу вмісту - це може давати помилкові спрацьовування, але дозволяє виявляти критичну інформацію в складі будь-яких документів.

Для відповідності визначенню «повнофункціональна» DLP-система повинна відповідати таким основним функціональним критеріям, наведені на рис.1.38.

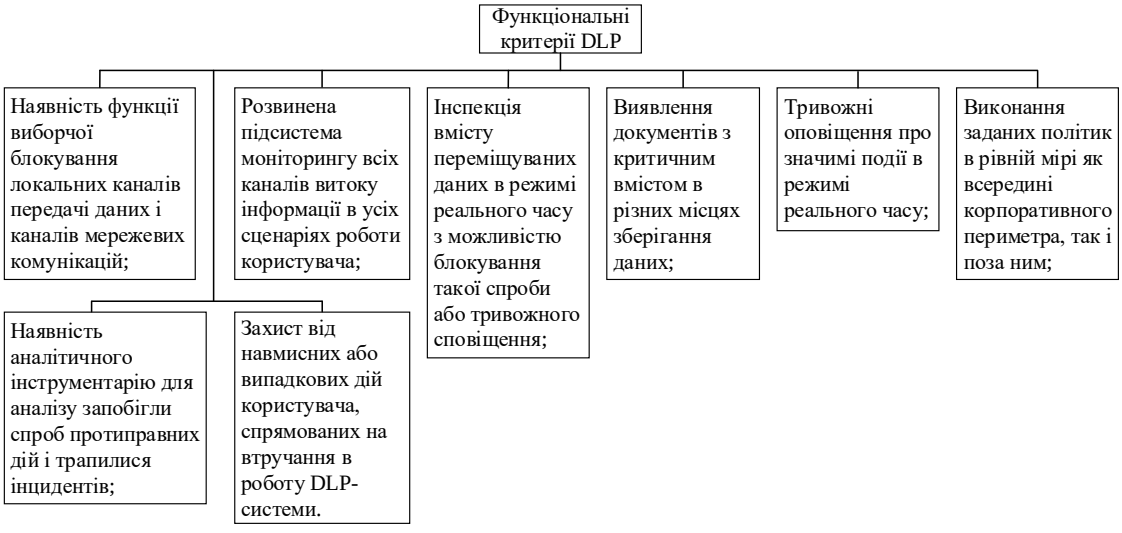


Рисунок 1.38 – Функціональні критерії для DLP-систем

Прийнято чотири критерії оцінки програмних продуктів, що реалізують функціональність DLP (рис.1.39).

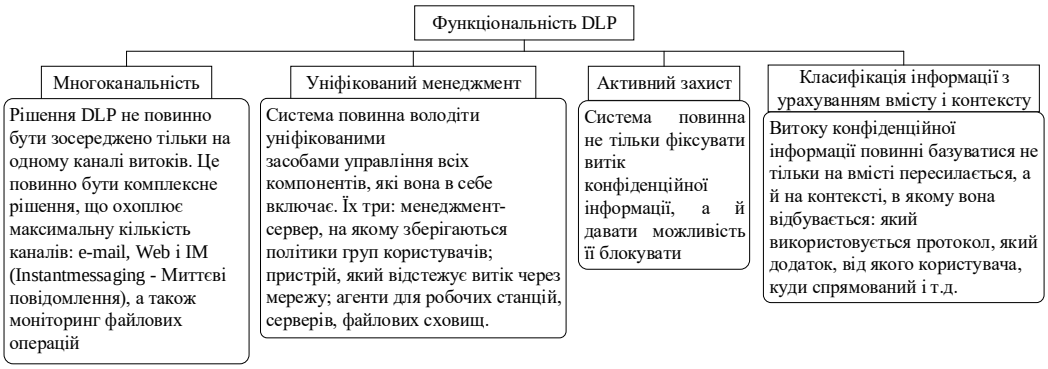


Рисунок 1.39 – Критерії оцінки функціональності DLP

Ефективний підхід до захисту від витоків інформації з комп'ютерів починається з використання механізмів контекстного контролю - контролю передачі даних для конкретних користувачів в залежності від форматів даних, типів інтерфейсів і пристроїв, мережевих протоколів, напрямки передачі, часу доби і т.д [11].

SIEM. SIEM поєднує системи управління інформаційною безпекою (SIM) і управління подіями безпеки. Перша фокусується на аналізі та оповіщенні за даними журналу подій і довготривалого сховища, дію другої направлено на аналіз в реальному часі і кореляцію (рис.1.40).

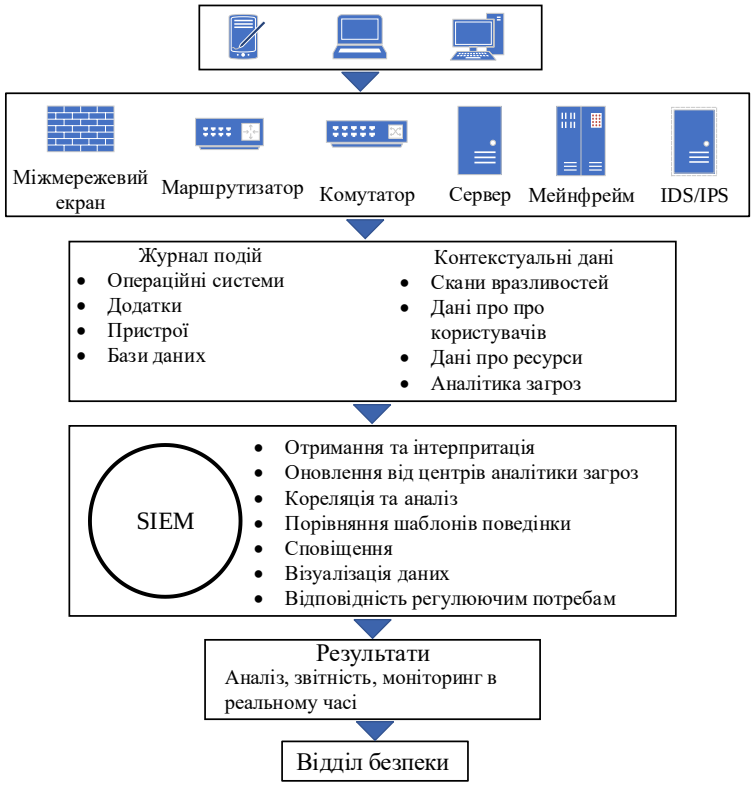


Рисунок 1.40 – Загальна схема роботи SIEM

Функції SIEM-систем зводяться до наступних, що зображені на рис.1.41.

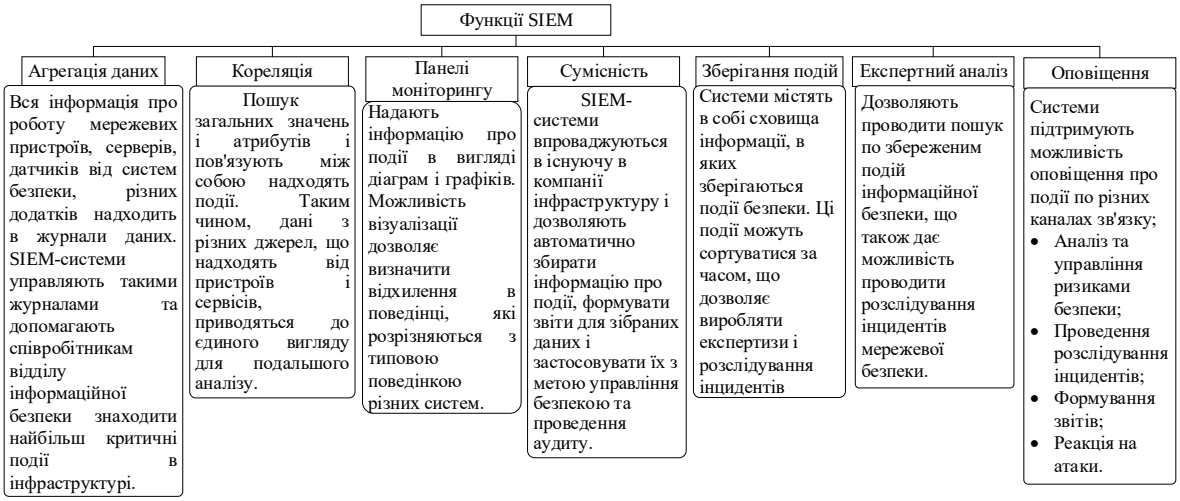


Рисунок 1.41 – Функціональність SIEM-систем

SIEM обробляє отриману інформацію відповідно до набору вбудованих правил. На виході SIEM формує інформаційну панель, звіти та повідомлення про події.

Були виявлені основні переваги SIEM-систем, приведені на рис.1.42.

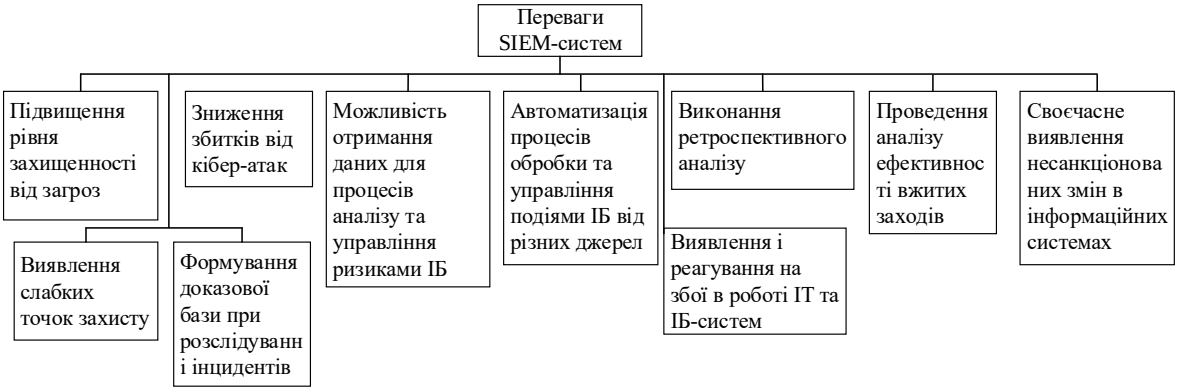


Рисунок 1.42 – Переваги SIEM-систем

SIEM система заздалегідь починає попереджати про початок проблем в системі або атаку хакерів. Вона виявляє аномалії в мережі, в серверах і в поведінці користувачів. SIEM дозволяє виявити приховану шкідливу активність в інфраструктурі.

Типові сценарії використання SIEM-системи (рис.1.43).

Рисунок 1.43 – Сценарії використання SIEM

Інтеграція SIEM дозволяє групам по забезпеченню безпеки отримувати точну базу інформації, за допомогої якої можна вести спостереження та реагувати на можливі загрози для організації.

На табл.1.1 наведено порівняння розглянутих раніше систем, з целья виявити найбільш оптимальне рішення.

Таблиця 1.1 – Порівняння сучасних систем

Критерій	PT-NAD	EDR	EPP	DLP	SIEM	АБС	CPSZDP	СПБШ
Варіант реалізації	Програмний	Програмний	Програмно-апаратний	Програмний	Програмний	Програмно-апаратний	Програмно-апаратний	Організаційно-технічний
Формування звітності	Ні	Ні	Ні	Так	Так	Так	Так	Ні
Оповіщення	Так	Так	Так	Так	Так	Ні	Так	Ні
Моніторинг системних змін	Так	Так	Ні	Так	Так	Ні	Так	Так
Аналіз ризиків	Так	Ні	Ні	Ні	Так	Так	Так	Ні
Виявлення слабких точок захисту	Ні	Ні	Ні	Так	Так	Ні	Так	Ні

Закінчення таблиці 1.1

Візуалізація аналізу інформації	Так	Ні	Ні	Так	Так	Ні	Ні	Ні
Оперативне прийняття рішення	Ні	Ні	Ні	Ні	Так	Ні	Ні	Так
Ретроспективний аналіз	Так	Ні	Ні	Ні	Так	Ні	Ні	Ні
Блокування загроз	Ні	Так	Так	Так	Ні	Ні	Так	Ні

Висновки до розділу 1

На основі вищерозглянутих популярних рішень в сфері інформаційної безпеки приходимо до висновку, що SIEM є найбільш комплексним, універсальним і покриває потреби користувачів, вони можуть впроваджуватися як і в маленькі фірми так і в компанії з сотнями робочих станцій. Завдяки докладної і чітко структурованої звітності, графіками, динамічним таблицями в SIEM системах, фахівці можуть приймати найбільш правильні рішення по захисту комп'ютерної інфраструктури, могуть бути вчасно повідомлені про свіжі проломи, які можуть призвести до тяжких наслідків.

2 ОГЛЯД ТА АНАЛІЗ SIEM-СИСТЕМ, МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ І МЕТОДИК ОЦІНКИ РИЗИКУ

2.1. Огляд SIEM-систем

SIEM-система повинна мати можливість успішного вирішення наступного комплексу завдань, які наведені на рис.2.1.

Рисунок 2.1 – Комплекс завдань SIEM-системи

SIEM здатна виявлення наступних небезпечних факторів, зображених на рис.2.2.

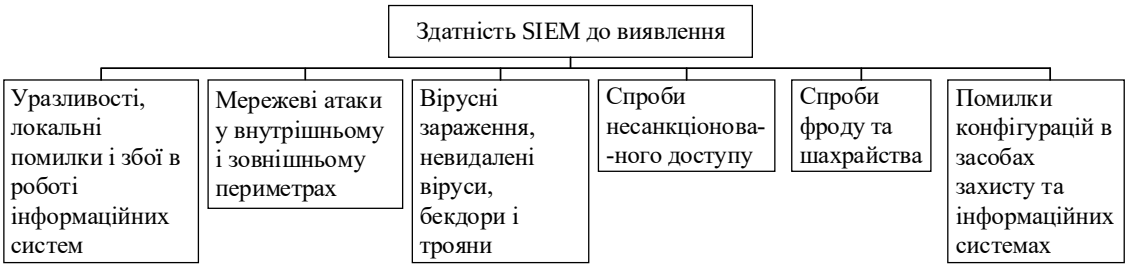


Рисунок 2.2 – Здатність SIEM-системи до виявлення небезпечних факторів

На виході SIEM-система формує звітність, процес формування звітність зображений на рис.2.3.

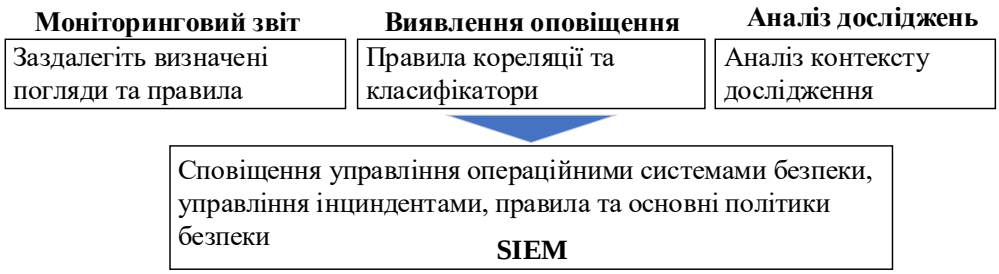


Рисунок 2.3 – Формування звітності SIEM-системи

SIEM - система складається з наступних компонентів, призначення яких описано на рис.2.4.

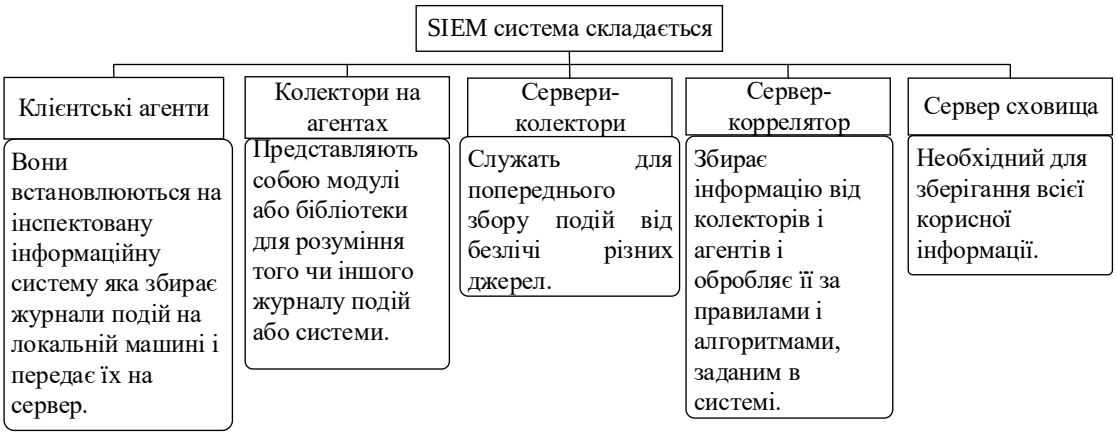


Рисунок 2.4 – Компоненти SIEM

На рис.2.5 представлені джерела для записів системного журналу: маршрутизатори, сервери, міжмережеві екрани та додатки. Може використовувати «Сенсори», що стежать за певною частиною мережі і постачає центральне ядро SIEM корелятивною інформацією.

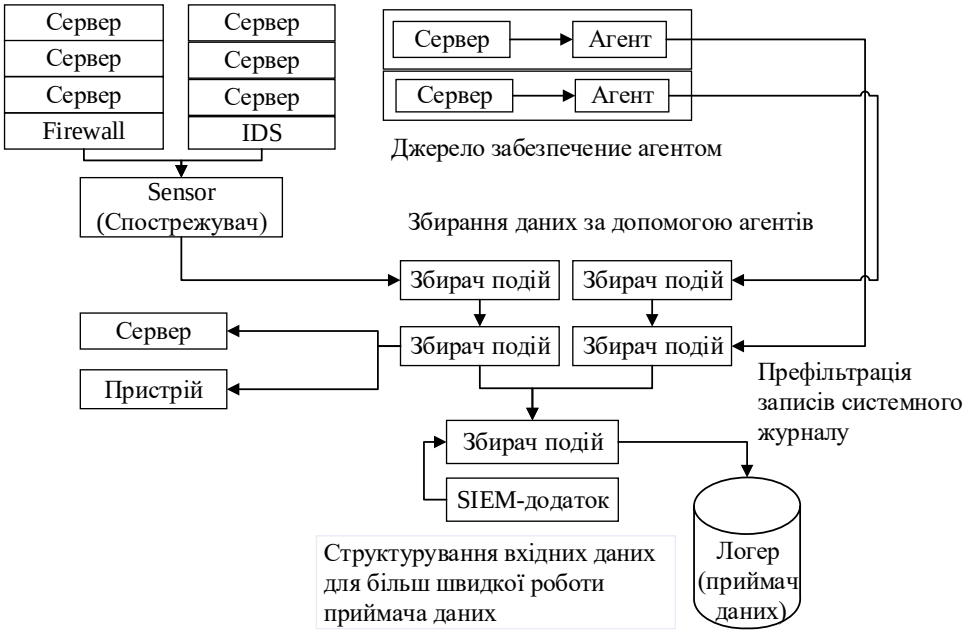


Рисунок 2.5 – Типова структура засоби управління подіями безпеки інформації в SIEM

Джерело може бути забезпечене агентом (складова програми, розширення або плагін, наданий SIEM, який виконує функції передачі або

перетворення записів системного журналу від цільової системи в колектор SIEM). Ключові особливості таких агентів: здатність префільтрації записів системного журналу, грунтуючись на їх ступеня небезпеки, і здатність структурувати вхідні дані для більш кращої роботи логера. Агенти передають записи по спеціально відведеному захищеному каналу.

Система SIEM не здатна самостійно запобігати інцидентам, не має вбудованих захисних функцій. Метою подібних систем є визначення першопричини того чи іншого інциденту за деякими ознаками.

Для досягнення даної мети перед системами класу SIEM ставляться завдання, наведені на рис.2.6.

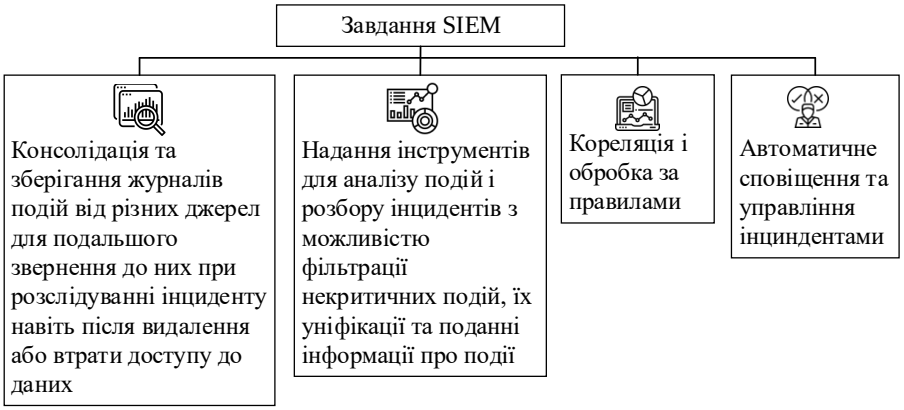


Рисунок 2.6 – Завдання систем класу SIEM

Наочно з процесом приоритизации можна ознайомитися за допомогою спрощеної схеми, зображеної на рис.2.7.

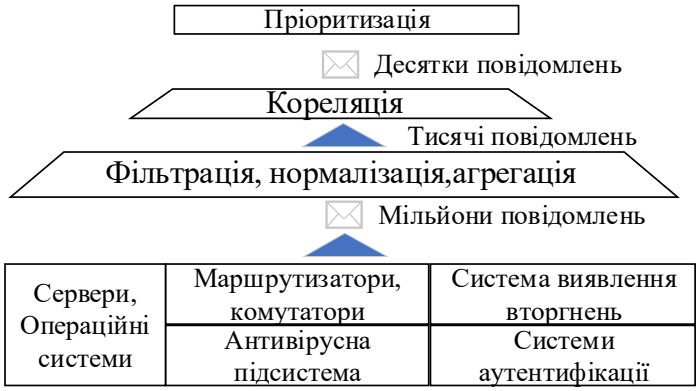


Рисунок 2.7 – Спрощена схема пріотерізації повідомлень в SIEM-системі

Процес кореляції. Для постановки задачі досліджень слід визначити місце і роль процесу кореляції в SIEM-системах. Процес кореляції спрямований на вирішення наступних завдань (рис.2.8).

Рисунок 2.8 – Завдання кореляції в SIEM-системах

Процес виконання кореляції починається зі збору даних з різнорідних джерел і закінчується на етапі формування звіту про поточний стан захищеності.

Механізм кореляції – це процес визначення відносин між подіями, а також причинно-наслідкових залежностей між ними, дозволяє виявляти шкідливі дії та аномальну поведінку, визначати джерело і мета комп'ютерної атаки, виявляти багатокрокові атаки і залежить від конкретної реалізації.

Основними вихідними даними, які використовуються SIEM-системою для вирішення зазначених завдань, є записи журналів аудиту (logs), протоколюється події в інформаційній інфраструктурі, звані «подіями безпеки». Дані події відображають такі дії користувачів і програм, які можуть вплинути на ІБ [11].

На рис.2.9 зображено процес кореляції SIEM-системи.

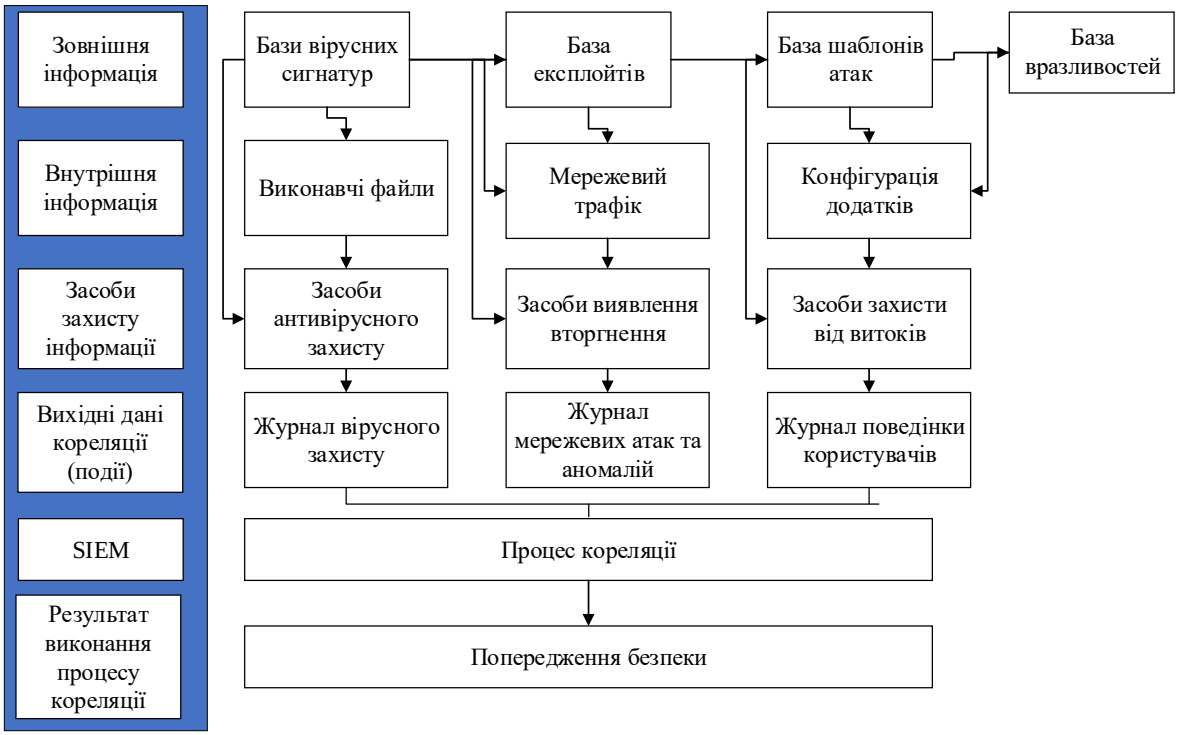


Рисунок 2.9 – Процес кореліції SIEM-системи

Проведемо порівняльний аналіз підходів до кореляції подій безпеки.

Таблиця 2.1 – Порівняльний аналіз підходів до кореляції подій безпеки

Характеристика	Алгоритми		
	На основі подібності	На основі знань	Імовірнісни
Комбінація подій безпеки від різних показників безпеки	Так	Так	Так
Вимоги попередніх знань (навчання алгоритму)	Так	Так	Ні
Точність (виявлення неправдивих подій безпеки)	Так	Так	Припущення
Виявлення багатокрокових атак	Ледве	Так	Припущення
Виявлення нових атак	Ні	Ні	Так
Рівень помилок	Середній	Низький	Високий
Обчислювальна здатність	Висока	Низька	Середня
Гнучкість і розширюваність	Висока	Висока	Низька

Основні джерела інформації для SIEM приведені на рис.2.10.

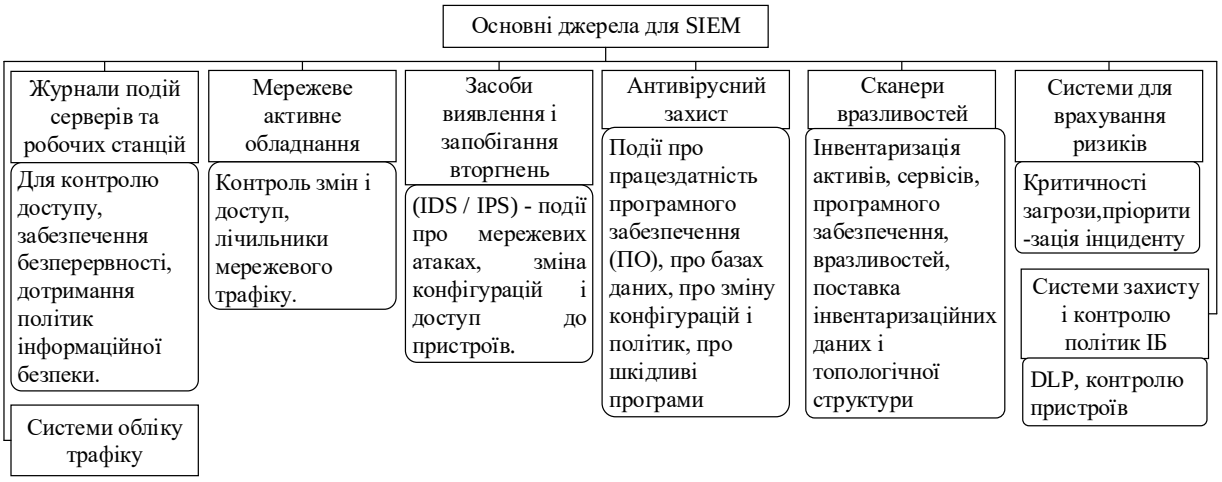


Рисунок 2.10 – Джерела для SIEM-систем

Збір даних від джерел здійснюється встановленими на них агентами [12]. У разі відсутності колектора, відповідного джерела, події можуть бути відправлені в форматі стандарту Syslog. Крім того, є можливість віддаленого збору даних (за допомогою з'єднання за протоколами NetBIOS, RPC, TFTP, FTP) (рис.2.11).

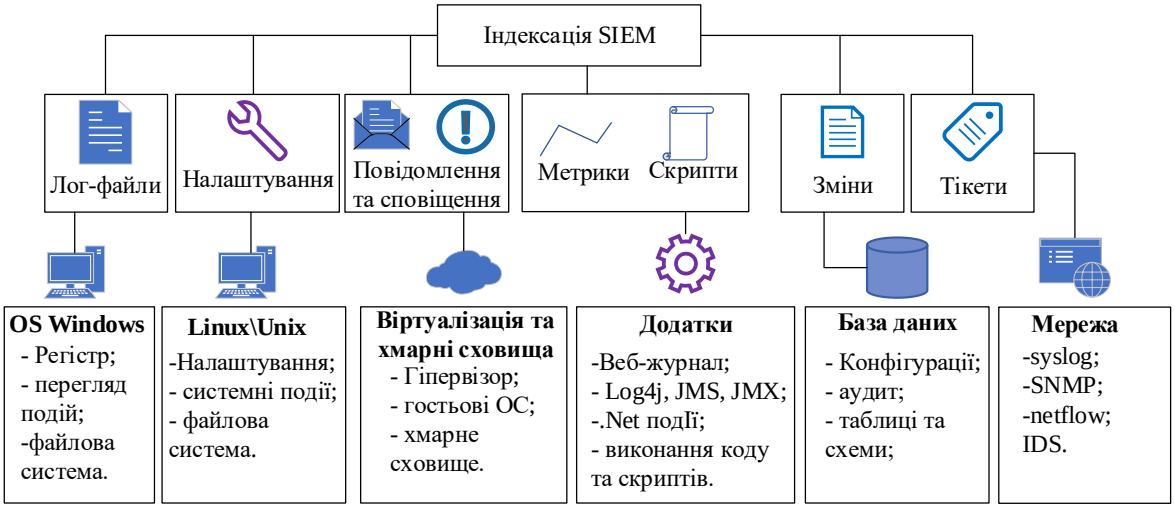


Рисунок 2.11 – Процес аналізу SIEM-системи

Крім широких можливостей по обробці великих потоків різнорідних даних, SIEM системи дозволяють виконувати ретроспективний аналіз подій безпеки і їх наслідків, представляти маршрути атак, моделювати і формувати нові правила виявлення інформаційних загроз і оцінки рівня їх критичності.

Для вирішення цих завдань в SIEM-системах використовуються так звані панелі управління (dashboards), які задають спосіб організації інформації,

необхідної для вирішення однієї або декількох завдань в графічному вигляді, що забезпечує її розуміння з першого погляду. Залежно від характеру виконуваної завдання можна виділити наступні види панелей управління, зображених на рис.2.12.

Рисунок 2.12 – Види панелей управління

Дослідження інцидентів безпеки зазвичай виконується за допомогою інтерактивних таблиць, елементи яких часто реалізуються у вигляді гіперпосилань, за якими здійснюється перехід до інших даних, завдяки чому значно спрощується пошук необхідної інформації [13].

Цікава модель візуалізації для аналізу подій безпеки одного хоста на основі матричного уявлення запропонована в системі Splunk. Події безпеки згруповані по сенсорам безпеки, які їх генерують: події системи аутентифікації користувачів, події системи виявлення вторгнень, значущі події, які визначаються за правилами користувачів і т. д. Події відображаються по осі Y. Тип події на графіку кодується кольором, інтенсивність кольору вказує число подій в заданий період часу. По осі X відкладається час (рис.2.13).

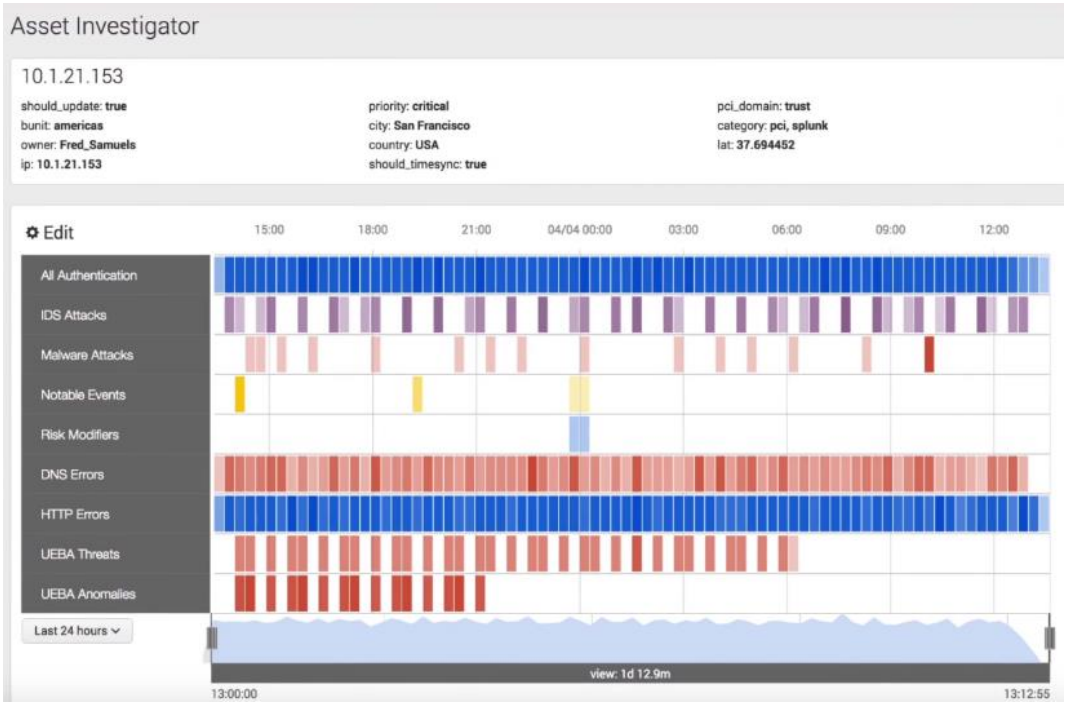


Рисунок 2.13 – Аналізу подій безпеки в Splunk ES

SIEM допомагає досягнути майже повної автоматизації процесу виявлення загроз, тим самим змістивши акцент уваги на критичні загрози, дозволяє своєчасно виявляти аномалії і ризики, забезпечити безперервність роботи IT-сервісів шляхом грамотної настройки кореляційних механізмів, що, в сукупності, дозволяє істотно скоротити можливі фінансові втрати [14].

SIEM, як і інші системи ІБ, не є комплексним вирішенням проблеми. 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 наступних проблем, зображених на рис.2.14.

Рисунок 2.14 – Результат неправильного використання SIEM-системи

Однак грамотно поведінку навченого персоналу системи дозволить:

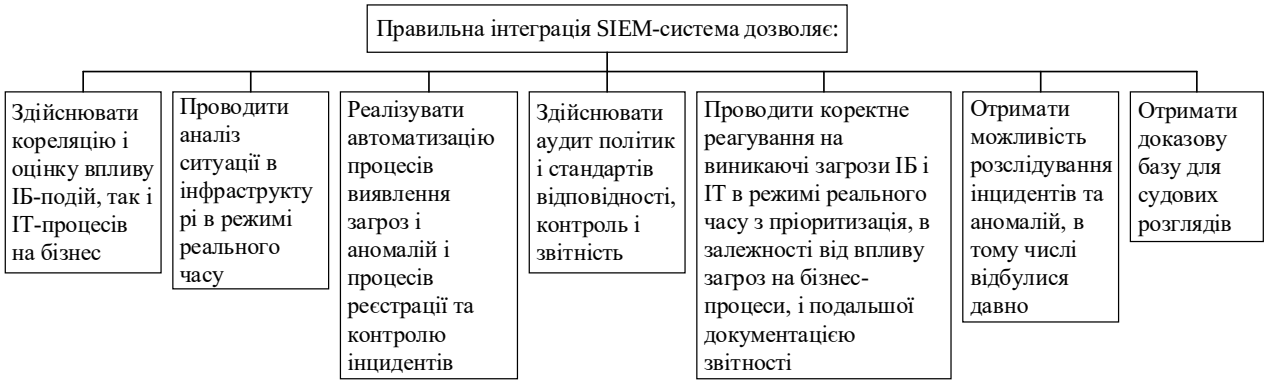


Рисунок 2.15 – Результат грамотного використання SIEM-системи

Максимальна перевага SIEM досягається за рахунок включення максимально можливого набору інформаційних потоків безпеки.

На рівні інфраструктури агенти SIEM можуть бути розміщені на серверах або настільних комп'ютерах, міжмережевих екранах або пристроях IDS / IPS для передачі подій безпеки в базу даних і механізм обробки подій. У деяких випадках події системного журналу включаються SIEM, і це один з найпростіших і простих способів інтеграції системної інформації.

Метою SIEM є те, що групи по забезпеченню безпеки можуть стати більш результативним, оснащеними для виявлення і реагування на загрози

національній безпеці. Після впровадження SIEM, плани реагування та втручання в систему повинні бути протестовані і оцінені так, щоб, при необхідності, заходи з протидії могли бути виконані швидко і точно для пом'якшення передбачуваної загрози.

SIEM дозволяє акцентувати увагу тільки на критичних і дійсно важливих загрози, працювати не з подіями, а з інцидентами, своєчасно виявляти аномалії і ризики, запобігати фінансовим втрати і підвищувати ефективність і безпеку роботи компанії в цілому.

2.2. Аналіз класифікаторів SIEM

Під час дослідження SIEM систем були визначені такі основні класифікаційні ознаки, які приведені на рис.2.16.

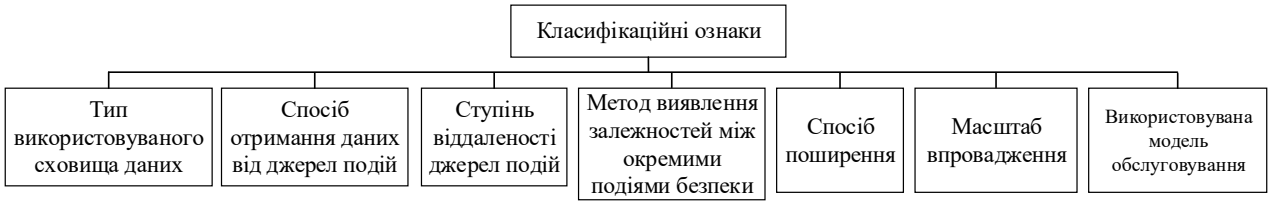


Рисунок 2.16 – Класифікаційні ознаки SIEM-системи

Для організації сховища даних в системах SIEM можуть застосовуватися:

1. Реляційні системи управління базами даних.

2. Нереляційних сховища даних.

За способом отримання даних від джерел подій виділяють системи SIEM (рис.2.17).

Рисунок 2.17 – Способи отримання даних від джерел

Зміст деяких механізмів за рівнями ієрархії SIEM-системи (рис.2.18).

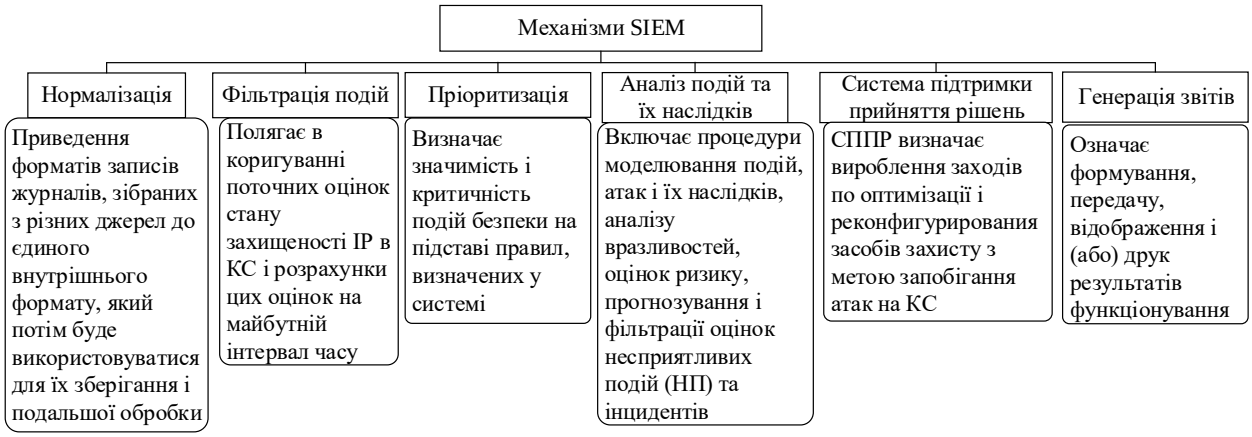


Рисунок 2.18 – Механізми SIEM-систем

У більшості випадків комерційні SIEM системи дозволяють працювати як з використанням агентів, так і без них. Серед переваг способу збору даних без використання агентів слід зазначити відсутність необхідності установки і обслуговування додаткового програмного забезпечення на пристроях джерел подій. Недоліком такого підходу є підвищене навантаження на канал зв’язку між джерелом і сервером, оскільки події пересилаються в необробленому

вигляді, а фільтрація, агрегація і нормалізація виконуються тільки на сервері обробки [15].

За ступенем віддаленості джерел подій виділяють наступні класи рішень SIEM:

1. З джерелами подій в межах контрольованої зони.

2. З територіально розподіленими джерелами подій.

Розглянутий класифікаційний ознака дозволяє розрізняти системи SIEM з локальним і віддаленим керуванням.

У першому випадку, коли керуюча система (сервер обробки, консоль адміністрування) і об’єкт управління (джерело подій) знаходяться в межах контрольованої зони, допускається не використовувати засоби шифрування, що управляють, і переданих даних.

У другому випадку застосування засобів криптографічного захисту процесу віддаленого управління є обов'язковим. Системи управління інцидентами безпеки реалізують різні технології виділення послідовностей контрольованих дій (сценаріїв комп’ютерних атак і ін.) з метою формування відповідних інцидентів безпеки.

Серед методів виявлення залежностей між двома і більше подіями безпеки виділяють наступні, що зображені на рис.2.19.

Рисунок 2.19 – Методи виявлення залежностей

Аналіз відомих джерел показує, що практично всі сучасні SIEM системи в базовій версії поставки застосовують один метод кореляції - на основі заздалегідь заданих правил обробки.

За способом розповсюдження всі рішення SIEM поділяються на два класи:

1. З відкритим вихідним кодом.

2. Комерційні.

Залежно від масштабу впровадження (розгортання) системи управління інцидентами безпеки поділяються на такі класи:

1. Малі.

2. Середні.

3. Великомасштабні.

Класифікаційна ознака характеризує узагальнену оцінку трьох показників: числа підключених джерел, кількості оброблюваних подій в секунду, обсягу сховища, що виділяється для зберігання зареєстрованих подій.

Таблиця 2.2 – Масштаби впровадження SIEM систем

Масштаб впровадження	Число підключених джерел	Кількість оброблюваних подій в секунду	Обсяг сховища, для зберігання зареєстрованих подій
Малий	≤ 300	≤ 1500	≤ 800 Гбайт
Середній	400-800	2000-7000	4-8 Тбайт
Великомасштабні	≥ 900	≥ 15000	≥ 10 Тбайт

По використовуваній моделі обслуговування виділяють наступні класи систем SIEM:

1. Локальної установки.

2. Як послуга (hosted SIEM, SIEM as a service).

Системи управління інцидентами безпеки локальної установки на увазі традиційну модель обслуговування, при використанні якої програмне забезпечення (додатки SIEM рішення) встановлюється і обслуговується користувачем в локальній інфраструктурі організації.

У разі застосування моделі обслуговування SaaS користувачі отримують SIEM рішення, повністю обслуговує провайдером послуг ІБ. Основна перевага моделі SaaS полягає в зниженні витрат, пов'язаних з установкою, оновленням і підтримкою відповідного програмно-апаратного забезпечення. При цьому слід окремо зазначити, що користувач повинен забезпечити необхідну пропускну здатність і безперервність каналу зв’язку з постачальником послуг.

Таблиця 2.3 – Класифікація популярних SIEM систем

№	Класифікаційна ознака	Зміст класифікатора
1	Тип використовуваного сховища даних	1.1 Реляційне сховище даних
		1.2 Нереляційне сховище даних
2	Спосіб отримання даних від джерел подій	2.1 З використанням додатків-агентів (agent-based)
		2.2 Без використання додатків-агентів (agentless)
3	Ступінь віддаленості джерел подій	3.1 З джерелами подій в межах контрольованої зони
		3.2 З територіально розподіленими джерелами подій
4	Метод виявлення залежностей між окремими подіями безпеки	4.1 Заснований на заздалегідь заданих правилах обробки (rule-based)
		4.2 Кінцевий автомат
		4.3 Міркування на основі прецедентів
		4.4 Байєсова мережа
		4.5 Нейронна мережа
5	Спосіб поширення	5.1 З відкритим вихідним кодом
		5.2 Комерційний
6	Масштаб впровадження	6.1 Малий
		6.2 Середній
		6.3 Великий
7	Використовувана модель обслуговування	7.1 Локальна установка
		7.2 Як послуга (hosted SIEM)

На основі раніше визначених ознак розберемо три найпопулярніших рішення в сфері SIEM систем, а саме Splunk Enterprise Security, MaxPatrol SIEM, IBM QRadar, дані системи входять в топ найбільш використовуваних в світі.

Таблиця 2.4 – Класифікація популярних SIEM систем

№	Класифікаційна ознака	SIEM-рішення		
		Splunk Enterprise Security	MaxPatrol SIEM	IBM QRadar
1	Тип використовуваного сховища даних	1.1	1.2	1.1
2	Спосіб отримання даних від джерел подій	2.2	2.1, 2.2	2.1, 2.2
3	Ступінь віддаленості джерел подій	3.1	3.1, 3.2	3.1, 3.2
4	Метод виявлення залежностей між окремими подіями безпеки	4.3	4.1	4.1
5	Спосіб поширення	5.2	5.2	5.2
6	Масштаб впровадження	6.1, 6.2, 6.3	6.3	6.3
7	Використовувана модель обслуговування	7.1, 7.2	7.1	7.1, 7.2

2.3. Методи оцінки загроз та виявлення аномалій

Заснований на ризиках підхід до оцінки потенційних збитків від атак порушників і вибору заходів для його мінімізації отримав назву "Управління ризиками". Під управлінням ризиками мається на увазі повний комплекс алгоритмів і заходів з ряду виконуваних послідовно процесів, що відповідає існуючим міжнародним стандартам і практиці управління ризиками на підприємствах: ідентифікація, аналіз і прийняття ризиків, моніторинг і перегляд. Підставою розрахунку і аналізу ризиків є статистичні дані зі сховищ SIEM-системи, зібрані в процесі ідентифікації ризиків, а результати роботи системного аналітика використовуються особами або процесами з відповідних вузлів SIEM-систем, які приймають рішення в СППР [16].

В даний час моделі аналізу та оцінки ризиків проходять стадію розвитку, які розглядають управління ризиками як прийняття рішень в умовах невизначеності, а кількісні показники ризику - як критерії прийняття альтернативних або взаємодоповнюючих рішень в процесі будь-якої діяльності. Оцінки ризику розраховуються в залежності від ймовірності

реалізації НП в ІС. Розрізняють об'єктивні і суб'єктивні ймовірності настання НС. Оцінка об'єктивних ймовірностей настання НП - одна з важливих завдань в алгоритмі розрахунку оцінок ризику. При цьому використання цих об'єктивних оцінок для підвищення ефективності розрахунків оцінок ризику в ІС підприємства є важливим завданням в методиці розрахунку оцінок потенційних збитків від атак порушників.

SIEM-системи забезпечують аналіз в реальному часі подій безпеки, що виходять від мережевих пристроїв і додатків. Вони використовуються для журналювання даних, їх агрегації, а також зберігання. Обсяги інформації, що зберігається дуже великі, але її велика частина описує звичайну поведінку користувачів, яке не є шкідливим.

Лише малий відсоток цих даних - це інформація про різного роду порушення безпеки: вторгнення, впровадженні шкідливого ПЗ. Таким чином, проблему виявлення загроз безпеці можна звести до задачі виявлення аномалій або відхилень від нормального поведінки користувачів і системи в цілому.

Виявлення аномалій - це підгалузь машинного навчання, яка спрямована на пошук відстійних записів у наборах даних. Він також відомий як виявлення вторгнень, виявлення шахрайства, виявлення неправомірного використання або виявлення зовнішньої інформації відповідно до різних областей додатків. Однак основна ідея залишається такою ж: моделюється нормальна багатоваріантність даних і слід визначити випадки, що відрізняються від більшості, це процес знаходження елементів, подій або спостережень, які не відповідають очікуваним паттернам або значно відрізняються від інших елементів у множині даних [17]. Аномалії в різних джерелах можуть згадуватися як відхилення, викиди, шум або виключення.

Методи розпізнавання аномалій, зображені на рис.2.20.

Рисунок 2.20 – Методи розпізнавання аномалій

1) Класифікація. Пошук аномалій проходить в два етапи: навчання та розпізнавання. Класифікатор навчається на масиві маркованих даних, далі визначається приналежність до одного з відомих класів. В іншому випадку екземпляр позначається, як аномалія.

Найбільш широко вживаними механізмами реалізації розпізнавання аномалій за допомогою класифікації є: нейронні мережі, Байесови мережі, метод опорних векторів і метод на основі правил.

• Метод виявлення аномалій на основі нейронних мереж включає два етапи. Перший: нейронна мережа навчається розпізнаванню класів нормально поведінки на тренувальній вибірці. Другий: кожен екземпляр надходить в якості вхідного сигналу нейронної мережі. Система, заснована на нейронних мережах, може розпізнавати як один, так і кілька класів нормального поведінки.

Для знаходження аномалій за допомогою розпізнавання тільки одного класу використовуються репліквативние нейронні мережі. Що одержала широке поширення технологія нейронних мереж глибинного навчання (Deep Learning) успішно застосовується для вирішення даного завдання.

• Байєсова мережею є графічна модель, відображає імовірнісні залежності множини змінних і дозволяє проводити імовірнісний висновок за допомогою цих змінних. Вона складається з двох основних частин: графічна структура, яка визначає набір залежностей і незалежностей в множини

випадкових величин, що представляють суб'єкти предметної області, і набір імовірнісних розподілів, що визначають силу відносин залежності, закодованих в графічній структурі. Таким чином, застосування Байєсова мережі при ідентифікації аномалій полягає в оцінці ймовірності спостереження одного з нормальних або аномальних класів. Найбільш простий реалізацією даного підходу є Наївний байесовский підхід (Naive Bayes Approach).

• Метод опорних векторів (Support Vector Machine) застосовується для пошуку аномалій в системах, де нормальна поведінка видається тільки одним класом. Даний метод визначає межу регіону, в якому знаходяться екземпляри нормальних даних. Для кожного досліджуваного екземпляра визначається, чи знаходиться він в певному регіоні. якщо екземпляр виявляється поза регіоном, він визначається як аномальний.

• Останній метод грунтується на генерації правил, які відповідають нормальної поведінки системи. Примірник, який не відповідає цим правилам, розпізнається як аномальний. Алгоритм складається з двох кроків. Перший: навчання правил з вибірки за допомогою одного з алгоритмів, таких як RIPPER, Decision Trees і т.д. Кожному правилу привласнюється своє значення, яка пропорційна співвідношенню між числом навчальних примірників, що класифікуються, як правило, і загальним числом навчальних примірників, покриваються цим правилом. Другий крок: пошук для кожного тестового екземпляра правила, яке найкращим чином підходить до даного екземпляру. Система може розпізнавати як один, так і кілька класів поведінки.

2) Кластеризація. Виявлення аномалій може будуватися на наступному припущенні:

- Нормальні екземпляри даних відносяться до кластеру даних, в той час як аномалії не належать ні до одному з кластерів. Однак при такому формулюванні може виникнути проблема визначення чітких меж кластерів. Звідси випливає інше припущення:

- Нормальні дані ближче до центру кластера, а аномальні - значно далі. У разі, коли аномальні екземпляри не є одиничними, вони також можуть утворювати кластери. Таким чином, їх виявлення будується на наступному припущенні:

- Нормальні дані утворюють великі щільні кластери, а аномальні - маленькі і розрізнені. Однією з найпростіших реалізацій підходу на основі кластеризації є алгоритм k-means [19].

3) Статистичний аналіз. Даний клас методів зручний тим, що не вимагає заздалегідь визначених знань про вид аномалії. Методи статистичного аналізу підрозділяються на дві основні групи, що приведені на рис.2.21.

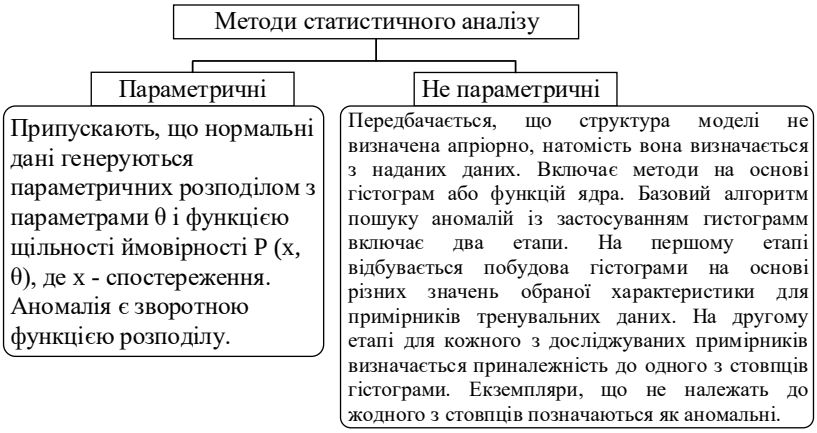


Рисунок 2.21 – Методи статистичного аналізу

4) Алгоритм найближчого сусіда. Два основні підходи грунтуються на наступних припущеннях (рис.2.22)

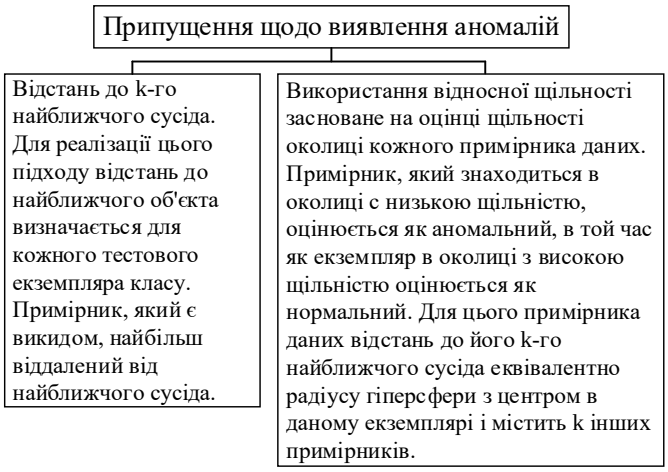


Рисунок 2.22 – Підходи до виявлення аномалій в алгоримті найближчого сусіда

5) Спектральні методи. Ця методика заснована на наступному припущенні - дані можуть бути вкладені в підпростір меншої розмірності, в якому нормальний стан і аномалії проявляються інакше. Спектральні методи часто застосовуються спільно з іншими алгоритмами для предобработки даних.

6) Гібридні методи. Прикладами гібридних систем розпізнавання аномалій можуть бути такі дослідження:

• Поєднання кластеризації і алгоритму найближчого сусіда в роботі.

• Паралельне використання суміщених алгоритмів Байесови мереж і вирішальних дерев, а також алгоритму найближчого сусіда з класифікацією на основі правил в роботі.

• Поєднання методу опорних векторів і нейронної мережі глибинного навчання в роботі.

На основі вищеописаних методів виявлення аномалій побудуємо порівняльну таблицю.

Таблиця 2.5 – Порівняння методів виявлення аномалій

Метод	Режим розпізнання	Результат	Робота без попереднього класу аномалій	Визначення класу аномалії
Класифікація	Контрольоване (supervised),напівконтрольоване (semi-supervised)	Мітка	Ні	Так
Кластеризація	Неконтрольоване(unsupervised), контрольоване(supervised)	Мітка	Ні	Ні
Статистичний аналіз	Напівконтрольоване (semi-supervised)	Ступінь	Ні	Ні
Алгоритм найближчого сусіда	Напівконтрольоване (semi-supervised)	Ступінь	Так	Ні

Закінчення таблиці 2.5

Метод	Режим розпізнання	Результат	Робота без попереднього класу аномалій	Визначення класу аномалії
Спектральні методи	Неконтрольоване (unsupervised), напівконтрольоване (supervised)	Мітка	Так	Ні

Методи машинного навчання для виявлення аномалій мають схожу функціональну архітектуру, представлену на рис.2.23.

Рисунок 2.23 – Архітектура методів виявляє аномалій

Можна виділити кілька стадій визначення аномалій та відхилень від нормальної поведінкі системи. Параметризація включає в себе збір і подальшу обробку даних з систем-моніторингу. Далі, на стадії навчання, будується модель системи з використанням ручних або автоматичних методів.

Алгоритми машинного навчання будують необхідну модель автоматично, отримуючи на вхід тренувальні дані. Методи машинного навчання для виявлення аномалій можна розділити на алгоритми, що вимагають навчання з учителем і не потребують цього.

Методи машинного машинного навчання наведені на рис.2.24.

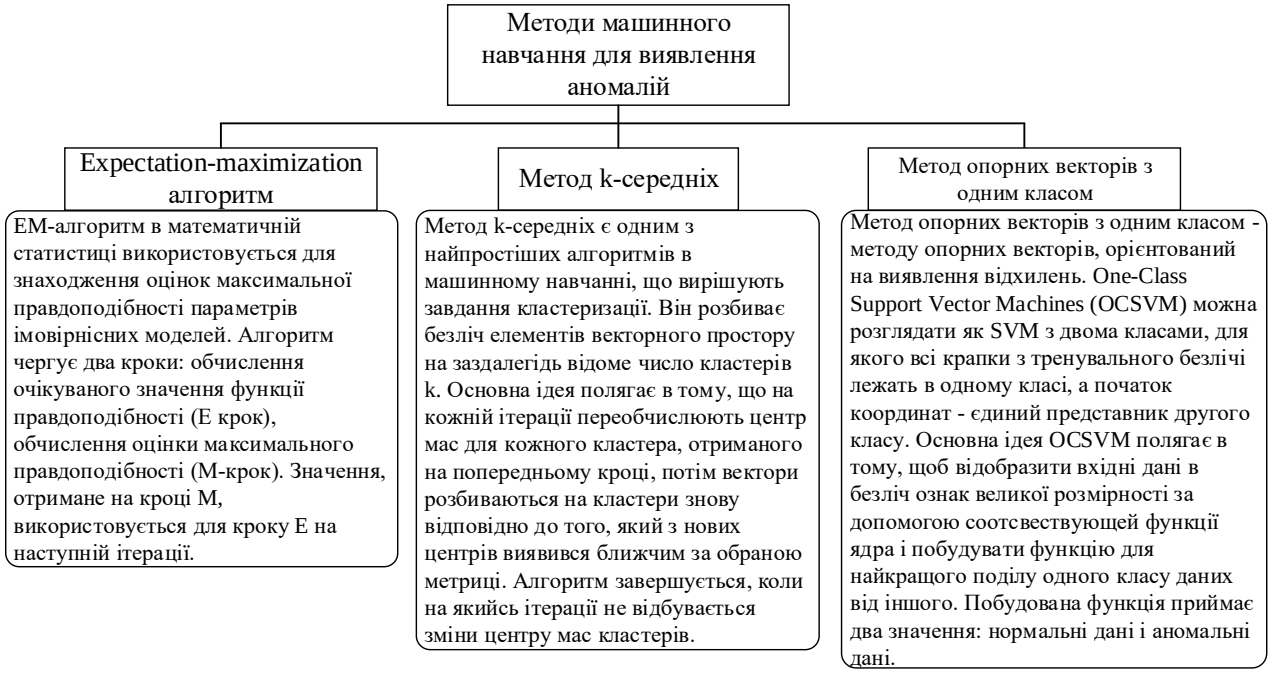


Рисунок 2.24 – Методи машинного навчання для виявлення аномалій

2.4. Класифікатори, використання класифікаторів

Для побудови метрик загроз на основі синергетичного підходу, користуються підходом побудови класифікатора загроз на основі інформаційно-аналітичної моделі методу подвійних трійок (рис.2.25) [19].

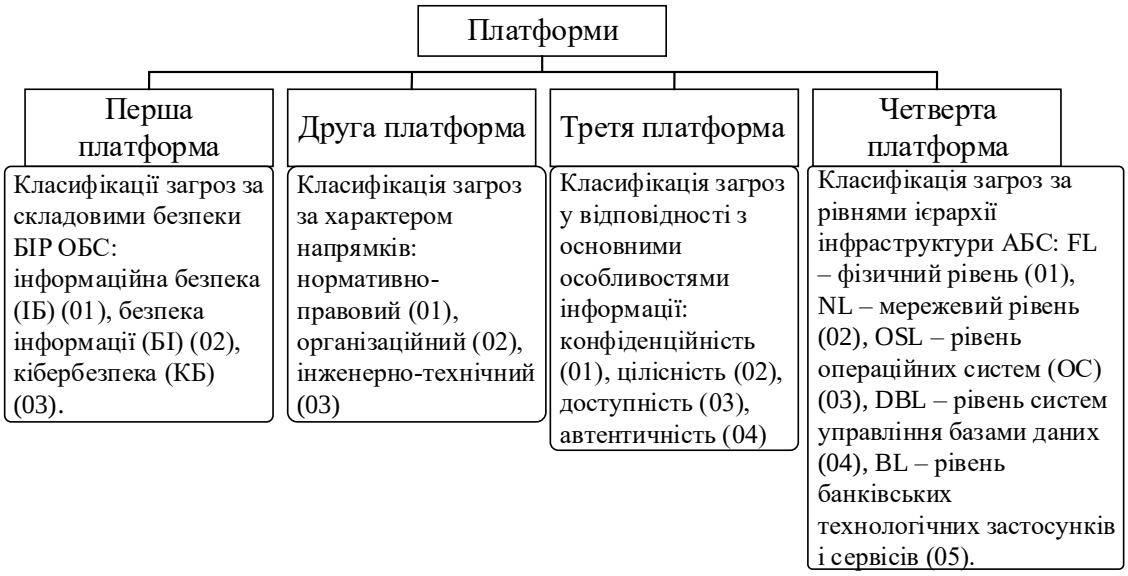
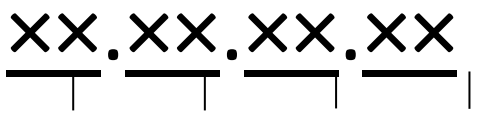


Рисунок 2.25 – Інформаційно-аналітична модель методу подвійних трійок

Частини класифікатора поділяються точкою і мають вигляд, зображений на рис.2.26.



(*1* – синергетична складова безпеки БІР, *2* – характер напрямків;
3 – особливості інформації; *4* – рівні ієрархії інфраструктури АБС).

Рисунок 2.26 – Складові узагальненого класифікатора

Формування метричних коефіцієнтів загроз експертами за послугами безпеки. Нехай *j* – послуги безпеки БІР. Основними послугами безпеки БІР є *C* –конфіденційність; *I* – цілісність; *A* – доступність; *Au* – автентичність. Тоді класифікатор за чотирма послугами безпеки описується виразом вигляду $j = \{C, I, A, Au\}$ Класифікатор містить *N* загроз. У складанні вагових коефіцієнтів прояву кожної загрози на послуги безпеки БІР брали участь *K* експертів (рис.2.27) [20].

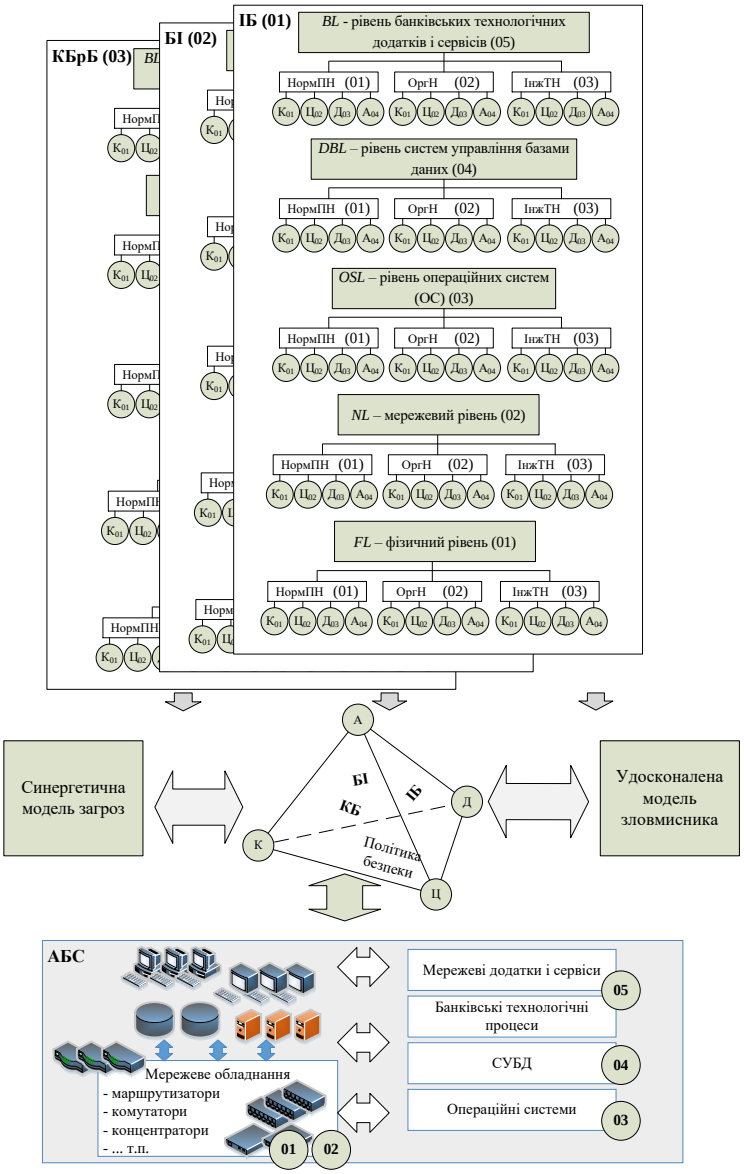


Рисунок 2.27 – Взаємозв’язок структурної схеми класифікатора загроз з АБС ОБС

Позначимо через i поточний номер загрози $(\{i\}_1^N)$, через k – поточний номер експерта, який виконував оцінку $(\{k\}_1^K)$. Середнє значення оцінки експертів за всіма загрозами для певної послуги безпеки може бути записане [21]:

$$w^j = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{ik}^j , \qquad (2.1)$$

де w_{ik}^j – значення метричного коефіцієнта, виставленого k-м експертом для i-ї загрози j-ї послуги безпеки; N – кількість загроз; K – кількість експертів.

Формування ідентифікаторів загроз за складовими класифікатора. На цьому кроці експерти формують цифрове значення (код) ідентифікатора загрози за відповідними складовими класифікатора.

Визначення реалізації кожної *i*-ї загрози з урахуванням імовірності прояву атаки (її виникнення) здійснюється за виразом:

$$w_i^j P_i^j = \frac{1}{K} P_i^j \sum_{k=1}^{N} w_{ik}^j. \qquad (2.2)$$

Для кожної послуги безпеки та *i*-ї загрози:

$$w_i^C \alpha_i^C = \frac{1}{K} \alpha_i^C \sum_{k=1}^{K} w_{ik}^C \text{ – послуга конфіденційність;}$$

$$w_i^I \alpha_i^I = \frac{1}{K} \alpha_i^I \sum_{k=1}^{K} w_{ik}^I \text{ – послуга цілісність;}$$

$$w_i^A \alpha_i^A = \frac{1}{K} \alpha_i^A \sum_{k=1}^{K} w_{ik}^A \text{ – послуга доступність;}$$

$$w_i^{Au} \alpha_i^{Au} = \frac{1}{K} \alpha_i^{Au} \sum_{k=1}^{K} w_{ik}^{Au} \text{ – послуга автентичність,}$$

де $w_{ik}{}^C$, $w_{ik}{}^I$, $w_{ik}{}^A$, $w_{ik}{}^{Au}$ – експертні вагові коефіцієнти послуг безпеки: конфіденційності, цілісності, доступності, автентичності; α_i^C, α_i^I, α_i^A, α_i^{Au} – ваговий коефіцієнт послуги безпеки: конфіденційності, цілісності, доступності, автентичності прояву атаки *i*-ї загрози [22].

Визначення реалізації виникнення декількох загроз для обраної послуги розраховується з урахуванням виразу:

$$W_{synerg}^C = \sum_{i=1}^{M} w_i^C \alpha_i^C \text{ – послуга конфіденційність;}$$

$$W_{synerg}^I = \sum_{i=1}^{M} w_i^I \alpha_i^I \text{ – послуга цілісність;}$$

$$W_{synerg}^A = \sum_{i=1}^{M} w_i^A \alpha_i^A \text{ – послуга доступність;}$$

$$W_{synerg}^{Au} = \sum_{i=1}^{M} w_i^{Au} \alpha_i^{Au} \text{ – послуга автентичність,} \qquad (2.3)$$

де *M* – кількість декількох загроз, які вибрані експертом з ІБ банку з множини $\{i\}_i^M$, яка є підмножиною усієї множини загроз класифікатора, тобто $M \le N$.

При формуванні метричних коефіцієнтів уважається, що отримані

результати належать до незалежних загроз, у випадку їх залежності (збіг класифікатора загроз) необхідно скористатися виразом визначення повної ймовірності залежних подій [23]:

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

Підсумкова оцінка *i*-ї загрозі осереднюється за кількістю експертів відповідно до виразу:

$$x_i = \frac{\sum_{k=1}^{K} x_k \times k_k}{K}, \tag{2.4}$$

де x_k– оцінка *k*-го експерта впливу *i*-ї загрози;

k_k – рівень компетентності експерта;

K– кількість експертів.

Мірою погодженості думок експертів вважається дисперсія, що обчислюється за виразом:

$$\sigma_x^2 = \frac{1}{K}\sum_{k=1}^{K} k_k \left(x_k - x_i\right)^2. \tag{2.5}$$

Статистична значимість отриманих результатів з імовірністю 1 – α_i, становить: $\left[x_i - \Delta, x_i + \Delta\right]$, де величина x_i розподілена за нормальним законом із центром у x_i і дисперсією σ_x^2 . Тоді Δ визначається за виразом:

$$\Delta = t\sqrt{\sigma_x^2 / N}, \tag{2.6}$$

де *t* – величина, що підкоряється розподілу Стьюдента для *K* – 1 ступенів свободи, *K* – кількість експертів [24].

Визначення сумарної загрози за складовими безпеки з урахуванням виразу розраховується:

$$W_{synerg}^{IB} = \sum_{i=1}^{N}\left(w_i^C \bigcap w_i^I \bigcap w_i^A \bigcap w_i^{Au}\right)\alpha_i,$$

$$W_{synerg}^{KB} = \sum_{i=1}^{N}\left(w_i^C \bigcap w_i^I \bigcap w_i^A \bigcap w_i^{Au}\right)\alpha_i,$$

$$W_{synerg}^{BI} = \sum_{i=1}^{N}\left(w_i^C \bigcap w_i^I \bigcap w_i^A \bigcap w_i^{Au}\right)\alpha_i. \tag{2.7}$$

Визначення узагальненої синергетичної загрози на БІР:

$$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \bigcup W_{synerg}^{KB} \bigcup W_{synerg}^{BI}. \quad (2.8)$$

Визначення узагальненої синергетичної загрози з урахуванням її гібридності розраховується:

$$W_{synerg}^{\text{hybrid}\,C,I,A,Au} = W_{synerg}^{C} \bigcap W_{synerg}^{\text{I}} \bigcap W_{synerg}^{A} \bigcap W_{synerg}^{Au}. \quad (2.9)$$

На виході отримуємо удосконалений класифікатор загроз безпеці БІР, що ґрунтується на синергетичній моделі загроз.

Висновки до розділу 2

Розглянуто основні можливості систем, також були визначені основні класифікаційні можливості за якими було проведено порівняння найпопулярніших систем в сфері SIEM.

Запропонована концепція, заснована на синергетичному підході до вибору найбільш ефективних напрямків досягнення поставлених цілей безпеки БІР в АБС з урахуванням величини ризику на кожному рівні і забезпеченням ефективного контролю за виконанням функцій системи управління інформаційною безпекою організацій банківського сектора.

3 РОЗРОБКА КЛАСИФІКАТОРУ БЕЗПЕКИ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

3.1. Аналіз поточного стану безпеки. Методика оцінки аналізу АБС

Для забезпечення безпеки банківських інформаційних ресурсах в автоматизованих банківських системах використовуються наступні засоби (рис.3.1).

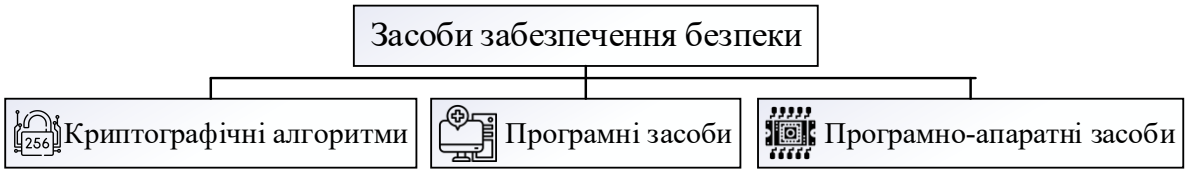


Рисунок 3.1 – Засоби забезпечення безпеки БІР

Для її побудови ще на етапі проектування використовуються різні моделі безпеки, що дозволяють змоделювати роботу елементів комплексної системи захисту інформації та спрогнозувати можливість забезпечення безпеки активів БІн в АБС [25].

Використання моделей безпеки на етапі проектування і функціонування КСЗІ дозволяє без додаткових капітальних, людських і енергетичних витрат провести дослідження і отримати оцінку якості функціонування КСЗІ, ефективність протидії відомим сучасним загрозам на всі складові безпеки: ІБ, КБ, БІ БІР в АБС, змоделювати деструктивні заходи і спрогнозувати можливі економічні витрати при втраті банківської інформації (рис.3.2).

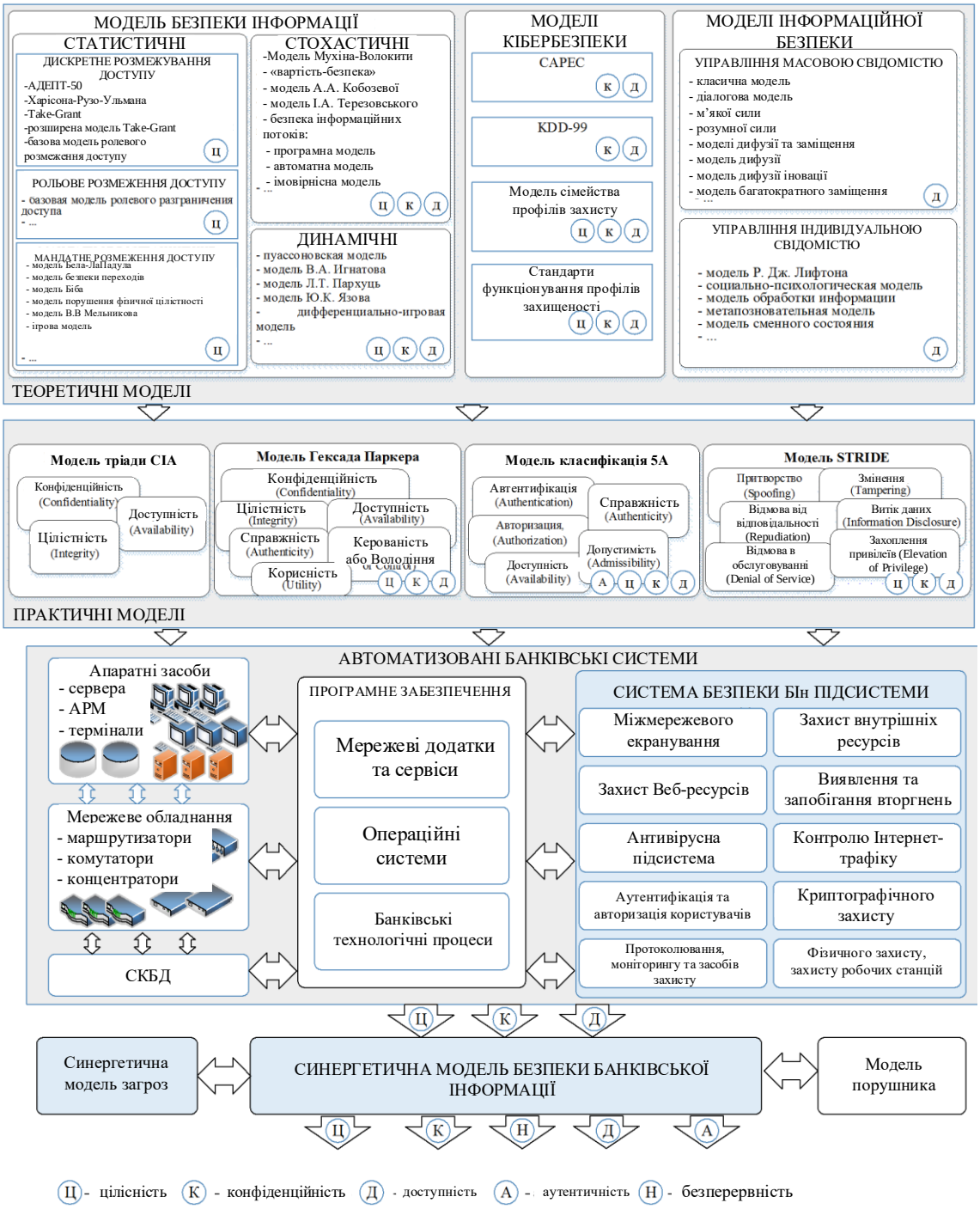


Рисунок 3.2 – Узагальнений підхід формування синергетичної моделі безпеки БІн

Аналіз рис. 3.2. показав, що при формуванні комплексної системи захисту інформації, як правило, використовується модель ЦКД (цілісність-конфіденційність-доступність) або її похідні.

Перший підхід побудови і оцінки функціонування КСЗІ заснований на виконанні вимог одного з регуляторів (стандартів) безпеки. Тоді критерієм

ефективності можуть бути мінімальні сумарні витрати на виконання поставлених функціональних вимог. Основним недоліком такого підходячи є відсутність динамічного підходу ("запізнювання вимог регулятора") по відношенню до бурхливо наростаючим можливостям загроз.

Другий підхід побудови і оцінки КСЗІ заснований на принципі "розумної достатності", що в свою чергу не дає змоги вчасно прогнозувати деструктивні заходи загрозам і "закладає" певні ризики реалізації загроз на активи бін. Крім цього, такий підхід будується на експертну грошову оцінку та, відповідно, носить суб'єктивний характер, що вимагає "постійних" додаткових досліджень всього комплексу заходів, за оцінкою поточного стану ІБ банку.

3.2. Аналіз синергетичного підходу до оцінки загроз на банківську інформацію

Для оцінки поточного стану інформаційної безпеки банку і відповідно оцінки ефективності функціонування КСЗІ в роботі [26] пропонується використовувати синтез чотирьох моделей (рис.3.3).

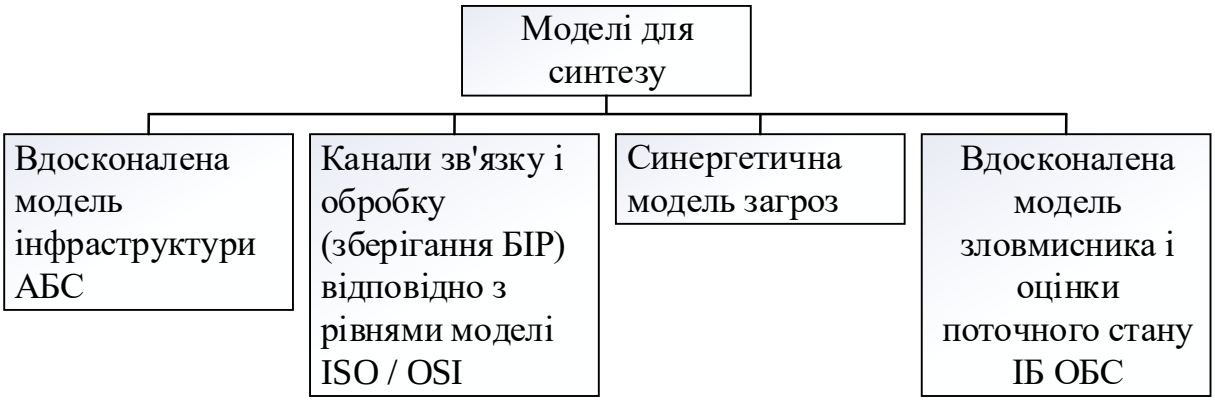


Рисунок 3.3 – Синтез чотирьох моделей для оцінки поточного стану ІБ

Синергетична модель загроз представлена на рис. 3.4:

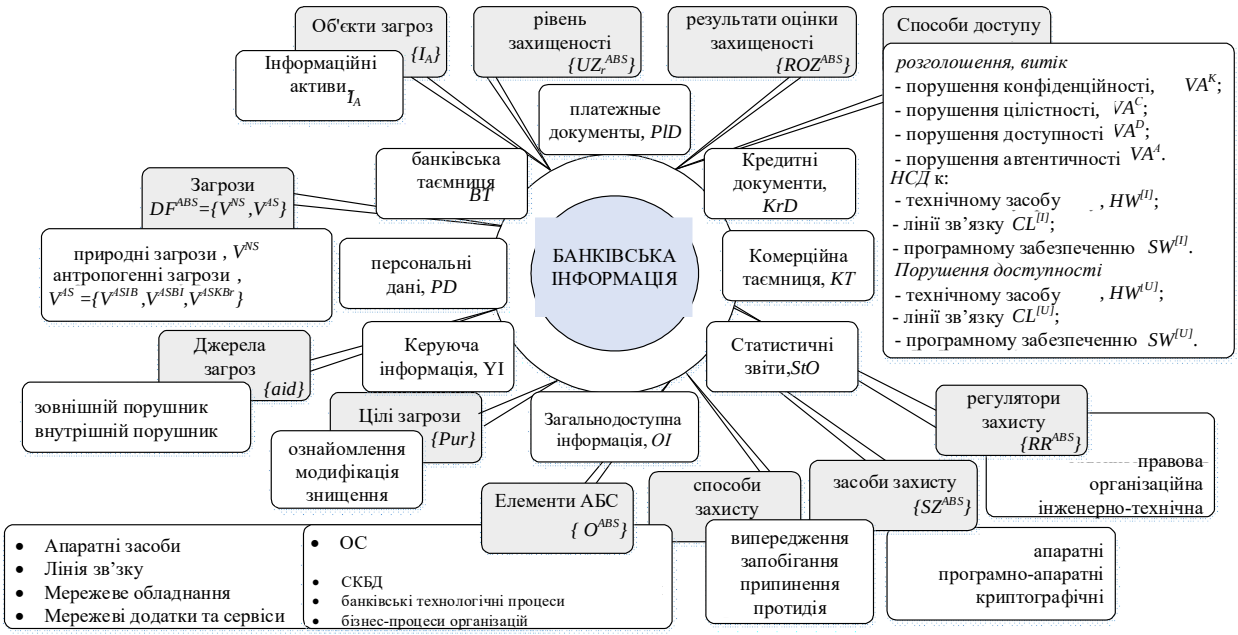


Рисунок 3.4 – Структурна схема концептуальної синергетичної моделі безпеки БІн

Даний підхід дозволяє забезпечити оцінку сучасних загроз з урахуванням їх вдосконалення (синергізму і гібридності) на всі складові безпеки: ІБ, КБ, БІ БІР АБС, визначити критичні точки уразливості в КСЗІ, можливість захисту БІР від загроз наявними криптографічними засобами КСЗІ, відповідність регуляторам з ІБ , і отримати якісну оцінку поточного стану безпеки інфраструктури АБС, і комплексування, оцінити вплив сучасних гібридних загроз на функціонування АБС, можливість проникнення і несанкціонованого доступу до активів БІР, а також функціональну ефективність засобів КСЗІ в АБС.

3.3. Методологічні аспекти синергетичного підходу до оцінки поточного стану інформаційної безпеки банку

На основі методології побудови системи безпеки БІР на рис. 3.5 представлена взаємозв'язок основних моделей, що використовуються в підході оцінки поточного стану інформаційної безпеки банку. Для оцінки

ефективності функціонування комплексної системи захисту БІР в АБС при синергетичному підході необхідно виконати етапи, представлені на рис. 3.6 - 3.8. Представлені кроки на рис. 3.6-3.8 дозволяють "зв'язати" інформаційні активи з погрозами, лініями і елементами.

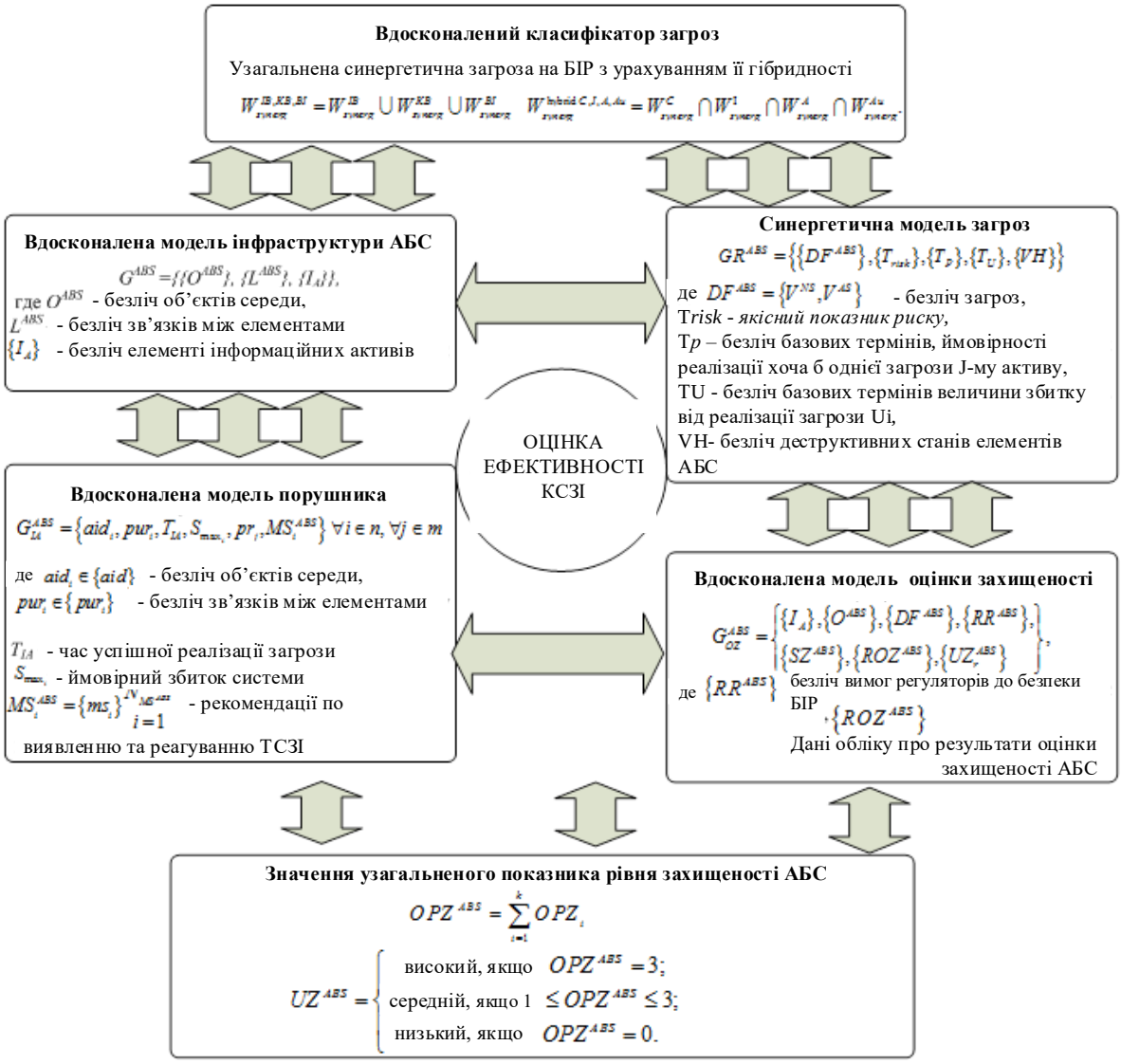


Рисунок 3.5 – Взаємозв'язок моделей в синергетичному підході

Синергетичний підхід до оцінки ефективності функціонування комплексних засобів захисту інформації дозволяє комплексувати загрози, їх вплив на елементи інфраструктури та лінії зв'язку в АБС, а також прогнозувати деструктивні заходи з протидії різним типам зловмисників.

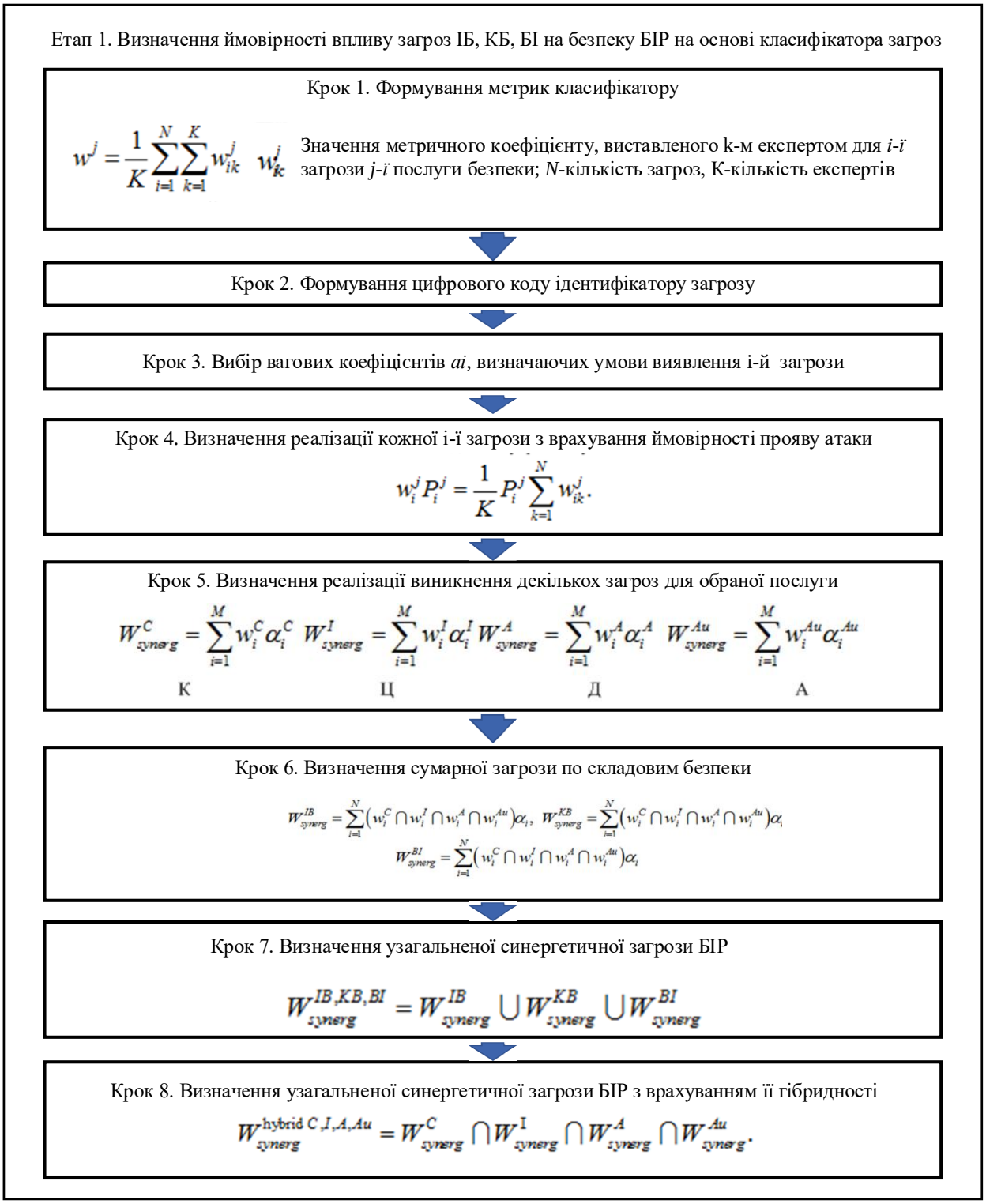


Рисунок 3.6 – Перший етап оцінки ефективності функціонування КСЗІ на основі синергетичного підходу оцінки загроз

Крім цього синергетична модель загроз враховує гібридність і синергізм сучасних загроз, їх вплив як на окремі складові безпеки: ІБ, КБ, БІ, так і на безпеку БІР в цілому (рис.3.7).

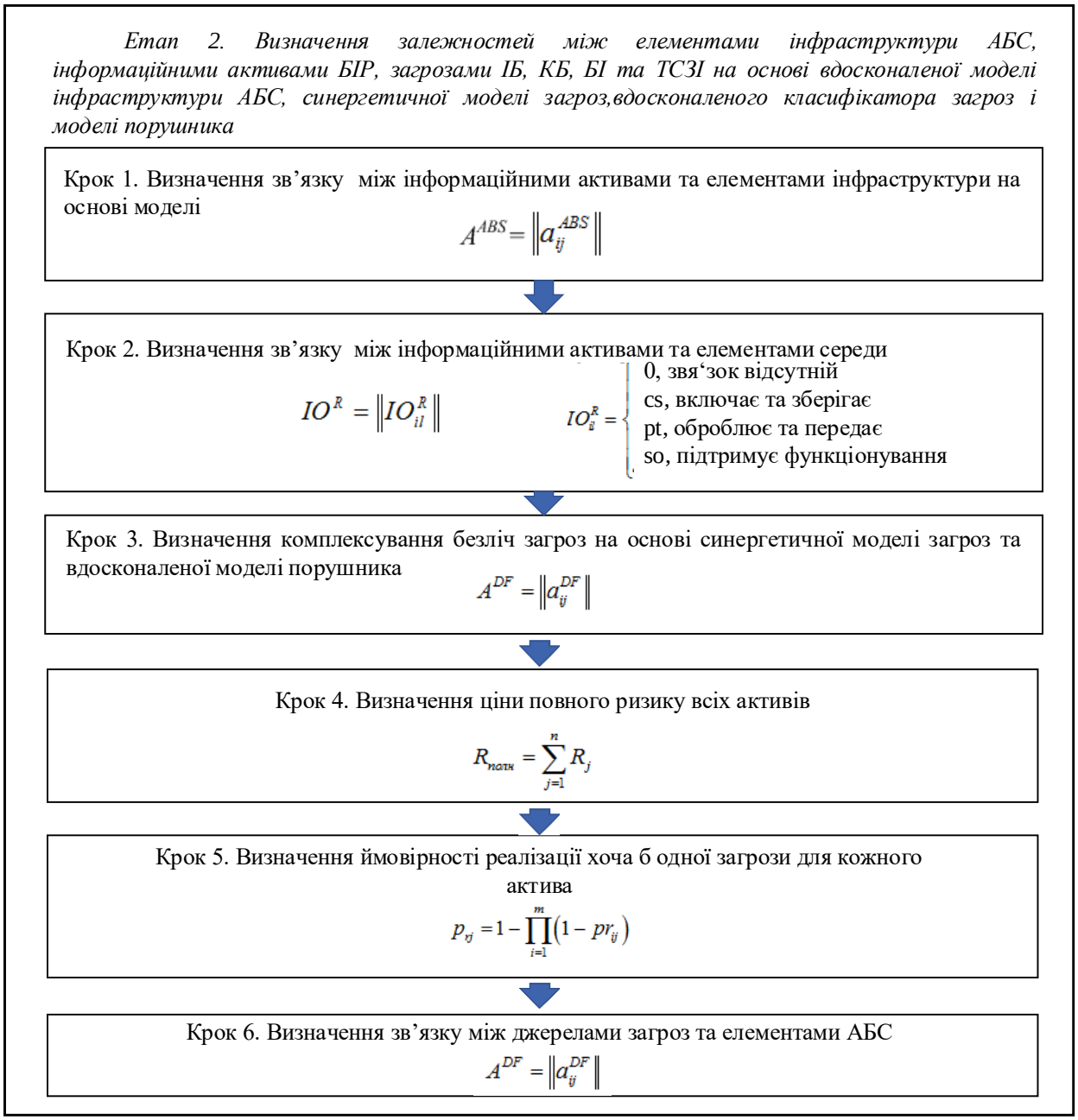


Рисунок 3.7 – Другий етап оцінки ефективності функціонування КСЗІ на основі синергетичного підходу оцінки загроз

$$\|A^{DF}\| = \begin{cases} 1, \text{ якщо для } j\text{-го інформаційного активу існує } i \text{ загроза} \\ 0, \text{ якщо для } j\text{-го інформаційного активу не існує } i \text{ угроза} \end{cases}$$

Кожен механізм захисту БІн в АБС $SZ_i \in \{SZ^{ABS}\}$ характеризується вектором $SZ_i = (T_{SZ}, T_V, C_{SZ})$, де T_{SZ} – тип засобу захисту, T_V – час впровадження, C_{SZ} – вартість. Таким чином, це дозволяє провести дослідження

можливості "перекриття" наявними в КСЗІ технічними засобами забезпечити "протистояння" сучасним загрозам (рис.3.8).

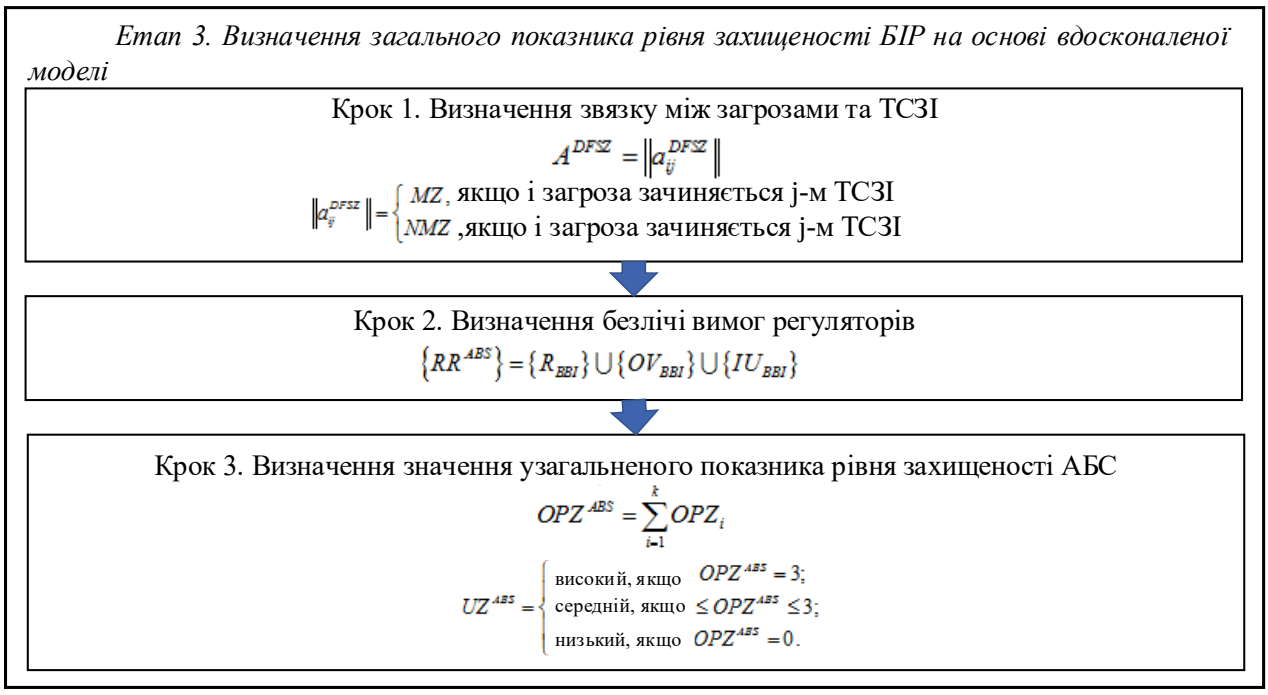


Рисунок 3.8 – Третій етап оцінки ефективності функціонування КСЗІ на основі синергетичного підходу оцінки загроз

Отримана оцінка захищеності БІн дозволяє визначити найбільш цінні інформаційні активи, ефективність використовуваних засобів для їх захисту, а також ступінь відповідності системи ТСЗІ вимогам до захисту і рівнем захищеності регуляторів, виявити найбільш уразливі місця і виробити рекомендації щодо підвищення, в разі необхідності, захищеності АБС ОБС.

3.4 Оцінка ефективності функціонування КСЗІ в умовах гібридності загроз

Представлені на електронному ресурсі URL: http://bdu.fstec.ru/threat загрози (рис. 3.9) дозволяють сформувати множини загроз на БІР і приступити до першого етапу оцінки поточного стану ІБ банку (оцінки ефективності функціонування КСЗІ АБС ОБС) [27].

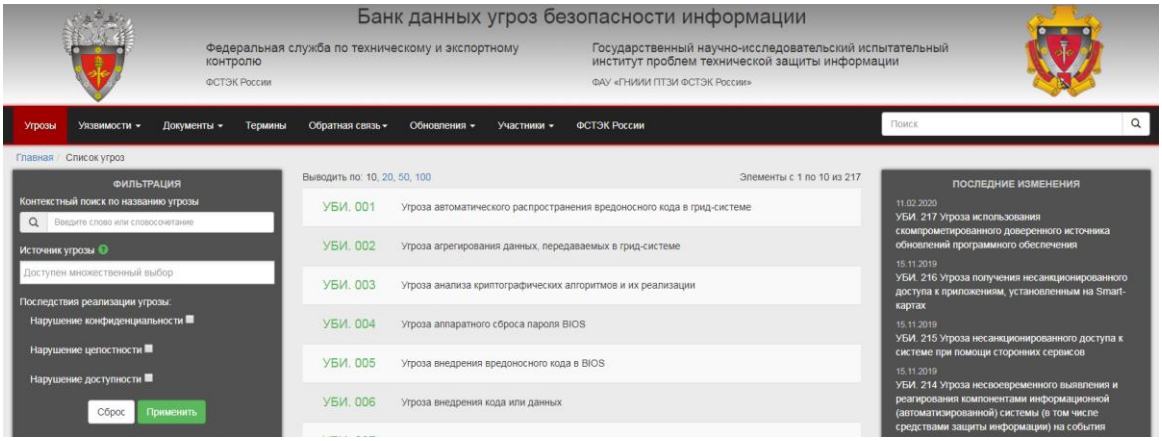


Рисунок 3.9 – Вибір множини загроз з ресурсу "Банк даних загроз безпеки інформації"

Розроблений програмний ресурс експерименту регламентує порядок його організації і проведення (рис. 3.10).

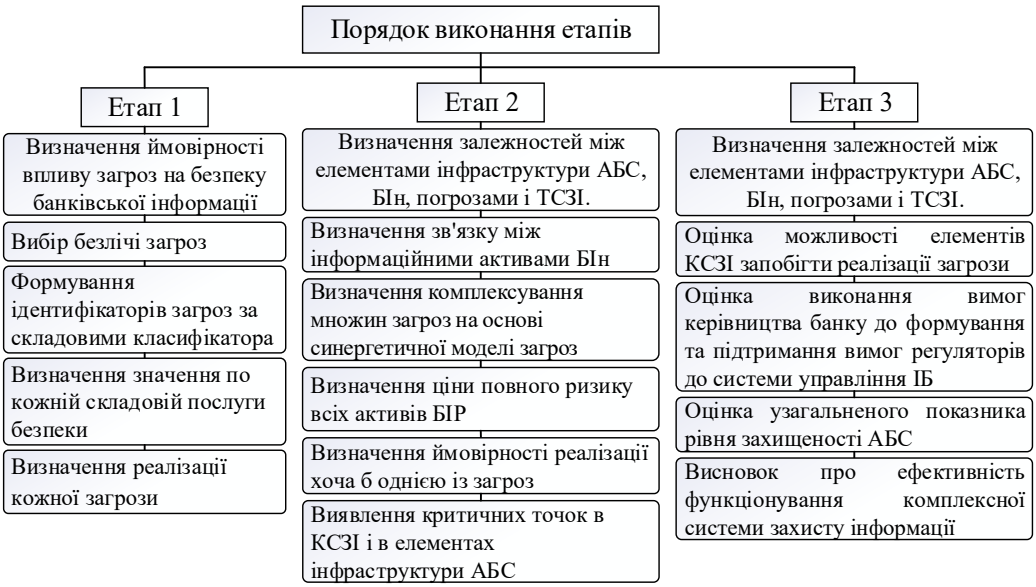


Рисунок 3.10 – Короткий огляд регламенту щодо порядку виконання основних етапів

Етап 1. Визначення ймовірності впливу загроз на безпеку БІн

Результати кроку 1 представлені на рис. 3.9 – в таблиці відображені результати роботи експертів щодо формування метричних даних для класифікатора загроз.

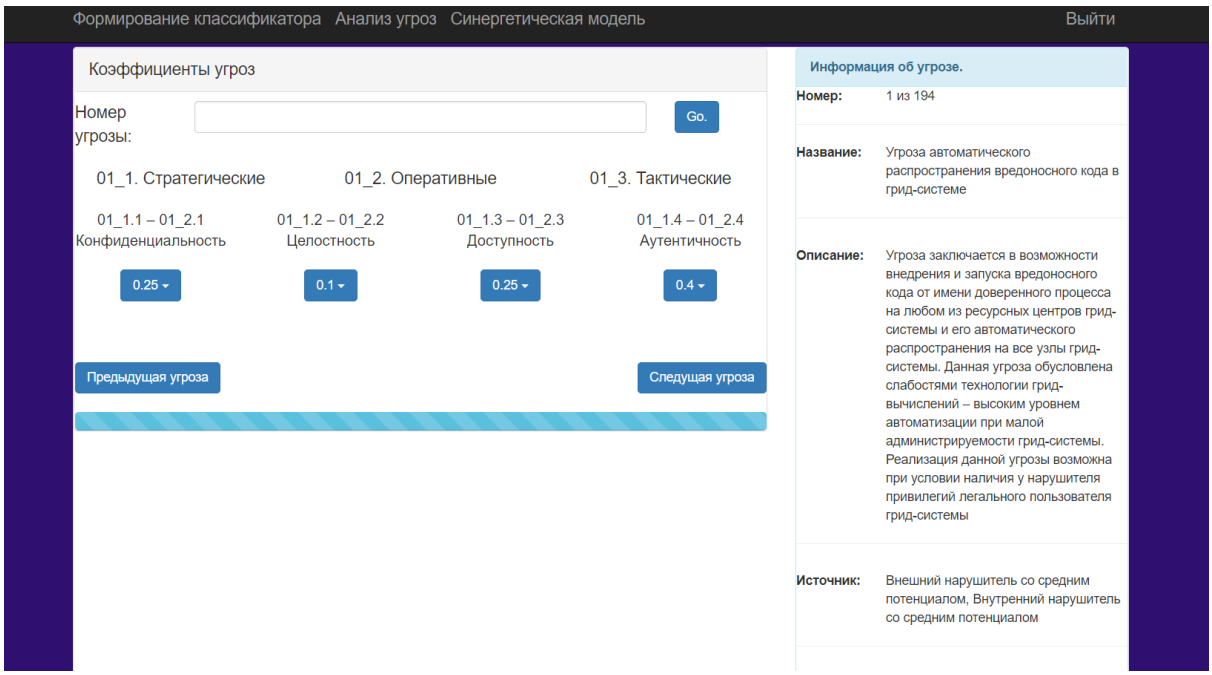


Рисунок 3.11 – Формування метричних коефіцієнтів загроз експертами з ІБ

Крок 2. Формування ідентифікаторів загроз за складовими класифікатора. На даному етапі експерти формують цифрове значення (код) ідентифікатора загрози за відповідними складовими класифікатора. Складовими класифікатора є:

- складова безпеки БІР ОБС: ІБ (01), БІ (02), КБ (03)
- характер напрямків: нормативно-правовий (01), організаційний (02), інженерно-технічний (03)
- основні особливості інформації: конфіденційність (01), цілісність (02), доступність (03), автентичність (04)
- рівні ієрархії інфраструктури АБС: FL - фізичний рівень (01), NL - мережевий рівень (02), OSL - рівень операційних систем (ОС) (03), DBL - рівень систем управління базами даних (04), BL - рівень банківських технологічних додатків і сервісів (05) (рис. 3.12).

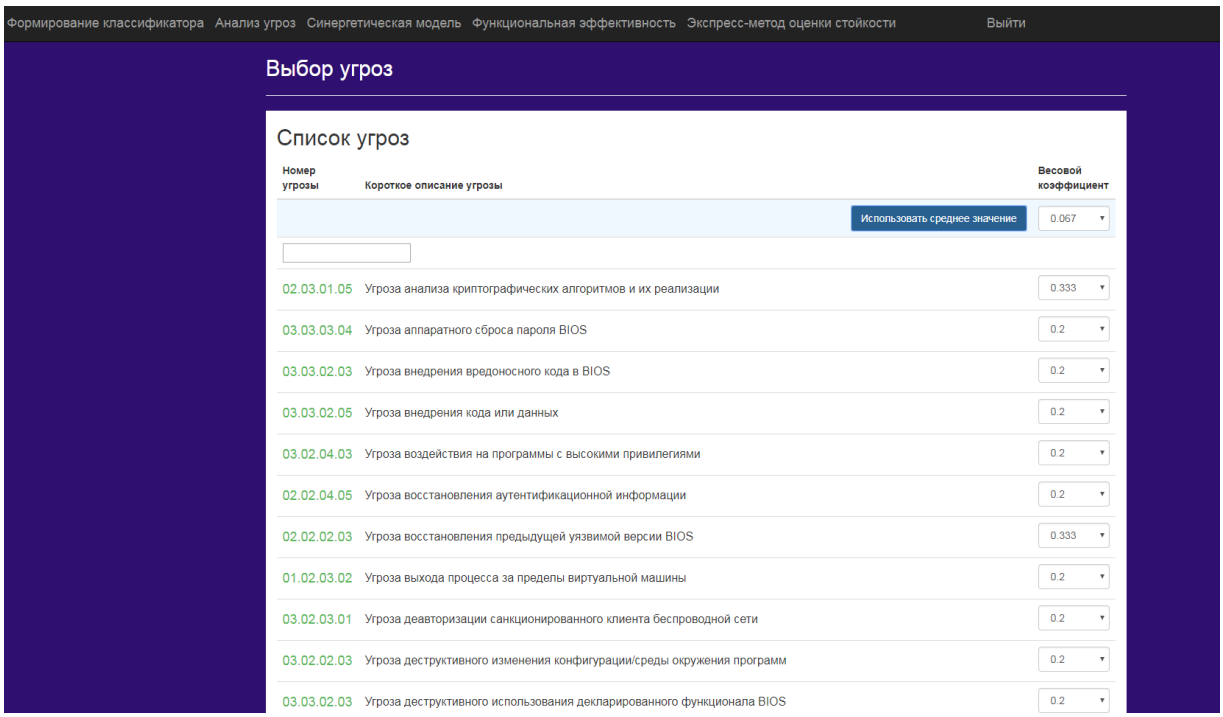


Рисунок 3.12 – Формування класифікатора загроз

На третьому кроці з урахуванням таблиці значень вагових коефіцієнтів αі виникнення і-й загрози експертами визначається значення по кожній складовій послуги безпеки, з ранжируванням отриманого результату (рис. 3.13).

Таблиця 3.1 – Таблиця визначення ймовірності виникнення загроз в залежності від частоти їх прояву

Вагові коефіцієнти α_i	Умови прояви загрози
0,067	загроза проявляється не частіше ніж один раз на 5 років
0,133	загроза проявляється не частіше ніж один раз на рік
0,2	загроза проявляється не частіше одного разу місяць
0,267	загроза проявляється не частіше ніж один раз на тиждень
0,333	загроза проявляється щодня

Статистична обробка результатів роботи експертами усереднюється за кількістю експертів, при цьому за міру узгодженості оцінок роботи експертів приймається дисперсія усередненої їх оцінки.

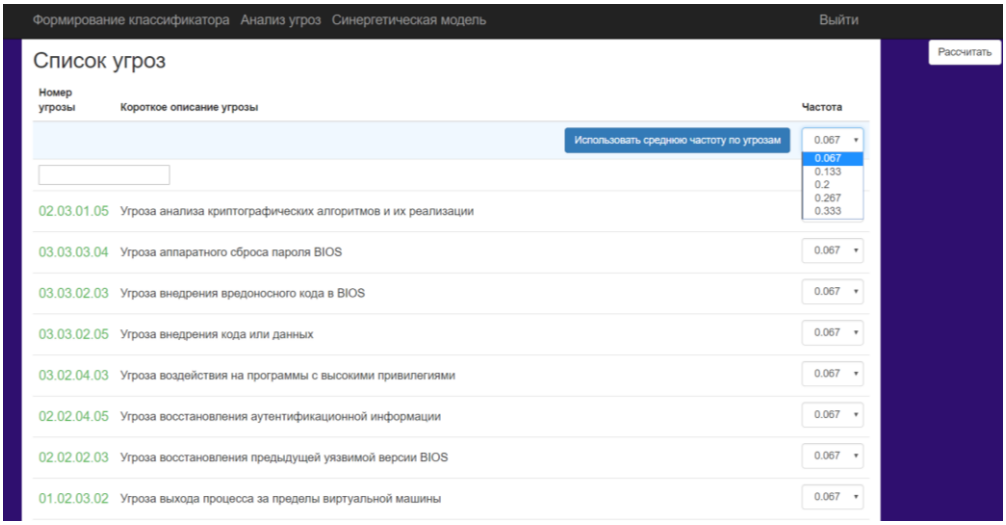


Рисунок 3.13 – Формування вагових коефіцієнтів кожної загрози

Крок 4. Визначається реалізація кожної і-ї загрози з урахуванням ймовірності прояви атаки її виникнення (рис. 3.14).

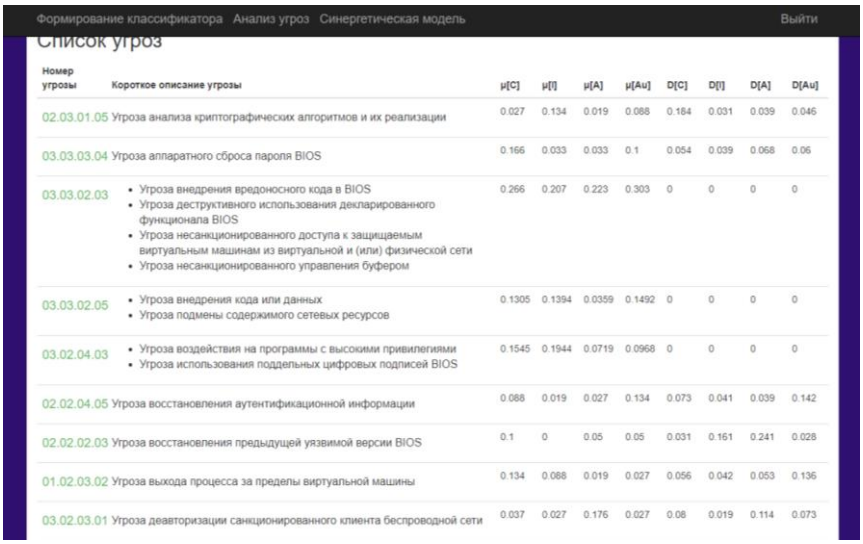


Рисунок 3.14 – Реалізація кожної *і-ї* загрози

Крок 5. Визначення реалізації виникнення декількох загроз для обраної послуги.

Крок.6. Визначення узагальненої синергетичної загрози на БІР

Крок.7. Визначення узагальненої синергетичної загрози на БІР

Крок 8. Визначення узагальненої синергетичної загрози з урахуванням її гібридності.

Результати виконання кроків 5-8 представлені у вигляді таблиці 3.2 (рис. 3.15).

Таблиця 3.2 – Результати оцінки загроз на основі синергетичного підходу

Складові безпеки	Послуги безпеки				
	C, W^{C}_{synerg}	*I*, W^{I}_{synerg}	*A*, W^{A}_{synerg}	*Au*, W^{Au}_{synerg}	Сума
IB, W^{IB}_{synerg}	0.009	0.112	0.108	0.126	0.0000137
KB, W^{KB}_{synerg}	0.142	0.155	0.123	0.047	0.0001272
BI, W^{BI}_{synerg}	0.099	0.061	0.088	0.141	0.0000749
Сума	0.25	0.328	0.319	0.314	
$W^{IB,KB,BI}_{synerg} = W^{IB}_{synerg} \bigcup W^{KB}_{synerg} \bigcup W^{BI}_{synerg}$ = =0,0002+0,0014+0,0007= **0.000216**		$W^{\mathrm{hybrid}\,C,I,A,Au}_{synerg} = W^{\mathrm{C}}_{synerg} \bigcap W^{\mathrm{I}}_{synerg} \bigcap W^{A}_{synerg} \bigcap W^{Au}_{synerg}$ = = 0,471×0,566×0,542×0,53= **0.008214**			

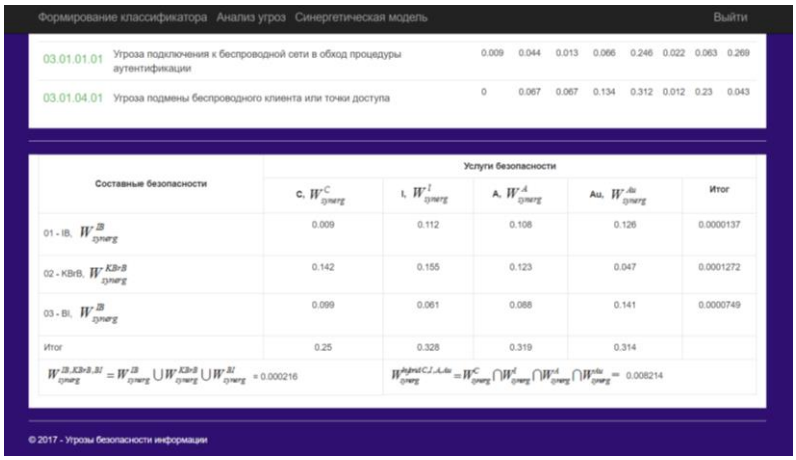


Рисунок 3.15 – Результати дослідження гібридності і синергізму загроз на БІ

Етап 2. Визначення залежностей між елементами інфраструктури АБС, БІн, погрозами і ТСЗІ.

Визначення зв'язку між інформаційними активами БІР $\{I_A\}$ та елементами інфраструктури АБС $A^{ABS} = \left\| a_{ij}^{ABS} \right\|$. Кожен елемент $I_{A_i} \in \{I_A\}$ описується вектором $I_{A_i} = \left(Type, A^C, A^I, A^A, A^{Au}, C_Y\right)$, *Type* – тип інформаційного активу, описується множиною базових значень $Type = \{BT, PID, RrD, KT, StO, Ol, YI, PD\}$, де *BT* –комерційна таємниця; *PID* – платіжні документи; *KrD* – кредитні документи; *KT* – комерційна таємниця; *StO* – статистичні звіти; *Ol* – загальнодоступна інформація; *YI* – керівна інформація; *PD* – персональні дані. Значення A^C – конфіденційність; A^I – цілісність; A^A – доступність; A^{Au} –

автентичність; *СУ* – безперервність – властивості інформації, які необхідно забезпечувати. Вони приймають значення 1 – якщо властивість необхідно, 0 – в іншому випадку (рис. 3.16).

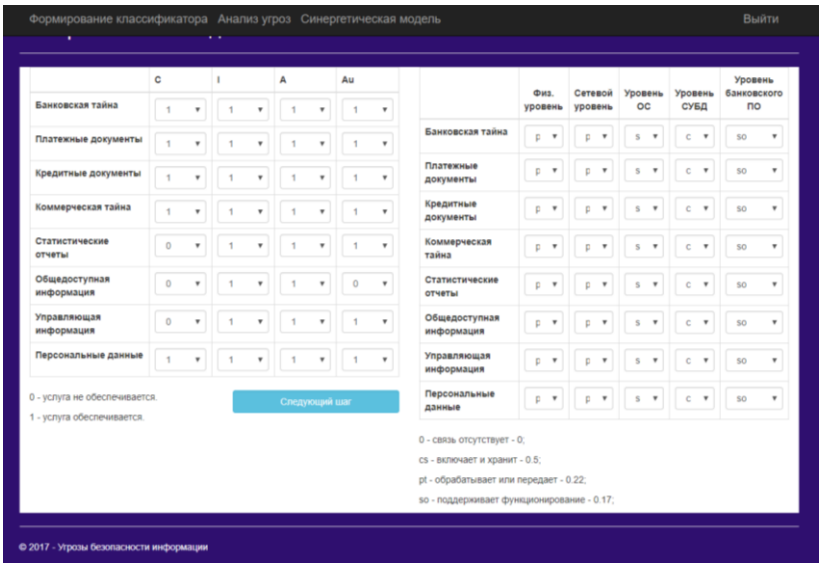


Рисунок 3.16 – Взаємозв'язок між БІР і послугами безпеки (зліва), бін і елементами архітектури АБС (праворуч)

Крок 2. Визначення зв’язку між інформаційними активами $\{I_A\}$ й об’єктами середовища (рис. 3.16, табл. 3.3, 3.4). Кожен елемент $O_l \in \{O^{ABS}\}$ описується вектором $O_l = \{Y^{ABS}, IO\}$, де Y^{ABS} – рівень ієрархії інформаційної структури, яка визначається множиною $Y^{ABS} = \{FL, NL, OSL, DBL, BL\}$, де *FL* – фізичний рівень; *NL* – мережевий рівень; *OSL* – рівень операційних систем (ОС); *DBL* – рівень систем управління базами даних; *BL* – рівень комерціних технологічних застосунків і сервісів [28]. Для визначення типу зв’язку та існуючого відношення I^{OR} між інформаційними активами БІР і об’єктами АБС використовується правило:

$$IO^R = \left\| IO_{il}^R \right\|,$$

де IO_{il}^R – відображає наявність і тип зв’язку між *i*-м інформаційним активом та *l*-м об’єктом середовища АБС. При цьому $\forall i \in \{I_A\}$, а $\forall l \in \{O^{ABS}\}$:

$$IO_{il}^{R} = \begin{cases} 0 \ – \text{ зв'язок відсутній;} \\ cs – \text{включає і зберігає;} \\ pt – \text{обробляє або передає;} \\ so \ – \text{ підтримує функціонування.} \end{cases}.$$

Таблиця 3.3 – Надання послуг інформаційним активам БІР

Назва, I_{A_i}	*C*	*I*	*A*	*Au*
BT	1	1	1	1
PID	1	1	1	1
KrD	1	1	1	1
KT	1	1	1	1
StO	0	1	1	1
Ol	0	1	1	0
YI	0	1	1	1
PD	1	1	1	1

Таблиця 3.4 – Взаємозв’язок інформаційних активів БІР з елементами узагальненої інфраструктури АБС

Назва, I_{A_i}	Фізичний рівень	Мережевий рівень	Рівень ОС	Рівень СУБД	Рівень комерційного ПЗ
BT	*pt*	*pt*	*so*	*cs*	*so*
PID	*pt*	*pt*	*so*	*cs*	*so*
KrD	*pt*	*pt*	*so*	*cs*	*so*
KT	*pt*	*pt*	*so*	*cs*	*so*
StO	*pt*	*pt*	*so*	*cs*	*so*
Ol	*pt*	*pt*	*so*	*cs*	*so*
YI	*pt*	*pt*	*so*	*cs*	*so*
PD	*pt*	*pt*	*so*	*cs*	*so*

Кожному параметру присвоюються вагові категорії за правилом Фішберна, заснованому на тому, що зміна вагових коефіцієнтів критеріїв підкоряється спадній арифметичній прогресії.

При цьому перший критерій (*i = 1*), розташований першим в строго упорядкованому за важливістю ранжируваному ряду критеріїв *i* = 1, 2, ..., *n*, є

найбільш важливим і має найбільший ваговий коефіцієнт. Це правило задається виразом:

$$w_i = \frac{2(N-n+1)}{N(N+1)},$$

де w_i – ваговий коефіцієнт Фішберна;

N – загальна кількість параметрів;

n – порядковий номер параметра;

i – кількість параметрів.

Відповідно до виразу Фішберна маємо [29]:

$$w_1 = \frac{2 \times N}{N(N+1)},\ w_N = \frac{2}{N(N+1)},\ \gamma = \frac{w_1}{w_N} = N,$$

де γ – кратність відмінності вагових коефіцієнтів один від одного.

Таким чином, $cs = 0.5, \quad pt = 0.22, \quad so = 0.17.$

Крок 3. Визначення комплексування множини загроз на основі синергетичної моделі загроз й удосконаленої моделі зловмисника.

Синергетична модель загроз формально описується виразом:

$$GR^{ABS} = \left\{ \left\{ DF^{ABS} \right\}, \left\{ T_{risk} \right\}, \left\{ T_P \right\}, \left\{ T_U \right\}, \left\{ VH \right\} \right\},$$

Удосконалена модель визначена п’ятьма категоріями зловмисника та формально описується виразом:

$$G_{IA}^{ABS} = \left\{ aid_i, pur_i, T_{IA}, S_{\max_i}, pr_j, MS_i^{ABS} \right\} \forall i \in n, \forall j \in m,$$

де aid_i – ідентифікатор зловмисника (категорія зловмисника); pur_i – мета зловмисника; T_{IA} – час успішної реалізації загрози; $S_{\max_i}$ – ймовірнісний збиток системи; pr_j – ймовірність реалізації хоча б однієї загрози j-му активу; MS_i^{ABS} – рекомендації щодо виявлення, реагування ТЗЗІ.

На основі запропонованих моделей здійснюється комплексування множини загроз (рис. 3.17, табл. 3.3):

$$DF^{ABS} = \left\{ V^{NS} \right\} \bigcup \left\{ V^{AS} \right\},$$

де $\{V^{AS}\} = \{V^{ASIB}\} \bigcap \{V^{ASKB}\} \bigcap \{V^{ASBI}\}$, де $\{V^{NS}\}$ – клас природних джерел загроз; $\{V^{AS}\}$ – клас антропогенних загроз, де $\{V^{ASIB}\}$ – множина загроз ІБ; $\{V^{ASKB}\}$ – множина загроз КБ; $\{V^{ASBI}\}$ – множина загроз БІ.

Синергитическая модель.

	Банковская тайна	Платежные документы	Кредитные документы	Коммерческая тайна	Статистические отчеты	Общедоступная информация	Управляющая информация	Персональные данные
02.03.01.05	0.33	0.33	0.33	0.33	0.33	0.22	0.33	0.33
03.03.03.04	0.02	0.02	0.02	0.02	0.02	0	0.02	0.02
03.03.02.03	0.05	0.05	0.05	0.05	0.05	0	0.05	0.05
03.03.02.05	0.02	0.02	0.02	0.02	0.02	0	0.02	0.02
03.02.04.03	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066
02.02.04.05	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066
02.02.02.03	0.332	0.332	0.332	0.332	0.166	0.116	0.166	0.332
01.02.03.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02
03.02.03.01	0.066	0.066	0.066	0.066	0.066	0	0.066	0.066
03.02.02.03	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
03.03.02.03	0.05	0.05	0.05	0.05	0.05	0	0.05	0.05
01.01.03.05	0.088	0.088	0.088	0.088	0.088	0	0.088	0.088
03.03.02.04	0.066	0.066	0.066	0.066	0.066	0	0.066	0.066
03.01.03.02	0.1	0.1	0.1	0.1	0.1	0	0.1	0.1
01.01.03.04	0.05	0.05	0.05	0.05	0.05	0	0.05	0.05
03.03.03.03	0.2	0.2	0.2	0.2	0.2	0	0.2	0.2
02.03.01.02	0.24	0.24	0.24	0.24	0.24	0	0.24	0.24
03.01.03.02	0.267	0.267	0.267	0.267	0.267	0	0.267	0.267
01.01.02.05	0.033	0.033	0.033	0.033	0.033	0	0.033	0.033
03.03.03.03	0.013	0.013	0.013	0.013	0.013	0	0.013	0.013
01.01.03.05	0.133	0.133	0.133	0.133	0.1	0.088	0.1	0.133
03.03.03.01	0.2	0.2	0.2	0.2	0.166	0.1	0.166	0.2
02.03.03.05	0.033	0.033	0.033	0.033	0.033	0	0.033	0.033
03.03.03.05	0.267	0.267	0.267	0.267	0.2	0.112	0.2	0.267
01.01.03.05	0.2	0.2	0.2	0.2	0.166	0.1	0.166	0.2
02.03.02.03	0.2	0.2	0.2	0.2	0.166	0.1	0.166	0.2
01.02.03.03	0.2	0.2	0.2	0.2	0.182	0.116	0.182	0.2
01.02.04.05	0.267	0.267	0.267	0.267	0.179	0.091	0.179	0.267
03.02.03.03	0.2	0.2	0.2	0.2	0.15	0.084	0.15	0.2

Рисунок 3.17 – Ймовірність виникнення *i*-ї загрози на інформаційні активи БІР

Результати визначення ціни повного ризику всіх активів БІР (крок 4-й) наведені в табл. 3.5.

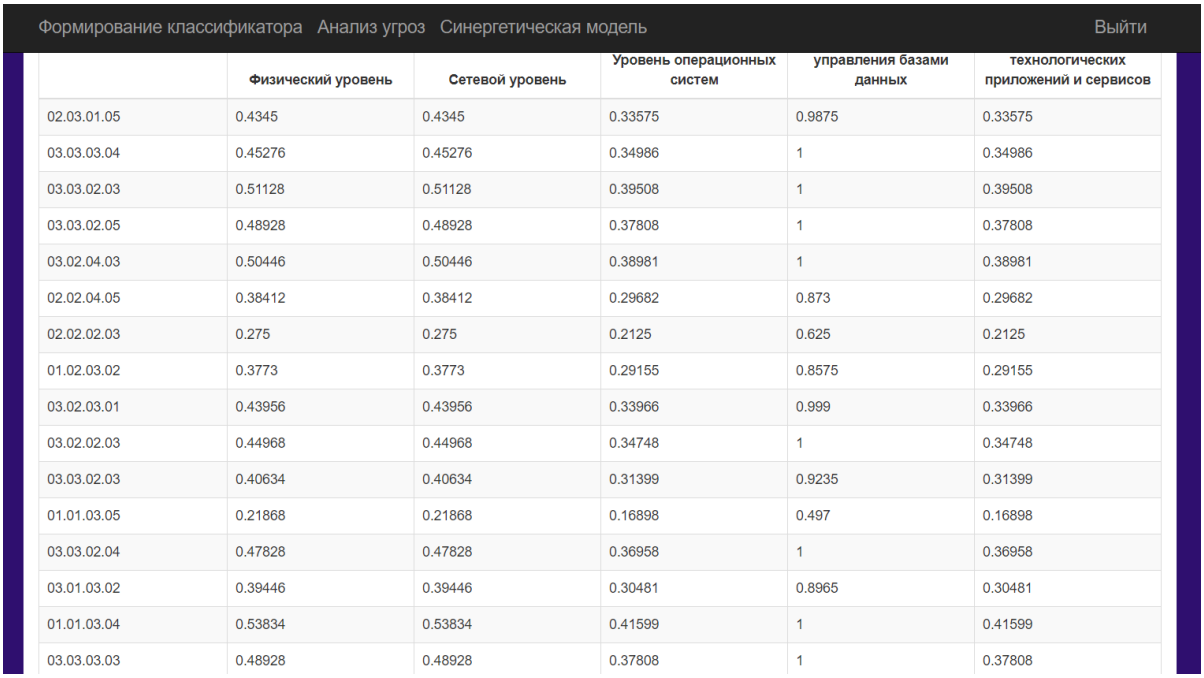
Таблиця 3.5 – Визначення ймовірності реалізації хоча б однієї загрози для кожного активу БІР

ID угрозы	*BT*	*PID*	*KrD*	*KT*	*StO*	*Ol*	*YI*	*PD*
02.03.01.05	0.268	0.268	0.268	0.268	0.241	0.153	0.241	0.268
03.03.03.04	0.332	0.332	0.332	0.332	0.166	0.066	0.166	0.332
03.03.02.03	0.332	0.332	0.332	0.332	0.249	0.166	0.249	0.332
03.03.02.05	0.333	0.333	0.333	0.333	0.223	0.113	0.223	0.333
03.02.04.03	0.332	0.332	0.332	0.332	0.222	0.189	0.222	0.332
02.02.04.05	0.268	0.268	0.268	0.268	0.18	0.046	0.18	0.268
02.02.02.03	0.2	0.2	0.2	0.2	0.1	0.05	0.1	0.2
01.02.03.02	0.268	0.268	0.268	0.268	0.134	0.107	0.134	0.268
03.02.03.01	0.267	0.267	0.267	0.267	0.23	0.203	0.23	0.267
03.02.02.03	0.268	0.268	0.268	0.268	0.241	0.222	0.241	0.268
…	…	…	…	…	…	…	…	…
03.03.02.03	0.267	0.267	0.267	0.267	0.2	0.112	0.2	0.267
01.01.03.05	0.133	0.133	0.133	0.133	0.114	0.101	0.114	0.133
03.03.02.04	0.332	0.332	0.332	0.332	0.199	0.116	0.199	0.332
03.01.03.02	0.267	0.267	0.267	0.267	0.182	0.094	0.182	0.267
01.01.03.04	0.332	0.332	0.332	0.332	0.299	0.189	0.299	0.332
3.01.01.01	0.2	0.2	0.2	0.2	0.186	0.086	0.186	0.2
03.01.04.01	0.132	0.132	0.132	0.132	0.132	0.066	0.132	0.132
03.01.04.05	0.268	0.268	0.268	0.268	0.249	0.115	0.249	0.268
03.01.04.05	0.268	0.268	0.268	0.268	0.228	0.094	0.228	0.268

На п'ятому кроці визначаються ймовірності реалізації хоча б однією із загроз (рис. 3.17).

Результат шостого кроку першого етапу дозволяє визначити, що

дозволяє виявити критичні точки в КСЗІ і в елементах інфраструктури АБС, на рис. 3.18 - відображені у вигляді "1". Таким чином, даний підхід дозволяє представити докази середньостатистичній людині з технічною освітою вразливі місця несанкціонованого доступу до відповідних активів банківської інформації на основі реалізації конкретної загрози.



	Физический уровень	Сетевой уровень	Уровень операционных систем	управления базами данных	технологических приложений и сервисов
02.03.01.05	0.4345	0.4345	0.33575	0.9875	0.33575
03.03.03.04	0.45276	0.45276	0.34986	1	0.34986
03.03.02.03	0.51128	0.51128	0.39508	1	0.39508
03.03.02.05	0.48928	0.48928	0.37808	1	0.37808
03.02.04.03	0.50446	0.50446	0.38981	1	0.38981
02.02.04.05	0.38412	0.38412	0.29682	0.873	0.29682
02.02.02.03	0.275	0.275	0.2125	0.625	0.2125
01.02.03.02	0.3773	0.3773	0.29155	0.8575	0.29155
03.02.03.01	0.43956	0.43956	0.33966	0.999	0.33966
03.02.02.03	0.44968	0.44968	0.34748	1	0.34748
03.03.02.03	0.40634	0.40634	0.31399	0.9235	0.31399
01.01.03.05	0.21868	0.21868	0.16898	0.497	0.16898
03.03.02.04	0.47828	0.47828	0.36958	1	0.36958
03.01.03.02	0.39446	0.39446	0.30481	0.8965	0.30481
01.01.03.04	0.53834	0.53834	0.41599	1	0.41599
03.03.03.03	0.48928	0.48928	0.37808	1	0.37808

Рисунок 3.18 – Виявлення критичних точок в АБС

3.5. Оцінка поточного стану інформаційної безпеки банку

Етап 3. Визначення узагальненого показника рівня захищеності БІР. На першому кроці етапу проводиться оцінка можливості елементів КСЗІ запобігти реалізації загрози за рахунок відповідних програмних (програмно-апаратних засобів КСЗІ). Що дозволяє попередньо оцінити функціональну ефективність КСЗІ.

З урахуванням, що АБС відносяться до критичних кібернетичним інформаційних систем (ККІС) і руйнування (проникнення / реалізація загрози, НСД) "руйнують" цілісність активів БІн, що в свою чергу приводь до руйнування всієї ККІС, можна зробити висновок про оцінку ефективності КСЗІ вже на цьому кроці (рис. 3.19) [30].

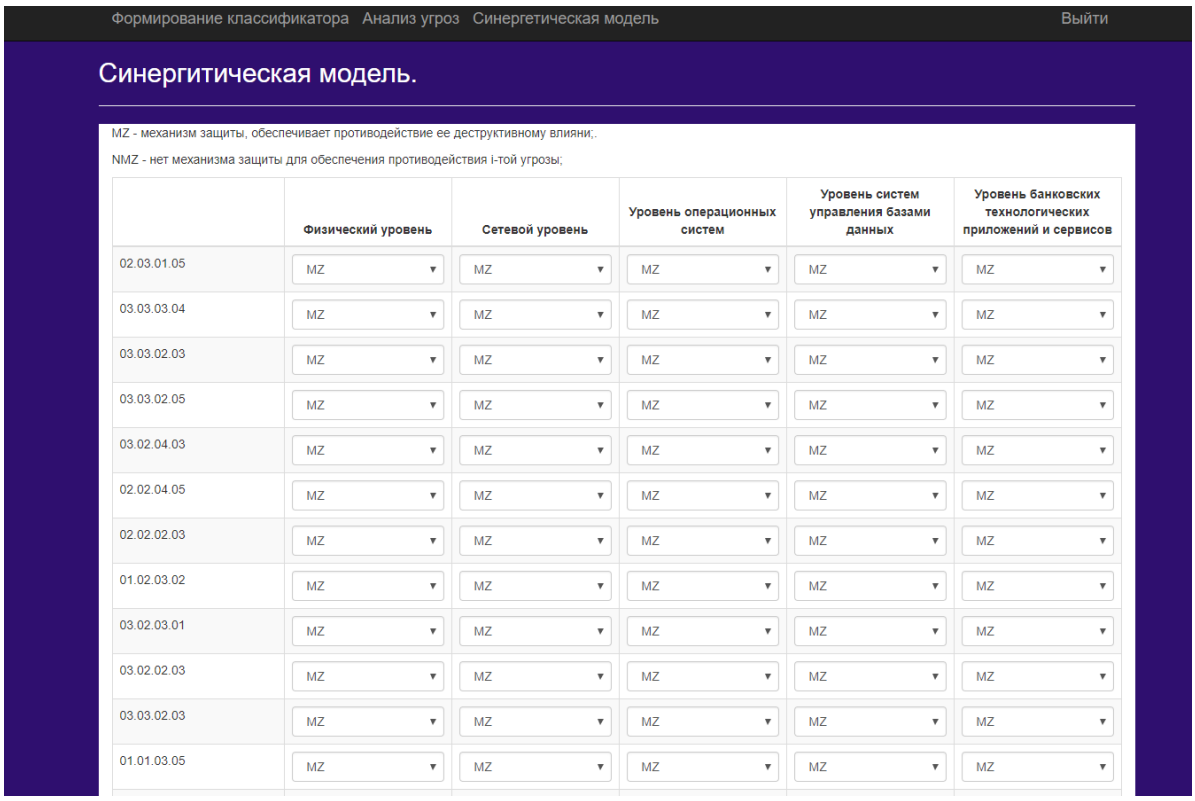


Рисунок 3.19 – Оцінка ефективності деструктивних заходів КСЗІ щодо запобігання реалізації гібридних загроз

На другому кроці на основі вимог [31-33] проводиться оцінка виконання вимог керівництва банку до формування та підтримання (виконання) вимог регуляторів до системи управління інформаційної безпеки. Результати оцінки виконання вимог регуляторів приведені на рис. 3.20.

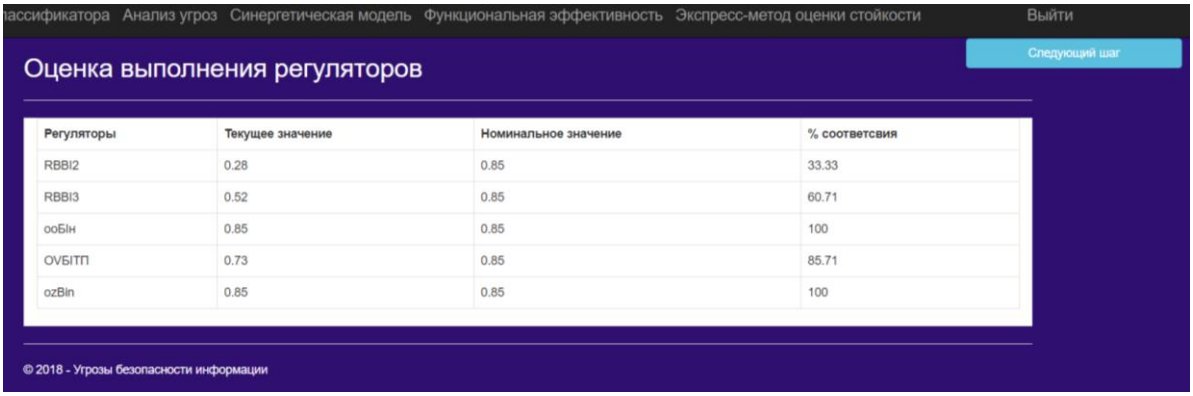


Рисунок 3.20 – Виконання вимог регуляторів до СУ ІБ

На третьому кроці проводиться оцінка узагальненого показника рівня захищеності АБС, який дозволяє оцінити рівень відповідності ТСЗІ, вимогам

регуляторів, і наявність критичних точок в інфраструктурі АБС (рис.3.21).

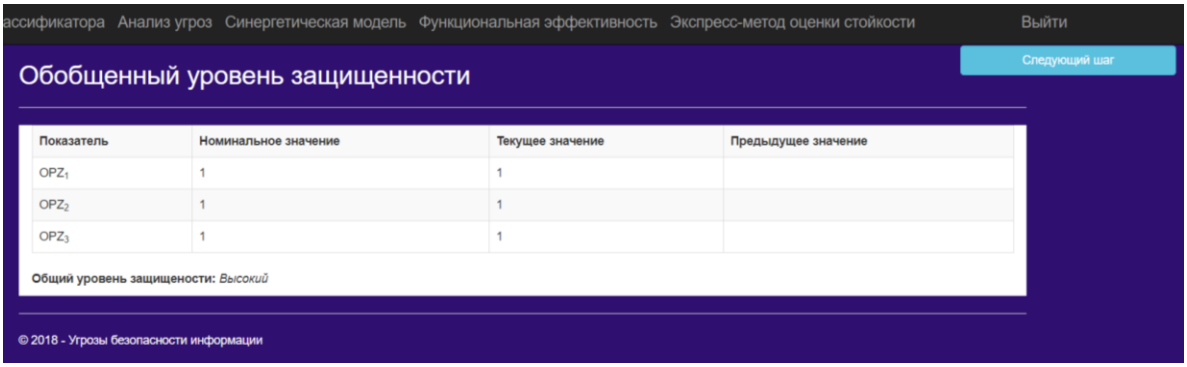


Рисунок 3.21 – Визначення узагальненого показника рівня захищеності банківської інформації в АБС

Висновки до розділу 3

На підставі оцінки рівня захищеності робиться висновок про ефективність функціонування комплексної системи захисту інформації. даний показник прямо пропорційний якісної оцінки поточного стану інформаційної безпеки організації банківського сектора, і є одним з найбільш "впливових" компонентів при прийнятті рішення.

Запропонована концепція дозволяє визначити найбільш ймовірні загрози, спрямовані на порушення безпеки інформаційних ресурсів. Концепція охоплює всі основні напрямки розвитку діяльності банку безпеки банківських інформаційних ресурсів, ґрунтується на синергетичному підході до вибору найбільш ефективних напрямків досягнення цілей безпеки банківських інформаційних ресурсів на кожному з рівнів моделі управління стратегічним управлінням безпеки банківських інформаційних технологій з урахуванням величини ризику на кожному рівні і забезпеченням дієвого контролю за виконанням функцій системи управління інформаційною безпекою установ банківського сектору.

ВИСНОВКИ

У роботі вирішена актуальна науково-прикладна задача створення веб-додатку, який дозволяє на понятійному рівні провести оцінку поточного стану рівня безпеки в організаціях банківського сектору, для чого:

1. Проведений аналіз сучасних загроз на автоматизовані банківські системи показав, що в умовах стрімкого росту обчислювальних можливостей, появи повномасштабних квантових комп'ютерів вони стримляться к комплексуванню з методами соціальної інженерії, що спонукає до появи синергетичного та/або гібридного характеру. Тому слід розглядати їх в комплексі з урахуванням їх впливу на всі складові безпеки: кібербезпеки, інформаційної безпеки, та безпеки інформації.

2. Для забезпечення протидії синергії та гібридності сучасних загроз використовуються програмні (програмно-апаратні) застосунки/засоби виявлення їх дії та/або виявлення відхилення від нормального стану роботи відповідних систем. Серед яких окремо можливо виділити SIEM-системи, які дозволяють автоматизувати процес обробки та управління подіями ІБ від різних джерел.

3. Для оцінки поточного стану рівня безпеки в організаціях банківського сектору, проаналізовані практичні моделі, та визначений підхід на основі синергетичної моделі загроз, яка на відмову від існуючих дозволяє враховувати послуги безпеки, та синергію та гібридність сучасних загроз.

4. Розроблений веб-застосунок, базується на класифікаторі, який як і запропонований підхід враховує синергію та гібридність сучасних загроз на компоненти автоматизованих банківських систем, що дозволяє не тільки оцінити поточний стан рівня безпеки, а також визначити критичні точці в інфраструктурі автоматизованих банківських систем, та можливість технічних засобів безпеки.

За результатами дипломної роботи було опубліковано тези доповіді на міжнародній науково-практичній конференції [34].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Євсєєв С. Оцінка забезпечення безперервності бізнес-процесів в організаціях банківського сектора на основі синергетичного підходу, ч. 2 / С. Євсєєв, Ю. Хохлачова, О. Король. // Сучасна спеціальна техніка. Науково-практичний журнал. – 2017. – №2. – С. 10–17.

2. Грищук Р. В. Основи кібернетичної безпеки: Монографія / Р. В. Грищук, Ю. Г. Даник. – Житомир: ЖНАЕУ, 2016.

3. Олифер В. Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер. – Москва: Горячая линия. Телеком, 2015. – 644 с.

4. Євсєєв С. П. Аналіз захисту в національній системі масових електронних платежів / С. П. Євсєєв. // Інформаційна безпека. – 2014. – №3. – С. 15.

5. Юдін О. К. Інформаційна безпека. Нормативно-правове забезпечення / О. К. Юдін. – Київ: НАУ, 2011. – 639 с.

6. W. Ten, G. Manimaran, and C.-C. Liu, “Cybersecurity for criticalinfrastructures : Attack and defense modeling”, IEEETrans. Syst., Man Cybern. A, vol. 40, no. 4, pp.853 – 865, 2010.

7. Равенков П. В. Защита информации в банке: основные угрозы и борьба с ними [Електронний ресурс] / П. В. Равенков. – 2011. – Режим доступу до ресурсу: http://www.crmdaily.ru/novosti-rynka-crm/568-zashhita-informacii-v-banke-osnovnye-ugrozy-i-borba-s-nimi.html.

8. Security of Internet Banking – A Comparative Study of Security Risks and Legal Protection in Internet Banking in Thailand and Germany [Online].Available: http://www.thailawforum.com/articles/internet-banking-thailand.html. Acessed on: Des. 09, 2017.

9. Positive Technologies Network Attack Discovery. Описание продукта. [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.ptsecurity.com/upload/corporate/ru-ru/products/nad/PT-NAD-Data-Sheet-rus.pdf.

10. GARTNER MAGIC QUADRANT (MQ) FOR ENDPOINT PROTECTION PLATFORMS (EPP) [Електронний ресурс]. – 2019. – Режим

доступу до ресурсу: https://www.crowdstrike.com/resources/reports/gartner-magic-quadrant-endpoint-protection-platforms-2019/.

11. Яковлєв В. В. Інформаційна безпека та захист інформації в корпоративних мережах / В. В. Яковлєв, А. А. Корнієнко., 2002. – 328 с.

12. Романець Ю. В. Захист інформації в комп’ютерних системах і мережах / Ю. В. Романець, П. А. Тимофєєв, В. Ф. Шаньгина. – 2001: Радио и связь, 2001. – 376 с.

13. Кирилов В. А. Система збору та кореляції подій (SIEM) як ядро системи інформаційної безпеки / В. А. Кирилов. // Вісник технологічного університету. – 2016. – №13. – С. 135.

14. Коломієць М. В. Методика візуалізації топології комп'ютерної мережі для моніторингу безпеки / М. В. Коломієць, А. А. Чечулін, І. В. Котенко. – Санкт-Петербург: Санкт-петербурзький інститут інформатики та автоматизації РАН, 2016. – 807 с.

15. Федорченко А. В. Кореляція інформації в системах на основі графа зв'язків типів подій / А. В. Федорченко, І. В. Котенко. – Санкт-Петербург: Університет ІТМО, 2018. – 67 с.

16. Hryshchuk R., Construction methodology of information security system of banking information in automated banking systems : monograph / R. Hryshchuk, S. Yevseiev, A.Shmatko //– Vienna.: Premier Publishing s. r. o., 2018. – 284 p.

17. Анікін І. В. Технологія інтелектуального аналізу даних для виявлення внутрішніх порушників / І. В. Анікін. // Науково-технічні відомості СПбДПУ. – 2010. – №6. – С. 117.

18. Венбо М. Сучасна криптографія: теорія і практика / Мао Венбо. – Київ: Видавничий дім «Вільямс», 2005. – 768 с.

19. Бучик С. С. Методика експертного оцінювання функціональних профілів загроза державних інформаційних ресурсів / С. С. Бучик. // Відкриті інформаційні технології. – 2015. – №70. – С. 271–280.

20. Milov O.V. Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems / Milov O., Voitko A., Husarova I.,

Domaskin O., Ivanchenko E., Ivanchenko I., Korol O., Kots H, Opirskyy I., Fraze-Frazenko O.// Eastern-European Journal of Enterprise Technologies, 2019, v.9, N 2, pp. 56-68.

21. Домарєв Д. Методика оцінювання захищеності інформаційних систем за допомогою СУІБ “Матриця” / Д. Домарєв, В. Домарєв, С. Прокопенко. // Захист інформації. – 2013. – №1. – С. 80–86.

22. Бучик С. С. Методологія аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів / С. С. Бучик. // Захист інформації. – 2016. – №1. – С. 81–89.

23. Евсеев С. П. Синергетическая модель оценки безопасности банковской информации / С. П. Евсеев. // Науково-технічний журнал “Інформаційна безпека”. – 2016. – №4. – С. 104–118.

24. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень / Р. В. Грищук. – Житомир: Рута, 2010.

25. Аткіна В. С. Модель захищеності організацій банківської системи Російської Федерації / В. С. Аткіна. // Известия ПФУ. – 2013. – №12. – С. 187–193.

26. Кузнецов А. В. Спосіб визначення реєстрованих подій / А. В. Кузнецов, С. В. Ненашев. // Питання кібербезпеки. – 2015. – №13. – С. 23–25.

27. Банк даних загроз безпеки інформації ФСТЕК Росії [Електронний ресурс] – Режим доступу до ресурсу: https://bdu.fstec.ru/vul/.

28. Керівний документ. Безпека інформаційних технологій. Загальна методологія оцінки безпеки інформаційних технологій [Електронний ресурс]. – 2002. – Режим доступу до ресурсу: http://fstec.ru/component/attachments/download/293.

29. Шнайер Б. Генерация случайных и псевдослучайных последовательностей // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C / Б. Шнайер. – Москва: Триумф, 2002. – 816 с.

30. Домарев В. В. Безпека інформаційних технологій. Методологія створення систем захисту / В. В. Домарев, Р. В. Климчук., 2013. – 688 с.

31. РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» [Електронний ресурс]. – 2009. – Режим доступу до ресурсу: www.cbr.ru/credit/gubzi_docs/st22_09.pdf.

32. Дослідження атак типу «Міжсайтовий підробка запитів» / А. В.Барабанов, А. И. Лавров, А. С. Марков, И. А. Полотнянщиков. // Питання кібербезпеки. – 2016. – №5. – С. 43–50.

33. Анципов А. В. Методика оцінки надійности програмних засобів / А. В. Анципов, В. В. Бахтізін. // Білоруський державний університет інформатики і радіоелектроніки. – 2010. – №4. – С. 48–53.

34. Макаренко А. О. Аналіз оцінки поточного стану інформаційної безпеки на основі SIEM-систем / А. О. Макаренко, С. П. Євсеев, А. А. Юрченко. // Інформаційна безпека та інформаційні технології. – 2020. – С. 13–14.