ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

АНАЛІЗ ОЦІНКИ ПОТОЧНОГО СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ SIEM-СИСТЕМ

Керівник роботи:
д.т.н., проф. Євсеєв С.П.
Виконав:
студент 4-го курсу,
групи 6.04.125.012.18.1
Макаренко А.О

- Мета роботи:

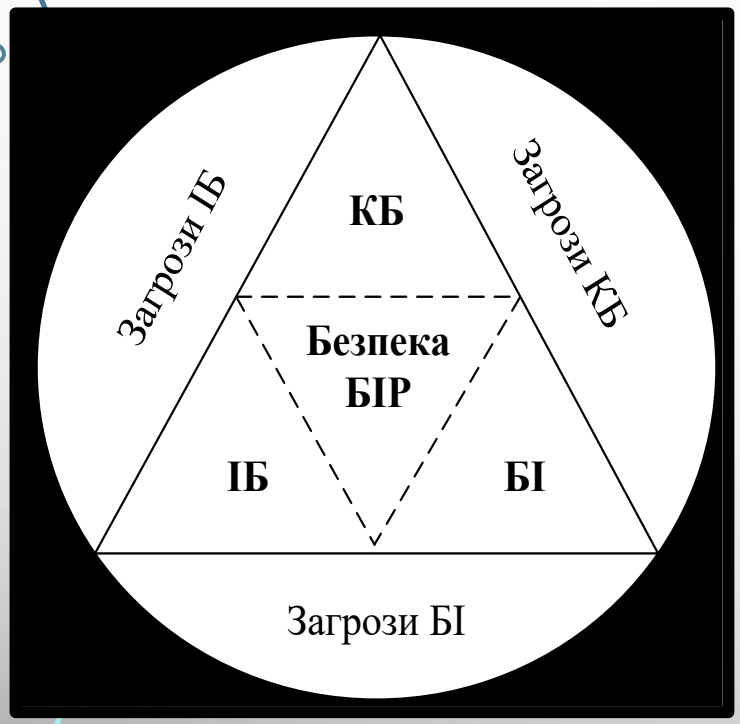
  Оцінювання ознак гібридності і синергізму загроз на банківську інформацію в автоматизованих банківських системах на основі запропонованого класифікатора, а також огляд сучасних рішень в сфері забезпечення безпеки БІР.
- Об’єкт дослідження

  Процес оцінювання реалізації загроз в банківському секторі.
- Предмет дослідження

  Аналіз сучасного стану банківських інформаційних ресурсів на основі SIEM-систем, формування ознак задля класифікації рішень в сфері SIEM. Проведення аналізу моделей, методів та систем БІР банківських організацій як складової систем з критичною кібернетичною інфраструктурою держави.
- Завдання:

  1) Проаналізувати сучасні загрози на АБС, програмно-апаратні (програмні засоби) поточного стану оцінки рівня безпеки організації банківського сектору.
  2)Аналіз принципів побудови, функцій SIEM.
  3) Аналіз практичних моделей забезпечення безпеки.
  4) Аналіз використання оцінки поточного рівня безпеки організаціях банківського сектору на основі синергетичної моделі загроз.
  5) Розробка веб-додатку, який дозволяє провести оцінку рівня поточного стану безпеки організації банківського сектору.

КЛАСИФІКАЦІЯ ЗАГРОЗ НА ОРГАНІЗАЦІЇ БАНКІВСЬКОГО СЕКТОРУ СИСТЕМ



Інформаційна безпека

Підключення до КС як активного ретранслятора

Копіювання і викрадення ПЗ

Несанкціоноване використання інформації підвищеного рівня секретності

Витяг інформації з статистичних БД на основі зв'язків між секретною та несекретною інформацією

Створення помилкових тверджень про отримання платіжних документів

Несанкціоноване введення даних

Несанкціоноване використання інформації високого рівня секретності

Перехоплення електромагнітного випромінювання від дисплеїв

Внесення змін до даних та програми для підробки і фальсифікації фінансових документів

Інформаційна безпека

Фішинг

Фармінг

Скрімінг

Телефонний фішинг

Безпека інформації

Копіювання даних з терміналів

Копіювання даних з обладнання і магнітних носіїв

Відмова абонента від факту прийому (передачі) або створення помилкових відомостей про час прийому (передачі) повідомлень для зняття з себе відповідальності за виконання цих операцій

Зміна або знищення даних на магнітних носіях

Виявлення паролів при викраденні або візуальному спостереженні

Візуальне перехоплення інформації виведеної на екран дисплеїв або введення з клавіатури для виявлення паролів, ідентифікаторів і процедур доступу

Нейролінгвістичне програмування (НЛП)

Віртуальне викрадення

Виявлення паролів користувачів

Несанкціоноване перевищення повноважень на доступ

Знищення, модифікація і блокування інформації

Використання програмних засобів для подолання захисних можливостей системи.

DoS - атаки

U2R - атаки

R2L - атаки

Кібернетична безпека

Безпека інформації

Back

Neptune

Land

Smurf

Pod

Teardrop

Buffer overflow

Rootkit

Loadmodule

Perl

Imap

Spy

Multihop

Ftp write

Xlock

Http tunnel

Nmap

Mscan

Satan

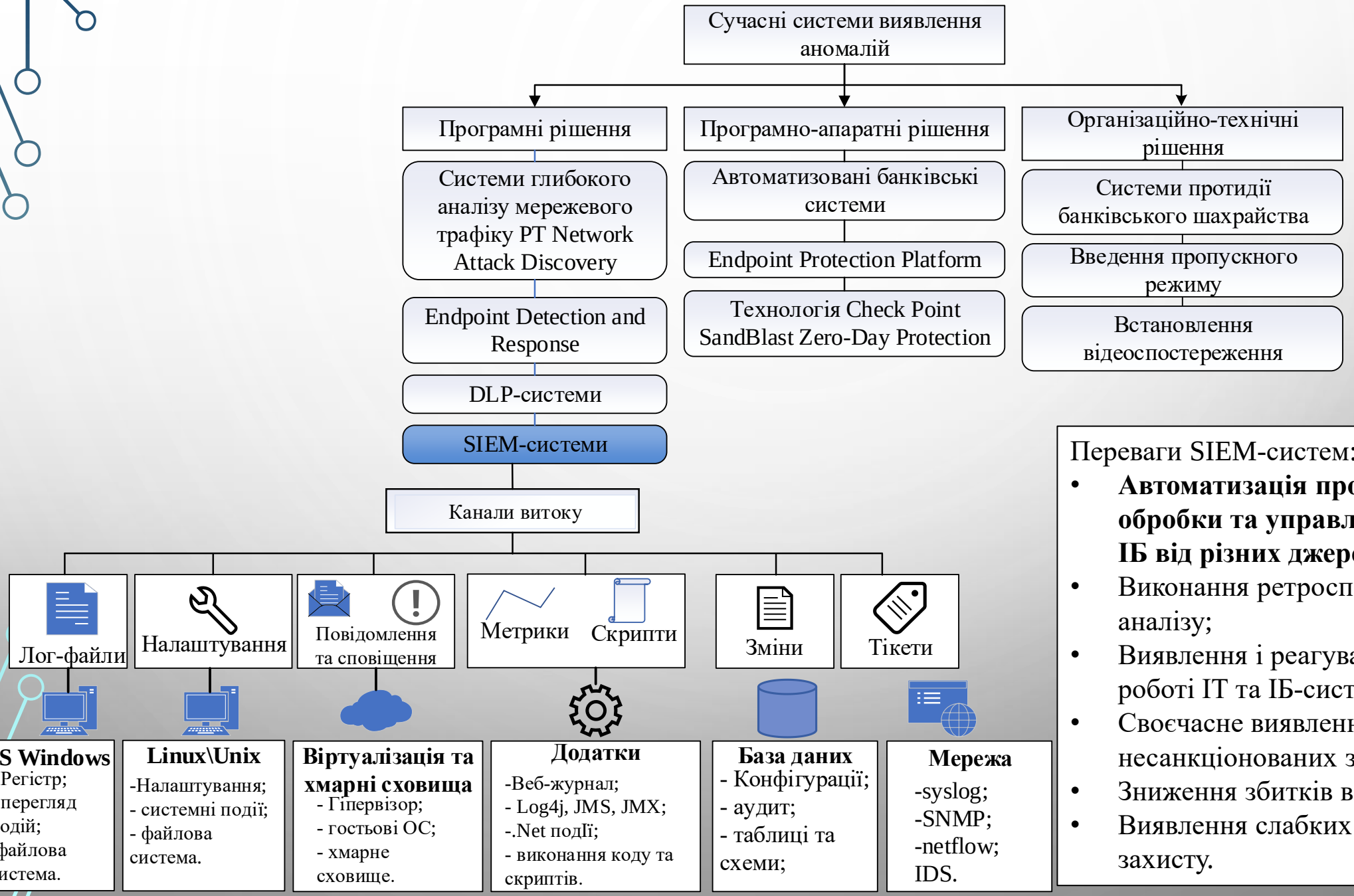
IP sweep

Port sweep

Saint

Кібернетичні атаки

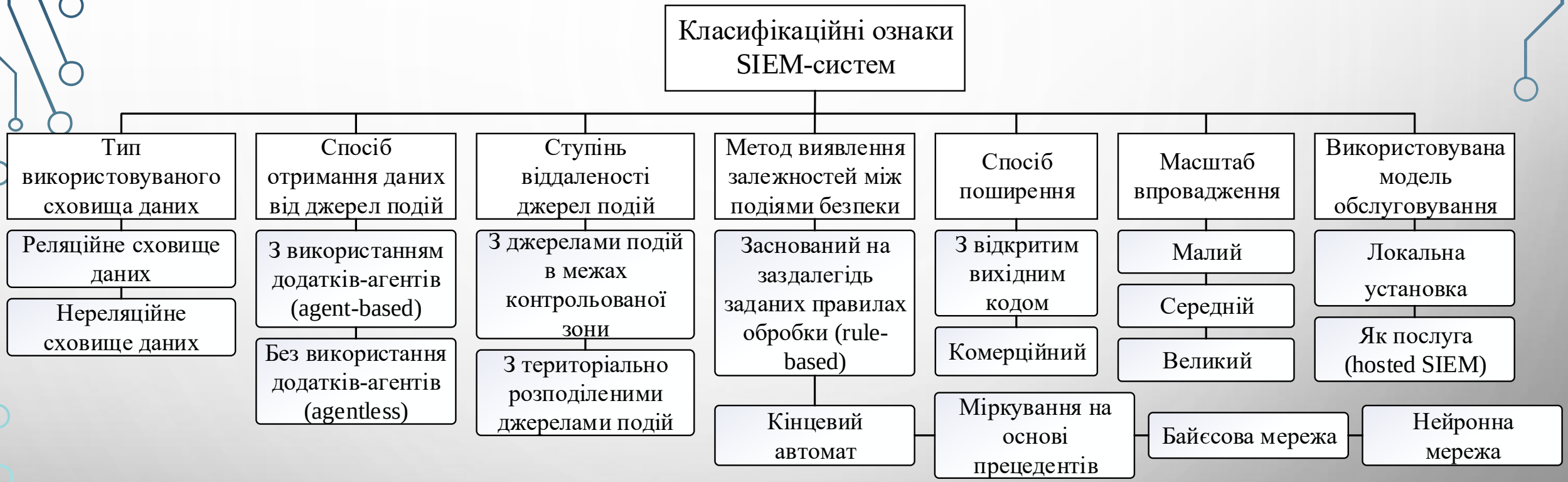
КЛАСИФІКАЦІЯ СИСТЕМ ВИЯВЛЕННЯ АНОМАЛІЙ В РОБОТІ



Переваги SIEM-систем:

- **Автоматизація процесів обробки та управління подіями ІБ від різних джерел;**
- Виконання ретроспективного аналізу;
- Виявлення і реагування на збої в роботі ІТ та ІБ-систем;
- Своєчасне виявлення несанкціонованих змін в ІС;
- Зниження збитків від кібер-атак;
- Виявлення слабких точок захисту.

КЛАСИФІКАЦІЯ SIEM-СИСТЕМ



СКЛАДОВІ ТА ФУНКЦІЇ SIEM-СИСТЕМ

SIEM система складається

Клієнтські агенти	Колектори на агентах	Сервери-колектори	Сервер-коррелятор	Сервер сховища
Вони встановлюються на інспектовану інформаційну систему яка збирає журнали подій на локальній машині і передає їх на сервер.	Представляють собою модулі або бібліотеки для розуміння того чи іншого журналу подій або системи.	Служать для попереднього збору подій від безлічі різних джерел.	Збирає інформацію від колекторів і агентів і обробляє її за правилами і алгоритмами, заданим в системі.	Необхідний для зберігання всієї корисної інформації.

Комплекс завдань SIEM

Збір,обробка та аналіза подій безпеки, що надходять в систему

Виявлення в реальному часу атак, порушень критеріїв і політики безпеки

Аналіз та управління ризиками на основі об'єктивних і експертних оцінок

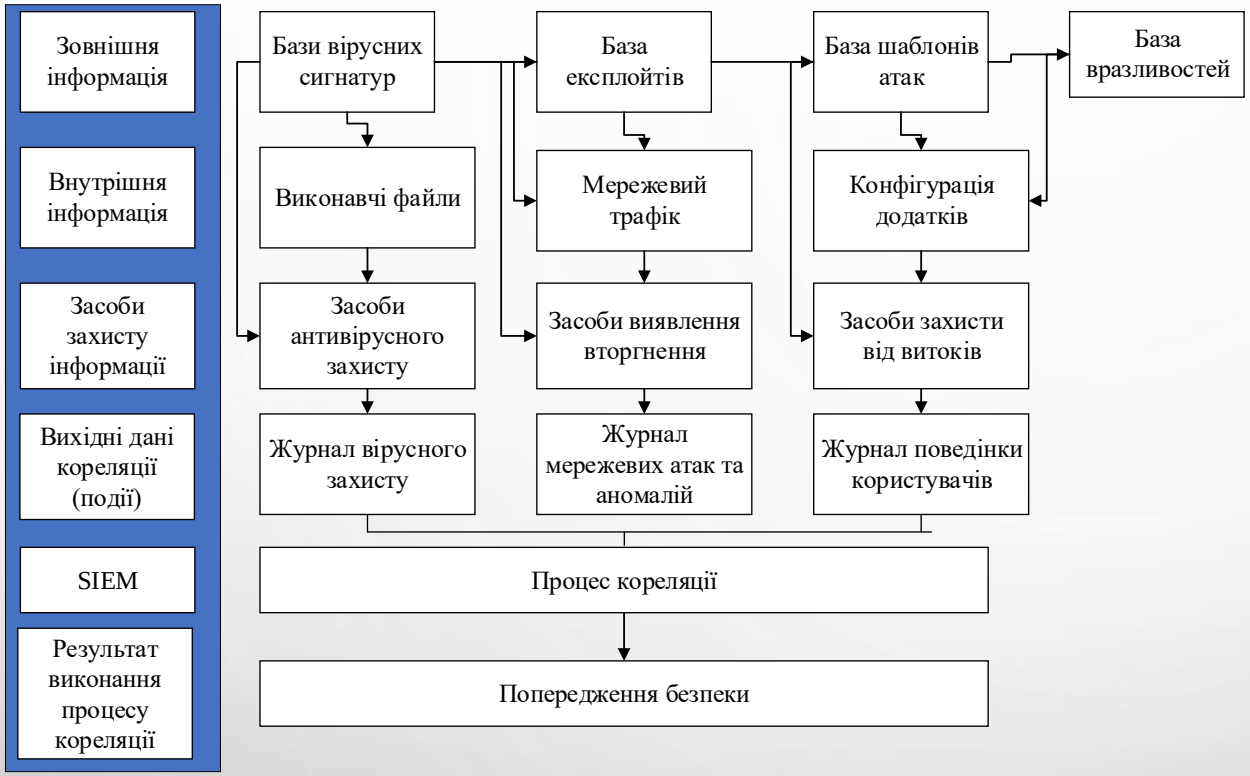
Оперативна оцінка захищеності критично важливих IP

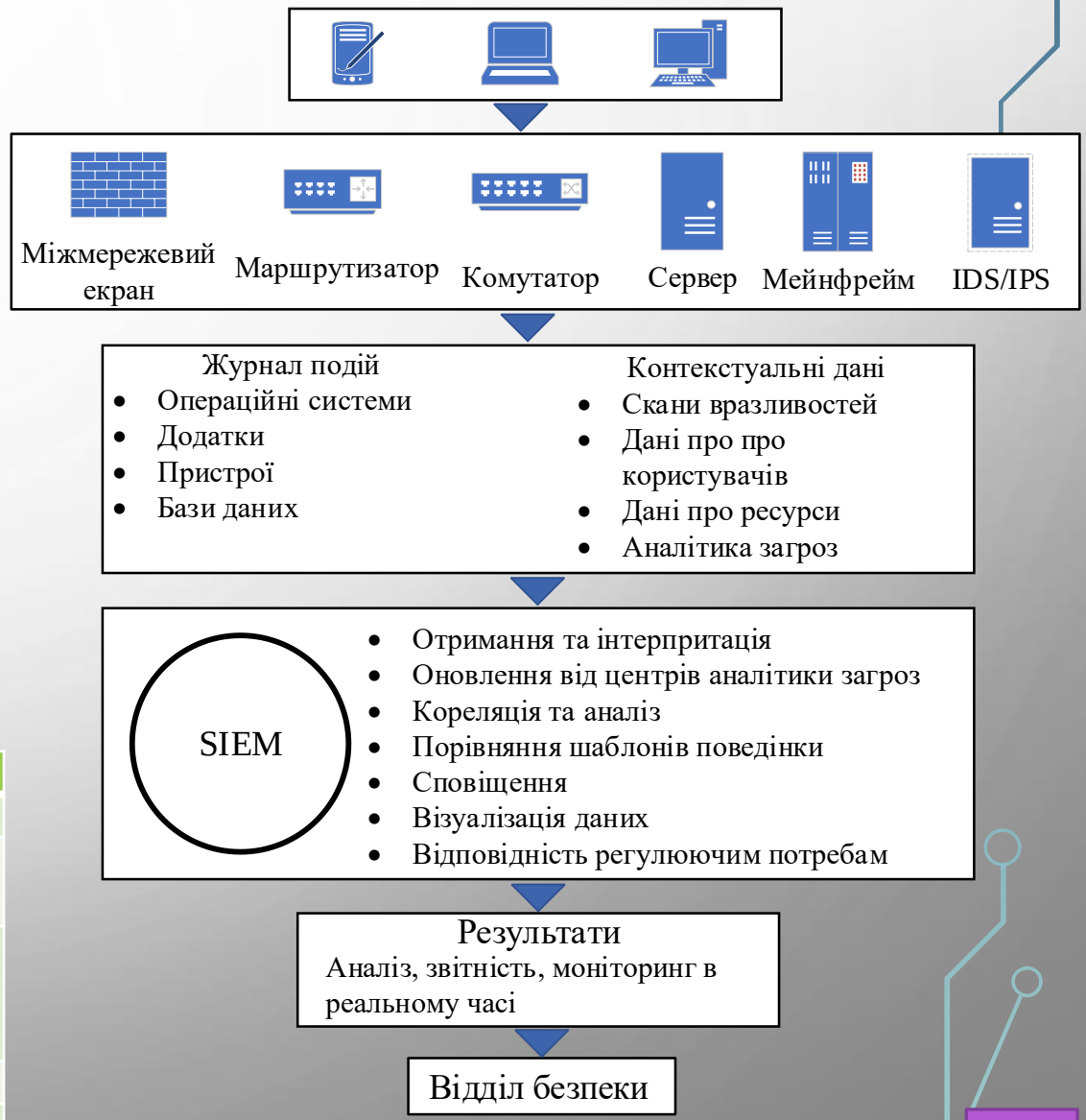
Проведення розслідувань інцидентів

Формування звітних документів

Прийняття ефективних рішень щодо захисту інформації

ЗАГАЛЬНА СХЕМА РОБОТИ ТА ПРОЦЕСУ КОРЕЛЯЦІЇ SIEM-СИСТЕМ

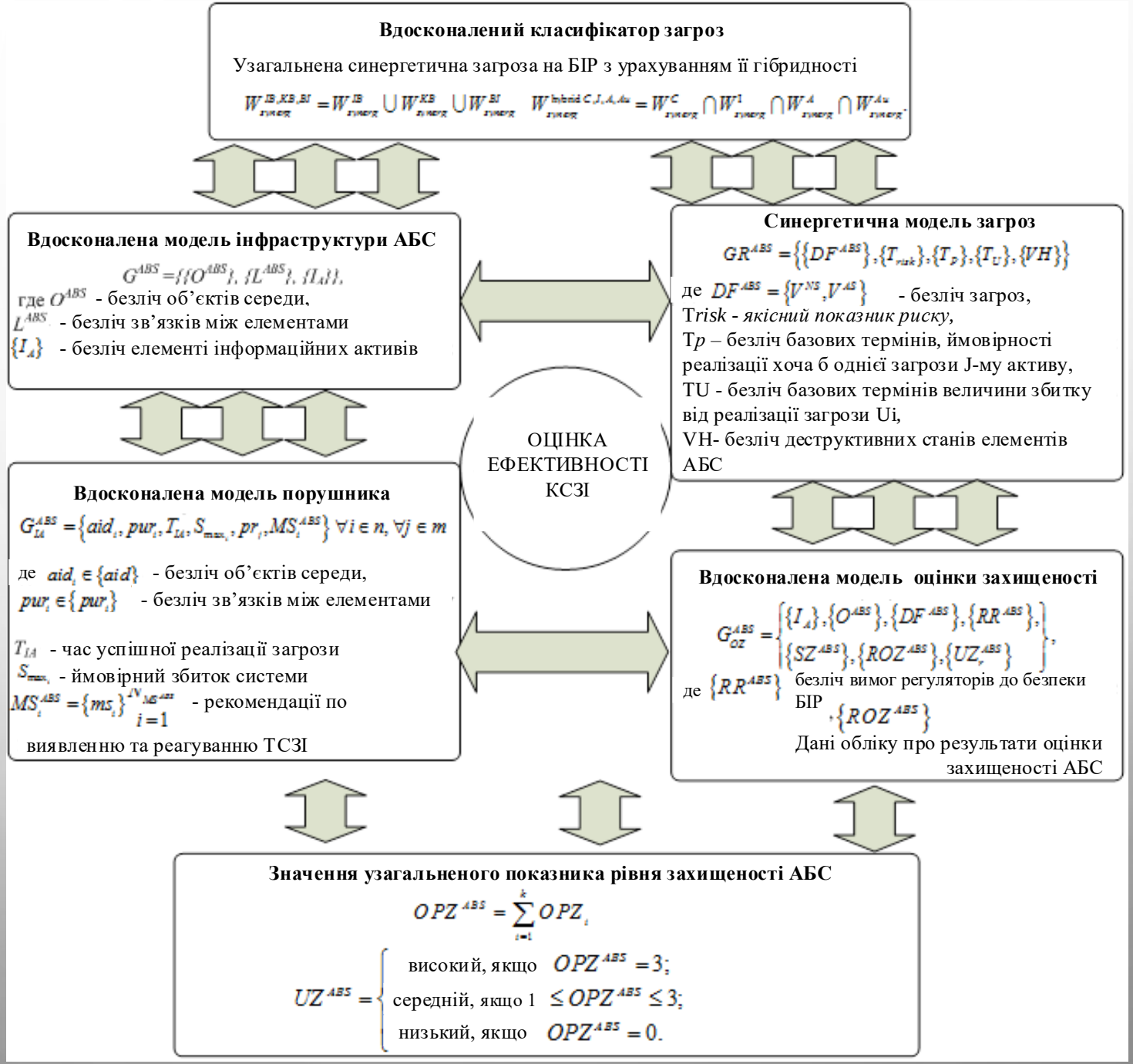




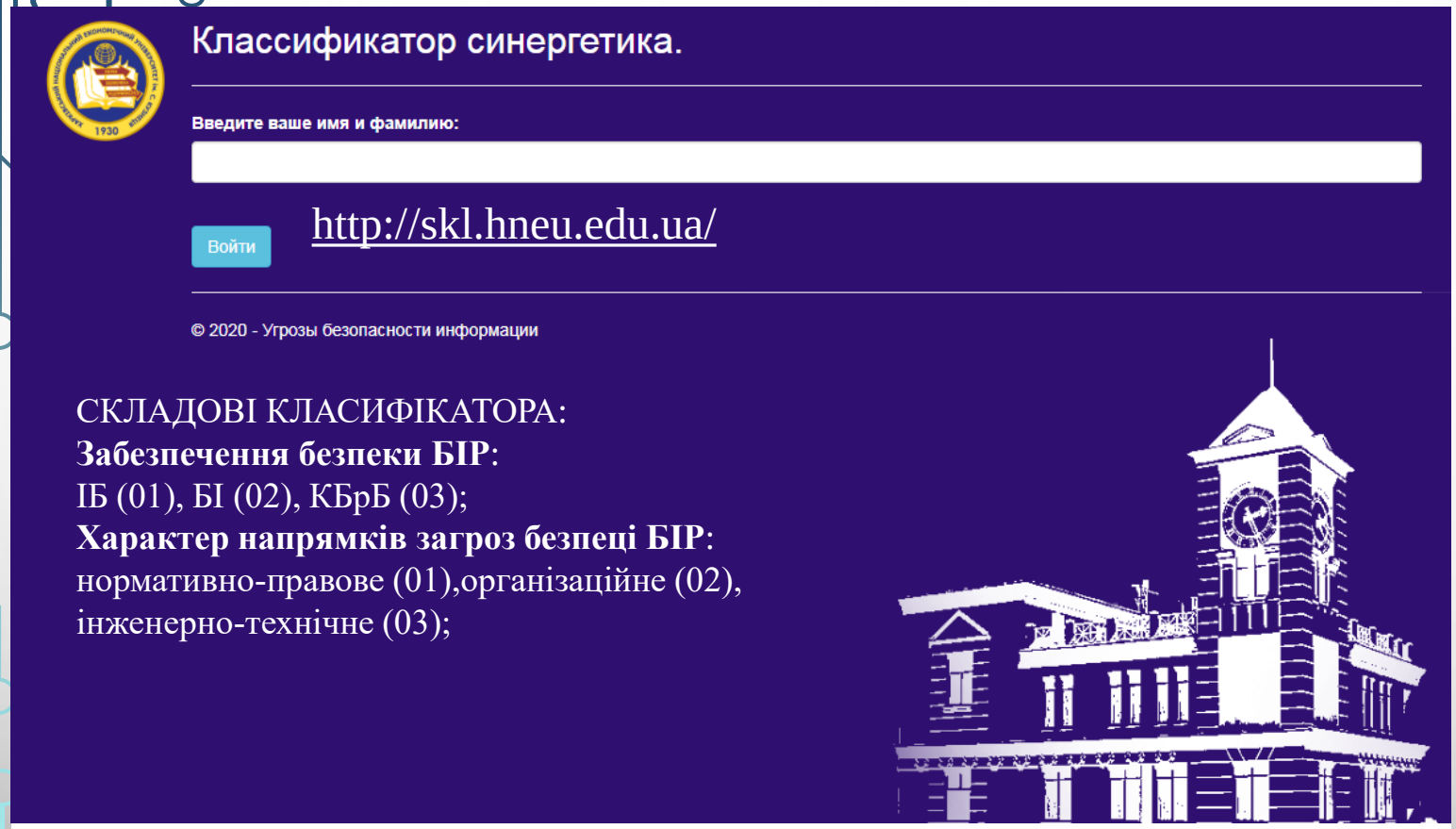
Критерії оцінки	Splunk
Оповіщення	Пошта, месенджери
Прийняття рішень в рамках процесу обробки інцидентів	Ручне
Наявність встановлених правил кореляції	181 в Splunk ES штатно. +343 в безкоштовному додатку Splunk Security Essentials
Терміни впровадження	Від 2 тижнів
Наявність встановлених графічних панелей	57

АНАЛІЗ ПРАКТИЧНИХ МОДЕЛЕЙ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

СИНЕРГЕТИЧНА МОДЕЛЬ ЗАГРОЗ


Вдосконалений класифікатор загроз
Узагальнена синергетична загроза на БІР з урахуванням її гібридності
$W_{synergy}^{IB,KB,BI} = W_{synergy}^{IB} \cup W_{synergy}^{KB} \cup W_{synergy}^{BI}$
$W_{synergy}^{hybrid\,C,I,A,Au} = W_{synergy}^{C} \cap W_{synergy}^{I} \cap W_{synergy}^{A} \cap W_{synergy}^{Au}$
Вдосконалена модель інфраструктури АБС
$G^{ABS} = \{\{O^{ABS}\}, \{L^{ABS}\}, \{I_A\}\}$,
где O^{ABS} - безліч об'єктів середи,
L^{ABS} - безліч зв'язків між елементами
$\{I_A\}$ - безліч елементі інформаційних активів
Синергетична модель загроз
$GR^{ABS} = \{\{DF^{ABS}\}, \{T_{risk}\}, \{T_p\}, \{T_U\}, \{VH\}\}$
де $DF^{ABS} = \{V^{NS}, V^{AS}\}$ - безліч загроз,
Trisk - *якісний показник риску*,
Tp – безліч базових термінів, ймовірності реалізації хоча б однієї загрози J-му активу,
TU - безліч базових термінів величини збитку від реалізації загрози Ui,
VH- безліч деструктивних станів елементів АБС
ОЦІНКА ЕФЕКТИВНОСТІ КСЗІ
Вдосконалена модель порушника
$G_{IA}^{ABS} = \{aid_i, pur_i, T_{IA}, S_{max_i}, pr_i, MS_i^{ABS}\}\ \forall i \in n, \forall j \in m$
де $aid_i \in \{aid\}$ - безліч об'єктів середи,
$pur_i \in \{pur_i\}$ - безліч зв'язків між елементами
T_{IA} - час успішної реалізації загрози
S_{max_i} - ймовірний збиток системи
$MS_i^{ABS} = \{ms_i\}_{i=1}^{N_{MS^{ABS}}}$ - рекомендації по виявленню та реагуванню ТСЗІ
Вдосконалена модель оцінки захищеності
$G_{OZ}^{ABS} = \left\{\begin{matrix}\{I_A\}, \{O^{ABS}\}, \{DF^{ABS}\}, \{RR^{ABS}\}, \\ \{SZ^{ABS}\}, \{ROZ^{ABS}\}, \{UZ_r^{ABS}\}\end{matrix}\right\}$,
де $\{RR^{ABS}\}$ безліч вимог регуляторів до безпеки БІР
$\{ROZ^{ABS}\}$
Дані обліку про результати оцінки захищеності АБС
Значення узагальненого показника рівня захищеності АБС
$OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i$
$UZ^{ABS} = \begin{cases} \text{високий, якщо } OPZ^{ABS} = 3; \\ \text{середній, якщо } 1 \le OPZ^{ABS} \le 3; \\ \text{низький, якщо } OPZ^{ABS} = 0. \end{cases}$

КЛАСИФІКАТОР ЗАГРОЗ БЕЗПЕЦІ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ



СКЛАДОВІ КЛАСИФІКАТОРА:
Забезпечення безпеки БІР:
ІБ (01), БІ (02), КБрБ (03);
Характер напрямків загроз безпеці БІР:
нормативно-правове (01),організаційне (02),
інженерно-технічне (03);

Засоби розробки:

.NET

Bootstrap

MySQL

Властивості БІР:
конфіденційність (01), цілісність (02), доступність (03), автентичність (04);

Рівні ієрархії інфраструктури АБС:
FL – фізичний рівень (01), NL – мережевий рівень (02),
OSL – рівень операційних систем (ОС) (03),
DBL – рівень систем управління базами даних (04),
BL – рівень банківських технологічних додатків і сервісів (05).

Крок 1

Весовые коэффициенты угроз

Номер угрозы: Go.

01_1. Стратегические	01_2. Оперативные	01_3. Тактические	
01_1.1 – 01_2.1 Конфиденциальность	01_1.2 – 01_2.2 Целостность	01_1.3 – 01_2.3 Доступность	01_1.4 – 01_2.4 Аутентичность
0.1	0.1	0.1	0.7

Предыдущая угроза | Следущая угроза

Крок 2

Список угроз

Номер угрозы	Короткое описание угрозы
02.03.01.05	Угроза анализа криптографических алгоритмов и и
03.03.03.04	Угроза аппаратного сброса пароля BIOS
03.03.02.03	Угроза внедрения вредоносного кода в BIOS

Крок 3

Список угроз

Номер угрозы	Короткое описание угрозы	μ[C]
02.03.01.05	Угроза анализа криптографических алгоритмов и их реализации	0.064
03.03.03.04	Угроза аппаратного сброса пароля BIOS	0.066
03.03.02.03	• Угроза внедрения вредоносного кода в BIOS • Угроза деструктивного использования декларированного функционала BIOS • Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети • Угроза несанкционированного управления буфером	0.314

Крок 4

Составные безопасности	Услуги безопасности				
	C, W^{C}_{synerg}	I, W^{I}_{synerg}	A, W^{A}_{synerg}	Au, W^{Au}_{synerg}	Итог
01 - IB, W^{IB}_{synerg}	0.069	0.076	0.079	0.1	0.0000414
02 - KB, W^{KB}_{synerg}	0.091	0.142	0.097	0.04	0.0000501
03 - BI, W^{IB}_{synerg}	0.045	0.059	0.082	0.065	0.0000142
Итог	0.205	0.277	0.258	0.205	
$W^{IB,KB,BI}_{synerg} = 0.000106$		$W^{hybrid\,C,I,A,Au}_{synerg} = 0.003003$			

	C	I	A	Au
Банковская тайна	1	1	1	1
Платежные документы	1	1	1	1
Кредитные документы	1	1	1	1
Коммерческая тайна	1	1	1	1
Статистические отчеты	0	1	1	1
Общедоступная информация	0	1	1	0
Управляющая информация	0	1	1	1
Персональные данные	1	1	1	1

0 - услуга не обеспечивается.

Крок 5

	Физ. уровень	Сетевой уровень	Уровень ОС	Уровень СУБД	Уровень банковского ПО
Банковская тайна	pl	pl	sc	cs	so
Платежные документы	pl	pl	sc	cs	so
Кредитные документы	pl	pl	sc	cs	so
Коммерческая тайна	pl	pl	sc	cs	so
Статистические отчеты	pl	pl	sc	cs	so
Общедоступная информация	pl	pl	sc	cs	so
Управляющая информация	pl	pl	sc	cs	so
Персональные данные	pl	pl	sc	cs	so

Синергитическая модель.

Крок 6

	Банковская тайна	Платежные документы	Кредитные документы	Коммерческая тайна	Статистические отчеты	Общедоступная информация
02.03.01.05	0.267	0.267	0.267	0.267	0.203	0.115
03.03.03.04	0.2	0.2	0.2	0.2	0.134	0.07
03.03.02.03	0.2	0.2	0.2	0.2	0.068	0.048
03.03.02.05	0.2	0.2	0.2	0.2	0.18	0.152
03.02.04.03	0.2	0.2	0.2	0.2	0.198	0.132

Крок 7

	Физический уровень	Сетевой уровень	Уровень операционных систем	Уровень систем управления базами данных	Уровень банковских технологических приложений и сервисов
02.03.01.05	0.40832	0.40832	0.31552	0.928	0.31552
03.03.03.04	0.29436	0.29436	0.22746	0.669	0.22746
03.03.02.03	0.26048	0.26048	0.20128	0.592	0.20128
03.03.02.05	0.33264	0.33264	0.25704	0.756	0.25704
03.02.04.03	0.33616	0.33616	0.25976	0.764	0.25976
02.02.04.05	0.2486	0.2486	0.1921	0.565	0.1921
02.02.02.03	0.43032	0.43032	0.33252	0.978	0.33252

ОЦІНКА ПОТОЧНОГО СТАНУ РІВНЯ БЕЗПЕКИ ОБС

Крок 8

MZ - механизм защиты, обеспечивает противодействие ее деструктивному влияни;.

NMZ - нет механизма защиты для обеспечения противодействия i-той угрозы;

	Физический уровень	Сетевой уровень	Уровень операционных систем	Уровень систем управления базами данных	Уровень банковских технологических приложений и сервисов
02.03.01.05	MZ	MZ	MZ	MZ	MZ
03.03.03.04	MZ	MZ	MZ	MZ	MZ
03.03.02.03	MZ	MZ	MZ	MZ	MZ
03.03.02.05	MZ	MZ	MZ	MZ	MZ
03.02.04.03	MZ	MZ	MZ	MZ	MZ

Крок 9

ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	0	0,25	0,5	0,75	1	н/о
Оцінка степені виконання вимог за напрямом "менеджмент ІБ організації"									
IU 1.1	упровадження процесного підходу до діяльності банку	обов'язковий	категорія 2	☑	☐	☐	☐	☐	☐
IU 1.2	упровадження ризик-орієнтованого підходу до забезпечення інформаційної безпеки банку	обов'язковий	категорія 2	☑	☐	☐	☐	☑	☐
IU 1.3	запровадити процес управління ризиками інформаційної безпеки в рамках системи управління ризиками банку	обов'язковий	категорія 2	☐	☐	☐	☐	☑	☐

Крок 9

Оценка выполнения регуляторов

Регуляторы	Текущее значение	Номинальное значение	% соответсвия
RBBI2	0.34	0.85	40

Крок 10

Обобщенный уровень защищенности

Показатель	Номинальное значение	Текущее значение	Предыдущее значение
OPZ_1	1	1	
OPZ_2	1	1	
OPZ_3	1	0	

Общий уровень защищености: *Средний*

ВИСНОВКИ

1. Проведений аналіз сучасних загроз на автоматизовані банківські системи показав, що в умовах стрімкого росту обчислювальних можливостей, появи повномасштабних квантових комп'ютерів вони стримляться к комплексуванню з методами соціальної інженерії, що спонукає до появи синергетичного та/або гібридного характеру. Тому слід розглядати їх в комплексі з урахуванням їх впливу на всі складові безпеки: кібербезпеки, інформаційної безпеки, та безпеки інформації.
2. Для забезпечення протидії синергії та гібридності сучасних загроз використовуються програмні (програмно-апаратні) застосунки/засоби виявлення їх дії та/або виявлення відхилення від нормального стану роботи відповідних систем. Серед яких окремо можливо виділити SIEM-системи, які дозволяють автоматизувати процес обробки та управління подіями ІБ від різних джерел.
3. Для оцінки поточного стану рівня безпеки в організаціях банківського сектору, проаналізовані практичні моделі, та визначений підхід на основі синергетичної моделі загроз, яка на відмоу від існуючих дозволяє враховувати послуги безпеки, та синергію та гібридність сучасних загроз.
4. Розроблений веб-застосунок, базується на класифікаторі, який як і запропонований підхід враховує синергію та гібридність сучасних загроз на компоненти автоматизованих банківських систем, що дозволяє не тільки оцінити поточний стан рівня безпеки, а також визначити критичні точці в інфраструктурі автоматизованих банківських систем, та можливість технічних засобів безпеки.

ДЯКУЮ ЗА УВАГУ