Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: *" Аналіз методик оцінки ризиків інформаційної безпеки у банківських системах "*

Виконав: студент

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)

Назарук О.Ю.
підпис (прізвище та ініціали)

Керівник *Максимчук О.О.*
підпис (прізвище та ініціали)

Нормоконтроль *Лобур Т.Б.*
підпис (прізвище та ініціали)

Завідувач кафедри *Загородна Н.В.*
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2022

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Назаруку Олександру Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз методик оцінки ризиків інформаційної безпеки у банківських системах

Керівник роботи Максимчук О.О., асистент каф. КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «23» 03 2022 року № 4/7-178

2. Термін подання студентом завершеної роботи 17.06.2022

3. Вихідні дані до роботи

4. Зміст роботи (перелік питань, які потрібно розробити)

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Пулька Ч.В., проф. кафедри МТ		

7. Дата видачі завдання 16.02.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.02 – 19.02	*Виконано*
2.	Аналіз, формалізація завдання методик оцінок ризиків	20.02 – 27.02	*Виконано*
3.	Опрацювання джерел в галузі дослідження	28.02 – 16.03	*Виконано*
4.	Розроблення програмного коду	17.03 – 20.03	*Виконано*
5.	Проведення експериментальних досліджень	20.03-05.04	*Виконано*
6.	Оформлення розділу «Аналіз системи управління безпекою банківської інформації»	06.03 – 17.04	*Виконано*
7.	Оформлення розділу «Аналіз основних загроз, методів виявлення аномалій і методик оцінки ризику»	18.04 – 29.04	*Виконано*
8.	Оформлення розділу «Моделювання процесу кібератаки»	30.04 – 13.05	*Виконано*
9.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи хорони праці»	14.05 – 21.05	*Виконано*
10.	Оформлення кваліфікаційної роботи	22.05 – 05.06	*Виконано*
11.	Нормоконтроль	06.06 – 12.06	*Виконано*
12.	Перевірка на плагіат	10.06 – 15.06	*Виконано*
13.	Попередній захист кваліфікаційної роботи	16.06 – 19.06	*Виконано*
14.	Захист кваліфікаційної роботи	24.06.2022	

Студент _____ *Назарук О.Ю.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Максимчук О.О.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аналіз методик оцінки ризиків інформаційної безпеки у банківських системах // Назарук Олександр Юрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем та програмної інженерії, кафедра кібербезпеки, група СБс–42 // Тернопіль, 2022 // С. – , рис. – , табл. – , слайдів – , бібліогр. – .

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, НСМЕП, БАНКІВСЬКА СИСТЕМА, МЕТОД ОЦІНКИ РИЗИКІВ, КЛАСИФІКАТОР ЗАГРОЗ.

Об'єктом дослідження є процес менеджменту управління безперервної роботи інфраструктури автоматизованої банківської системи.

Предметом дослідження є методики оцінки захищеності банківської інформації.

Метою роботи є дослідження відхилень від нормальної роботи та/або аномальної роботи щодо оцінки захисту банківської інформації (банківських інформаційних ресурсів), що дозволяє створювати правильний контур безпеки безперервності бізнес процесів від сучасних цільових атак.

Розглянуто законодавчі акти у сфері захисту банківських транзакцій в національній системі масових електронних платежів (НСМЕП). Проведений аналіз основних вимог стандартів до формування та розгортання системи управління інформаційною безпекою. Проведений аналіз загроз на складові безпеки: кібербезпеку, інформаційну безпеку та безпеку інформації, що дозволяє формувати синергічну модель загроз та створювати класифікатор загроз в автоматизованих банківських системах.

Результати можуть бути впроваджені в системи контролю за відхиленням від нормальної роботи автоматизованих банківських систем, а також систем критичного призначення.

ANNOTATION

Analysis of techniques of information safety risks assessment in banking systems // Nazaruk Oleksandr Yuriiovych // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and software engineering, Department of Cybersecurity // Ternopil, 2022 // P. - 53, Fig.-26, Table - 2, Slides - 13, References - 39.

Keywords: INFORMATION SECURITY, NSMEP, BANKING SYSTEM, RISK ASSESSMENT METHOD, THREATS CLASSIFIER.

The object of research is the process of managing the continuous operation of the infrastructure of an automated banking system.

The subject of the study is the methods for assessing the security of banking information.

The aim of the work is to study deviations from normal operation and / or abnormal work to assess the protection of banking information (banking information resources), which allows you to create the correct security loop for business continuity from modern targeted attacks.

Legislative acts in the field of protection of banking transactions in the national system of mass electronic payments (NSMEP) are considered. The analysis of the main requirements of the standards for the formation and deployment of an information security management system was carried out. An analysis of threats into security components was carried out: cybersecurity, information security and information, which makes it possible to form a synergistic threat model and create a threat classifier in automated banking systems.

The results can be implemented in systems for monitoring deviations from the normal operation of automated banking systems, as well as systems for critical purposes.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

НСМЕП – національна система масових електронних платежів.

СЗІ – система захисту інформації.

КСЗІ – комплексна система захисту інформації.

АБС – автоматизована банківська система.

АКС – автоматизована карткова система.

СУКП – система управління критичного застосування.

СУІБ – система управління інформаційною безпекою.

SIEM – (Security information and event management, “управління подіями та інформацією про безпеку”) – клас програмних продуктів, призначених для збору та аналізу інформації про події безпеки.

ICS – information and communication systems, інформаційно-комунікаційні системи.

CPS – cyberphysical systems, кіберфізичні системи.

CCIS –critical cybernetic information systems, інформаційно-критичні кібернетичні системи.

ІБ – інформаційна безпека.

КБ – кібербезпека.

БІ – безпека інформації.

БІР – банківські інформаційні ресурси.

БІн – банківська інформація.

ВСТУП

Розвиток соціуму на початку XXI століття характеризується переходом від інформаційного суспільства до високотехнологічного, що забезпечує перенасиченість інформаційними та комунікаційними технологіями, розвиток глобалізаційних процесів в економіці, динаміку інформатизації сфери зв'язку, енергетики, транспорту, систем видобутку та зберігання газу і нафти, банківської системи, оборонної та національної безпеки, структури забезпечення роботи центральних органів влади, перехід на методи електронного документообігу [1–3]. Інформаційні процеси, які відбуваються в світі, на перший план висувають найважливіше завдання забезпечення інформацйної безпеки. Розвиток Інтернету та інших інформаційно-комунікаційних технологій створює нові загрози і форми міжнародних конфліктів, включаючи інформаційні війни, протиборства в мережі, хакерські атаки і т.п. Розвиток інформаційно-телекомунікаційних мереж та комп'ютерних технологій дають можливості суспільству, використовувати новий вид злочинів – кіберзлочинність [4; 6].

В умовах появи повномасштабного квантового комп'ютера ставиться під сумнів стійкість практично всіх алгоритмів симетричної та несиметричної криптографії, а бурхливе зростання обчислювальних ресурсів IT, і технологій "G" сприяє збільшенню зростання атак на інформаційно-комунікаційні (ICS) і кіберфізичні системи (CPS), які є ядром сучасних інформаційно-критичних кібернетичних систем (CCIS). В таких умовах першочерговим завданням підтримки необхідного рівня безпеки є класифікація сучасних загроз, які комплексируются з методами соціальної інженерії, і набувають ознак синергії і гибридности. У роботі розглядається синергетична модель загроз на ICS/CPS, яка враховує спрямованість загроз на синергію і гибридность та вплив на складові безпеки: інформаційну безпеку (ІБ), кібербезпеку (КБ), безпеку інформації (БІ). Такий підхід дозволяє використовувати, запропонований в [37] уніфікований класифікатор загроз кіберфізичних систем, забезпечити формування множин критичних загроз, критичних точок в елементах

інфраструктури ICS/CPS, на основі мінімальних обчислювальних, людських, і економічних витрат. Для запобігання або забезпечення контуру безпеки в кіберфізичних процесах для проведення аналізу відхилень від нормальної роботи та/або злому системи необхідно вирішення уніфікованого підходу до побудови класифікації загроз з урахуванням їх синергізму та гібридності.

1 АНАЛІЗ СИСТЕМИ УПРАВЛІННЯ БЕЗПЕКОЮ БАНКІВСЬКОЇ ІНФОРМАЦІЇ У АВТОМАТИЗОВАНИХ БАНКІВСЬКИХ СИСТЕМАХ

1.1 Аналіз основних законодавчих актів у сфері захисту банківських транзакцій в автоматизованих банківських системах

Враховуючи розвиток науки і техніки в останні десять років, також інтенсивне застосування високотехнологічних розробок в банківській сфері сутність і зміст категорії БІР під котрими в роботі є “банківська інформація” (БІн) безперечно змінилась. На сьогоднішній день, БІР є основна компонента існуючих АБС. З вище наведеногоо і спираючись на [20,22, 27, 37], можна сказати, що під БІР в широкому сенсі розуміють сукупність відомостей, які пов’язані із Статутними документами та Керівництвом банківських установ, організаційно-правовою формою банківських установ, теперішнім виглядом банківської установи і її працівників, формами і видами банківського обслуговування, кількістю клієнтів і їх складом, операціями з клієнтськими рахунками, наявністю кореспондентських застосунків і технічним забезпеченням банку. Враховуючи тлумачення категорії “банківські інформаційні ресурси” чи “банківська інформація” маючи на меті подальше її коректне застосування пропонують ознакову класифікація БІР (БІн) (рис. 1.1).

Рисунок 1.1 – Ознакова класифікація БІР

На рис.1.1 явно видно перевагу ознакової класифікації БІР. Вона розгортає основну суть категорії. Наприклад, по видах банківська інформація є організаційною, технологічною або параметричною.

Банківська інформація являється інформацією, котра відображає характер зв'язків банку із клієнтами.

Під терміном "технологічна банківська інформація" розуміємо дані, які описують і пояснюють принципи банківського управління, під час якого відбуваються всі види банківської діяльньності та інформація, що застосовується в банківських системах захисту новітніх високотехнологічних розробок.

Термін "параметрична банківська інформація" означає інформацію, яка описує показники кількості. Ці дані показують капітал діючого банку, а так як, кожний банк повинен мати кредитний портфель, то дані цього показника, показують величину цього портфеля, в той момент колм здійснюються різного роду діяльність банку. Важливою перевагою нашої класифікації є проявляння новостворених ознак, котрі характеризують аспекти категорії банківської інформації в даній класифікації є можливість розширення множини ознак.

Із даної класифікації випливає висновок, що в підсистемах АБС Банку циркулюють БІР різного рівня конфіденційності від незакритої інформації, до відомостей, які мають інформацію з обмеженим доступом. У документообігу АБС банку також присутні: платіжні доручення та інші розрахунково-грошові звіти, документи, відомості особових рахунків, узагальнена інформація та інші конфіденційні документи і т.д., котрі також можуть відноситисяі до поняття БІР.

Отже, в найзагальнішому виді під банківськими інформаційними ресурсами (банківською інформацією) є інформація, яка виникає під банківської діяльності. Це відомості які характеризують банк, фінансовий стан, надійність і виконання законодавства.

Дану інформацію можна взяти зі статуту банку, його ліцензій, бухгалтерських балансів та іншої документації. Ця вся інформація є дуже

важливими характеристиками не тільки самого банку, але і осіб, з котрими банк знаходиться в правовідносинах. Наприклад БІР здатна показати інформацію про існування рахунків або вклади, а також про будь-які банківські операції, пов’язані з ними.

Всі діючі основні нормативні акти, що регулюють вище описані процеси державного рівня в зібрані у вигляді структурованої схеми (рис. 1.2).

Рисунок 1.2 – Чинна нормативна база діяльності АБС в Україні

Проведений аналіз показав, що автоматизовані банківські системи відносяться до об’єктів критичної інфраструктури, що дозволяють створювати зловмисникам цільові атаки на організації банківського сектору. АБС можливо розглядати як синтез між класичними комп’ютерними мережами, так і кіберфізичними мережами з елементами Інтернет-речей. На рис. 1.3 наведена структурна модель такого синтезу.

Такий підхід дозволяє стверджувати про необхідність формування системи захисту інформації, яка не тільки забезпечує протидію сучасним загрозам, а також дозволяє сформувати профілі безпеки. А також формувати

нові підходи щодо класифікації сучасних загроз за всіма складовими безпеки: кібербезпеки, безпеки інформації та інформаційної безпеки.

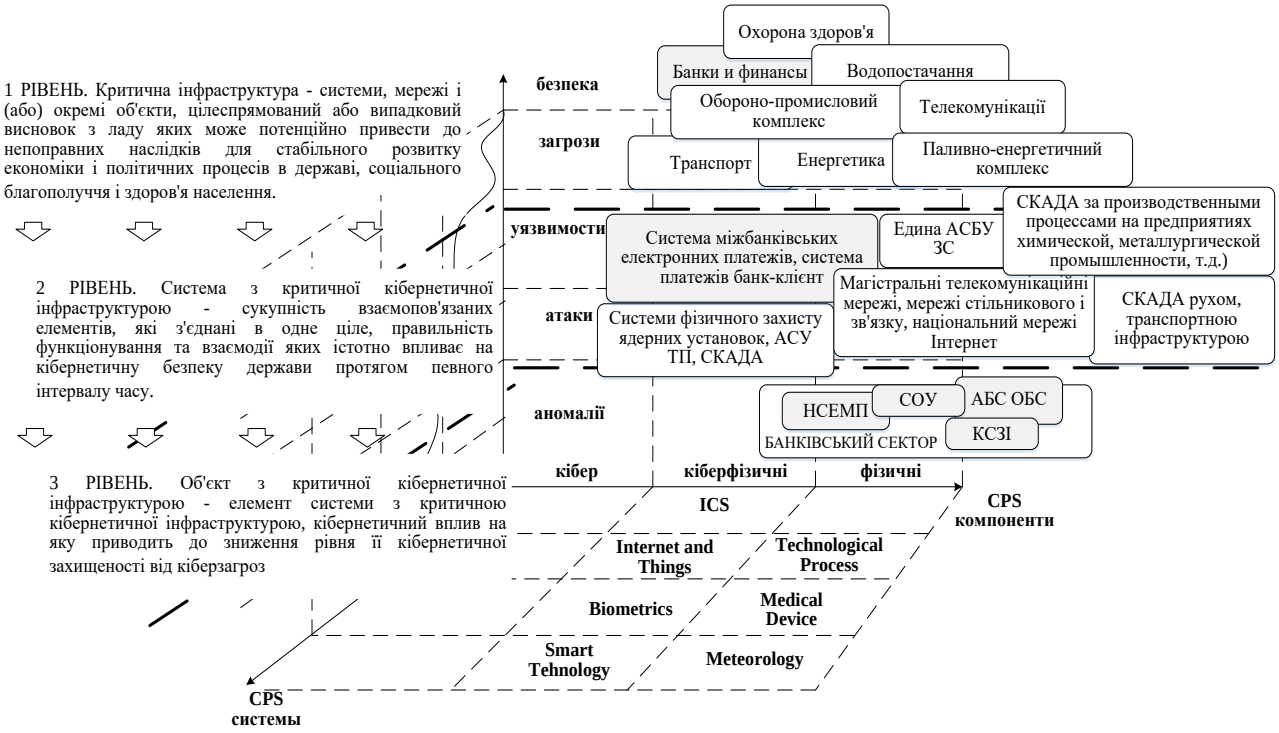


Рисунок 1.3 – Взаємозв’язок ІККС з CPS

Для формування складових класифікатора, а також забезпечення об’єктивної моделі загроз, яка дозволяє враховувати ознаки синергізму – вплив загроз на всі послуги безпеки за окремою складовою, та гібридність – вплив загроз на одну послугу за всіма складовими безпеки.

1.2 Загальна характеристика НСМЕП

Як відомо [14], наведені дані АБС, можна реалізувати шляхом впровадження технологічних засобів, що забезпечують безпеку БІР:

– системи, керують базами даних або так звані розподілені бази даних);

– сховища даних, OLAP- і OLTP- технологій оброблення даних (системи оперативного аналітичного оброблення і системи оперативного оброблення транзакцій);

– системи, що відповідають за пошук перевірених даних, їх вилучення;

– розподіл систем обчислення, здійснення реального створення банківського інформаційного простору, включаючи філіали, партнерів і клієнтів, а також організовування спільної роботи користувачів;

– забезпечення надійної безпеки при підключенні банківської системи до зовнішніх мереж (Інтернет);

– різного роду забезпечення (математичне, технічне, програмне);

– інформаційної аналітики та системи прийняття і підтримки рішень (decision support systems, DSS);

– забезпечення процесів захисту інформації;

– системи віддаленої роботи з програми передбачення поведінки курсів фондовими ринками;

– CRM-системи управління клієнтських відносин;

– програма реалізації фронт-офісу взаємодії з клієнтом;

– система, підтримує внутрішні процеси (організація та виконавча діяльність персоналу і менеджменту);

– створення спеціального доступу до кожного рівня секретності інформації індивідуально;

– антивірусний захист;

– інтернет-картки й інтернет-магазини;

–центр оброблення викликів (call- центри) та IP-телефонія;

– здійснення підтримки доступу різних каналів: Інтернет, мобільна мережа, телефон, SMS, WAP та ін.;

– підтримання множинних стандартів обліку, також управлінський облік;

– дослідження та підтримання в області планомірного інформаційного розвитку АБС.

На рис. 1.4. наведено приклад АБС НСЕМП.

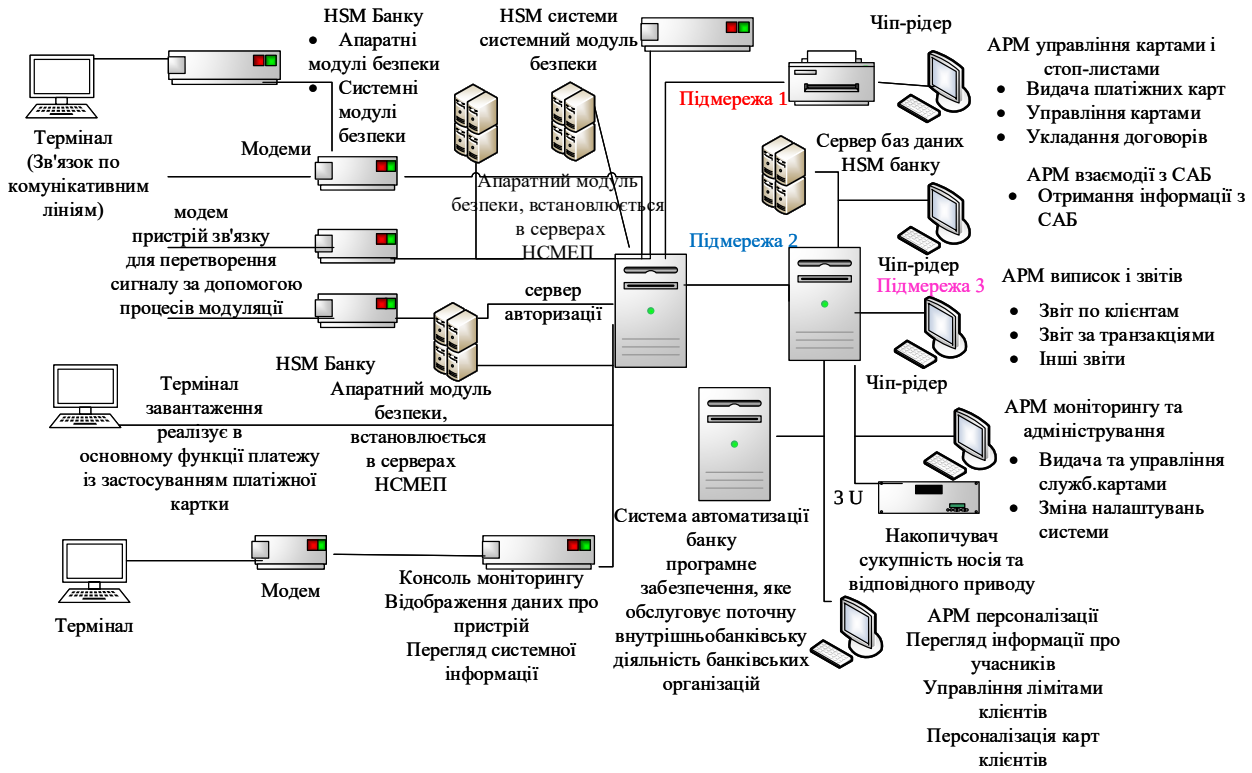


Рисунок 1.4 – Структурна схема АБС НСЕМП

Аналіз організаційної структури НСМЕП показує, що в основі функцій її роботи застосовується *автоматизована карткова система (АКС)* – програмно-технічний комплекс, який забезпечує виконання функцій НСМЕП щодо емісії карток, оброблення інформації про операції їх застосування, управління банкоматами і терміналами і т.д.). Дана система відноситься до складної багаторівневої системи управління критичного застосування (СУКЗ), в якої передавання інформації вимагає контроль безпеки на кожному рівні [37].

Дана система інтегрується в систему банків і множину типів терміналів, в т.ч. переносні, які працюють в автономно, і банкомати, що виконують більш широкий спектр функцій. НСМЕП керує потоками електронних грошей, зв’язком локальних мереж і терміналів. Для надійної роботи електронна платіжна система має бути надійно захищена.

З точки зору безпеки в НСМЕП є такі вразливі місця: пересилання платіжних та інших повідомлень між клієнтом і банком чи між банками;

оброблення інформації всередині організацій відправника та отримання повідомлень; доступ клієнтів до засобів які акумульовані на рахунках.

1.3 Основні вимоги національних стандартів до функцій СУІБ

Для забезпечення формування системи безпеки використовуються як правило не тільки рекомендації НБУ, а також міжнародні регулятори. Практика показує, що чітко можна виділити основні 2 групи методів оцінки ризиків безпеки [19, 20, 23, 28, 29]. Перша група дозволяє встановити рівень ризику через оцінювання ступеня відповідності певному наборові вимог щодо забезпечення безпеки інформації. Як джерела цих вимог у банківській ссфері України виступають міжнародні і національні керівні документи, які систематизуються у виді схеми, яку подано на рис. 1.5.

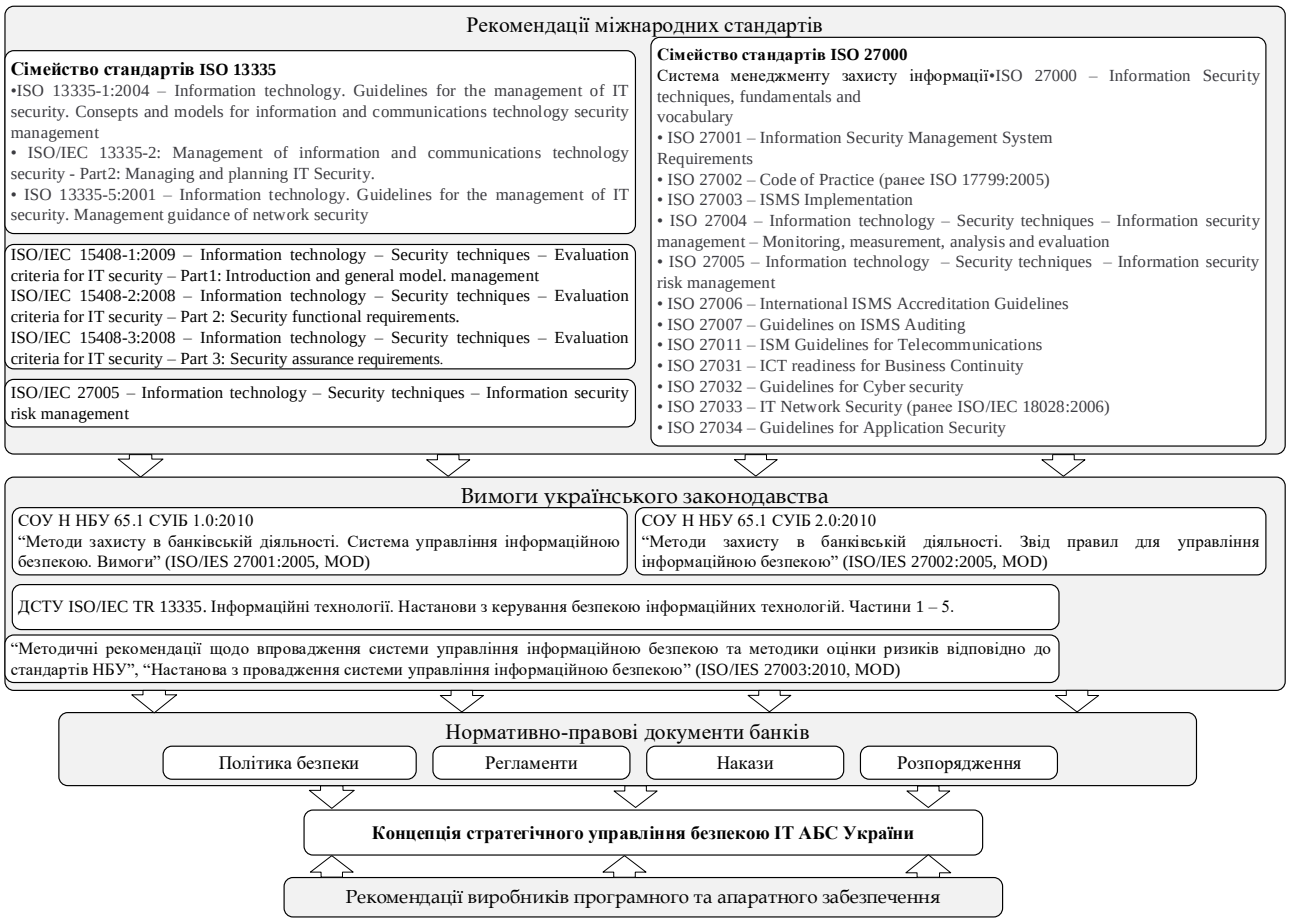


Рисунок 1.5 – Систематизація джерел вимог до безпеки ІТ АБС України

Відповідно Концепції основними функціями системи безпеки та СУІБ є [8, 9]:

- розуміння вимог інформаційної безпеки організації і необхідність розробки політики та цілей інформаційної безпеки;

- провадження безпеки і забезпечення її функціонування задля управління загрозами інформаційній безпеці організації у контексті загальних бізнес-загроз банку;

- моніторингу та перегляду продуктивності і ефективності СУІБ (система управління інформаційної безпеки).

Як правило СУІБ використовує модель “Плануй-Виконуй-Перевіряй-Дій” (“Plan-Do-Check-Act”), у подальшому ПВПД (PDCA), яку застосовують для структуризації всіх процесів СУІБ, яка наведена на рис. 1.6.

СУІБ забезпечує вибір адекватних і взаємопов'язаних заходів безпеки, які захищають інформаційні ресурси СУІБ і гарантують конфіденційність зацікавленим сторонам [8]. Основні етапи побудови СУІБ банку наведені на рис. 1.7.

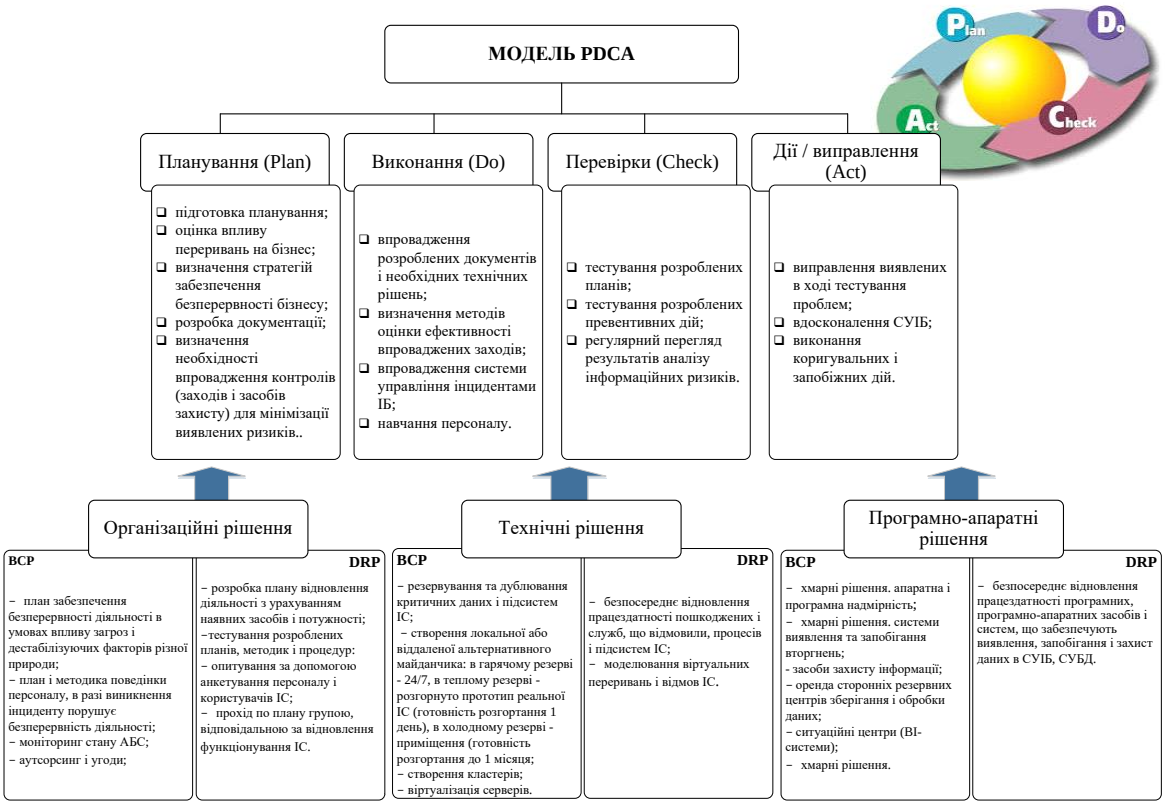


Рисунок 1.6 – Основні функції моделі PDCA

Рисунок 1.7 – Етапи побудови СУІБ комерційного банку

Ухвалення моделі ПВПД (PDCA) відображає принципи, встановлені Керівництвом ОЕСР, що регулюють безпеку інформаційних систем і мереж. Цей стандарт надає надійну модель для впровадження принципів цієї установки, що впливають на оцінку ризиків, проектування і впровадження безпеки, управління безпекою та повторну її оцінку.

Друга група методів оцінки ризиків безпеки інформації базується на визначенні імовірності реалізації атак, та рівнів їх шкоди. У разі величини ризику обчислюється окремо кожної загрози й у випадку представляється як добуток імовірності реалізованої загрози на значення потенційного збитку від цієї загрози. Власником БІн визначається обсяг збитків, а ймовірність її реалізації обчислюють групою експертів (аудиторська повірка). Відрізняються методи першої та другої груп застосуванням різних шкал величини ризику. В першому випадку параметри ризику показуються в кількісних значеннях. В другому випадку застосовуються якісні шкали. Відповідно до вимог стандартів НБУ застосування СУІБ, котра має бути впроваджена, є банк. Тому важливо в умовах збільшення числа загроз безпеці ІТ АБС уточнити бізнес-процеси/банківські продукти [26], котрі працюють з БІН, що підлягає захисту. У нинішніх умовах такого переліку можна віднести [26]: платіжні документи;

платіжні документи внутрішні; документи на перекази грошові; персональні дані працівників та клієнтів банку; інші документи. Крім того, вирішення всього комплексу питань, пов'язаних із забезпеченням безпеки БІН та ІТ АБС України має вирішуватися у комплексі та нерозривно одне від одного, гармонійно доповнюючи та заповнюючи, у разі потреби, один одного. Просте комплексування сил та засобів у кожному окремому випадку задля забезпечення безпеки ІТ АБС є недоцільним як із практичної, і наукової точок зору.

На рис. 1.8 наведені основні функції системи управління, а також основні рекомендації щодо формування та створення комплексу заходів СУІБ щодо безперервної роботи системи НСЕП. Крім цього, СУІБ враховує функціональність АБС щодо надання цифрових послуг електронного банкінгу: авторизацію, ідентифікацію, автентифікацію користувачів, обробку передачу та зберігання банківських документів, а тож необхідні послуги безпеки: конфіденційність, цілісність та доступність.

Рисунок 1.8 – Основні функції системи управління

На рис.1.9–1.10 наведені основні заходи щодо створення, функціонування, аналізу та модифікації СУІБ.

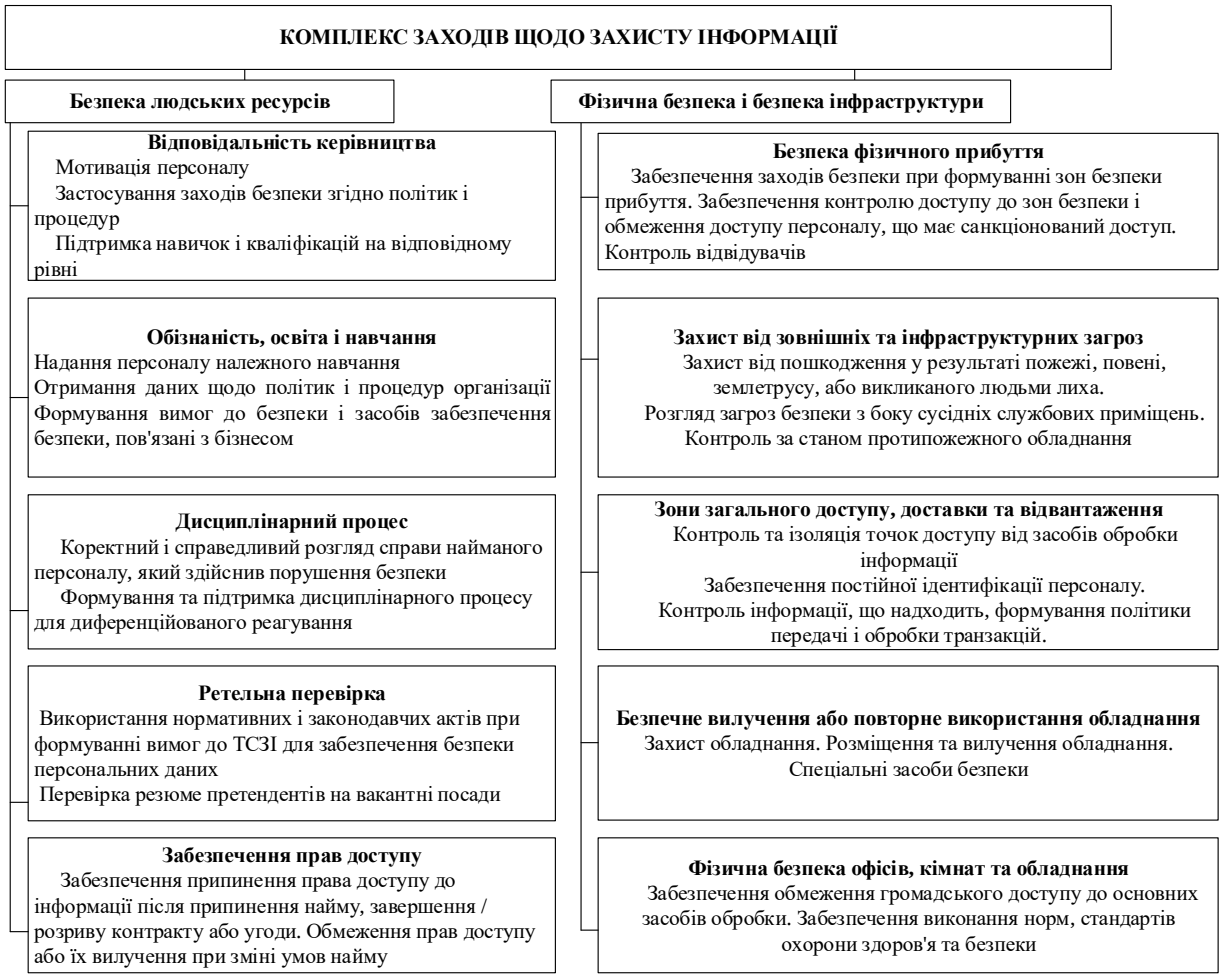


Рисунок 1.9 – Комплекс дій із захисту банківських транзакцій

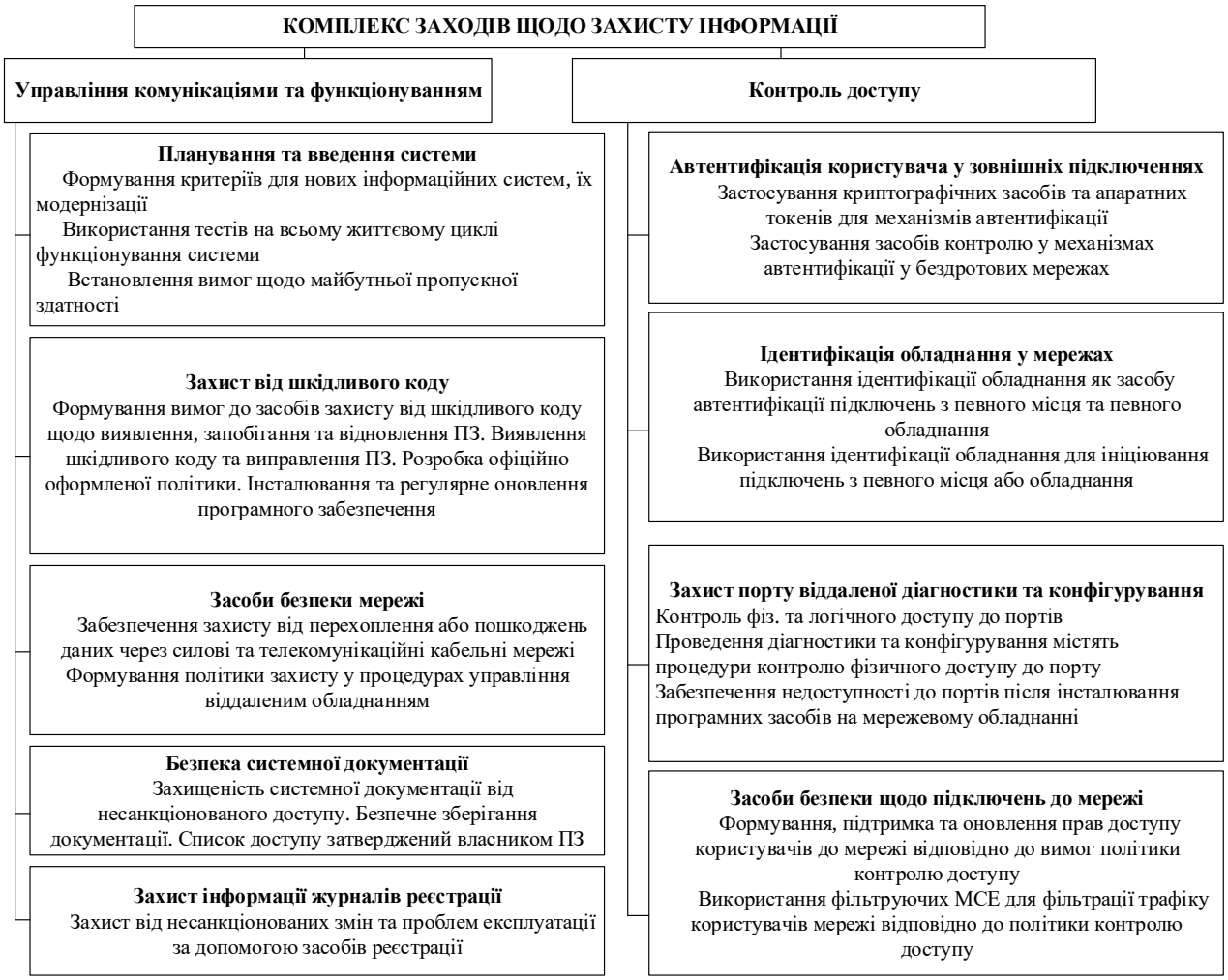


Рисунок 1.10 – Комплекс дій із захисту банківських транзакцій

1.4 Аналіз основних механізмів безпеки інформації у НСМЕП

Міжнародні стандарти ISO 7498, ISO/IEC 10181, що здатні забезпечити необхідні величини для безпеки, здатні визначити 5 базових загальнодоступних послуг, основні з них є дві: цілісність та аутентифікація. Щоб забезпечити використання механізмів безпеки, багато з яких були реалізовані на базі перетворення інформації, що здійснюється завдяки криптографічним методам. Структуризована схема КСЗ БІР НСЕМП показана на рис.1.11.

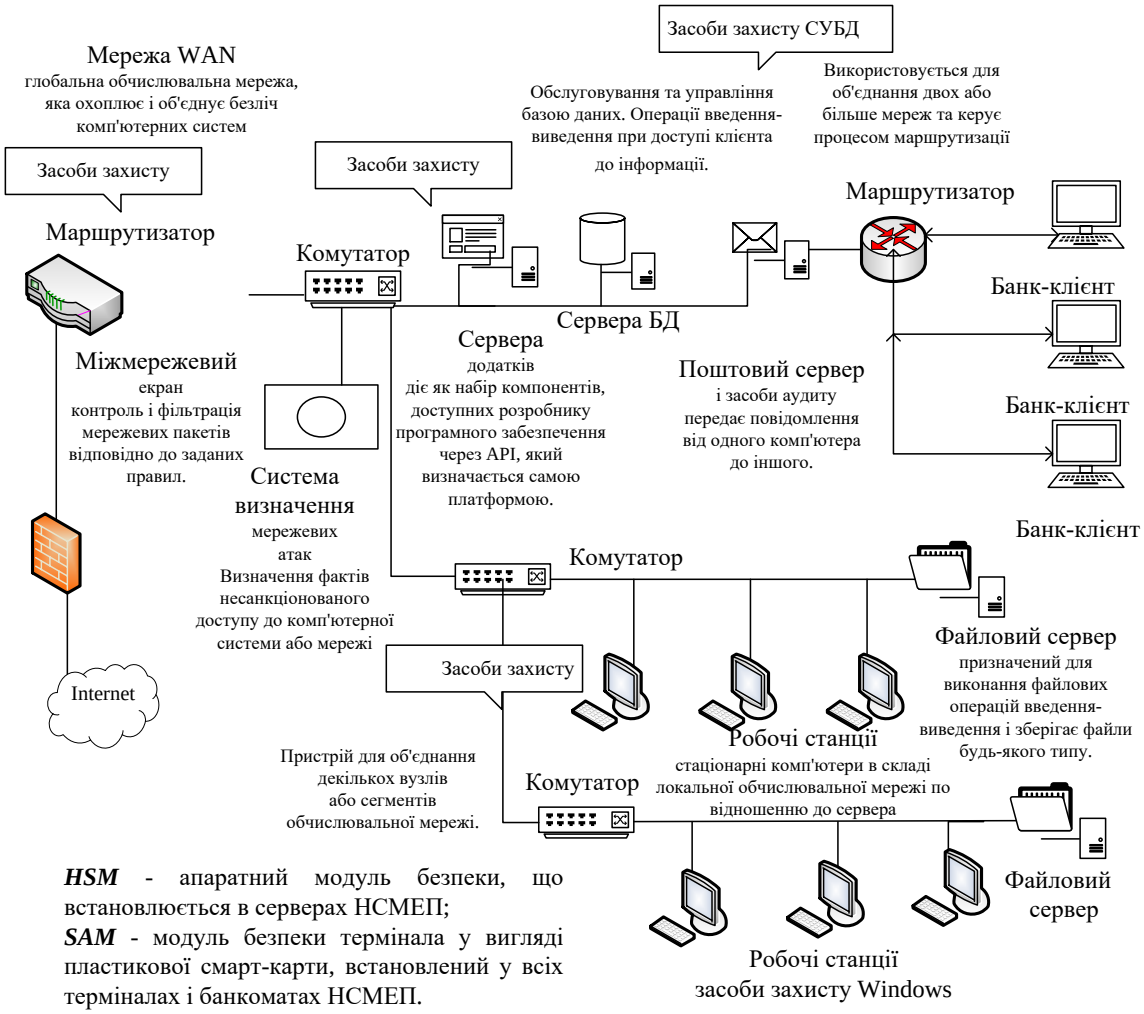


Рисунок 1.11 – Структуризована схема СУІБ НСМЕП

Забезпечення ведення електронного документообігу в АБС застосовують електронні ключі (сертифікати) згідно стандарту ДСТУ ISO/IEC 9594-8:2006 [37], прикладом системи комплексного захисту інформації (СКЗІ) може бути центр сертифікації ключів (ЦСК) “Шифр Х.509”. Система КЗІ “Шифр-Х.509” призначена для:

– створення відкритих ключів;

– забезпечення послугами ЕЦП державні органи влади, місцевого самоврядування, підприємств, організацій та установ будь-якої форми власності також фізичних осіб.

Функціональне призначення СКЗІ “Шифр-Х.509”:

– забезпечити управління сертифікатами та ключами відповідно до ДСТУ ISO/IEC 9594-8:2006;

– забезпечити криптографічний захисту закритої і відкритої інформації.

СКЗІ “Шифр-Х.509” являється програмним комплексом, функціонування засобів якого відбувається у середовищі ОС електронно-обчислювальної техніки та взаємодія з загальним програмним прикладним забезпеченням, загальна структура якого наведена на рис. 1.12.

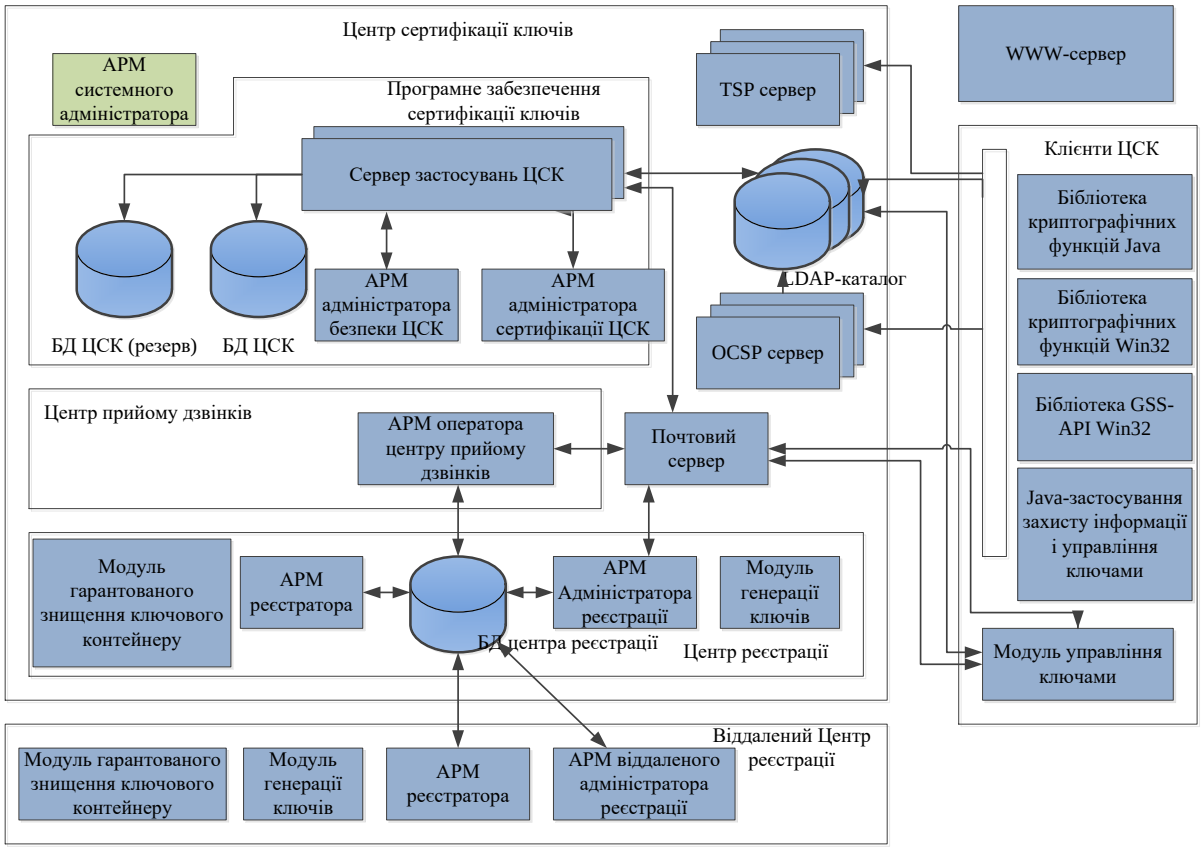


Рисунок 1.12 – Структуризована схема СКЗІ “Шифр-Х.509”

Топологія мережі СКЗІ “Шифр-Х.509” показана на рис. 1.13.

Проведений аналіз системи показує, що сьогодні для забезпечення основних послуг використовуються симетричні та несиметричні криптосистеми. Симетричні криптосистеми на 3–5 порядків швидше за швидкістю криптоперетворень, але забезпечують тимчасову стійкість. Несиметричні системи навпаки, забезпечують гарантовану стійкість (стійкість основана на NP-повної задачі) але на 3–5 порядків повільніше ніж симетричні криптосистеми. Тому, як правило, використовуються в АБС для передачі

ключових даних симетричних криптосистем, та/або формуванні цифрового підпису.

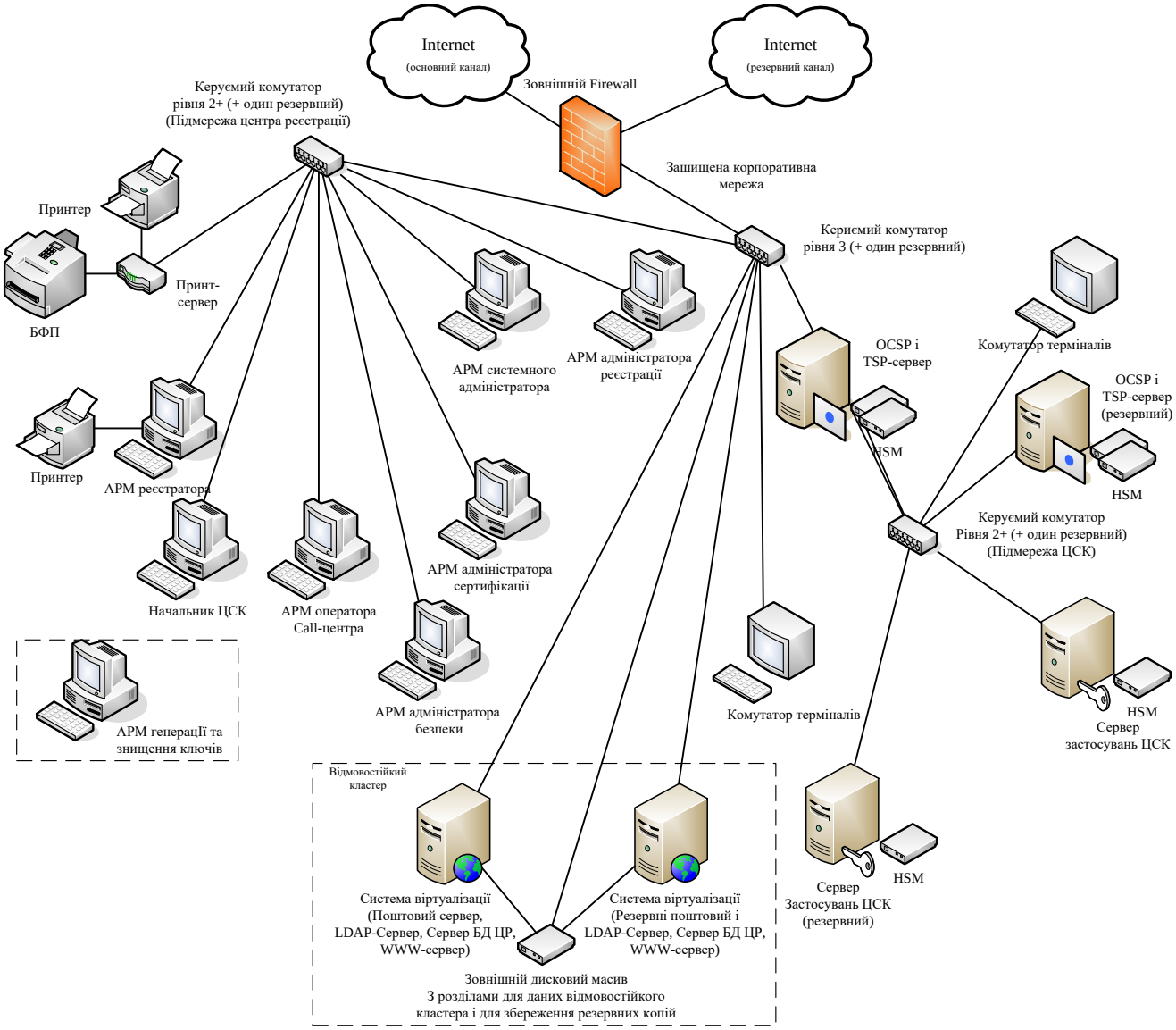


Рисунок 1.13 – Типова топологія мережі СКЗІ “Шифр-Х.509”

СКЗІ “Шифр-Х.509” підтримує криптографічні алгоритми:

– формування образу даних, на основі алгоритму ГОСТ 34311-95;

– управління ключами шифрування забезпечує протоколом Діффі-Геллмана;

– шифрують / розшифровують дані та імітозахист, що базуються на алгоритмом ГОСТ 28147-89 (ДСТУ ГОСТ 28147-2009);

– формування і перевірка ЕЦП здійснюється за алгоритмом ДСТУ 4145-2002.

Система КЗІ «Шифр-Х.509» призначена для:

– створення структури незакритих ключів (створення ЦСК, в т.ч. акредитованих, реєстраційних центрів в рамках відповідальності ЦСК, надання абонентам засобів управління ключами),

– забезпечення послугами ЕЦП державних органів влади та місцевого самоврядування, підприємств, установ і організацій, а також фізичних осіб.

Функціональним призначенням СКЗІ «Шифр-Х.509» є:

– забезпечення управління сертифікатами та ключами відповідно до ДСТУ ISO / IEC 9594-8:2006;

– забезпечення криптографічного захисту закритої і відкритої інформації: обчислення і перевірка ЕЦП даних відповідно до ДСТУ 4145-2002, шифрування і імітозахист даних згідно ГОСТ 28147-89, формування геш-функції згідно ГОСТ 34.311-95.

СКЗІ «Шифр-Х.509» програмний комплекс, засоби якого функціонують в середовищі ОС ЕОТ та взаємодіють із загальним програмним прикладним забезпеченням.

Всі криптографічні перетворення в рамках СКЗІ «Шифр-Х.509» виконуються програмними криптографічними бібліотеками, що входять до складу програмного вироби «Шифр+».

Засоби підсистеми управління ключами та сертифікатами, які входять до складу СКЗІ «Шифр-Х.509», на алгоритмічній та програмному рівнях, є єдиними виробами та призначені для використання у складі комплексів обробки і передачі інформації.

Виконавчі засоби СКЗІ «Шифр-Х.509» є окремими програмними компонентами (бібліотеками), які самостійно не експлуатуються і призначені для застосування як складові частини при побудові комплексів обробки і передачі інформації.

Система підтримує декілька варіантів зберігання ключової інформації:

– Зашифрований ключовою контейнер з парольованим доступом. Може зберігатися на будь-якому носії: USB Flash Storage, CD/DVD або на жорсткому диску.

– Зовнішній пасивний апаратний носій ключової інформації. Ключ знаходиться всередині ключового контейнера записаного в пристрій і витягується з нього при необхідності.

Підтримуються носії, що реалізують протокол PKCS#11 (носії компанії Автор, SafeNet, Giesecke & Devrient та ін.). На рис. 1.14 наведено взаємозв'язок між механізмами і застосовуваними стандартами в СУІБ НСМЕП.

Програмна реалізація механізмів, що розглядалися є програмні засоби криптографічного захисту інформації "Грифон-Б" і "Грифон-Л", які призначені для криптографічного захисту закритої інформації в АБС та застосовуються з метою обміну інформацією в корпоративній мережі банку, з клієнтами, що працюють з системою "Клиієнт-Банк", в системі обслуговування пластикових карт [**Error! Reference source not found.**; **Error! Reference source not found.**; **Error! Reference source not found.**].

Перелік процедур КЗІ "Тайфун - PKCS # 11" містить процедури, що виконують захист цілісності та конфіденційності інформації, забезпечують автентифікацію відправників повідомлень використовуючи механізми криптозахисту (ЕЦП, шифрування, формування імітовставок і хеш-функцій) вбудовуючи в конкретні прикладні системи [**Error! Reference source not found.**].

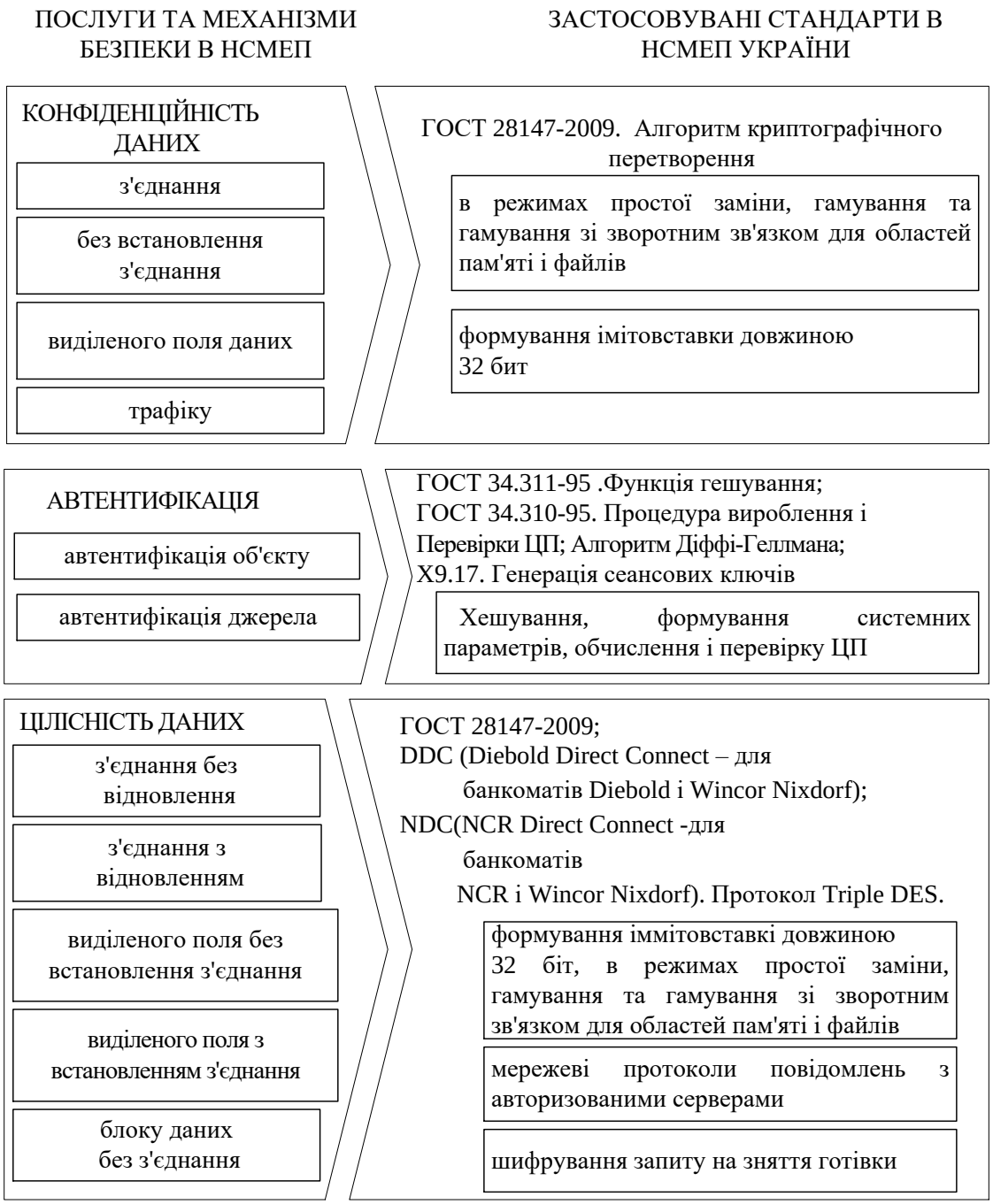


Рисунок 1.14 – Взаємозв’язок між послугами безпеки і механізмами в НСМЕП

Процедури, що входять до бібліотеки:

– шифрують / розшифровують дані за алгоритмом ГОСТ 28147-2009;

– формують / перевіряють імітовставки за алгоритмом ГОСТ 28147-2009;

– формують / перевіряють ЕЦП за алгоритмами ДСТУ 4145-2002, ГОСТ 34.310-95, 34.311-95;

– формують ключі шифрування по схемі Діффі-Геллмана (використовують відкритий розподіл ключів згідно вимог ISO 11166-94).

Швидкісні характеристики програмних засобів, котрі реалізують алгоритми криптоперетворень (для ПК на базі Intel Celeron 2,4 ГГц):

– швидкість шифрування / розшифрування в режимі простої заміни БСШ ГОСТ 28147-2009 не менше 8 Мбайт/с;

– швидкість обчислення геш-функції згідно ГОСТ 34.311 – 95 не менше 3 Мбайт/с;

– формування ЕЦП згідно ГОСТ 34.310-95 за довжини ключа 512 біт не більше 0,003 с;

– час перевірки ЕЦП згідно ГОСТ 34.310-95 за довжини ключа 512 біт не більше 0,006 с;

– формування ЕЦП згідно ГОСТ 34.310-95 за довжини ключа 1024 біт не більше 0,01 с;

– час перевірки ЕЦП згідно ГОСТ 34.310-95 за довжини ключа 1024 біт не більше 0,02 с;

– формування ЕЦП (з обчисленням предпідпису) відповідно до ДСТУ 4145-2002 для основного поля степені 163 не більше 0,0068 с;

– при перевірці ЕЦП відповідно до ДСТУ 4145-2002 для основного поля степені 163 не більше 0,013 с.

Криптографічні перетворення в бібліотеці “Тайфун-PKI PKCS#11” реалізуються з застосуванням бібліотеки програмних процедур криптозахисту інформації “Тайфун-W32” версії 2.01.

Система захищеної електронної пошти “Бриз” використовується для здійснення обміну електронними повідомленнями у форматі SMF-70, захищеними з застосуванням механізмів криптозахисту (ЕЦП, шифрування / розшифрування, формування імітовставок), між абонентами електронної пошти (ЕП), які зареєстровані на вузлах ЕП через мережу передачі вільного типу з відповідними критеріями НД ТЗІ 2.5-004-99 [**Error! Reference source not found.**].

Удосконалення вимог до захисту БІР враховуючи актуальні кіберзагрози, установлення вимог з організації заходів по забезпеченні ІБ та кіберзахисту банків, Правління НБУ в [**Error! Reference source not found.**] вказало основні механізми – криптоалгоритми симетричної криптографії (ГОСТ-28147-2009, “Калина-256”, AES, з ключем не менше 128 біт – для забезпечення цілісності та конфіденційності даних), несиметричної криптографії (алгоритми Діффі-Геллмана, алгоритм Ель-Гамаля, як звичайні, та на еліптичних кривих, алгоритм RSA, з довжиною чисел 2048 біт – забезпечення обміну ключів), забезпечення аутентичності з використанням MAC-кодів “Купина”. Аналіз змін, які запропоновані у ПЗ вказують про підвищення вимог до рівня криптостійкості (див. рис. 1.5).

1.5 Висновки до розділу 1

Проведені дослідження засвідчили, що розвиток обчислювальних ресурсів дав змогу розширити спектр банківських послуг на основі використання Інтернет-ресурсів та електронного банкінгу, але використання симетричних та несиметричних криптосистем може стати під загрозу під час появи повномасштабного квантового комп’ютера.

Аналіз законодавчої бази банківської діяльності показав, що вона, в цілому, ґрунтується на світових стандартах, що визначають основні принципи побудови СУІБ, рекомендації протидії кібератакам на банківські системи. Неповнота нормативно-методичного забезпечення безпеки інформації, перш за все в області показників і критеріїв, істотно ускладнює, а іноді не дозволяє об’єктивно оцінити ефективність системи захисту даних.

Використання технології відкритих ключів дозволяє створювати незалежні від людини системи забезпечення ЗА (ідентифікація, авторизація, автентифікація) та забезпечити послуги конфіденційності, цілісності та автентичності в сучасних АБС, за рахунок використання цифрового сертифікату, який є зв’язком між клієнтом організації

2. АНАЛІЗ ОСНОВНИХ ЗАГРОЗ, МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ І МЕТОДИК ОЦІНКИ РИЗИКУ

2.1 Побудова моделі загроз

Аналізуючи відповідність рівнів складності ПЗ, технічну грамотність зловмисників, результати оцінок кількості кібератак, також АБС, та, які отримані багатьма компаніями на ринку периферійних мережевих пристроїв та кібербезпеки [37], дозволяє оперувати таким висновком: при наростанні кіберзлочинності та обчислювальних можливостей в сьогоденні та близькому майбутньому, потрібно враховувати, що відбудеться ріст не тільки значної кількості та технічно-складних кібератак, але й раціональне перенаправлення на мережеве периферійне обладнання.

Беручи до уваги результати досліджень [**Error! Reference source not found.**; **Error! Reference source not found.**; **Error! Reference source not found.**; **Error! Reference source not found.**; **Error! Reference source not found.**; **Error! Reference source not found.**; **Error! Reference source not found.**; 37] можна стверджувати, що основні загрози кібербезпеці АБС, спрямовані на припинення роботи процесів, що відповідають за управління чи контроль, створюватимуться такі кібератаки, що об’єднаються в такі чотири основні класи, їх зміст розкритий на рис. 2.1.

Запропонована класифікація (рис. 2.1) свідчить, що кібератаки різних класів не залежно від призначення мають місце на різних рівнях моделі відкритих систем OSI, значить мають свої завдання впливу на БІР.

Враховуючи суб’єктивні та об’єктивні причини, загрози, які описані вище, важливі для великої кількості відових, проектованих АБС. Так як існує взаємозв’язок для різного роду безпек, і враховуючи те, що потрібно розробити ефективні безпечні системи БІР, пропонується новітня модель загроз безпеці систем БІР. Надалі ця модель буде вживатись, як синергетична (рис. 2.2).

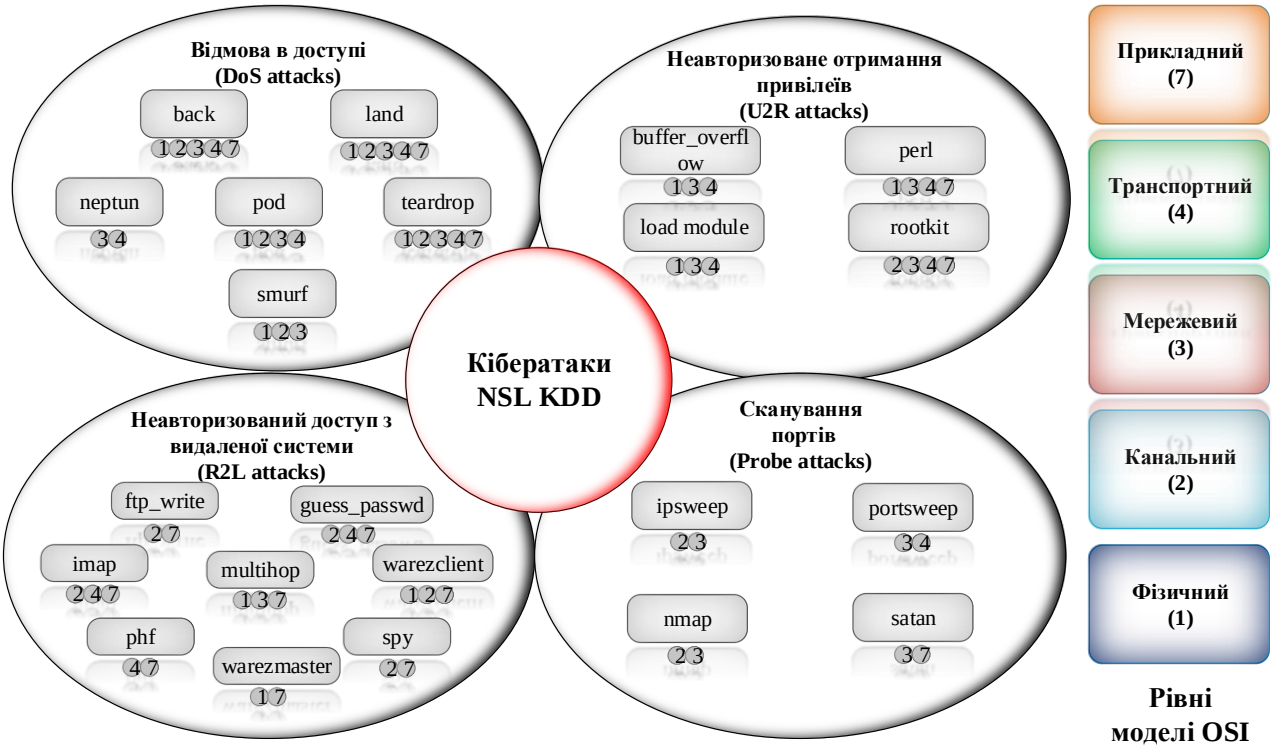


Рисунок 2.1 – Класифікація кібератак на АБС згідно моделі OSI

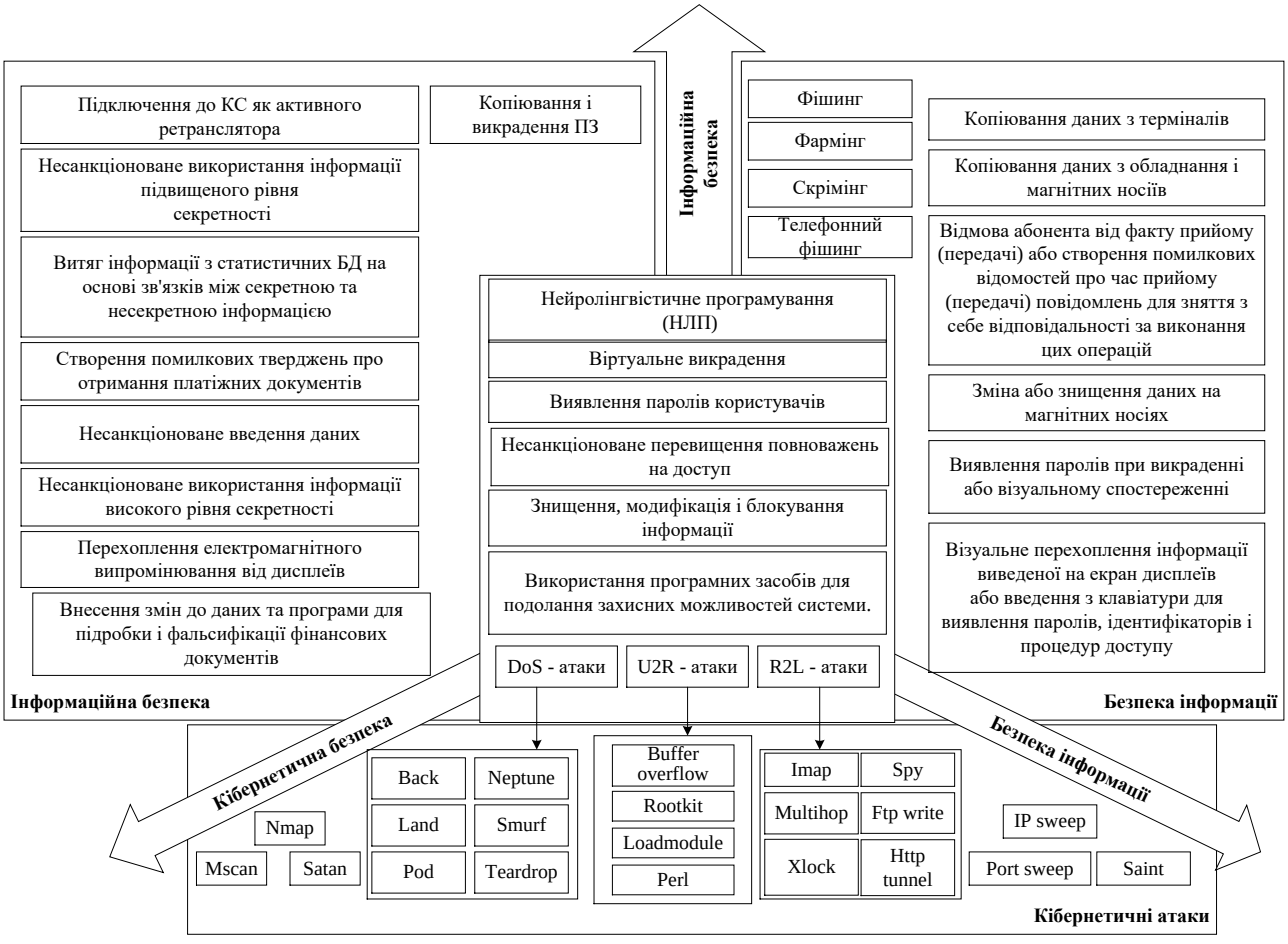


Рисунок 2.2 – Синергетична модель загроз безпеці БІР

Характеристикою даної моделі (рис. 2.2) є сформовані логічні зв’язки існуючи загроз, які застосовуються для різноманітних профілів безпеки.

В роботі [37] автори пропонують вдосконалений варіант класифікатора загроз на банківську інформацію, як одного з ресурсів інформаційних критичних кібернетичних систем (ІККС) держави, з урахуванням їх синергізму і синергії на складові безпеки, на рис. 2.3 приведена структурна схема пропонованого рішення. Однак пропонований підхід не враховує економічні аспекти забезпечення безпеки і вимагає подальших досліджень. Синергетична модель загроз на складові безпеки кіберсистемДля формування моделі загроз як правило користуються адаптованої моделлю тріади CIA (confidentiality, integrity, availability), яка є підставою для її подальших модифікацій практичних моделей. Однак, в умовах постквантовой криптографії (в умовах появи повномасштабного квантового комп’ютера), фахівцями ність США ставиться під сумнів забезпечення необхідного рівня безпеки сучасними симетричними і несиметричними криптосистемами [31]. Крім цього використання і стрімке зростання технологій “G” може суттєво змінити вектор використання кіберпростору, як основного каналу передачі інформації між Кіберсистеми і інформаційно-комунікаційними системами, що в значній мірі знижує рівень безпеки і може практично звести його до нуля.

В таких умовах, необхідно розглядати в комплексі загрози – їх комплексування і гибридность, що призводять до появи синергетичного ефекту з подальшим збільшенням імовірності реалізації загрози на основі синтезу з методами соціальної інженерії. Для побудови класифікатора загроз кіберфізіческіх систем на рис. 2.4 пропонується структурна схема методологічних основ даного класифікатора.

2.2 Побудова нової синергетичної моделі загроз

В роботі [37] авторами запропоновано принципово новий підхід методології побудови систем безпеки на основі синергетичної моделі загроз,

яка забезпечує формування методологічних основ побудови класифікатора сучасних загроз на кіберфізичні системи.

Відповідно до стандарту ISO / IEC 27001 до: 2013 загрози поділяються на навмисні, випадкові і / або екологічні. Типовими прикладами можуть бути технічні збої, несанкціоновані дії, втручання в програмне забезпечення, фізичний збиток, компрометація функцій, і т. Д. Однак, стандарт, як і інші нормативні міжнародні акти не розглядає синергію і гибридность сучасних загроз, їх комплексування з методами соціальної інженерії , що істотно підвищує ризик реалізації загрози.

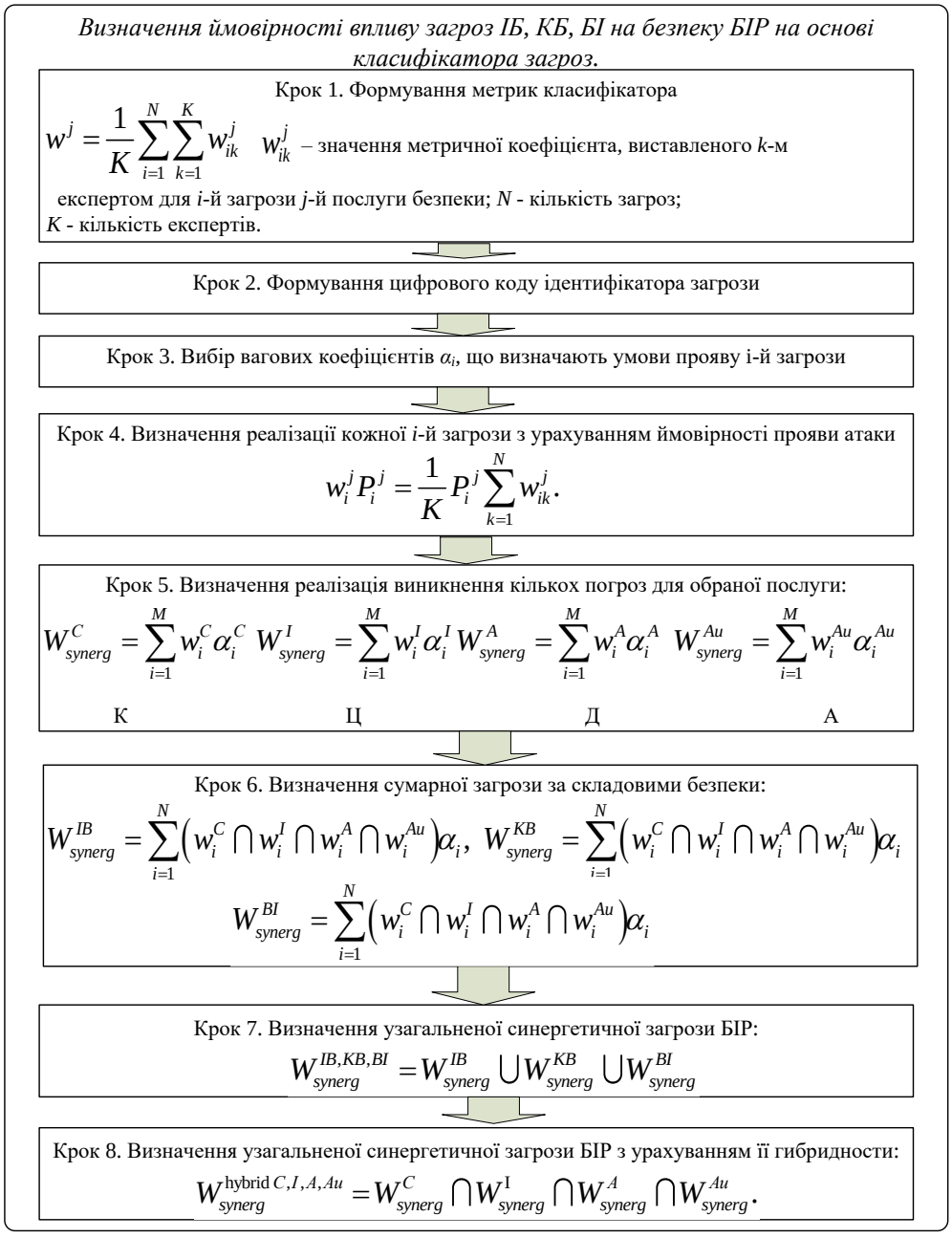
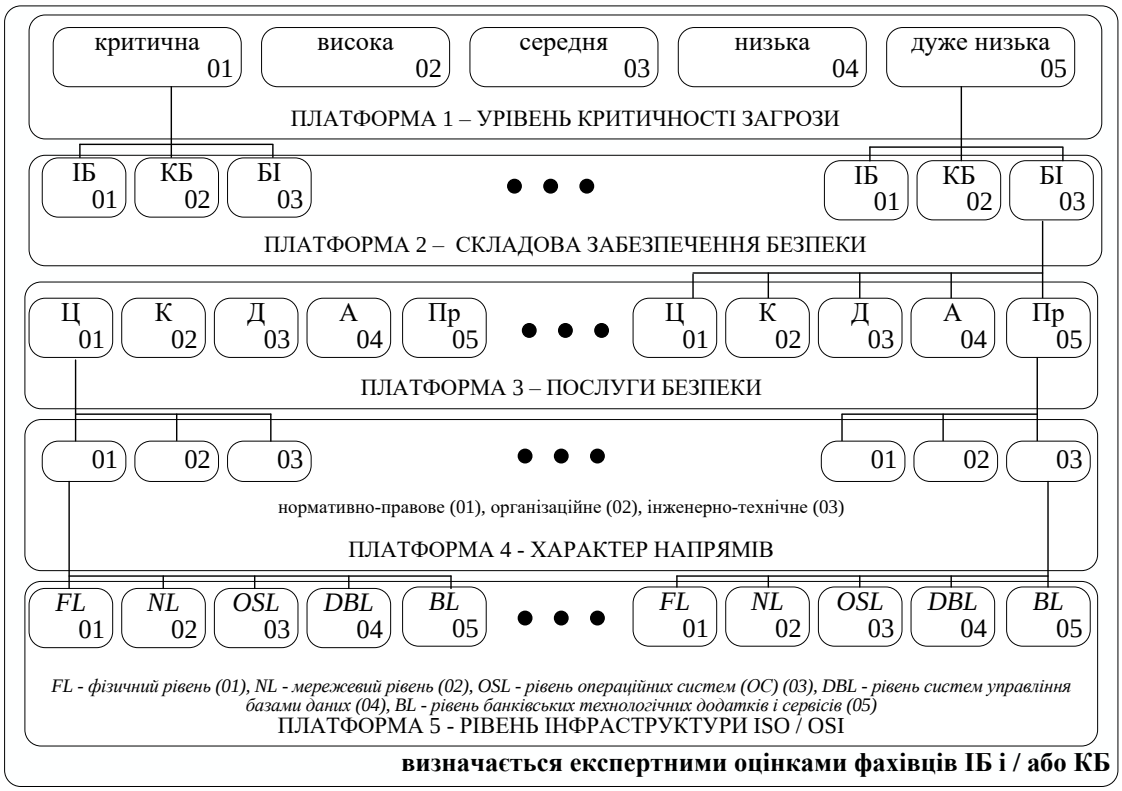


Рисунок 2.3 –Ймовірності загроз на основі синергетичної моделі загроз



КРОК 1. ФОРМУВАННЯ МЕТРИЧНИХ КОЕФІЦІЄНТІВ ПОГРОЗ ДЛЯ ICS І CPS

$$w_{ICS}{}^{j} = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{ICS\,ik}{}^{j}, \quad w_{CPS}{}^{j} = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{CPS\,ik}{}^{j}$$

КРОК 2. ФОРМУВАННЯ ВАГОВИХ КОЕФІЦІЄНТІВ УМОВ ПРОЯВИ ПОГРОЗ ДЛЯ ICS І CPS

$$\alpha_i^{ICS}, i \in [0{,}067;0{,}133;0{,}2;0{,}267;0{,}333], \alpha_i^{CPS}, i \in [0{,}067;0{,}133;0{,}2;0{,}267;0{,}333]$$

КРОК 3. ВИЗНАЧЕННЯ РЕАЛІЗАЦІЇ КОЖНІЙ ЗАГРОЗИ ДЛЯ ICS І CPS

$$w_{ICSi}{}^{j} P_{ICSi}{}^{j} = \frac{1}{K} P_{ICSi}{}^{j} \sum_{k=1}^{N} w_{ICSik}{}^{j}, \text{ где } P_{ICSi}{}^{j} \in \{\alpha_i^{ICS}\}, \; w_{CPSi}{}^{j} P_{CPSi}{}^{j} = \frac{1}{K} P_{CPSi}{}^{j} \sum_{k=1}^{N} w_{CPSik}{}^{j}, \text{ где } P_{CPSi}{}^{j} \in \{\alpha_i^{CPS}\}$$

КРОК 4. ВИЗНАЧЕННЯ РЕАЛІЗАЦІЇ КІЛЬКОХ ПОГРОЗ НА ПОСЛУГУ БЕЗПЕКИ

$$W_{ICS\,synerg}{}^{C} = \sum_{i=1}^{M} w_{ICSi}{}^{C} \alpha^{ICS\,C}{}_{i} \bigcup W_{CPS\,synerg}{}^{C} = \sum_{i=1}^{M} w_{CPSi}{}^{C} \alpha^{CPS\,C}{}_{i} \quad \cdots$$

$$W_{ICS\,synerg}{}^{Aff} = \sum_{i=1}^{M} w_{ICSi}{}^{Aff} \alpha^{ICS\,Aff}{}_{i} \bigcup W_{CPS\,synerg}{}^{Aff} = \sum_{i=1}^{M} w_{CPSi}{}^{Aff} \alpha^{CPS\,Aff}{}_{i}$$

КРОК 5. ВИЗНАЧЕННЯ СУМАРНОЮ ПОГРОЗ НА СКЛАДОВІ БЕЗПЕКИ

$$W_{synerg}^{IS} = \sum_{i=1}^{N} \left(w_{ICSi}{}^{C} \cap w_{ICSi}{}^{I} \cap w_{ICSi}{}^{A} \cap w_{ICSi}{}^{Au} \cap w_{ICSi}{}^{Aff} \right) \alpha_i^{ICS} \cup$$

$$\cup \sum_{i=1}^{N} \left(w_{CPSi}{}^{C} \cap w_{CPSi}{}^{I} \cap w_{CPSi}{}^{A} \cap w_{CPSi}{}^{Au} \cap w_{CPSi}{}^{Aff} \right) \alpha_i^{CPS}$$

КРОК 6. ВИЗНАЧЕННЯ ЕКОНОМІЧНИХ ВИТРАТ НА ЗАПОБІГАННЯ АТАКИ

$$Tr_{ICS\,R}{}^{A} = \left\{ Tr_i \mid \left(P_i^A - C_i^A \right) > 0 \right\} \; \forall Tr_i \in Tr \Rightarrow Tr_L^{ICS} = \arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \cdot K_l^A$$

$$Tr_{CPS\,R}{}^{A} = \left\{ Tr_i \mid \left(P_i^A - C_i^A \right) > 0 \right\} \; \forall Tr_i \in Tr \Rightarrow Tr_L^{CPS} = \arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \cdot K_l^A$$

визначається автоматично на основі математичних виразів

Рисунок 2.4 – Структурна схема класифікатора загроз

Запропонований підхід враховує можливості сучасних загроз, їх синергію і гибридность, можливість подання з методами соціальної інженерії.

Розглянемо більш докладно пропонований підхід до формування класифікатора загроз. На першому етапі експертам пропонується, використовуючи свій досвід сформувати кортежі класифікатора загроз на основі 5 платформ. Перша платформа визначає рівень критичності загрози (критична, висока, середня, низька, дуже низька), що дозволяє на 5 кроці провести розрахунки економічної “рентабельності” критичних загроз.

Друга платформа визначає ставлення до складовою забезпечення безпеки (інформаційна безпека (ІБ), кібербезпека (КБ), безпеку інформації (БІ), що дозволяє на 5 кроці отримати оцінку синергетичного ефекту на окрему зі складових загроз. Третя платформа визначає спрямованість загрози на послуги безпеки (цілісність, конфіденційність, доступність, автентичність і причетність), що дозволяє на 4 кроці отримати оцінку впливу кількох погроз на послуги безпеки, і визначити вектор напрямку впливу на елементи інфраструктури. Четверта платформа визначає характер напрямків впливу загроз (нормативно-правове, організаційне, інженерно-технічне).П'ята платформа забезпечує оцінку спрямованості на елементи інфраструктури і дозволяє “виявити” критичні точки в КСЗІ. При цьому для об’єктивності суджень експертів використовуємо вагові коефіцієнти компетентності експертів (k_k) представлені в табл. 2.1.

Таблиця 2.1 – Ваговий коефіцієнт компетентності експертів

№ з/п	Кваліфікація експертів	Значення вагового коефіцієнта (k_k)
1	міжнародний експерт в області ІБ, КБ, БІ	1,0
2	національний експерт в області ІБ, КБ, БІ	0,95
3	сертифікований міжнародний фахівець в області ІБ, КБ, БІ	0,9
4	повний доктор наук в області ІБ, КБ, БІ	0,9
5	начальник служби безпеки	0,85
6	доктор філософії в області ІБ, КБ, БІ	0,8
7	співробітник служби безпеки	0,7
8	системний адміністратор	0,6
9	інженер служби безпеки	0,5
10	аспірант за спеціальністю в області ІБ, КБ, БІ	0,4

Сумарна оцінка і-ї загрози визначається кількістю експертів відповідно до виразу:

$$\widetilde{x_i} = \frac{\sum_{k=1}^{K} x_k \times k_k}{K}, \tag{2.1}$$

де xk– показник впливу і-ї загрози оцінка на k-го експерта;

kk – показник рівня, що відповідає за компетентність експерта;

K– показник, що відповідає за кількість експертів.

Міра узгодженості оцінок експертів є дисперсія, яка визначена за виразом:

$$\sigma_x^2 = \frac{1}{K}\sum_{k=1}^{K} k_k (x_k - \widetilde{x_i})^2. \tag{2.2}$$

Статистична імовірність результатів 1 – αі, виглядає так: $[\widetilde{x_i} - \Delta, \widetilde{x_i} + \Delta]$, де значення хі враховуючи нормальний закон, розподіляється з центром в $\widetilde{x_i}$ и дисперсией σ_x^2. Тоді Δ визначається виразом:

$$\Delta = t\sqrt{\sigma_x^2 / N}, \tag{2.3}$$

де t – величина для K – 1 ступенів свободи з розподіла Стьюдента.

Для формування метричних (вагових) коефіцієнтів загроз (рис. 4) і їх впливу на послуги безпеки введемо такі позначення:

j – послуга безпеки, як для ICS, так і для CPS. Основні послуги безпеки: C -конфіденціальность; I – цілісність; A – доступність; Au – автентичність, Aff – причетність (на замовлення). Таким чином, в класифікаторі формується кортеж послуг безпеки; N – кількість загроз; K – кількість експертів, які брали участь в експертній оцінці загроз; $\{i\}_1^N$ – потоковий номер i-ї загрози; $\{k\}_1^K$ – потоковий номер експерта.

Для виконання оцінки гібридної і синергетичної складових впливу сучасних загроз використовуємо таку послідовність дій:

1 крок. Визначення усередненої оцінки експертів по всім загрозам для даної послуги безпеки:

$$w_{ICS}{}^{j} = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{ICSik}{}^{j}, \quad w_{CPS}{}^{j} = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{CPSik}{}^{j}, \tag{2.4}$$

де $w_{ICS}{}_{ik}^{j}$ – значення метричного коефіцієнта, який виставлений k-м експертом для i-ї загрози j-ї послуги безпеки для ICS, w_{CPSik}^{j} – значення метричної коефіцієнта, що виставляється k-м експертом для j-ї послуги безпеки i-ї загрози для CPS.

2 крок. Формування вагових коефіцієнтів умов прояви загроз для ICS і CPS (табл.2):

$\alpha_i^{ICS}, i \in [0,067; 0,133; 0,2; 0,267; 0,333], \alpha_i^{CPS}, i \in [0,067; 0,133; 0,2; 0,267; 0,333]$

.

3 крок. Визначення реалізації загрози для ICS і CPS:

$$w_{ICS_i}{}^{j} P_{ICS_i}{}^{j} = \frac{1}{K} P_{ICS_i}{}^{j} \sum_{k=1}^{N} w_{ICS_{ik}}{}^{j}, \text{ где } P_{ICS_i}{}^{j} \in \{\alpha_i^{ICS}\}, \quad w_{CPS_i}{}^{j} P_{CPS_i}{}^{j} = \frac{1}{K} P_{CPS_i}{}^{j} \sum_{k=1}^{N} w_{CPS_{ik}}{}^{j}, \text{ где } P_{CPS_i}{}^{j} \in \{\alpha_i^{CPS}\} \tag{2.5}$$

Таблиця 2.2 – Вибір вагових коефіцієнтів a_i прояви i-ї загрози

α_i	умови прояви
0,067	Загроза є не частіше ніж один раз на 5 років
0,133	Загроза є не частіше ніж один раз на рік
0,2	Загроза є не частіше ніж один раз на місяць
0,267	Загроза є не частіше ніж один раз на тиждень
0,333	Загроза є щодня

Для кожної послуги безпеки і i-ї загрози:

– для ICS:

$$w_{ICSi}^{C}\alpha_{ICSi}^{C} = \frac{1}{K}\alpha_{ICSi}^{C}\sum_{k=1}^{K} w_{ICSik}^{C}$$ – послуга конфіденційності ;

$$w_{ICSi}^{I}\alpha_{ICSi}^{I} = \frac{1}{K}\alpha_{ICSi}^{I}\sum_{k=1}^{K} w_{ICSik}^{I}$$ – послуга цілісності;

$$w_{ICSi}^{A}\alpha_{ICSi}^{A} = \frac{1}{K}\alpha_{ICSi}^{A}\sum_{k=1}^{K} w_{ICSik}^{A}$$ – послуга доступності;

$$w_{ICSi}^{Au}\alpha_{ICSi}^{Au} = \frac{1}{K}\alpha_{ICSi}^{Au}\sum_{k=1}^{K} w_{ICSik}^{Au}$$ – послуга автентичності,

$$w_{ICSi}^{Aff}\alpha_{ICSi}^{Aff} = \frac{1}{K}\alpha_{ICSi}^{Aff}\sum_{k=1}^{K} w_{ICSik}^{Aff}$$ – послуга причетності,

де $w_{ICSi}^{C}, w_{ICSi}^{I}, w_{ICSi}^{A}, w_{ICSi}^{Au}, w_{ICSi}^{Aff}$ – експертні вагові коефіцієнти послуг безпеки: цілісності, конфіденційності, доступності, автентичності і причетності; α_{ICSi}^{C}, α_{ICSi}^{I}, α_{ICSi}^{A}, α_{ICSi}^{Au}, α_{ICSi}^{Aff} – ваговий коефіцієнт послуги безпеки: цілісності, конфіденційності, доступності, автентичності і достовірності появи атаки і-ї загрози.

– для CPS:

$$w_{CPSi}^{C}\alpha_{CPSi}^{C}=\frac{1}{K}\alpha_{CPSi}^{C}\sum_{k=1}^{K}w_{CPSik}^{C}$$ – послуга конфіденційності ;

$$w_{CPSi}^{I}\alpha_{CPSi}^{I}=\frac{1}{K}\alpha_{CPSi}^{I}\sum_{k=1}^{K}w_{CPSik}^{I}$$ – послуга цілісності;

$$w_{CPSi}^{A}\alpha_{CPSi}^{A}=\frac{1}{K}\alpha_{CPSi}^{A}\sum_{k=1}^{K}w_{CPSik}^{A}$$ – послуга доступності;

$$w_{CPSi}^{Au}\alpha_{CPSi}^{Au}=\frac{1}{K}\alpha_{CPSi}^{Au}\sum_{k=1}^{K}w_{CPSik}^{Au}$$ – послуга автентичності,

$$w_{CPSi}^{Aff}\alpha_{CPSi}^{Aff}=\frac{1}{K}\alpha_{CPSi}^{Aff}\sum_{k=1}^{K}w_{CPSik}^{Aff}$$ – послуга причетності,

де $w_{CPSi}^{C}, w_{CPSi}^{I}, w_{CPSi}^{A}, w_{CPSi}^{Au}, w_{CPSi}^{Aff}$ – експертні вагові коефіцієнти послуг безпеки: цілісності, конфіденційності, доступності, автентичності і причетності; α_{CPSi}^{C}, α_{CPSi}^{I}, α_{CPSi}^{A}, α_{CPSi}^{Au}, α_{CPSi}^{Aff} – ваговий коефіцієнт послуги безпеки: цілісності, конфіденційності, доступності, автентичності і достовірності прояви атаки і-ї загрози.

4 крок. Визначення реалізації кількох погроз на послугу безпеки:

$$W_{ICS\,synerg}^{C}=\sum_{i=1}^{M}w_{ICSi}^{C}\alpha_{i}^{ICSC}\bigcup W_{CPS\,synerg}^{C}=\sum_{i=1}^{M}w_{CPSi}^{C}\alpha_{i}^{CPSC}$$ – синергічний ефект на послу конфіденційності;

$$W_{ICS\,synerg}^{I}=\sum_{i=1}^{M}w_{ICSi}^{I}\alpha_{i}^{ICSI}\bigcup W_{CPS\,synerg}^{I}=\sum_{i=1}^{M}w_{CPSi}^{I}\alpha_{i}^{CPSI}$$ – синергічний ефект на послугу цілісність;

$$W_{ICS\,synerg}^{A}=\sum_{i=1}^{M}w_{ICSi}^{A}\alpha_{i}^{ICSA}\bigcup W_{CPS\,synerg}^{A}=\sum_{i=1}^{M}w_{CPSi}^{A}\alpha_{i}^{CPSA}$$ – синергічний ефект на послугу доступність;

$$W_{ICS\,synerg}^{Au}=\sum_{i=1}^{M}w_{ICSi}^{Au}\alpha_{i}^{ICSAu}\bigcup W_{CPS\,synerg}^{Au}=\sum_{i=1}^{M}w_{CPSi}^{Au}\alpha_{i}^{CPSAu}$$ – синергічний ефект на услугу автентичність;

$$W_{ICS\,synerg}^{Aff}=\sum_{i=1}^{M}w_{ICSi}^{Aff}\alpha_{i}^{ICSAff}\bigcup W_{CPS\,synerg}^{Aff}=\sum_{i=1}^{M}w_{CPSi}^{Aff}\alpha_{i}^{CPSAff}$$ – синергічний ефект на послугу причетність, (2.6)

де M – кількість кількох погроз, які обрані експертом з множини $\{i\}_i^M$, яка є підмножиною множини загроз класифікатора, $M \le N$.

При формуванні метричних коефіцієнтів вважається, що отримані результати відносяться до незалежних загрозам, в разі їх залежності (збіг кортежів загроз) необхідно використати вираз визначення повної імовірності залежних подій:

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

5 крок. Визначення сумарної загрози за складовими безпеки з урахуванням виразу (2.6):

$$\begin{aligned}
W_{synerg}^{IS} &= \sum_{i=1}^{N}\left(w_{ICSi}^{\ C} \cap w_{ICSi}^{\ I} \cap w_{ICSi}^{\ A} \cap w_{ICSi}^{\ Au} \cap w_{ICSi}^{\ Aff}\right)\alpha_i^{ICS} \cup \\
&\cup \sum_{i=1}^{N}\left(w_{CPSi}^{\ C} \cap w_{CPSi}^{\ I} \cap w_{CPSi}^{\ A} \cap w_{CPSi}^{\ Au} \cap w_{CPSi}^{\ Aff}\right)\alpha_i^{CPS} \\
W_{synerg}^{CS} &= \sum_{i=1}^{N}\left(w_{ICSi}^{\ C} \cap w_{ICSi}^{\ I} \cap w_{ICSi}^{\ A} \cap w_{ICSi}^{\ Au} \cap w_{ICSi}^{\ Aff}\right)\alpha_i^{ICS} \cup \\
&\cup \sum_{i=1}^{N}\left(w_{CPSi}^{\ C} \cap w_{CPSi}^{\ I} \cap w_{CPSi}^{\ A} \cap w_{CPSi}^{\ Au} \cap w_{CPSi}^{\ Aff}\right)\alpha_i^{CPS}, \\
W_{synerg}^{SI} &= \sum_{i=1}^{N}\left(w_{ICSi}^{\ C} \cap w_{ICSi}^{\ I} \cap w_{ICSi}^{\ A} \cap w_{ICSi}^{\ Au} \cap w_{ICSi}^{\ Aff}\right)\alpha_i^{ICS} \cup \\
&\cup \sum_{i=1}^{N}\left(w_{CPSi}^{\ C} \cap w_{CPSi}^{\ I} \cap w_{CPSi}^{\ A} \cap w_{CPSi}^{\ Au} \cap w_{CPSi}^{\ Aff}\right)\alpha_i^{CPS}.
\end{aligned} \qquad (2.7)$$

Для визначення узагальненої синергетичної загрози:

$$W_{synerg}^{IS,CS,SI} = W_{synerg}^{IS} \cup W_{synerg}^{CS} \cup W_{synerg}^{SI}. \qquad (2.8)$$

Для визначення узагальненої синергетичної загрози з урахуванням її гибридности для ICS:

$$W_{ICS\,synerg}^{\text{hybrid}\,C,I,A,Au,Aff} = W_{ICS\,synerg}^{\ C} \cap W_{ICS\,synerg}^{\ \text{I}} \cap W_{ICS\,synerg}^{\ A} \cap W_{ICS\,synerg}^{\ Au} \cap W_{ICS\,synerg}^{\ Aff}. \qquad (2.9)$$

Для визначення узагальненої синергетичної загрози з урахуванням її гибридности для CPS:

$$W_{CPS\,synerg}^{\text{hybrid}\,C,I,A,Au,Aff} = W_{CPS\,synerg}^{\ C} \cap W_{CPS\,synerg}^{\ \text{I}} \cap W_{CPS\,synerg}^{\ A} \cap W_{CPS\,synerg}^{\ Au} \cap W_{CPS\,synerg}^{\ Aff}. \qquad (2.10)$$

Для визначення узагальненої гібридної синергетичної загрози:

$$W_{synerg}^{\text{hybrid } IS,CS,SI} = W_{ICS\,synerg}^{\text{hybrid } C,I,A,Au,Aff} \bigcup W_{CPS\,synerg}^{\text{hybrid } C,I,A,Au,Aff} . \quad (2.11)$$

6 крок. Визначення економічних витрат на запобігання атаки.

Введення вартісних показників загроз дозволяє реалізувати алгоритм побудови рейтингу потенційних загроз і важливості інформаційних ресурсів, що підлягають захисту.

Пропонований в [37] алгоритм реалізує наступні дії. Обидві сторони нападу визначаються важливості (рейтинг) атак, які економічно доцільно проводити.

1-й крок. Визначення атак, ефект від реалізації яких перевищує витрати на їх проведення:

$$Tr_R^A = \left\{ Tr_i \mid \left(P_i^A - C_i^A \right) > 0 \right\} \forall Tr_i \in Tr \quad (2.12)$$

де Tr_R^A – множина потенційних загроз, реалізація яких ефективна для атакуючого;

Tr_i – загроза *i*-му інформаційного ресурсу;

P_i^A – оцінка вартості успішності реалізації атаки на *i*-й ресурс з боку атакуючого;

C_i^A – вартість проведення атаки на і-й ресурс з боку атакуючого;

2-й крок. Визначення напрямку захисту, яке забезпечує ефект вище, ніж витрати на їх забезпечення:.

$$Tr_C^D = \left\{ Tr_j \mid \left(P_i^D - C_i^D \right) > 0 \right\} \forall Tr_j \in Tr \quad (2.13)$$

де Tr_C^D – множина загроз, проти яких економічно доцільно вибудовувати захист;

P_i^D – оцінка вартості втрати і-го інформаційного ресурсу для сторони захисту;

C_i^D – вартість захисту і-го інформаційного ресурсу для сторони захисту;

3-й крок. Визначення коефіцієнтів важливості для атакуючих. Визначаються як частки виграшу від загальної суми виграшу, яка може бути отримана потенційно при реалізації всього комплексу загроз для нападників:

$$K_i^A = \frac{P_i^A - C_i^A}{\sum_{i=1}^{M}\left(P_i^A - C_i^A\right)}, \forall Tr_i \in Tr_R^A, M = \left|Tr_R^A\right|, \quad (2.14)$$

де K_i^A – рейтинговий коефіцієнт (важливості) реалізації загрози *i*-му інформаційного ресурсу;

M – потужність множини відібраних потенційно ефективних загроз для атакуючої сторони.

4-й крок. Визначення коефіцієнтів важливості для захисників. Визначаються як частки виграшу від загальної суми виграшу, яка може бути отримана потенційно при реалізації всього комплексу захисних заходів:

$$K_j^D = \frac{P_i^D - C_i^D}{\sum_{i=1}^{N}\left(P_i^D - C_i^D\right)}, \forall Tr_j \in Tr_C^D, N = \left|Tr_C^D\right|, \quad (2.15)$$

де K_j^D – рейтинговий коефіцієнт (важливості) вибудовування захисту *j*-го інформаційного ресурсу.

5-й крок. Відбір критичних загроз на основі оцінки добутку коефіцієнтів важливості атакуючого і нападника виявляється максимальним:

$$Tr_l = \arg\max_{\forall Tr_l \in Tr_C^D} K_l^D \cdot K_l^A. \quad (2.16)$$

2.3 Висновки до розділу 2

Аналіз сучасних підходів щодо аномальної роботи формує потребу використання універсального класифікатору загроз, який повинен забезпечити врахування ознак гібридності та синергізму. Основною відмінністю пропонованого підходу є можливість враховувати не тільки думку експертів,

але і формувати об’єктивну оцінку і комплексування загроз, яка дозволяє формувати їх синергетичний ефект, і гибридность. Крім цього, використання моделі ISO в класифікаторі дозволяє “виявити” критичні місця в інфраструктурі не тільки кіберфізіческіх систем, але і в синтезі з Інтернет-технологіями кіберпростору і технологіями “G”.

Такий підхід, інтуїтивно дозволяє зосередиться на слабких місцях комплексного захисту з урахуванням економічних витрат в умовах малого фінансування і “рентабельності” здійснення атаки з боку зловмисників.

3. МОДЕЛЮВАННЯ ПРОЦЕСУ КІБЕРАТАКИ

3.1 Класифікація моделі порушника

Оцінка рівня загроз неможлива без оцінки можливостей самих нападників (зловмисників, кіберзлочинців і т.д.). Від їх “компетентності”, обчислювальних ресурсах, тимчасових характеристиках, їх мотивованості багато в чому залежить можливість реалізації загрози. Таким чином, невід’ємною частиною аналізу загроз є розробка моделі “небезпеки” порушника. Такий підхід дозволяє сформувати безлічі загроз в залежності від можливостей нападників, сформувати безліч можливих впливів, оцінити стан превентивних захисних засобів. Для формування вагових коефіцієнтів “небезпеки” порушників пропонується використовувати таку класифікацію порушників, рис. 5, при цьому ІККС можуть бути як частиною CPS, так і складати окрему кіберфізіческую систему. Основою категорії 5 (рис. 3.1) використана таксономія в роботі [37].

Таким чином, запропонована класифікація дозволяє ввести елементи безлічі категорій зловмисників $L_i^{del} \in \left\{ L_i^{del} \right\}$: L_1^{del} – користувачі ICS (CPS); L_{11}^{del} – керівництво ICS (CPS), L_{12}^{del} – службовці ICS (CPS), L_{13}^{del} – користувачі “в зоні ризику”; L_2^{del} – експлуатаційний персонал; L_3^{del} – технічний допоміжний персонал; L_4^{del} – особи, які не є співробітниками ICS (CPS), L_5^{del} зовнішні зловмисники: L_{51}^{del} – кібертерористи, L_{52}^{del} – спецслужби, L_{53}^{del} – хакери, L_{54}^{del} – кіберзлочинці, L_{55}^{del} – конкуренты, L_{56}^{del} – кримінал, L_{57}^{del} – вандали.

Формальну модель "небезпеки" порушника визначимо з урахуванням пропозицій авторів [32–34]:

$$G_{CPS}^{ICS} = \left\{ aid_i, \beta_i^{ICS} \in \left\{ \beta_i^{ICS} \right\}, \beta_i^{CPS} \in \left\{ \beta_i^{CPS} \right\}, p_{rj}, r_{\text{motiv}}, T \right\}, \quad (3.1)$$

де $aid_i \in \{aid\}$ – ідентифікатор порушника (категорія порушника), $\beta_i^{ICS} \in \left\{\beta_i^{ICS}\right\}$ – ваговий коефіцієнт можливостей порушника для ICS, $\beta_i^{CPS} \in \left\{\beta_i^{CPS}\right\}$ – ваговий коефіцієнт можливостей порушника для CPS, T – час успішної реалізації загрози, p_{rj} – ймовірність реалізації хоча б однієї загрози j-му активу, i – загроза, $\forall i \in n$, n – количество угроз, j – інформаційний ресурс (актив), $\forall j \in m$, m – кількість активів; r_{motiv} – ймовірність мотивації зловмисника до реалізованої загрози.

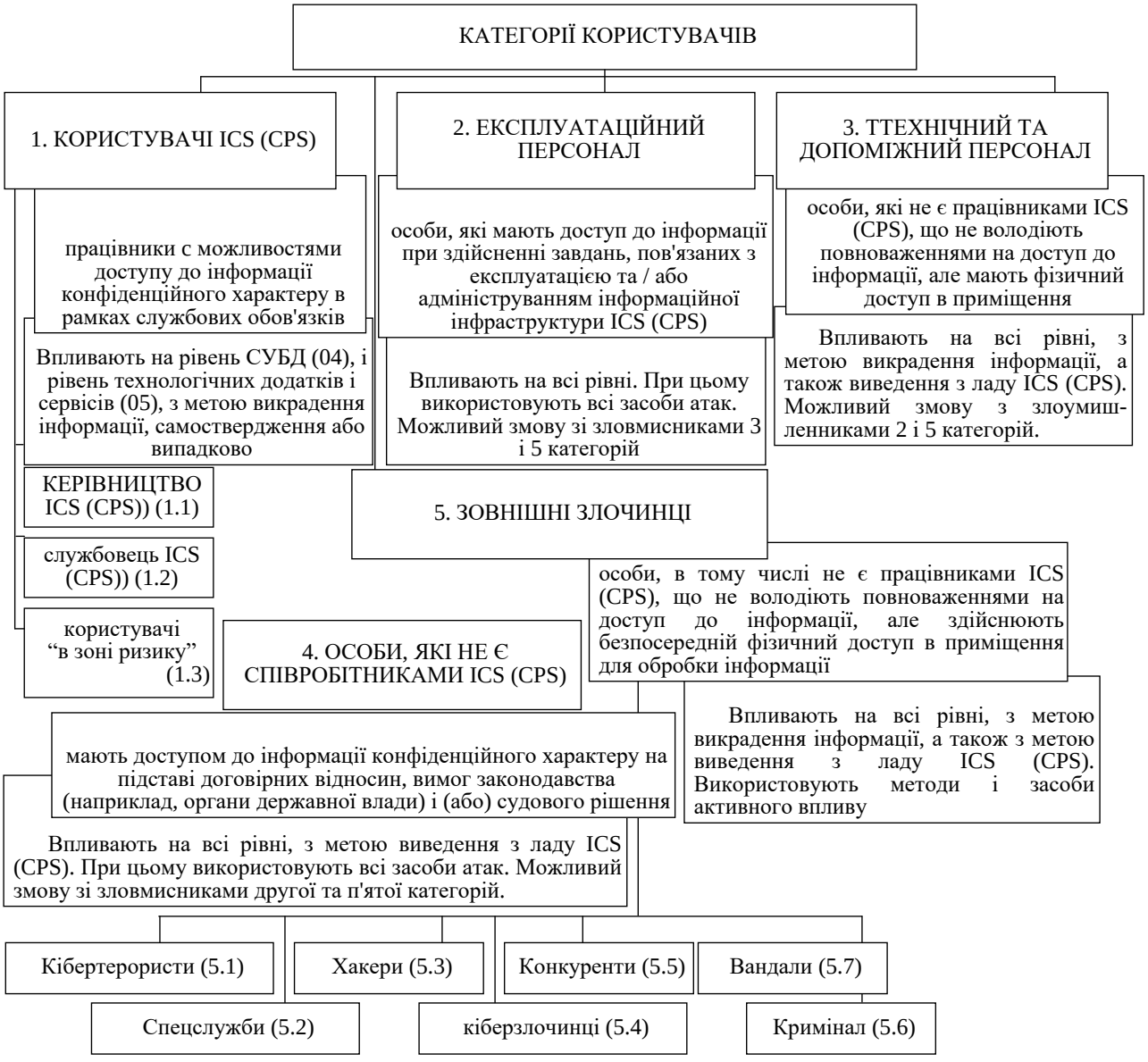


Рисунок 3.1 – Класифікація зловмисників

Аналіз класифікації зловмисників, дозволяє сформувати експертну оцінку і отримати ваговий коефіцієнт можливості реалізації загроз (*i*-ї загрози).

Ваговий коефіцієнт “небезпеки” зловмисника визначимо за формулою:

$$\gamma_{ICS}^{CPS} = \frac{1}{N}\sum_{i=1}^{N}\gamma_{ICS\ i}^{CPS},\ \text{где}\ \gamma_{ICS\ i}^{CPS} = \left(\beta_i^{ICS} \cup \beta_i^{CPS}\right) \times p_{rj} \times r_{motiv}, \qquad (3.2)$$

де $\beta_i^{ICS} = W_{cp}^{ICS} \cap W_{cash}^{ICS} \cap T^{ICS}$, $\beta_i^{CPS} = W_{cp}^{CPS} \cap W_{cash}^{CPS} \cap T^{CPS}$ – вагові коефіцієнти можливостей порушника для ICS і CPS (відповідно), W_{cp}^{ICS} (W_{cp}^{CPS}) – обчислювальні ресурси порушника (1 – необмежені ресурси кібертерористів, 0,75 – ресурси держави (спецслужб), 0,5 – ресурси кіберзлочинців, 0,25 – ресурси криміналу, конкурентів, хакерів, 0,001 – ресурси вандалів;T^{ICS} (T^{CPS}) – час виконання загрози (1 – загроза реалізується кожег день, 0,75 – загроза реалізується раз в тиждень, 0,5 загроза реалізується раз в місяць, 0,25 – загроза реалізується раз в рік, 0,001 – необмежений час);

W_{cash}^{ICS} (W_{cash}^{CPS}) – економічні можливості нападників (1 – необмежені ресурси кібертерористів, 0,75 – ресурси держави (спецслужб), 0,5 – ресурси кіберзлочинців, 0,25 – ресурси криміналу, конкурентів, хакерів, 0,001 – ресурси вандалів.

У табл. 3.1 наведено вихідні дані критеріїв і показників експертної оцінки його знаходження.

Таблиця 3.1 –Вихідні дані критеріїв і показників експертної оцінки вагового коефіцієнта “небезпеки” порушника

Категорія	показники оцінки вагового коефіцієнта							
	$\beta_i^{ICS} \in \{\beta_i^{ICS}\}$			$\beta_i^{CPS} \in \{\beta_i^{CPS}\}$			p_{rj}	r_{motiv}
	W_{cp}^{ICS}	T^{ICS}	W_{cash}^{ICS}	W_{cp}^{CPS}	T^{CPS}	W_{cash}^{CPS}		
критична	1	1	1	1	1	1	1	1
висока	0,75	0,75	0,75	0,75	0,75	0,75	0,75	0,75
середня	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5
низькка	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25
дуже низька	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,001

3.2 Розробка методики визначення категорії порушника

Аналіз табл. 3.1 дозволяє сформувати таблицю відповідності категорії зловмисників і елементів інфраструктури ICS, CPS, і дозволяє в зворотному порядку визначити категорію зловмисника.

Аналіз класифікації зловмисників дозволяє сформувати безліч {Hj}, що визначає рівні впливу на ICS (CPS):

- рівень технічних каналів (H0);
-фізичний рівень стека протоколів TCP / IP (H1);
- канальний рівень стека протоколів TCP / IP (H2);
- мережевий рівень стека протоколів TCP / IP (H3);
- транспортний рівень стека протоколів TCP / IP (H4);
- рівень шкідливого впливу (H5);
- рівень закладних пристроїв (H6);
- прикладний рівень стека протоколів TCP / IP (H7);
- рівень системи захисту інформації (H8).

У табл.4 визначено співвідношення категорій порушника і рівнів їх впливу.

Таблиця 3.2 – Співвідношення категорій порушника і рівнів їх впливу

категорія		рівні впливу							
	H_0	H_1	H_2	H_3	H_4	H_5	H_6	H_7	H_8
L_1^{del}	0	0	0	0	0	0	0	1	1
L_{11}^{del}	1	1	0	0	0	0	1	1	1
L_{12}^{del}	0	0	0	0	0	0	0	1	1
L_{13}^{del}	0	0	0	0	0	0	0	1	1
L_2^{del}	1	1	1	1	1	0	1	0	1
L_3^{del}	0	0	0	0	0	0	1	1	0
L_4^{del}	1	1	1	1	0	1	1	0	0
L_5^{del}	1	1	1	1	1	1	1	1	0
L_{51}^{del}	1	1	1	1	1	1	1	1	1
L_{52}^{del}	1	1	1	1	1	1	1	1	1
L_{53}^{del}	1	1	1	1	0	1	1	0	0
L_{54}^{del}	1	1	1	1	1	1	1	0	1
L_{55}^{del}	1	1	1	1	0	1	1	0	0
L_{56}^{del}	1	0	0	0	0	1	1	0	0
L_{57}^{del}	1	0	0	0	0	1	0	0	0

Таким чином, для визначення категорії зловмисника на основі аналізу табл.3.2, класифікатора загроз пропонується методика визначення категорії порушника, яка зводиться до наступного алгоритму;

1. Вибирається ознака класифікації з множини $\{H\}$, що визначає рівні впливу на ICS (CPS);

2. Визначається кортеж загрози за пропонованим класифікатором

3. Формується вектор V_{ij} на основі кортежу і сформованого безлічі критичних загроз (на основі оцінки добутку коефіцієнтів важливості атакуючого і нападника).

4. За допомогою вектора V_{ij} визначається максимальна категорія порушника відповідно до табл. 4, починаючи з порушника першої категорії (L_1^{del}).

Таким чином, на основі запропонованої методики будується перелік критичних загроз для кожної категорії порушників.

При виключення суб'єктів атак з числа потенційних порушників можна зменшити максимальну категорію порушника, а, отже, і кількість критичних загроз.

Оцінка показників ступеня небезпеки зловмисників і ступеня реалізації захисних заходів

Оцінка показників ступеню небезпеки зловмисників і ступеня реалізації заходів захисту визначимо набори зважених метрик, котрі набувають значення в інтервалі [0; 1]. Метрика характеризує ступінь відповідності ознаки зловмисника чи захисний засіб заданому цільового значення.

Для оцінки ступеню “небезпеки” порушника використовуємо запропоновану модель $G_{CPS}^{ICS} = \left\{ aid_i, \beta_i^{ICS} \in \left\{ \beta_i^{ICS} \right\}, \beta_i^{CPS} \in \left\{ \beta_i^{CPS} \right\}, p_{rj}, r_{\text{motiv}}, T \right\}$. Для описання множини характеристик використовуємо індекс h: $G_{CPS_h}^{ICS}$, де $(\{h\}_1^{G_{CPS}^{ICS}})$.

Обозначимо j – послуги безпеки, как для ICS, так і для CPS. Основні послуги безпеки: C – показник конфіденційності; I – показник цілісності; A – показник доступності; Au – аутентичність, Aff – причетність. Таким чином, формується кортеж послуг безпеки $j = \{C, I, A, Au, Aff\}.$ Позначимо через і поточний номер зловмисника $(\{i\}_1^L)$, через k – потоковий номер експерта, котрий проводив оцінку $(\{k\}_1^K)$, L– кількість зловмисників, К – кількість

експертів, w_{kih}^{j} – експертна оцінка k-го експерта для h-ї характеристики i-го зловмисника для j-ї послуги безпеки..

Середній показни оцінок всіх експертів по всій сукупності характеристик всіх зловмисників, в тому числі для j-ї послуги безпеки буде виглядати так:

$$w^{j} = \frac{1}{KLG_{CPS}^{ICS}} \sum_{k=1}^{K} \sum_{i=1}^{L} \sum_{h=1}^{G_{CPS}^{ICS}} \gamma_{ICS\ kih}^{CPS\ j} \times w_{kih}^{j}, \tag{3.3}$$

де $\gamma_{ICS\ kih}^{CPS\ j}$ – ваговий коефіцієнт h-ї метрики для j-ї послуги для i-го зловмисника.

Нормування вагових коефіцієнтів: $\sum_{k=1}^{K} \sum_{i=1}^{L} \sum_{h=1}^{G_{CPS}^{ICS}} = 1$.

Таким самим способом ми можемо описувати ступінь захищеності ТСЗІ. Для цього використовуємо величезну кількість характеристик B = {cryptographic resistance, стійкість ТСЗІ (Cr), обсяг ключових даних (Key data amount, Sc), складність виконання прямого і зворотного криптографічного перетворення (шифрування / розшифрування) (encryption / decryption of data, OE)}.

З вище вказаної інформації випливає така множина використовуваних характеристик ТСЗІ: B = {Cr, Sc, OE}. Щоб описати такі множини характеристик застосовується індекс g: Bg, де $(\{g\}_1^B)$. Для зручності обчислення вводимо таке позначення w_{kg}^{j} – це буде показник оцінки характеристики ТСЗІ – g, експертом k для j-ї послуги безпеки, при незалежності дій зловмисника та ступені захисту системи.Середнє значення оцінок всіх експертів, що реалізують заходи по захисту j-ї послуги безпеки набуває вигляду:

$$\psi^{j} = \frac{1}{KB} \sum_{k=1}^{K} \sum_{g=1}^{B} \left(\beta_{kg}^{j} \times w_{kg}^{j} \right), \tag{3.4}$$

де β_{kg}^{j} – ваговий коефіцієнт g-ї метрики j-ї послуги безпеки для k-го експерта. Нормування коефіцієнтів ваги: $\sum_{k=1}^{K}\sum_{g=1}^{B}\beta_{kg}^{j}=1$.

Щоб відбувся процес кореляції між характеристиками захищених систем ти ступенем “небезпеки" зловмисника, між множинами G_{CPS}^{ICS} та B. Використуємо матрицю M розмірністю [G_{CPS}^{ICS} × B], яка ще має і іншу назву “матриця парних порівнянь”. При g-та захисна характеристика Bg взагалі блокує h-ту властивість порушника (або загрозу, що реалізується цим порушником), то Mhg = 1, в противному випадку Mhg = 0 Можливі також проміжні величини, коли загроза / характеристика зловмисника закрита не повністю. Отже, $\left\|M_{hg}\right\|$ – матриця коефіцієнтів, котрі пов'язують між собою загрози / характеристики зловмисника з захисними заходами системи безпеки.

Тоді нові значення оцінок заходів захисту з використанням матриці M можна записати:

$$\left\|w_{kg}^{j}\right\|_{cor}=\left\|M_{hg}\times w_{kg}^{j}\right\|. \tag{3.5}$$

Тоді

$$\psi^{j}=\frac{1}{KB}\sum_{k=1}^{K}\sum_{g=1}^{B}\left(\beta_{kg}^{j}\times\left\|w_{kg}^{j}\right\|_{cor}\right). \tag{3.6}$$

Розширення класифікатора за рахунок введення економічних показників вартості здійснення атаки і вартості заходів протидії їй дозволяють отримати інтегральну оцінку безпеки системи. Для оцінки безпеки будемо використовувати відносні одиниці таким чином, що 1 буде відповідати максимальному рівню безпеки, який забезпечується системою безпеки в цілому, а 0 – відповідає ситуації, коли система безпеки не забезпечує захист жодного з ресурсів.

Визначення ймовірності реалізації загрози при граничні можливості захисту *A* і граничні можливості нападу *B* буде визначатися різницею *F (B) – F (A)*, де *A* – граничний рівень можливостей сторони захисту, *B* –

граничний рівень можливостей реалізації атаки боку нападу, *F(x)* – щільність ймовірності випадкової величини *x*.

Рівень безпеки визначимо як частку тих ресурсів, які захищені від кібератак. Легко бачити, що ця величина може бути визначена наступним чином:

$$S = F(B) - F(A) = \int_{-\infty}^{B} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} dt - \int_{-\infty}^{A} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} dt. \quad (3.7)$$

Графічне представлення поточного рівня безпеки при зміні можливостей сторін кіберконфлікта (відносні величини), наведені на рис. 3.2.

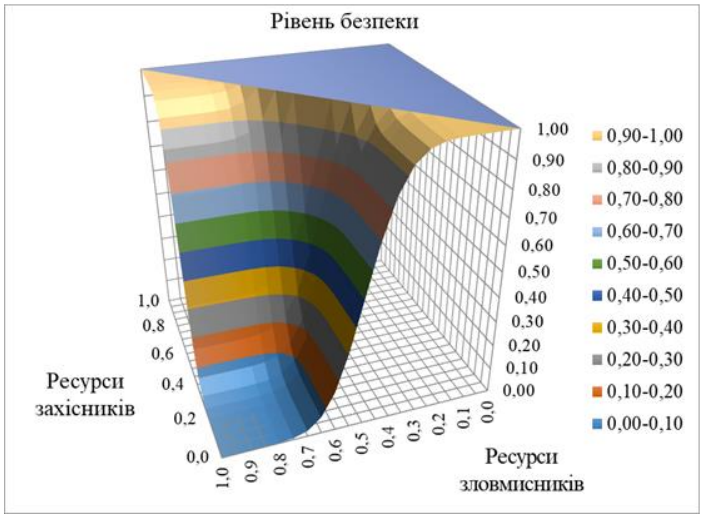


Рисунок 3.2 – Рівень безпеки в залежності від співвідношення ресурсів

Таким чином, наведені вирази (3.1–3.7) дозволяють на основі запропонованого класифікатора загроз, моделі “небезпеки” зловмисника, методики визначення категорії порушника, визначити безліч критичних загроз, критичні точки елементів інфраструктури ICS / CPS (CCIS), превентивні заходи і рівень безпеки системи в умовах недофінансування галузі безпеки, з урахуванням синергії і гибридности сучасних загроз.

Розширення класифікатора шляхом запровадження економічних показників вартості здійснення атаки/теракту та вартості заходів протидії їй дозволяють отримати інтегральну оцінку безпеки системи. Для оцінки безпеки застосовуються відносні одиниці. Таким чином, 1 відповідає максимальному рівню безпеки, який забезпечується системою безпеки в цілому, а 0 – відповідає ситуації, коли система

безпеки не забезпечує захист жодного з ресурсів. Додатковим показником може стати інтегрований показник якості обслуговування інформаційно-комунікаційної мережі, запропонований у роботі [37]. Для підвищення рівня безпеки (основних послуг безпеки) пропонується використовувати постквантові алгоритми на основі крипто-кодових конструкцій, запропоновані в роботах [1, 31, 37]. Пропоновані механізми інтегровано забезпечують необхідний рівень стійкості (2^{30}–2^{35} групових операцій), оперативності (швидкість криптоперетворень порівнянна з БСШ) та вірогідність ($P_{пом}$ 10^{-9}–10^{-12}) в умовах зростання обчислювальних ресурсів.

Для оцінки поточного стану ІБ, як правило, використовуються комплекси із систем виявлення/виявлення атак/відхилення від нормальної роботи та методик оцінки ризиків (рис. 3.3), які дозволяють сформувати якісну та/або кількісну оцінку поточного стану ІБ. У табл. 3.3 наведено порівняльну оцінку з пропонованим підходом, який дозволяє уніфікувати не тільки математичний апарат для отримання оцінки ІБ, але й значно спростити її проведення з урахуванням мінімізації фінансових витрат на ІБ.

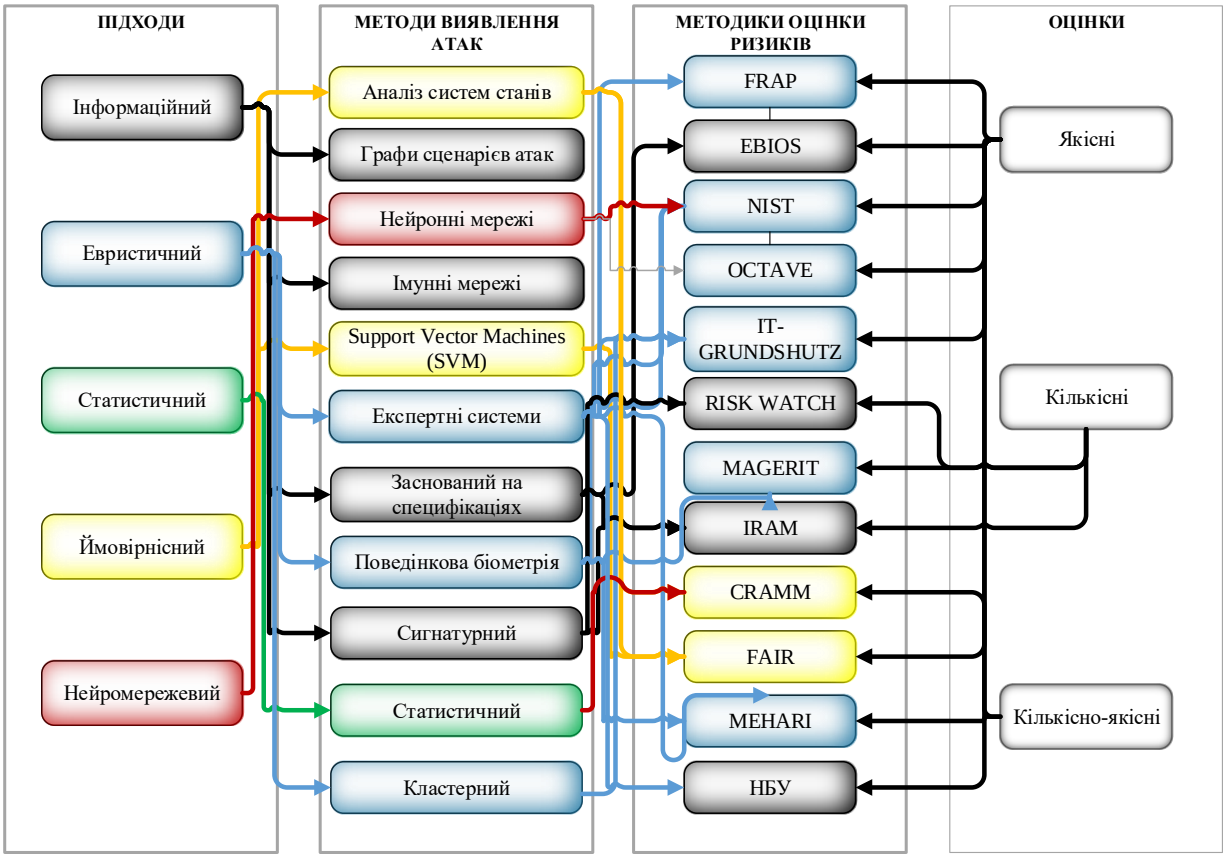


Рисунок 3.3 – Зв’язок методів виявлення атак з методиками оцінок ризиків

Таблиця 3.3 – Результати дослідження методик оцінки ризиків

Методика	Критерії								
	Якісна оцінка	кількісна оцінка	Комплексна оцінка	оцінка характеристик загроз		Економ. оптиміз ація	Оцінка викон. регулят орів	Ефект. превент ивних заходів	просто та розумі ння
				гібридні сть	синергі зм				
NIST	+	–	–	–	–	–	–	–	–
FAIR		–	+	–	–	–		+	+
EBIOS	+		–	–	–	–	–	+	–
MEHARI		–	+	–		–	–	–	–
OCTAVE	+	–	–	–	–	–	–	–	–
IT-GRUNDSHULTZ	+	–	–	–	–	–	–	+	–
IRAM	+	–	–	–	–	–	–	–	+/–
RISK WATCH	–	+	–	–	–	–		+	+
FRAP	+	–	–	–	–	–	–	–	–
CRAMM			+	–	–	–	–	+/–	+/–
MAGERIT	+	+	–	–	–	–	–	–	–
Запропонована методика	+	+	+	+	+	+	+	+/–	+

Проведений аналіз табл. 3.3 та рис. 3.3 показав, що для отримання оцінки поточного стану практично немає єдиного підходу. Кожен із представлених складається з комплексу систем та методик, у яких немає уніфікованого підходу до класифікації загроз. Як правило, використовуються відкриті бази, такі як KDD-99, CAPEC, CVE, які містять понад мільйон загроз без відповідної класифікації, що значно не дозволяє оперативно провести їх аналіз. Крім цього, загрози не класифікуються за механізмами безпеки, що не дозволяє враховувати їх комплексування, синергію та гібридність, що не дозволяє забезпечити об'єктивність їх оцінки та можливі збитки. Методики не дозволяють визначити взаємозв'язок між загрозами, інформаційними ресурсами, каналами зв'язку між

елементами інфраструктури ОКІ, визначити критичні точки між загрозами та засобами СЗІ, що дозволяє своєчасно визначити превентивні заходи захисту. Не одна з розглянутих систем та методик не дозволяє за загрозами визначити характеристику нападника, його можливості, що значно збільшує ризик несанкціонованого проникнення/злому СЗІ.

3.3 Висновки до розділу 3

На основі пропонованих моделей значно скорочуються вимоги до обчислювальних ресурсів для отримання поточного стану ІБ з урахуванням вимог міжнародних регуляторів та національних нормативних актів. Такий підхід дозволить проводити самооцінку стану ІБ, формувати превентивні заходи та СЗІ на основі аналізу критичних точок в елементах інфраструктури ГОМ, з урахуванням відповідних взаємозв'язків. Основними обмеженнями пропонованого підходу є формування уніфікованої бази загроз, їх оцінка експертами галузі кібербезпеки та/або інформаційної безпеки. Для забезпечення об'єктивності необхідна практична реалізація з подальшою апробацією в одній з областей ОКІ, що дозволить забезпечити практичну складову та оптимізувати формування превентивних заходів на основі запропонованої Концепції.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Показники ефективності та заходи щодо покращенню умов та охорони праці.

Результати дії заходів щодо поліпшення умов і охорони праці оцінюються за допомогою чотирьох груп показників: змін стану охорони праці, соціальних, соціально-економічних, економічних.

Зміни стану умов праці оцінюються за факторами:

а) зміна кількості машин і механізмів, виробничих будівель тощо, приведених у відповідність до вимог стандартів безпеки праці та інших нормативних актів;

б) поліпшення санітарно-гігієнічних показників, зменшення вмісту шкідливих речовин у повітрі; зниження рівнів шуму та вібрації, поліпшення освітленості тощо;

в) поліпшення психофізіологічних показників, зменшення фізичних і нервово-психічних навантажень, у тому числі монотонних умов праці;

г) поліпшення естетичних показників, раціональне компонування робочих місць і машин, упорядкування приміщень і території, поєднання кольорових відтінків тощо.

Зміни стану виробничого середовища за факторами оцінюються різницею абсолютних величин до і після запровадження заходів або досягнутих результатів з прогнозованими, а також порівнянням відносних показників, що характеризують ступінь відповідності тих чи інших факторів гранично допустимим концентраціям (ГДК), гранично допустимим рівням (ГДР) або заданим.

Комплексна оцінка змін стану умов праці виконується за показником приросту кількості робочих місць, на яких умови праці приведені у відповідність до нормативних вимог.

Соціальні результати заходів щодо поліпшення умов і охорони праці визначаються за наступними показниками:

а) збільшення кількості робочих місць, які відповідають нормативним вимогам (як у комплексі, так і за окремими факторами), та скорочення кількості працюючих у незадовільних умовах праці;

б) зниження рівня виробничого травматизму;

в) зменшення кількості випадків професійної захворюваності, пов'язаної з незадовільними умовами праці;

г) зменшення кількості випадків інвалідності внаслідок травматизму чи професійної захворюваності;

д) зменшення плинності кадрів через незадовільні умови праці.

Для оцінки соціальних результатів можуть також використовуватися інші показники (ступені задоволення працею та її престижності тощо).

Показники соціальної і соціально-економічної ефективності розраховуються як відношення величин соціальних або соціально-економічних результатів до витрат, необхідних для їх здійснення. Такі показники характеризують кількість умовних одиниць сукупного об'єму соціального чи соціально-економічного результату в розрахунку на одиницю витрат.

Правомірне також і обернене співвідношення суми витрат до соціального чи соціально-економічного результату. У цьому випадку оцінюється у грошовій формі одиниця отриманого соціального чи соціально-економічного результату.

Показники соціальної і соціально-економічної ефективності використовуються для визначення фактичного рівня питомих витрат, необхідних для зменшення кількості працюючих у незадовільних умовах праці, зниження рівня травматизму, захворюваності, плинності кадрів на різних підприємствах та в економіці в цілому.

Економічні результати заходів щодо поліпшення умов і охорони праці виражаються у вигляді економії за рахунок зменшення збитків внаслідок аварій, нещасних випадків і професійних захворювань в економіці в цілому та на кожному підприємстві.

Макроекономічна оцінка соціально-економічних результатів заходів виконується з урахуванням:

а) всіх соціальних та економічних результатів у різних сферах виробництва;

б) фактора часу в розрахунках витрат і результатів.

Економічне обґрунтування заходів щодо поліпшення умов і охорони праці виконується при умові досягнення соціального ефекту за допомогою порівняння економічних результатів цих заходів з витратами, необхідними для їх здійснення шляхом розрахунку двох основних показників: економічного ефекту та економічної ефективності.

Економічний ефект визначається як різниця між річними економічними результатами заходів та витратами на їх здійснення. Він розраховується в усіх випадках економічного обґрунтування заходів і використовується:

- для обґрунтування очікуваного (запланованого) ефекту наукових і проектних рішень для поліпшення умов і охорони праці;

- для вибору найбільш ефективного з двох чи кількох варіантів, що відрізняються за своєю дією на показники виробничого середовища, а також за своїми соціальними, соціально-економічними чи економічними результатами;

- для економічної оцінки фактично здійснених заходів з метою встановлення розмірів матеріального заохочення працівників підприємств, наукових і проектно-конструкторських організацій за поліпшення умов і охорони праці.

Економічна ефективність визначається як відношення економічних результатів до витрат. Вона розраховується в усіх випадках економічного обґрунтування і використовується з метою:

- визначення макроекономічних витрат на поліпшення умов і охорони праці;

- оцінки динаміки ефективності цих витрат;

- порівняльного аналізу ефективності витрат на різних підприємствах, у галузях народного господарства, регіонах;

- порівняння очікуваної (запланованої) і фактичної ефективності витрат.

Економічне обґрунтування заходів, які плануються на період, більший одного року, потребує врахування на ступних факторів:

- зміни стану виробничого середовища, зумовленого зростанням виробництва, впровадженням нової техніки і технологій, освоєнням нових видів продукції;

- зростання вимог до стану виробничого середовища;
- підвищення продуктивності й оплати праці;
- зміна вартості будівельно-монтажних робіт та обладнання.

Економічне обґрунтування заходів щодо поліпшення умов і охорони праці здійснюється в наступному порядку:

- визначається набір необхідних вихідних даних про зміну стану виробничого середовища на базі досягнутих соціальних результатів і техніко-економічних показників підприємства за базовим і впроваджуваним варіантами;
- визначаються витрати на реалізацію заходу;
- розраховується соціальна і соціально-економічна ефективність;
- розраховується економічний ефект за результатами здійснення заходу.

4.2 Естетичне оформлення робочого місця оператора ПК, верстату, установки.

Робоче місце - це частина простору, в якому інженер здійснює трудову діяльність, і проводить велику частину робочого часу. Робоче місце, добре пристосоване до трудової діяльності інженера, правильно і доцільно організоване, у відношенні простору, форми, розміру забезпечує йому зручне положення при роботі і високу продуктивність праці при найменшому фізичному і психічному напрузі.

При правильній організації робочого місця продуктивність праці інженера зростає з 8% до 20%. Згідно ГОСТ 12.2.032-78 конструкція робочого місця і взаємне розташування всіх його елементів повинне відповідати антропометричним, фізичним і психологічним вимогам. Велике значення має також характер роботи.

До чинників, які формують рівень естетичної свідомості, традиційно відносять естетичне почуття, естетичний смак, естетичний ідеал. Тобто йдеться про формування певної культури, зокрема естетичної. Естетична культура — це сукупність естетичних цінностей, які існують в суспільстві, способи і засоби їх створення та освоєння, хоча сама естетика є наукою про становлення чуттєвої культури людини.

Принцип службового дизайну — своєрідний естетичний феномен духовної культури працівника — нині особливо актуальний.

Дизайнерська активність пов'язана з прагненням наблизити естетику українського дизайну до рівня світових взірців. З огляду на це набуває значення вміння працівника застосовувати у своїй роботі закони колористики. Про це вміння свідчить насамперед оформлення службового кабінету, в якому працівникові доводиться перебувати іноді чи не половину доби. Відомо, що кольори по-різному впливають на людину, позначаються на її самопочутті, емоціях, поведінці, навіть можуть призводити до незрозумілої, на перший погляд, зміни пульсу та кров'яного тиску. А знання законів колористики допомагає уникнути стресових ситуацій. Отже, колір, його гармонійність є чинником, стимулятором духовного здоров'я і взагалі окрасою життя. Тому робоче місце, що враховує особисті риси, темперамент працівника, й не порушує природної кольорової гармонії, активізує виконання службового обов'язку.

Багатогранний зміст естетичної культури виявляється в її функціях, основними з яких є: формування естетичних принципів діяльності, подолання стандартного мислення, наповнення і систематизація досвіду.

Продуктивність праці людини значною мірою залежить від елементів зовнішнього оформлення середовища, в якому вона працює. Отже, такі елементи естетичного оформлення виробничого середовища, як зовнішній вигляд приміщення і знарядь праці, їх кольорова гама, наявність квітів в інтер'єрі та ін. також потрібно враховувати при організації робочого місця.

Важливим моментом є також раціональне розміщення на робочому місці документації, канцелярських товарів, що повинно забезпечити людині зручну

робочу позу, найбільш економічні руху і мінімальні траєкторії переміщення працюючого і предмета праці на даному робочому місці.

Створення сприятливих умов праці і правильне естетичне оформлення робочих місць має велике значення, як для полегшення праці, так і для підвищення його привабливості, позитивно впливає на продуктивність праці. Забарвлення приміщень і меблів повинна сприяти створенню сприятливих умов для зорового сприйняття, гарного настрою. У службових приміщеннях, в яких виконується одноманітна розумова робота, що потребує значної нервової напруги і великого зосередження, фарбування повинна бути спокійних тонів - малонасичені відтінки холодного зеленого або блакитного кольорів.

ВИСНОВКИ

1. Проведено аналіз визначення безпеки інформаційних ресурсів об'єктів критичної інфраструктури, основних механізмів та процедур для побудови моделі, що забезпечує безпеку ІР ОКІ, що базується на основі синергетичного підходу. Деталізовані такі характеристики безпеки об'єктів критичної інфраструктури як доступність, цілісність, конфіденційність та безпека. Введені визначення були покладені в основу вирішення наступних завдань. Проаналізований класифікатор загроз, який систематизує загрози, формує єдину базу загроз ОКІ, визначити синергетичний ефект та гібридність загроз, їх вплив не лише на складові безпеки, а й на елементи інфраструктури ОКІ. Такий підхід дозволяє не лише сформувати превентивні заходи, а й визначити можливості терориста-виконавця.

2. Проаналізована концепція моделювання структури та функціонування системи безпеки об'єктів критичної інфраструктури. В основу концепції покладено різноманіття моделей різних класів та рівнів, що використовуються тепер для моделювання як критичних інфраструктур, так і реалізації загроз різної природи та спрямованості на об'єкти критичної інфраструктури. Як моделі, що лежать в основі концепції моделювання, розглядалися такі: економічні, системно-динамічні, поведінкові теоретико-ігрові, графові та мережеві, агентно-орієнтовані, фізичні та геопросторові.

3. Сформовані моделі реалізації терористичного акту та ступеня захищеності кіберсистеми об'єкта критичної інфраструктури. Оцінки комплексного (ешелонного) захисту об'єкта критичної інфраструктури запропоновано формувати на основі ієрархічної структури синтезу систем захисту, Інтернет-технологій та комп'ютерних мереж із засобами захисту інформації на основі мобільних технологій. Такий підхід дозволяє сформувати синергетичну модель загроз об'єктам критичної інфраструктури з урахуванням впливу терористів на її елементи. Розроблено методику визначення категорії терориста-виконавця, в основі якої лежить аналіз формованої таблиці

взаємозв'язку категорії терористів-виконавців та елементів інфраструктури. Це дозволяє попередньо визначити категорію зловмисника щодо впливу на CIF та його можливості щодо проведення теракту. Аналіз рівня інфраструктури CIF та категорій терористів-виконавців дозволяє сформувати безліч рівнів впливу на CIF. На основі запропонованої методики визначається перелік критичних загроз кожної категорії порушників.

4. Сформовано методику оцінки рівня захищеності об'єктів критичної інфраструктури. В основі оцінювання лежить підхід до формування синергетичної моделі загроз, категорії зловмисників, їх цілі та можливості. Отримана в результаті аудиту оцінка захищеності CIF дозволяє визначити найцінніші інформаційні активи та ефективність використовуваних засобів для їхнього захисту. Отримані рішення дозволяють оцінити ступінь відповідності системи СЗІ CIF вимогам до захисту та рівня захищеності регуляторів, виявити найуразливіші місця та виробити рекомендації щодо підвищення захищеності CIF.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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.
2. Гандзюк М. П. Основи охорони праці: підручник. 3-є вид. [за ред. М. П. Гандзюка] / М. П. Гандзюк, Є. П Желібо, М. О.Халімовський. – К. : Каравела, 2006. – 392 с.
3. Постанова НБУ28.09.2017 № 95, “Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України”, [Электроний ресурс]. Доступно : http://zakon2.rada.gov.ua/laws/show/en/v0095500-17/page.
4. Д. Слободенюк, “Банковские технологии, Средства защиты информации в банковских системах”, [Электронный ресурс] Доступно: http://www.arinteg.ru/about/publications/press/sredstva-zashchity-informatsii-v-bankovskikh-sistemakh-131107.html
5. Р. В. Грищук, та Ю. Г. Даник. *Основи кібернетичної безпеки: Монографія* /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016
6. Е. В. Иванченко, и В. А. Хорошко, “Тенденции развития кибертерроризма”, *МНПК “Современные информационные и электронные технологии”*, Одесса, с. 105 – 106, 2014.
7. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. H.R. 3162.
8. ISO/IEC 27031:2011 Information Technology – Security Techniques – Guidelines for Information and Communication Technology Readiness for Business Continuity. [Online]. Available: http://www.iso.org/iso/ru/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44374
9. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534.
10. Доктрина інформаційної безпеки України, затверджено Указом Президента України від 25 лютого 2017 року № 47/2017. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/47/2017/paran2#n2.

11. Указ Президента України від 15 березня 2016 року № 96 “Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/96/2016/paran11#n11.

12. Р. В. Грищук, та Ю. Г. Даник, “Синергія інформаційних та кібернетичних дій”, *Труди університету. НУОУ*, № 6 (127), с. 132–143. 2014

13. В. Л. Бурячок, Р. В. Грищук, та В. О. Хорошко, під заг. ред. проф. В. О. Хорошка, *“Політика інформаційної безпеки”*, ПВП «Задруга»,. 2014.

14. Ю. Г. Даник та ін., “*Основи захисту інформації*” навч. пос., Житомир : ЖВІ ДУТ, 2015.

15. СНиП 2.09.04-87. Административные и бытовые здания. – М.: Стройиздат, 1995. – 18 с.

16. О. К. Юдін “Інформаційна безпека. Нормативно-правове забезпечення”, К. : НАУ, 2011.

17. І. С. Іванченко, В. О. Хорошко, Ю. Е.Хохлачова, та Д. В. Чирков під заг. ред. проф. В. О. Хорошка, *“Забезпечення інформаційної безпеки держави”*, К: ПВП “Задруга”, 2013.

18. О. Г. Корченко, О. Є. Архипов, та Ю. О. Дрейс, *“Оцінювання шкоди національній безпеці України у разі витоку державної таємниці”*, монографія, К: наук.-вид.центр НА СБУ України, 2014.

19. А. О. Корченко, Л. М. Скачек, та В. О. Хорошко, під заг. ред. проф. В. О. Хорошка, *“Банківська безпека”* підручник, К: ПВП “Задруга”, 2014.

20. С. Евсеев, Ю. Хохлачева, и О. Король, “Оценка обеспечения непрерывности бизнес-процессов в организациях банковского сектора на основе синергетического подхода, ч.1”, *Сучасна спеціальна техніка. Науково-практичний журнал*, № 1(48), с. 17 – 25. 2017.

21. С. Евсеев, Ю. Хохлачева, и О. Король, “Оценка обеспечения непрерывности бизнес-процессов в организациях банковского сектора на основе синергетического подхода, ч. 2”, *Сучасна спеціальна техніка. Науково-практичний журнал*, № 2(49), с. 10 – 17, 2017.

22. 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.

23. М. В. Старинський, “Щодо визначення поняття “банківська інформація” та виділення її видів”, [Електронний ресурс]. Доступно: uabs.edu.ua/images/.../K.../Starinskii_s_015.pdf. Дата звернення: Груд. 7.2017.

24. Р. В. Грищук, “Синтез систем інформаційної безпеки за заданими властивостями”, Вісник національного університету “Львівська політехніка”. Серія : Автоматика, вимірювання та керування : зб. наук. пр., ЛП, № 74, с. 271 – 276, 2012.

25. Р. В. Грищук, “Атаки на інформацію в інформаційно-комунікаційних системах”, Сучасна спеціальна техніка, №1(24), с.61 – 66. 2011.

26. Р. В. Грищук, і В. В. Охрімчук, “Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак”, Безпека інформації, Том 21, № 3, с. 276 – 282, 2015.

27. Ю. Г. Даник, Р. В. Грищук, “Синергетичні ефекти в площині інформаційного та кібернетичного протиборства”, Наук.-практ. конф. “Актуальні проблеми управління інформаційною безпекою держави”, Київ, 19 берез, 2015, с. 235 – 237.

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

29. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів національного банку України/ [Електронний ресурс]. Доступно: zakon.rada.gov.ua/laws/show/v0365500-11.

30. ДСТУ ISO/IEC 9594-8:2006 Інформаційні технології. Взаємозв’язок відкритих систем. Каталог. Частина 8. Основні положення щодо сертифікації відкритих ключів та атрибутів, [Електронний ресурс]. Доступно: http://document.ua/informaciini-tehnologiyi_-vzaemozvE28099jazok-vidkritih-sist-std10750.html.

31. Р. Грищук, та С. Євсеєв, “Методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах”, Науково-технічний журнал “Безпека інформації”, том 23, № 3, с. 204 – 214, 2017.

32. О. К. Юдін, С. С. Бучик, А. В. Чунарьова, та О. І. Варченко, “Методологія побудови класифікатора загроз державним інформаційним ресурсам”, Наукоємні технології, № 2 (22), с. 200 – 210, 2014.

33. О. К. Юдін, та С. С. Бучик, “Класифікація загроз державним інформаційним ресурсам нормативно-правового спрямування. Методологія побудови класифікатора”, Захист інформації, Том 17 (2), с. 108 – 116, 2015.

34. С. С. Бучик, “Теоретичні основи аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів”, Наукоємні технології, № 1 (29), с. 70 – 77. 2016.

35. С. С. Бучик, “Методологія аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів”, Захист інформації, №1 (18 , с. 81 – 89, 2016.

36. С. С. Бучик, “Методика експертного оцінювання функціональних профілів загроз державних інформаційних ресурсів”, Открытые информационные и компьютерные интегрированные технологии, № 70, с. 271 – 280, 2015.

37. Edited by Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.