Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
« » червня 2021р.

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи
бакалавра

(назва освітнього рівня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека

на тему: «Технологія оцінювання стану захищеності інформаційних ресурсів на основі дослідження джерел загроз інформаційній безпеці »

Виконавець: студентка IV курсу, групи КБ-41
Качмала Олександра Вікторівна
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Браіловський М.М.	

Нормоконтроль	Даков С. Ю.	

Київ 2021

Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«10» жовтня 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-41** **Качмалі Олександрі Вікторівні**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Технологія оцінювання стану захищеності інформаційних ресурсів на основі дослідження джерел загроз інформаційній безпеці

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №2 від 08.10.2020 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ
Захищеність інформаційних ресурсів, оцінка ризиків, SIEM- системи

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ
Необхідно ознайомитися з методами та засобами оцінювання стану захищеності інформаційних ресурсів, розробити методику, практично її дослідити та надати рекомендації

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблено методику технології оцінювання стану захищеності інформаційних ресурсів і досліджено на прикладі роботи із FortiSIEM-системою

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання:14 жовтня 2020 року

Завдання видав _____ М. М. Браіловський
(підпис) (ініціали, прізвище)

Завдання прийняла до виконання _____ О. В. Качмала
(підпис) (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	25.01.2021 – 28.01.2021	*виконано*
2	Аналіз літератури	29.01.2021 – 08.02.2021	*виконано*
3	Обґрунтування вибору рішення	09.02.2021 – 01.03.2021	*виконано*
4	Поняття захищеності інформаційних ресурсів та класифікація даних	02.03.2021 – 23.03.2021	*виконано*
5	Аналіз методів та засобів оцінки стану захищеності інформаційних ресурсів та процес управління безперервністю бізнесу	24.03.2021 – 07.04.2021	*виконано*
6	Розробка методики оцінювання стану захищеності інформаційних ресурсів	08.04.2021 – 29.04.2021	*виконано*
7	Дослідження розробленої методики і складання рекомендацій щодо її використання	30.04.2021 – 17.05.2021	*виконано*
8	Оформлення пояснювальної записки	18.05.2021 – 08.06.2021	*виконано*
9	Підготовка до захисту дипломної роботи	09.06.2021 – 21.06.2021	*виконано*

Завдання видав _____ М.М.Браіловський
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ О.В.Качмала
(підпис) (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 08 червня 2021 року.

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 60 сторінок основного тексту, 3 додатки. Список використаних джерел містить 57 найменувань і займає 6 сторінок.

Метою даної роботи є аналіз технологій оцінювання стану захищеності інформаційних ресурсів підприємства та підвищення їх рівня на основі дослідження джерел загроз інформаційній безпеці.

У роботі проаналізована існуюча література з оцінки захищеності інформаційний ресурсів в організації та установах, виконаний аналіз документів, порівняння, вивчення та узагальнення вітчизняної і зарубіжної практики з теми інформаційних ресурсів, розроблено рекомендації з функціональних можливостей використання SIEM-систем та рекомендоване практичне впровадження роботи FortiSIEM від Fortinet на сучасному етапі.

Проведено аналіз методів протидії витоку IP підприємства, а також продемонстровані приклади їх застосування, запропоновані підходи та методи можуть бути використані при плануванні та реалізації роботи на підприємстві.

Досліджено різні види технологій оцінювання стану захищеності інформаційних ресурсів. На основі даних досліджень в роботі практично виконано наступне: сформовано реєстр ризиків інформаційної безпеки по бізнес діяльності, визначено цінність активів організації, показано роботу із FortiSIEM від Fortinet.

Галузь використання – інформаційні технології

Ключові слова: система управління безперервністю бізнесу, інформаційні ресурси, оцінка ризику безпеки, використання SIEM-систем, робота FortiSIEM.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

API	–	Application Programming Interface
BIA	–	Business Impact Analysis
BCP	–	Business continuity plan
CMDB	–	Configuration management database
DLP	–	Data Loss Prevention
DRP	–	Disaster recovery plan
ERM	–	Enterprise risk management
EPP	–	Emergency Preparedness Plan
ISP	–	Internet Service Provider
MTO	–	Maximum Tolerable Outage
PAM	–	Privileged Account Management
RPO-	–	Recovery point objective
RTO-	–	Recovery time objective
SaaS	–	Software as a Service
БД (БнД)	–	база даних (банк даних)
БП	–	бізнес-процес
ДСТУ	–	Державні стандарти України
ІБ	–	інформаційна безпека
ІР	–	інформаційний ресурс
ІС	–	інформаційна система
ІТС	–	інформаційно - телекомунікаційна система
КСЗІ	–	комплексна система захисту інформації
НД ТЗІ	–	Нормативні документи в галузі технічного захисту інформації
ОСЗ	–	оцінювання стану захищеності

ПБ	–	політика безпеки
СЗІ	–	система захисту інформації
СУББ	–	система управління безперервністю бізнесу
СУІБ	–	система управління інформаційною безпекою
УББ	–	управління безперервністю бізнесу
ЦА	–	цінність активів

ЗМІСТ

ВСТУП

Організація інформаційної безпеки в сучасних умовах є важливим стратегічним чинником розвитку будь-якої компанії. Основна увага приділяється вимогам та рекомендаціям нормативно-методичної бази в галузі захисту інформації. Провідні компанії світу для забезпечення стабільності своїх бізнес-процесів задля уникнення можливості витоку інформації залучають додаткове програмне забезпечення до роботи інформаційних систем.

Актуальність роботи є важливою, оскільки, структура інформаційної безпеки підприємства потребує впровадження нових технологій захищеності інформаційних ресурсів і вдосконалення існуючих практик, формує цілі й керує ними, оцінює безпеку інформації та визначає потребу в додаткових заходах. Кінцевим результатом є визначення балансу між ймовірним збитком від несанкціонованого витоку інформації та розміром витрат для забезпечення захищеності інформаційних ресурсів. Загалом, необхідно дослідити підходи щодо оцінки рівня захищеності систем захисту, а це в свою чергу, залежить від багатьох показників (цінності інформації, статусу компанії, вартості інформації, що циркулює в межах організації, надійності програмно-апаратного комплексу тощо).

Запроваджуючи інформаційні системи, кожна організація очікує максимально корисної функціональності для підтримки своїх бізнес-процесів, забезпечення цілісності та зручного режиму доступу до кожного з ресурсів. Та на жаль, пандемія COVID-19 зробила за останній рік людей та суспільство надзвичайно вразливими в цьому відношенні. Особливо зазнала впливу сфера безпеки інформаційних систем: фахівці з дотримання вимог та керівники аудиту зіткнулися з проблемами, які вони ніколи не стикалися за свою кар’єру. Під час соціального дистанціювання необхідні комп’ютерні системи, мобільні пристрої та Інтернет, щоб працювати, спілкуватися, ділитися та отримувати інформацію. Кіберзлочинці почати використовувати дану

кризу у власних інтересах. Є наступні докази того, що зловмисні хакери використовують вразливості для власного збагачення. Наприклад:

- Фішингові кампанії та розповсюдження шкідливого програмного забезпечення через справжні веб-сайти або документи, що містять інформацію або поради щодо COVID-19, використовуються для зараження комп'ютерів та отримання облікових даних користувачів.
- Напади на критичну інфраструктуру або міжнародні організації, такі як Світова організація охорони здоров'я.
- Програми-вимагачі (ransomware), націлені на мобільні телефони осіб, що використовують програми нібито зі справжньою інформацію про COVID-19, для отримання платежів.
- Правопорушники, які отримують доступ до систем компаній, орієнтуючись на співробітників, які працюють на роботі та віддалено.
- Дезінформація або фейкові новини поширюються хакерами через фальшиві медіа-акаунти, щоб створити паніку, соціальну нестабільність і недовіру до урядів або до заходів, вжитих їх органами охорони здоров'я.

Потрібно бути особливо обережними та посилити заходи безпеки, оскільки, окрім величезної кризи охорони здоров'я та економіки, яку спричиняє пандемія, ця ситуація глибоко впливає на глобальну панораму кіберзагроз. Про це свідчить звіт Інтерполу, в якому вони обстежили 48 країн-членів та 4 приватних партнерів щодо наслідків для кіберзлочинності[1].

Зловмисники змінюють свої дії, під час атак на приватних осіб, великі компанії, уряди та важливі інфраструктури, які, зважаючи на ситуацію перевантаження та колапсу, стали більш вразливими, так, в березні 2020 р. мільйони працівників були відправлені на роботу додому їхніми роботодавцями, контроль безпеки та конфіденційності, встановлений безпосередньо на робочому місці в кабінетах, раптом став неактуальним. А працівникам із захисту інформації довелося активізувати швидке вирішення нових загроз (наприклад, встановити безпечні зв'язки для віддаленої роботи

кадрів, запобігати появі нових мережевих загроз, спрямованих на підприємство, проводити аудити та подання нормативних документів, дотримуватися забезпечення законодавчих та договірних зобов’язань).

Організації та установи стали дуже чутливими до ризиків безпеки та конфіденційності, які створюють технології, що підтримують віддалену роботу (наприклад, системи телеконференцій). Компанії зрозуміли, що коли провайдери SaaS не мають надійного контролю безпеки всередині та навколо їхніх систем, зловмисники можуть проникнути в IT-системи провайдерів SaaS, а потім використовувати постачальника для атаки на них. Дослідження Coalfire у 2020 р. показало, що для більшості організацій зростаючі зобов'язання щодо дотримання норм складають 40% і більше бюджетів IT-безпеки, в свою чергу - 58% компаній розглядають дотримання вимог як матеріальну перешкоду для виходу на нові ринки[2].

Пам’ятаючи про зовнішні загрози та їх наслідки, підприємствам, організаціям та установам потрібно зосередити свою енергію на двох важливих аспектах: захисті конфіденційних даних та зборі доказів, що доводять відповідні гарантії безпеки та конфіденційності. За даними Інтерполу, кіберзлочинність у цій галузі буде продовжувати зростання та погіршить економічну нестабільність у багатьох країнах світу.

Корпоративні мережі надають функціональне забезпечення. Однак, є певні особливості у проектуванні даних мереж у порівнянні із локальними, зокрема, підвищується складність системи захисту інформації. Відповідно зростає складність системи захисту. Рекомендовано застосовувати типові рішення щодо стандартних уніфікованих компонентів: наприклад, у прикладному програмному забезпеченні таким рішенням виступають універсальні сервіси.

Питанням технологій оцінювання стану захищеності інформаційних ресурсів (ІР) займалися видатні українські: Бурячок В.Л.[11], Виноградова Н.В.[38], Довгаль Ю.С.[3], Пархоменко І.І.[18], Самохвалов Ю. Я. [51], Толюпа С. В. [12], Хорошко В.О.

[9] та зарубіжні науковці: Роберт Джефін [21], Дастін Хіт [14], Кім Ліндрос [28], Лінда Розенкранс [52], Кевін Стайн [40], Стівен Таддоніо [30] та ін.

Нині актуальним постає питання компромісу між традиційною безпекою, простотою використання, вартістю, складністю системи тощо[3]. Надважливими питаннями в забезпеченні діяльності організації та установи є розроблення планів безперервності бізнесу для всіх критичних бізнес-процесів, а саме визначення ефективного способу виконання бізнес-процесу на конкретний сценарій збою, в той же час власник є відповідальним за щорічний перегляд планів та їх підтримку. Особливу роль на підприємстві відіграє оцінка ризику, що загалом полягає у визначенні розміру збитків установи через порушення захисту, конфіденційності, цілісності та доступності кожного конкретного інформаційного ресурсу [4].

У практиці зарубіжних корпорацій невід'ємною частиною відповідності вимогам сучасним стандартам інформаційної безпеки є управління ризиками, яке розглядається як складова ефективного менеджменту підприємства. Дані стандарти є своєрідними настановами для фахівців з інформаційної безпеки як реалізувати методологію оцінки ризиків, зменшувати їх вплив та управляти ними. Тому **тема бакалаврської роботи** є актуальною та своєчасною.

Об'єкт дослідження – оцінка стану захищеності інформаційних ресурсів на основі досліджень загроз ІБ.

Предмет дослідження – джерела загроз інформаційній безпеці організації та установи.

Мета роботи – підвищення рівня захищеності організацій та установ на основі дослідження джерел загроз інформаційній безпеці.

***Завдання роботи*:**

–узагальнити джерела та теоретичні засади проблематики обраної теми;

–визначити склад і зміст поняття захищеності інформаційних ресурсів та класифікації даних;

–проаналізувати принципи ефективного управління ризиками на підприємстві у контексті системи управління безперервністю бізнесу;

–провести якісну та кількісну оцінку стану захищеності ІР на основі дослідження джерел загроз;

–охарактеризувати процеси управління інформаційними ризиками та методологію їх застосування;

–дослідити загальні принципи роботи SIEM-систем;

–визначити на практиці основні переваги впровадження роботи FortiSIEM від Fortinet в роботу організації та установи.

Методи дослідження: методи експертного оцінювання, розрахунок ризиків, політика безпеки підприємства, SIEM- системи.

В кваліфікаційній роботі надано характеристику технології оцінювання стану захищеності інформаційних ресурсів на основі дослідження джерел загроз інформаційній безпеці, проаналізовано методи та засоби оцінки стану захищеності інформаційних ресурсів та процес управління безперервністю бізнесу. Розроблено і досліджено методику оцінювання стану захищеності інформаційних ресурсів і складено рекомендації щодо її використання. Як наслідок, практично впроваджено роботу FortiSIEM від Fortinet, що може бути використано при плануванні та реалізації роботи в організаціях та установах.

РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ОЦІНКИ СТАНУ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТА ПРОЦЕС УПРАВЛІННЯ БЕЗПЕРЕРВНІСТЮ БІЗНЕСУ

1.1.Поняття захищеності інформаційних ресурсів, зміст та класифікація даних, сутність проблеми

Відповідно до закону України «Про інформацію» від 02.10.1992 № 2657-XII висвітлимо поняття суб'єктів та об'єктів інформаційних відносин: фізичні, юридичні особи, об'єднання громадян, владні структури - суб'єкти інформаційних відносин. Об'єктом інформаційних відносин є інформація [5].

Забезпечення інформаційно-комунікаційними технологіями залежить від доступності, цілісності та конфіденційності інформаційних ресурсів та являється стратегічно важливим моментом, що є складовою національної безпеки України, та захищає її економічну стабільність і соціальне благополуччя населення. Водночас, сучасне українське суспільство достатньо уразливе від зловмисників, що протиправно використовують кіберпростір [6]. У даний час фахівці з кібербезпеки постійно наголошують на питаннях інформаційної безпеки інформаційних систем, включно із ресурсами державних та приватних структур, для зменшення негативних наслідків кібернетичного впливу.

Глобальна інформатизація основних сфер життєдіяльності людини: економіки, оборонного комплексу, органів державного та громадського управління, закладів науки та освіти являються головним пріоритетом в розвитку сучасного українського суспільства. Крім того, держава докладає зусиль щодо вирішення проблеми про забезпечення безпеки громадських відносин у існуючому кіберпросторі, про що вказує затверджені Указом Президента України від 15 березня 2016 року № 96/2016 Стратегія кібербезпеки України [7] та Стратегія національної безпеки України від 14 вересня

2020 року № 392 [8].

Керуючись еталонною моделлю забезпечення кібербезпеки, система її функціонального забезпечення відносно суб'єкта впливу реалізовує функцію протидії[9].

Рисунок 1.1- Базова модель забезпечення кібернетичної безпеки

За оцінкою відомого фахівця у сфері з економічної безпеки Д.М. Гладких за 2019 рік у всьому світі кіберзлочинці нанесли економічного збитку на 2,5 трильйона доларів США [10].

Аналізуючи приріст кіберзлочинів у світі, зауважимо, що протидіяти зловмисникам має об'єднання суспільства, приватного сектору та окремих громадян, обов'язковим також є регулювання з боку держави при сприянні правоохоронних органів. Відповіддю на це мають стати запобіжні заходи, що носять системний характер, а також захист інформації на різних рівнях: загальному, спеціальному та індивідуальному.

Отже, протидія кіберзлочинності є одним із найважливіших напрямів соціального управління, що має охоплювати та реалізовувати систему різноманітних заходів: політичних, економічних, правових, організаційно-управлінських, культурно-виховних і технічних[11]. Як наслідок, суспільство отримує комплексність, об'єктивність, наукову доцільність, законність, що дозволяє здійснювати ефективну діяльність щодо захисту їхніх інтересів від потенційно небезпечних посягань в кіберпросторі[9].

Фахівці з інформаційної безпеки підкреслюють, що одним із найважливіших процесів перевірки ефективності системи забезпечення інформаційної безпеки є аналіз та управління інформаційними ризиками, що включає різноманітні заходи і способи забезпечення безпеки інформаційних ресурсів [12]. Керуючись поняттям ризику, можна кількісно і якісно визначити ефективність системи захисту інформації, рівень безпеки дій та правильність прийнятих рішень.

Для будь-якої організації, враховуючи специфіку її інформаційної системи, відокремимо послідовність дій щодо забезпечення режиму інформаційної безпеки (ІБ) на підприємстві:

– актуальна політика безпеки;

– конкретно визначені межі діяльності системи управління інформаційною безпекою та обґрунтування цілей її впровадження;

– оцінка ризиків по ймовірності їх виникнення на підприємстві;

– постійний контроль дотримання режиму ІБ;

– управління ризиками;

– своєчасний та систематичний аудит системи управління ІБ.

Здебільшого, написання політики безпеки зводиться і складається з наступних послідовних дій:

1. Унормування державних та міжнародних керівних настанов, положень і стандартів в галузі ІБ на основі вимог політики ІБ компанії, включно із:

- управлінням доступом до обчислювальних засобів, програмам і даних;

- антивірусний захист;

- питання резервного копіювання, окремо у хмарних сховищах;

- своєчасне повідомлення про інциденти в області ІБ та ін.

2. Систематизація на підприємстві засобів та заходів щодо управління інформаційними ризиками та ,відповідно, визначення рівня захищеності інформаційної системи (ІС) [12].

3. Поділ контрзаходів щодо захисту інформації за нормативно-правовими,

організаційно-управлінськими, технологічними і апаратно-програмними рівнями.

4. Постійна перевірка ІС на відповідність стандартам в області ІБ, періодичний перегляд положень політики ІБ, приділення безпосередньої уваги керівництва, щоквартальне навчання всіх співробітників і т. д [13].

Таким чином, надавання пріоритетів з точки зору безпеки означає класифікацію усіх зібраних та оброблених організацією даних, які повинні бути засекречені. Створення задовільної політики класифікації даних - це перший крок до захисту конфіденційної інформації в установі. Адже саме класифікація даних та аналіз ризиків відіграють вирішальну роль у забезпеченні безпеки та відповідності нормативним вимогам у кожній організації.

На думку Головного операційного директора Vigilant Cyber Systems (США, Вінстон-Сейлем (Winston-Salem), штат Північна Кароліна)) Дастіна Хіта: "Класифікація даних сьогодні є найважливішим аспектом інформаційної безпеки та управління будь-яким бізнесом сьогодні"[14].

Політика класифікації даних - це всеосяжний план, що використовується для класифікації збереженої інформації компанії на основі рівня її чутливості, забезпечення належної обробки та зниження організаційного ризику. Вона визначає та допомагає захищати конфіденційні дані за допомогою правил, процесів та процедур для кожного класу відповідно до класифікації даних.

Класифікації є індивідуальними для кожної організації і завжди визначають рівень чутливості даних. Наприклад, одна компанія може використовувати відкриту, або для службового користування, або конфіденційну інформацію, тоді як інша використовує таємну, цілком таємну та особливої важливості [15] (Закон України «Про інформацію» документ 2657-XII, чинний, поточна редакція — Редакція від 16.07.2020, підстава - 692-IX) . Ефективна політика регулює спосіб обробки, зберігання та використання кожної класифікації даних із урахуванням вимог щодо конфіденційності, цілісності, доступності.

Політика класифікації даних повинна відігравати важливу роль у загальній політиці безпеки та відображати готовність до ризику організації та установи. Її ефективність даних допоможе відповідати нормативним вимогам, найкращим галузевими практикам та очікуваннями споживачів і партнерів. Нижче наведено наступні переваги політики класифікації даних:

–створює та передає визначену структуру правил, процесів та процедур захисту даних;

–забезпечує ефективну систему підтримки цілісності даних та відповідності нормативним вимогам;

–допомагає уніфікувати стратегію управління даними;

–керує інвестиціями в засоби контролю за безпекою на основі виявлення конфіденційних даних.

Для підвищення ефективності роботи організації необхідно застосувати наступні практичні дії:

– базування класифікації на основі конкретних критеріїв організації щодо конфіденційності після проведення ретельної нормативної оцінки;

– використання технології автоматизації для спрощення класифікації шляхом швидкого аналізу та групування даних на основі встановлених рекомендацій;

– визначення та розуміння власного профілю даних: де і ким була зібрана інформація, де вона зберігається, хто відповідає за підтвердження точності даних, хто відповідає за управління даними в організації;

– встановлення чітких цілей щодо політики та ідеології компанії;

– встановлення права власності для делегування відповідальності та забезпечення підзвітності;

– дотримання того, щоб політика була простою та зрозумілою, використовуючи якомога менше класифікацій;

– перегляд політики не рідше 1 разу на рік.

Саме перегляд і, як наслідок, оновлення політики класифікації даних має вирішальне значення для досягнення цілей управління організацією. Кожне рішення, яке стосується даних, прийняте на підприємстві, повинно базуватися на правильному, оновленому статусі класифікації даних [12]. Успішні компанії не відстають від внутрішніх змін - таких, як прийняття нових технологічних систем, змін до нормативних вимог, і ,відповідно, оновлюють свою політику класифікації даних. Крім того, вони переконуються, що всі члени команди, що обробляють системи та дані, знають, що є в поточній версії їх політики класифікації даних.

1.2. Принципи ефективного управління ризиками кібербезпеки на підприємстві, сфера застосування та структура СУББ

Управління ризиками кібербезпеки здійснюється різними способами на різних рівнях, у тому числі на рівні системи, організації та підприємства, як показано на рисунку 1.2, де зображено ієрархічні зв'язки підприємства для управління ризиками кібербезпеки. Загальноприйнятою практикою є те, що окремі команди системного рівня несуть відповідальність за відстеження відповідних ризиків[16].

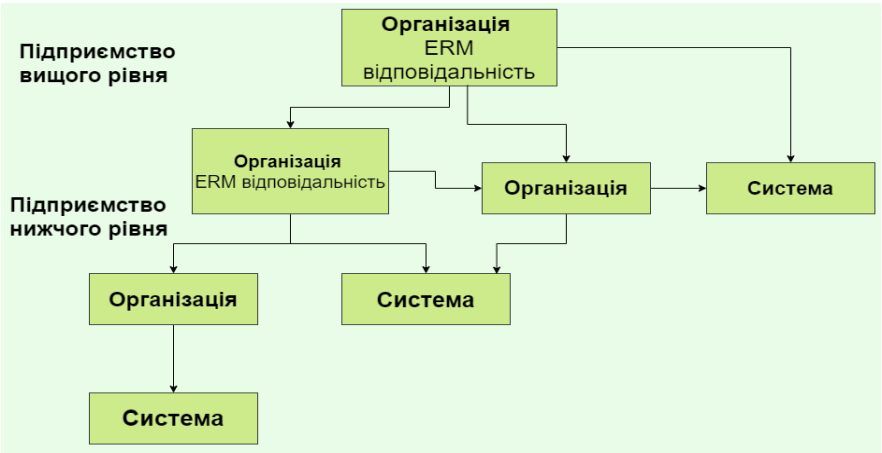


Рисунок 1.2- Ієрархія підприємства для управління ризиками кібербезпеки

Інституціоналізація програми практичної оцінки ризику є важливою для підтримки ділової діяльності організації [17] та забезпечує ряд переваг :

— Програми оцінки ризиків допомагають гарантувати, що найбільші ризики для організації визначаються та постійно розглядаються. Такі програми допомагають гарантувати, що досвід та найкращі практики персоналу використовуються для розробки кроків для запобігання або пом'якшення ситуацій, які можуть перешкоджати виконанню діяльності організації.

— Оцінка ризиків допомагає персоналу в організації краще зрозуміти ризики для ділових операцій. Вони також вчать їх, як уникати ризикованих дій, таких як розкриття паролів або іншої конфіденційної інформації, та розпізнавання підозрілих подій. Це розуміння частково зростає завдяки вдосконаленому спілкуванню між менеджерами бізнесу, персоналом системної підтримки та фахівцями з безпеки.

— Оцінка ризиків забезпечує механізм досягнення консенсусу щодо того, які ризики є найбільшими та які кроки доцільні для їх пом'якшення. Використані процеси спонукають до дискусій і, як правило, вимагають вирішення суперечок. Це, в свою чергу, підвищує ймовірність того, що керівники підприємств зрозуміють необхідність узгодженого контролю, впевнюються, що засоби контролю відповідають бізнес-цілям організації та підтримують їх ефективне впровадження. Керівники на практиці вже встановили, що вибраний таким чином контроль, швидше за все, буде ефективно прийнятий, ніж контроль, який застосовується персоналом поза організацією.

— Офіційна програма оцінки ризиків забезпечує ефективний засіб для повідомлення результатів оцінки та рекомендування дій керівникам підрозділів, а також вищим посадовим особам корпорації[18]. Стандартні формати звітів та періодичний характер оцінок надають організаціям засоби структуризованого розуміння інформації, що повідомляється, та порівняння результатів між підрозділами з часом.

Зрештою, оцінки ризиків безпеки на підприємстві є невід’ємною складовою пріоритетності проблем безпеки. Неформальне проведення таких оцінок може бути цінним доповненням до процесу відстеження питань безпеки, і офіційні оцінки мають

вирішальне значення при визначенні розподілу часу та бюджету у великих організаціях[16].

Навпаки, частковий підхід до розстановки пріоритетів щодо питань безпеки може призвести до катастрофи, особливо якщо проблема потрапляє до категорії високого ризику, а в кінцевому підсумку нехтується.

IT-орієнтовані переваги проведення оцінки ризику безпеки на підприємстві включають:

- Забезпечення об’єктивного підходу до бюджетування витрат на IT-безпеку та оцінки витрат.

- Забезпечення стратегічного підходу до управління IT-безпекою шляхом надання альтернативи для прийняття та обговорення рішень.

- Забезпечення основи для подальшого порівняння змін, внесених до заходів безпеки IT.

Розглянемо кожен крок процесу управління ризиками кібербезпеки більш докладно:

1. Визначення ризиків кібербезпеки

Gartner визначає IT-ризик як "потенціал для незапланованого, негативного результату бізнесу, що включає збій або неправильне використання IT". Отже, визначення ризику - це перший крок у процесі управління. Даний процес розпочинається з розуміння загроз, вразливостей та їхніх наслідків [19].

Загрози - це обставини або події, які можуть негативно вплинути на діяльність або активи організації через несанкціонований доступ до інформаційних систем. Загрози можуть проявлятися скрізь - у кібератаках, людському факторі, відмовах у структурі або конфігурації обладнання та навіть стихійних лихах.

Вразливості можна визначити як слабкі місця в інформаційній системі, процедурі безпеки, внутрішньому контролі або реалізації, які можуть бути використані джерелом загроз.

Наслідки найкраще визначити як несприятливі результати, що виникають, коли загрози використовують вразливості. Їх вплив вимірює тяжкість наслідків, і організація повинна буде оцінити такі витрати, намагаючись оцінити ризик.

2.Оцінка ризиків кібербезпеки

Оцінки ризиків підкреслюють важливість безпеки у організації і відіграють вирішальну роль у майбутньому управлінні ризиками. Даний процес передбачає декілька кроків:

- Надання переліку усіх активів та класифікація їхньої важливості.

- Визначення усі можливих загроз та уразливостей на підприємстві. На цьому етапі необхідно усунути всі вже відомі уразливості за допомогою відповідних засобів контролю.

- Оцінка ймовірності виникнення події загрози та проведення "аналізу впливу", щоб оцінити потенційні витрати. Це послужить керівництвом для інформування рішень щодо управління ризиками та заходів реагування на ризик [17].

3.Визначення можливих заходів щодо зменшення ризиків кібербезпеки

Одним із найважливіших етапів управління ризиками є розуміння всіх варіантів зменшення ризику в межах організації. IT команда підприємства може використовувати як технологічні, так і методичні практики, але кращим є поєднання обох. Заходи щодо зменшення технологічного ризику включають шифрування, брандмауери, програмне забезпечення для виявлення загроз та автоматизацію для підвищення ефективності системи. Найкращі методичні практики зменшення ризику включають навчальні програми з кібербезпеки, оновлення програмного забезпечення, рішення для управління привілейованим доступом (PAM), багатофакторну автентифікацію доступу та динамічне резервне копіювання даних [19].

4.Постійний моніторинг

Після того, як організація визначила, оцінила та зменшила ризики необхідно проводити постійний моніторинг, оскільки відбуваються зміни у законодавстві, існує ризик постачальника – необхідно обов’язково оцінити та задокументувати контроль за

безпекою, дотримуватись усіх вимог в ході співпраці із новими постачальниками і необхідно приділяти постійну увагу внутрішньому використанню IT - знати, які технології використовують внутрішні команди в організації та як вони дотримуються норм безпеки.

Найважливішу роль в цьому процесі відіграє система управління безперервністю бізнесу (СУББ) – складова частина системи управління інформаційною безпекою (СУІБ), в рамках якої встановлюються процеси безперервності бізнесу, здійснюється управління цими процесами та їх моніторинг.

Завдяки даній системі можна швидко повернутися до продуктивної роботи після зриву або збою у бізнес-процесах і, таким чином, скоротити час простоїв. Це ефективний спосіб зменшити подальші витрати та створити систему управління ризиками, що забезпечує правову визначеність. Підприємство також отримує значну конкурентну перевагу завдяки високому рівню доступності інформації у будь-якій час[20].

Обов’язково відзначимо, що комплексна СУББ повинна застосовувати орієнтований на процеси підхід і вимагає взаємодії між процесами управління, бізнес-процесами та процесами підтримки. Аналіз впливу на бізнес (Business Impact Analysis (BIA)) визначає основні процеси та оцінює їх вимоги щодо доступності[21]. Після аналізу компанії розробляються стратегії та плани протидії потенційним ризикам та проводять тести та навчання на основі сценаріїв. BIA– прогнозує наслідки порушення ділової функції і процесу та збирає інформацію, необхідну для розробки стратегій відновлення. Потенційні сценарії збитків слід визначати під час оцінки ризику[17].

Основні результати, пов'язані з BIA, включають:

- Визначення пріоритетності товарів та послуг, що мають важливе значення як стратегічні пріоритети безперервності бізнесу, які слід захищати та як швидко потрібно відновити надання продуктів / послуг.

- Інвентаризація ділової діяльності та ресурсів для встановлення того, що потрібно захищати та / або відновлювати після настання зриву.

- Встановлення часових рамок відновлення, які допомагають організації визначати, коли потрібно відновлювати ресурси, і допомагають у встановленні пріоритетів у варіантах пом’якшення ризику та виборі стратегій реагування та відновлення. Цілі часу відновлення (RTO) повинні бути встановлені таким чином, що, якщо їх досягти, це дозволить організації виконати свої стратегічні пріоритети.

RTO - ціль часу відновлення (recovery time objective) - допустимий час простою сервісу в разі збою [22].

Виявлення та оцінка впливу катастроф на бізнес забезпечує основу для інвестицій у стратегії відновлення, а також у стратегії запобігання та пом'якшення наслідків.

Бізнес-процес – сукупність взаємопов’язаних видів діяльності, метою яких є створення та подальша реалізація будь-якого продукту чи послуги. Кожен бізнес-процес має стартову та кінцеву точку і загалом ряд послідовних дій із виконання підтримки предмета діяльності на всіх етапах циклу подій [23]. Вище керівництво організації є безпосереднім власником бізнес-процесів і в процесах СУББ відіграє наступні ролі:

–погодження стратегій безперервності для критичних бізнес-процесів на підприємстві;

–вирахування показників робочої стійкості для критичних бізнес-процесів підприємства [24];

–надання достатніх фінансових коштів та ресурсів.

1.3 Життєвий цикл процесу управління безперервністю бізнесу

У відповідь на COVID-19 та соціальну дистанцію, організації переходять до альтернативних моделей роботи, відчуваючи підвищене напруження, швидке вичерпання ресурсів, утруднення в робочих процесах (можливі затримки в товарообміні, хвороба серед працівників, зміна умов праці, тощо). Тим не менше,

організації досягають своїх планів забезпечення безперервності бізнесу, передбачаючи роботу в надзвичайних ситуаціях та показуючи готовності до роботи під час пандемії. Зараз, як ніколи, управління безперервністю бізнесу (УББ) є критично важливим для будь-яких організацій [25].

Управління безперервністю бізнесу - це широкий термін, який охоплює кілька цілеспрямованих планів, щоб гарантувати, що організації зможуть продовжувати працювати через різні типи збоїв або катастроф [26].Ці плани описують як досягти стійкості в ділових операціях, загалом допомагаючи організаціям продовжувати працювати, перебуваючи під значним збоєм в роботі IT, втратою об'єкта, порушенням безпеки або, як склалося в даний час, пандемією.

Як продемонстровано нижче (рисунок 1.3) створення програми УББ починається з аналізу впливу на бізнес (Business Intelligence Analysis) і продовжується через план відновлення наслідків катастроф/ план аварійного відновлення (Disaster recovery plan), плану безперервності бізнесу (Business continuity plan), плану готовності до надзвичайних ситуацій (Emergency Preparedness Plan) та тестування плану (Plantesting). Протягом усього процесу зацікавлені сторони бізнесу із обов'язковим залученням IT-персоналу керують діяльністю організацією на основі плану по УББ [23].

Рисунок 1.3- Управління безперервністю бізнесу

Оскільки COVID-19 було оголошено пандемією, більшість організацій запровадили свої програми Систем управління бізнесу. Однак організаціям довелося швидко розробляти альтернативні робочі ситуації та коригувати свої ресурси. Незважаючи на цю складність, пандемія є своєрідною можливістю для організацій розвивати та вдосконалювати свої програми управління безперервністю бізнесу та краще позиціонувати себе для ефективного відновлення, коли трапляється чергова катастрофа або серйозні збої. Організації повинні спочатку зрозуміти основні компоненти програми УББ, включаючи компоненти та дії, які вони можуть вжити зараз для посилення ефективності своїх програм [27].

Аналіз впливу на бізнес- BIA. Аналіз впливу на бізнес забезпечує основу для всіх інших компонентів програми управління безперервністю бізнесу. Три основні компоненти, необхідні для заповнення BIA, включають визначення конкретних бізнес-процесів кожного відділу, кадрових ресурсів, необхідних для підтримки процесів, і всіх технологій для підтримки бізнес-процесів [28].

Оскільки організації працюють над виявленням бізнес-процесів та пов'язаних із ними залежностей, вони часто пропускають або неправильно фіксують наступні компоненти BIA:

- Мета часу відновлення (Recovery time objective (RTO)). Організації повинні визначити, як довго бізнес може функціонувати без визначеного процесу або технології, перш ніж вони відчують значний вплив на свою діяльність. Варто відзначити, що RTO слід враховувати як для бізнес-процесу, так і для технології, незалежно один від одного. Часто бізнес-процес потрібен швидше, ніж доступна технологія для його підтримки.

- Ціль точки відновлення (Recovery point objective (RPO)). Організації повинні визначити, наскільки динамічні дані в системі, щоб резервне копіювання могло виконуватися з необхідною частотою.

- Операційний вплив. BIA повинен визначити вплив, якщо процес не працює. Вплив можна описати кількома способами - фінансові витрати, юридичні або регулятивні негативні наслідки, репутаційна шкода - тому важливо вибрати масштаб впливу, який легко зрозуміти всім ключовим зацікавленим сторонам.

- Спілкування. Власники бізнес-процесів повинні слідкувати за компонентами BIA, включаючи RTO та RPO [22]. Із практичної точки зору варто наголосити на тому що, чим швидше потрібно відновлення, тим більші операційні витрати, тому очікування повинні бути належним чином встановлені та передані керівництву. Наприклад, якщо критичний процес повинен запрацювати протягом однієї години з інформацією в режимі реального часу, побудова системи, яка відповідає цим вимогам відновлення, коштуватиме значно дорожче, ніж процес, який може забезпечити кілька днів простою.

Існують можливості для вдосконалення планів реагування на основі ситуацій з якими сьогодні стикаються організації. Щоб зміцнити свій BIA, організації повинні:

– Регулярно проводити опитування своїх працівників щодо задоволеності робочими процесами;

– Визначити яким бізнес-процесам чи ресурсам слід надавати пріоритет над іншими.

– Оновлювати свій BIA для більш точної кількісної оцінки ресурсів, необхідних кожному бізнес-процесу.

– Постійно контролювати, що бізнес-процеси належним чином відображають RTO та RPO, як визначено раніше [22].

План ліквідації наслідків катастрофи -(Disaster recovery plan (DRP)) - це документ, який описує кроки організації щодо підключення IT-систем під час катастроф або збоїв та їх відновлення. Інформація, зібрана через BIA, спрямовує RPO та RTO певної технології у середовище, яке інформує IT про те, як будувати ці системи. Часто план ліквідації наслідків катастрофи містить типові для організацій помилки як:

- DRP, які зосереджені лише на одному типі катастрофи**.** Організації повинні переконатися, що DRP враховує різні типи збоїв, а не лише, наприклад, втрату основного постачальника послуг Інтернету (ISP).

- Плани, які не враховують жодних пунктів відмови. Повинні бути передбачені кроки для підтримки операцій, якщо виникає якась окрема точка відмови, наприклад один провайдер або один маршрутизатор на кожне місце.

Для того щоб уникнути перелічених вище помилок і зміцнити DRP, організаціям необхідно виконати наступні кроки:

1) Визначити прорахунки вимог до обладнання та використання ресурсів на основі потреби у підтримці мобільної робочої сили. Приклади того, з чим борються організації, включають:

–Віртуальні приватні підключення до мережі;

–Ноутбуки/ робочі станції, тощо;

–Периферійні пристрої (монітори, принтери, сканери, камери) і т. д.

2) Постійно оновлювати документацію на основі проблем або змін, з якими може зіткнутися організація під час міграції та розміщення робочої сили (працівників та постачальників) на наявність збоїв. Приклади включають:

–Елементи керування доступом (мережа);

–Зміни привілеїв (програми).

Отже, метою DRP є документування етапів відновлення - включаючи поетапну стратегію відновлення даних та систем із резервних копій та налаштування програм та ролей під час катастрофи, - що дає змогу виконувати ці дії кільком співробітникам [27].

План безперервності бізнесу-Business continuity plan (BCP))- детально описують людей, процеси та ресурси, необхідні для підтримки ділових операцій в умовах катастрофи або серйозних порушень нормальної ділової діяльності [28].Більш конкретно, BCP надають детальні кроки про те, які різні ділові відділи повинні робити, щоб продовжувати підтримувати як організацію, так і ключові зацікавлені сторони, часто, поки департаменти чекають відновлення IT-систем. Часто план безперервності бізнесу містить типові для організацій помилки як:

- Не надання належної уваги додатковим ресурсам, на які може покластися критичний бізнес-процес. Приклади включають залежність від інших департаментів щодо ресурсів або персоналу та залежність від постачальників для конкретних товарів чи послуг. Організації повинні переконатися, що BCP виключає всі відомі залежності.

- BCP має ефективно реагувати на певний тип збоїв або катастроф. Дозвіл приймати рішення під час надзвичайної ситуації, а не продумувати та документувати їх заздалегідь, збільшує ризик прийняття незадовільних або необдуманих рішень.

Для того щоб уникнути перелічених вище помилок і зміцнити BCP, організаціям необхідно виконати наступні кроки:

1) Опитування працівників про те, які ресурси потрібні для полегшення альтернативних ситуацій на робочому місці чи є потреба працівників виконувати робочі функції інших працівників. Організації повинні оновлювати ресурси BCP виходячи з цих додаткових потреб.

2) Практика належної ретельності з усіма критичними постачальниками. Через широкий спектр непередбачених потреб та ситуацій, що виникають в результаті пандемії COVID-19, організації здійснюють навігацію у складних відносинах з постачальниками. Організації повинні переконатися, що документація відображає зміни постачальника та включає всі критичні відносини з постачальниками.

3) Помітка про будь-які нові нормативні зміни, які могли б змінити час або вимоги до звітності та фінансові норми. Організаціям слід оновити документацію, календарі та інші ресурси, щоб відобразити нормативні зміни.

План готовності до надзвичайних ситуацій- (Emergency Emergency Preparedness Plan, EPP)- розроблений, щоб допомогти підтримати первинні реакції організацій на надзвичайні ситуації чи, наприклад, пандемії. Однією з цілей плану готовності до надзвичайних ситуацій є надання дієвої інструкції, яка захищає та рятує життя співробітників, які допомагають керувати організацією, та споживачів, яких вони обслуговують. Крім того, план готовності до надзвичайних ситуацій включає план реагування на аварії, який є практичною вказівкою яких вимог має дотримуватися IT-персонал у разі підозри на порушення або активну атаку. Часто план готовності до надзвичайних ситуацій містить типові для організацій помилки як:

- Відсутність практичних посібників для конкретних видів надзвичайних ситуацій. Нині більшість організацій мають план реагування на пандемію, але до інших надзвичайних ситуацій, які часто не враховуються, належать:

- Евакуація: стихійні лиха, такі як урагани та пожежі.

- Блокування: активні випадки стрілянини, обшуки зниклих або інші події.

- Негайний притулок на місці: екстремальні випадки, що вимагають від працівників та клієнтів залишатися у відведених місцях [30].

Відсутність комунікаційних планів та платформ для попередження зацікавлених сторін. Багато організацій не мають ефективних та надійних комунікаційних планів та пов'язаних платформ. Організації повинні переконатись, що контактна інформація та плани комунікацій їх співробітників є актуальними, включаючи тих, кому дозволено

спілкуватися зі ЗМІ, клієнтами, пацієнтами, членами та іншими. Там, де це доречно, також повинен бути встановлений план зв’язку з продавцями та третіми сторонами. Під час надзвичайної ситуації безцінний доступ до надійної платформи для підтримки ефективного спілкування [29].

Організації можуть використовувати уроки, отримані в результаті пандемії COVID-19, для посилення свого плану готовності до надзвичайних ситуацій шляхом:

- Документування за принципом "хто, що, як" політики організації щодо зовнішнього спілкування, включаючи тих, хто уповноважений створювати та надавати повідомлення, якою інформацією можна обмінюватися, і як - за допомогою яких каналів (електронною поштою, веб-сайтами, інформаційними бюлетенями) , що інформація буде доставлена. Усі ці деталі є критичними для комунікаційної стратегії організації.

- Оцінка потреб у персоналі. Деякі працівники можуть бути недоступними відразу під час надзвичайних ситуацій або пандемій, що призведе до прогалин ресурсів та втрати ефективності. Загалом, документування помилкових кроків, вироблених уроків та можливостей перехресного навчання, виявлених під час зривів, може допомогти організаціям навчатися та діяти ефективніше у майбутніх надзвичайних ситуаціях або катастрофах.

- Визначення того, яка технологія екстреного зв'язку буде використана для надсилання попереджень, оновлень та повідомлень працівникам. Якщо організації не мають такої платформи, зараз саме час інвестувати у це.

- Зокрема, під час пандемії COVID-19 організації повинні запитати, чи не відстежують вони внутрішньо випадки COVID-19, про які повідомляється, у межах робочої сили, і чи потрібно їм буде повідомляти про ризик впливу належним чином, коли знижуються вимоги щодо соціального дистанціювання[25].

- Навігаційна невизначеність. Організації стикаються з величезними проблемами. Ті, хто активно розробляє програми управління безперервністю бізнесу, здатні вирішити деякі з цих викликів на надійній основі. Хоча деякі організації можуть бути

більш підготовленими, ніж інші, ця пандемія - це унікальна можливість для організацій навчитися краще готуватися до небезпеки надзвичайних ситуацій, катастроф або навіть майбутніх пандемій.

Висновки за розділом 1

Підсумовуючи І Розділ, можемо стверджувати, що у 2020 році фахівці з інформаційної безпеки мали більше зовнішніх загроз та нових внутрішніх ризиків, і як результат, складність побудови робочого процесу через кризу COVID-19 (наприклад, встановлення безпечних зв'язків для віддалених робочих кадрів, відстеження загроз 24/7, запобігання появі нових мережевих загроз, спрямованих на робітників).

З точки зору безпеки необхідне надавання пріоритетів, що означає класифікацію усіх зібраних та оброблених організацією даних, які повинні бути засекречені. Створення задовільної політики класифікації даних - це перший крок до захисту конфіденційної інформації в організації. Управління даними є критично важливим для управління ризиками, так як це контролює та регулює конфіденційність, цілісність та доступність інформації у організації.

Управління безперервністю бізнесу охоплює кілька цілеспрямованих планів і гарантує, що організації зможуть продовжувати працювати незважаючи на різні типи збоїв або катастроф: втрату об'єкта, порушення безпеки, пандемію тощо, у тому числі навіть перебуваючи під значним тиском на IT-системи, будуть стійкими в ділових операціях.

РОЗДІЛ 2. РОЗРОБКА МЕТОДИКИ ОЦІНЮВАННЯ СТАНУ ЗАХИЩЕННОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ

2.1. Ідентифікація та оцінка загроз і вразливостей

Нині тенденції розвитку бізнесу в Україні демонструють важливість відстеження ризиків інформаційної безпеки для збереження конкурентоспроможності на ринку нашої держави. Гострою необхідністю є реалізація заходів захисту інформаційних активів. які постійно змінюються і тому. У даних умовах ризики інформаційної безпеки постійно змінюються, тому стає дедалі важче прогнозувати їх заздалегідь, як наслідок, збільшується кількість кіберзлочинів, часто змінювані нормативні вимоги, пряма залежність бізнесу від безперебійної роботи інформаційної системи підприємства.

У зв'язку із чим, незважаючи на складність процесу, інтеграція інформаційних систем в щоденних умовах набуває все більшого значення. Для цього необхідна побудова єдиного інформаційного простору та об'єднання функціоналу вже існуючих і нових інформаційних систем. Дані умови дозволяють опанувати оперативністю та стратегічним потенціалом управління компанією та його виробництвом.

Як правило, на підприємствах наразі використовується завчасний аналіз для попередження можливих проблем СУІБ. Одним із ключових факторів успішного запровадження і практичної роботи СУІБ є оцінка та аналіз ризиків ІБ.

Досвід кращих міжнародних практик показує, що кожна можлива загроза має бути ідентифікована та зафіксована під час виконання бізнес-процесу за такими принципами: джерела походження, ймовірність випадкових/ навмисних помилок персоналу, частота виникнення, вплив на роботу організації, масштаб втрат при їх настанні, тощо [31, с.4].

Перелік таких загроз в компанії має бути на постійному контролі департаментом інформаційної безпеки та безпосереднім керівництвом установи і переглядатися не рідше одного разу на рік вже з урахуванням частоти виникнення інцидентів інформаційної безпеки та коректності дій, направлених на пом'якшення наслідків[31, с.5].

Виявлення та аналіз ризиків – важливі процедури виявлення факторів ризиків ІБ і оцінки їх вагомості. Вони включають оцінку ризиків і методи їх зниження або зменшення пов'язаних з ними несприятливих для організації наслідків. На початку проведення аналізу проводиться фіксація відповідних факторів і оцінка їх вагомості. Такими факторами є: цінні активи підприємства, наявні та можливі вразливості, потенційні загрози.

Процес управління ризиками інформаційної безпеки здійснюється для всієї компанії і є безупинним та цілісним процесом, до якого можна застосувати ефективний принцип «ПВПД» (плануємо – виконуємо - перевіряємо - діємо)[31, с.9]. Розглянемо який більш детально: серед «запланованих» - аналіз ресурсів СУІБ та оцінка ризиків. До моделі «виконування» відносяться основні фази впровадження плану оброблення ризиків. Постійний моніторинг та перегляд ризиків- фаза «перевіряємо». І як кінцевий результат – «діємо» (постійна підтримка та удосконалення процесу управління ризиками інформаційної безпеки). Відповідальними за зі процеси, як правило, є керівництво установи.

За допомогою використання простої матриці ризиків, що допомагає підприємствам використовувати інформацію, яку вони вже отримали про кожну пару вразливості / загрози, яка була визначена спеціалістами з інформаційної безпеки, та нанести її на матрицю. Ризики, які одночасно можуть трапитись і матимуть серйозні наслідки, визначаються як найвищий пріоритет, тоді як ризики, які навряд чи відбудуться і мали б незначні наслідки- визначені як найнижчий пріоритет, а все інше міститься між цими граничними показниками [32].Рекомендується для великої організації з великою кількістю ризиків змоделювати більш поглиблену матрицю

ризиків 5 × 5; менші організації, у яких менше ризиків для визначення пріоритетів, можуть скористатися простою матрицею 3 × 3 і при цьому отримати ті ж переваги.

Постає практичне питання: «Чи повинна вся компанія використовувати єдину загальну матрицю оцінки ризиків або кожен відділ повинен мати свою власну?» У першому випадку матиме перевагу послідовний підхід. У іншому -дозволяє проводити більш цілеспрямовані оцінки. Зрештою, для організації найкраще мати можливість коригувати розмір та дизайн своєї матриці ризиків за необхідності [32].

Практично розглянемо і побудуємо матрицю 5 × 5 з оглядом на велику корпорацію:

Нехай матриця ризику 5х5 містить 5 рівнів ймовірності та тяжкості.

Ймовірність

1) Не є ймовірним;

2) Віддалена (малоймовірний, хоча можливий);

3) Час від часу (може траплятися зрідка під час стандартних операцій);

4) Ймовірно (очікувано, відбудеться в даний час);

5) Часті (можливо, трапляються, як того і очікується).

Серйозність

1) Незначна (небезпека не призведе до серйозних наслідків, або має віддалену можливість пошкодження);

2) Гранична (небезпека може спричинити пошкодження, але наслідки не будуть серйозними);

3) Помірна (небезпека може призвести до серйозних збоїв, пошкодження майна або обладнання, з великою ймовірністю відносно швидкого відновлення);

4) Критична (небезпека може призвести до серйозних травм, пошкодження майна або обладнання);

5) Катастрофічна (небезпека може повністю спинити роботу підприємства без довгої можливості відновлення і потребуватиме великого проміжку часу для повного відновлення).

Отже, які є переваги використання матриці ризику 5х5? Даний формат 5х5 дозволяє проводити оцінки ризиків з максимальною деталізацією та чіткістю.

Проте, які можливі недоліки використання матриці ризику 5х5?Деякі експерти стверджують, що матриця 5х5 є надто складною і занадто великою роботою для використання для менших проектів. Для деяких завдань стає сумнівно, чи справді необхідний такий рівень деталізації.

Ймовірність		Тяжкість				
		Катострофічна - 5	Критична -4	Помірна - 3	Гранична - 2	Незначна - 1
	Часто - 5	Висока- 25	Висока- 20	Серйозна -15	Серйозна -10	Середня- 5
	Ймовірно- 4	Висока- 20	Серйозна - 16	Серйозна - 12	Середня - 8	Середня - 4
	Нерегулярна - 3	Серйозна -15	Серйозна - 12	Середня - 9	Середня - 6	Низька - 3
	Віддалена -2	Серйозна -10	Середня - 8	Середня - 6	Середня - 4	Низька - 2
	Найменш ймовірно- 1	Середня- 5	Середня - 4	Низька - 3	Низька - 2	Низька - 1

Рисунок 2.1 - Матриця ризику 5х5, що містить 5 рівнів ймовірності та тяжкості наслідків

Отже, для проведення процесу ідентифікація та оцінка загроз і вразливостей необхідно виконати наступні завдання: застосувати модель аналізу ризиків «ПВПД», побудувати матрицю оцінювання ризиків підприємства, застосувати отримані результати до інформаційних активів. Як результат, описати можливі шляхи вдосконалення процесу управління ризиками на підприємстві.

2.2. Важливість управління ризиками та обґрунтування проведення оцінки ризику безпеки

Кібербезпека на фундаментальному рівні - це управління ризиками безпеки. Зосереджуючи належним чином увагу на управлінні дотриманням вимог щодо інформаційної безпеки в організації, обов'язковим структурне порівняння відповідності із системами, що використовуються для обробки, зберігання та транспортування інформації в організації. Захист цієї інформації вимагає правильної класифікації даних та конкретних вимог до контролю відповідно до інструкцій з інформаційної безпеки.

У зв'язку з цим, потрібно розробити та надати чіткі керівні вказівки щодо того, як буде здійснюватися впровадження та управління для захисту систем та їх інформації, обов'язково врахувавши який вплив має втрата, порушення або несанкціоноване розкриття інформації [33].

Управління ризиками на підприємстві є ключовим підходом до управління організацією. Незважаючи на те, що нормативні акти не вказують організаціям на те, як контролювати або захищати свої системи, вони вимагають, щоб ці системи були захищені та щоб організація доводила незалежним аудиторам, що їхня інфраструктура безпеки та контролю створена та діє ефективно [34]. Методологія оцінки ризиків на підприємстві стала усталеним підходом до виявлення та управління системним ризиком для організації. І, все більше і більше, цей підхід застосовується в різноманітних сферах.

Класично ризик безпеки IT розглядався як відповідальність IT або персоналу, що обслуговують мережі, оскільки ці працівники найкраще розуміють компоненти інфраструктури контролю. Однак, цей підхід має обмеження. Оскільки системи стають більш складними, інтегрованими та пов'язаними з третіми сторонами, бюджет безпеки та контролю швидко досягає своїх обмежень. Тому, щоб забезпечити найкраще використання наявних ресурсів, IT повинні розуміти відносну значимість різних наборів систем, додатків, даних, механізмів зберігання та зв'язку. Щоб задовольнити такі вимоги, організації повинні проводити оцінки ризиків безпеки, що застосовують підхід оцінки ризиків на підприємстві, та включати всіх зацікавлених сторін для

забезпечення вирішення всіх аспектів IT-організації, включаючи апаратне та програмне забезпечення, навчання поінформованості працівників та бізнес-процеси [35].

Оцінки ризиків безпеки підприємств проводяться, щоб дозволити організаціям оцінити, виявити та змінити загальний стан безпеки, а також гарантувати співробітникам та клієнтам безпеку операцій, ефективно управляти організацією та розгляд усієї установи з точки зору зловмисника. Цей процес необхідний для отримання зобов'язання керівництва організації розподіляти ресурси та впроваджувати відповідні рішення щодо безпеки.

Комплексна оцінка ризиків безпеки на підприємстві також допомагає визначити цінність різних типів даних, що генеруються та зберігаються в організації. Без оцінки різних типів даних в організації майже неможливо визначити пріоритети та розподілити технологічні ресурси там, де вони найбільше потрібні. Для точної оцінки ризику керівництво повинно визначити дані, які є найбільш цінними для організації, механізми зберігання цих даних та пов'язані з ними вразливості.

Отже, який ризик для безпеки підприємства, якщо не буде застосоване належне управління дотриманням вимог інформаційної безпеки? Компанія може не створити процеси управління ризиками та захисту інформації, які є обдуманими, конкретними, повторюваними та добре зрозумілими кожному, хто взаємодіє з конфіденційною інформацією, тому не буде виконане впровадження, сертифікація, перевірка та атестація рівня захисту інформації організації на основі її толерантності до ризиків[33, с.114].

Для того щоб усунути слабкі місця у вимогах відповідності для інформаційної безпеки, необхідно по-справжньому розуміти ризики, їх вплив на бізнес і те, як безпека вписується в загальну бізнес-стратегію організації. Можна також використовувати цю загальну бізнес-стратегію для безпосереднього формування та підтримки вибору системи управління дотриманням вимог інформаційної безпеки для програми кібербезпеки в цілому.

Обґрунтовуючи проведення оцінки ризику безпеки, організації мають багато причин для ініціативного та повторюваного підходу для вирішення проблем інформаційної безпеки. Законодавчі та нормативні вимоги, спрямовані на захист конфіденційних або особистих даних, а також загальні вимоги громадської безпеки створюють умови для компаній будь-якого розміру приділяти максимальну увагу та пріоритет ризикам ІБ [36].

Оцінка ризиків ІТ-безпеки приймає багато назв і може сильно відрізнятися з точки зору методу, строгості та обсягу, але основна мета залишається незмінною: виявити та кількісно оцінити ризики для інформаційних активів організації. Ця інформація використовується для визначення, як найкраще пом'якшити ці ризики та ефективно зберегти основну діяльність організації.

Серед ґрунтовних причин для проведення оцінки ризику безпеки на підприємстві можемо відокремити наступні:

- обґрунтування витрат. Додавання додаткових засобів захисту для забезпечення безпеки, як правило, передбачає додаткові витрати. Ефективний процес оцінки ризиків ІТ-безпеки повинен навчити ключових менеджерів бізнесу про найважливіші ризики, пов'язані з використанням технологій, а також автоматично та безпосередньо обґрунтовувати інвестиції в безпеку.

- продуктивність. Оцінка ризиків безпеки підприємств повинна покращити продуктивність ІТ-операцій, безпеки та аудиту. Вживаючи заходів для формалізації огляду, створення її загальної структури, збору знань про безпеку та закладання їх в базі даних системи підприємства та впровадження функцій самоаналізу, оцінка ризику може підвищити продуктивність діяльності організації.

- порушення бар’єрів. Безпека повинна вирішуватися як керівництвом організації, так і ІТ-персоналом. Керівництво підприємства відповідає за прийняття рішень, які стосуються відповідного рівня безпеки для організації. З іншого боку, ІТ-персонал відповідає за прийняття рішень, що стосуються реалізації конкретних вимог безпеки систем, програм, даних та засобів управління.

- самоаналіз. Система оцінки ризиків безпеки на підприємстві завжди повинна бути досить простою у використанні, без необхідності будь-яких знань з питань безпеки та IT-експертів. Це дозволить керівництву взяти на себе відповідальність за безпеку систем, програм та даних організації, що також дозволяє безпеці стати більш важливою частиною культури організації.

- комунікація. Отримуючи інформацію з декількох частин організації, оцінка ризику безпеки підприємства підвищує рівень комунікації та пришвидшує прийняття рішень.

Процеси оцінки ризиків на підприємстві та управління ризиками на підприємстві складають суть системи інформаційної безпеки. Це процеси, які встановлюють правила та керівні принципи політики безпеки, перетворюючи цілі системи інформаційної безпеки в конкретні плани реалізації ключових засобів контролю та механізмів, що мінімізують загрози та вразливості. Кожну частину технологічної інфраструктури слід оцінювати на предмет її профілю ризику. З цієї оцінки слід прийняти рішення ефективно і ефективно розподілити час та гроші організації на досягнення найбільш доцільної та найкращої загальної політики безпеки. Процес проведення такої оцінки ризику може бути досить складним і повинен враховувати вторинні та інші наслідки дії (або бездіяльності) при прийнятті рішення про те, як вирішити питання безпеки для різних IT-ресурсів [37].

Залежно від розміру та складності IT-середовища організації, може стати очевидним, що потрібна не стільки детальна оцінка точних значень та ризиків, скільки більш загальна пріоритетність. Визначення того, як розподіляються ресурси безпеки, повинно враховувати відношення ключових менеджерів бізнесу до ризику, оскільки вони глибше розуміють всесвіт ризиків безпеки організації та краще підготовлені для прийняття цього рішення.

Кожна організація має свою специфіку, тому рішення щодо того, яку оцінку ризику слід проводити, значною мірою залежить від конкретної організації. Якщо визначено, що всім потребам на даний момент є загальне розставлення пріоритетів,

може бути застосований спрощений підхід до оцінки ризику безпеки підприємства, і, навіть якщо вже визначено, що повинна бути проведена більш поглиблена оцінка, спрощений підхід може бути корисним першим кроком у формуванні огляду для керівництва процесом прийняття рішень в рамках цієї більш поглибленої оцінки.

Підхід до оцінки або методологія аналізує взаємозв'язок між активами, загрозами, вразливими місцями та іншими елементами. Існує безліч методологій, але загалом їх можна класифікувати на два основні типи: *кількісний та якісний аналіз*. Обрана методологія повинна мати можливість скласти кількісну заяву про вплив ризику та вплив проблем безпеки, а також деякі якісні заяви, що описують значення та відповідні заходи безпеки для мінімізації цих ризиків[38].

Оцінка ризиків для безпеки повинна бути постійною діяльністю. Комплексну оцінку ризиків безпеки підприємства слід проводити принаймні раз на два роки для вивчення ризиків, пов'язаних з інформаційними системами організації. Оцінка ризику безпеки підприємства може дати лише короткий огляд ризиків інформаційних систем у певний момент часу. Для критично важливих інформаційних систем настійно рекомендується проводити оцінку ризику безпеки постійно.

2.3. Процеси управління інформаційними ризиками, методологія їх застосування

Виконуючи процес оцінки ризиків насамперед аналізується вже створена система й середовище в компанії та виявляються ризики шляхом обробки зібраної інформації і конкретних даних. Потрібно уважно і послідовно враховувати всю відповідну інформацію, незалежно від її формату зберігання. Кілька видів інформації, яку найчастіше збирають, включає основні вимоги та цілі безпеки. А це в свою чергу:

–державні закони та нормативні акти, що стосуються мінімальних вимог контролю безпеки;

–архітектура та інфраструктура системи або мережі, наприклад, мережева діаграма, що показує, як налаштовуються та взаємопов'язані ресурси;

–інформація, доступна для громадськості або доступна на веб-сайті організації;

–фізичні активи, такі як апаратне забезпечення, у тому числі в центрі обробки даних, мережі та комунікаційних компонентах та периферійних пристроях (наприклад, настільний комп'ютер, ноутбук, тощо);

–операційні системи на ПК, серверах та системах управління мережею;

–сховища даних, такі як системи управління базами даних та файли;

–список усіх додатків;

–підтримувані протоколи та мережеві послуги, що пропонуються всередині IT-інфраструктури організації;

–застосовувані системи безпеки, такі як механізми контролю доступу, контроль змін, антивірус, контроль спаму та моніторинг мережі;

–розгорнуті компоненти безпеки, такі як брандмауер та системи виявлення вторгнень;

–критичні процеси, як бізнес-процес, процес роботи комп’ютера, мережевий процес та процес роботи додатків;

–механізми ідентифікації та автентифікації;

–документована політика безпеки, процедури та керівні принципи.

Отже, процеси управління інформаційними ризиками та сфера їх оцінки на підприємстві може охоплювати зв’язок внутрішньої мережі з Інтернетом, захист безпеки комп’ютерного центру, використання IT-інфраструктурою певного відділу або IT-безпеку всієї організації. Таким чином, цілі повинні визначати всі відповідні вимоги безпеки, такі як захист при підключенні до Інтернету, виявлення районів високого ризику в приміщеннях із комп’ютерами або оцінка загального рівня інформаційної безпеки відділу [37].

Ключові вимоги до безпеки повинні базуватися на бізнес-потребах, якими, як правило, керується вищий менеджмент, щоб визначити бажаний рівень захисту.

Фундаментальною складовою будь-якої оцінки ризику повинні бути відповідні нормативні вимоги, такі як Закон України «Про інформацію» від 02.10.1992 № 2657-XII, Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР, Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI, Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373, Постанова Кабінету міністрів України «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736, Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ:НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі; НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі, НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу, тощо.

Нижче наведено загальні завдання, які слід виконувати при оцінці ризику безпеки на підприємстві:

- визначення бізнес-потреб та зміни вимог, які можуть вплинути на загальний напрямок ІТ та безпеки;

- перегляд коректності та дієвості існуючої політики безпеки, стандартів, керівних принципів та процедур;

- аналіз активів, загроз та вразливих місць, включаючи їх вплив та ймовірність;

- оцінка фізичного захисту, що застосовується до обчислювального обладнання та інших мережевих компонентів;

- проведення технічного, процедурного огляду, аналізу архітектури мережі, протоколів та компонентів для забезпечення їх реалізації відповідно до політики безпеки;

- перегляд та перевірка конфігурації, впровадження, використання систем віддаленого доступу, серверів, брандмауерів, зовнішніх мережевих підключень, включаючи підключення до Інтернету клієнта;

- перегляд логічного доступу та інші механізми автентифікації;

- перегляд поточного рівня обізнаності персоналу в організації;

- перегляд угод, що стосуються послуг або товарів від постачальників та підрядників;

- розробка практичних технічних рекомендацій щодо усунення виявлених вразливих місць та зниження рівня ризику безпеки.

Складання карт загроз для активів та уразливостей може допомогти визначити їх можливі комбінації. Кожна загроза може бути пов'язана з певною вразливістю, або й з кількома. Якщо загроза не може використати вразливість, це не є ризиком для активу. Діапазон усіх можливих комбінацій слід зменшити перед проведенням аналізу ризику. Деякі комбінації можуть не мати сенсу або є мінімальна вірогідність їх здійснити. Цей взаємозв'язок активів, загроз та уразливостей є критичним для аналізу ризиків безпеки, але такі фактори, як обсяг проекту, бюджет тощо, можуть також впливати на рівні та величину відображень[39].

Після виявлення активів, загроз та уразливостей можна визначити вплив та ймовірність ризиків для безпеки [40].

Оцінка впливу (також відома як аналіз впливу або оцінка наслідків) оцінює ступінь загальної шкоди або збитків, які можуть виникнути в результаті експлуатації вразливості системи безпеки. Кількісними елементами впливу є показники доходів, прибутку, вартості, рівня обслуговування, нормативних актів та репутації. Необхідно враховувати рівень ризику, який можна допустити, і те, як і коли на активи може вплинути такий ризик. Чим серйозніші наслідки загрози, тим вищий ризик. Наприклад,

якщо ціни в тендерному документі скомпрометовані, витрати для організації будуть продуктом втраченого прибутку від цього контракту та втраченого навантаження на виробничі системи із мінімально відсотковою ймовірністю виграшу контракту.

Оцінка ймовірності оцінює ймовірність виникнення загрози. При цьому типі оцінки необхідно визначити обставини, які вплинуть на ймовірність виникнення ризику. Зазвичай ймовірність загрози зростає із збільшенням кількості авторизованих користувачів. Ймовірність може бути виражена через частоту виникнення, наприклад, раз на день, раз на місяць або раз на рік. Чим більша ймовірність виникнення загрози, тим вищий ризик. Може бути важко обґрунтовано оцінити вірогідність багатьох параметрів; отже, відносна ймовірність може бути використана як рейтинг.

Прикладом є висока ймовірність спроби використати нову вразливість до встановленої операційної системи, як тільки вразливість буде опублікована. Якщо постраждала система класифікується як критична, вплив також є великим. Як результат, ризик цієї загрози високий.

Для кожного ідентифікованого ризику необхідно визначити його вплив та ймовірність, щоб дати загальний оцінений рівень ризику. При складанні оцінки слід чітко визначити припущення. Дане двовимірне вимірювання ризику дозволяє легко наочно представити висновки по процесу оцінки [41].

У наш час управляти ризиками кібербезпеки на підприємстві складніше, ніж будь-коли. Забезпечення безпеки архітектури, систем сумісності може здатися надзвичайним навіть для найбільш досвідчених команд сьогодні. Так, Дейв Хеттер, консультант з питань кібербезпеки в Intrust IT з 30-річним досвідом роботи у галузі, пояснює: “Оскільки більша частина нашого фізичного світу пов’язана з віртуальним світом та знаходиться під його контролем, а більша частина нашої ділової та особистої інформації стає цифровою, ризики дедалі збільшуються» За словами фахівця, ще ніколи не було так складно побудувати процес управління ризиком кібербезпеки "[42]. Таким чином, виникає глобальне питання: «Чому сьогодні керувати кіберризиком набагато складніше, ніж будь-коли раніше?» Наприклад, дослідження Інституту

Понемона (Ponemon Institute) порахувало, що в середньому компанія передає 80% конфіденційної інформації в хмарі третім сторонам – хмарним постачальникам. Тобто, сучасні підприємства несуть відповідальність за треті сторони, які обробляють дані від їх імені. Таким чином, команди IT-безпеки мають в своїх обов'язках, окрім управління складною інфраструктурою, ще й ризик постачальників [43].

Наступним фактором складності управління кіберризиком є пандемія COVID-19, що стосується працівників, які віддалено працюють у незахищених мережах, шифрованими протоколами безпеки та скороченням бюджету та персоналу в організаціях, що обумовлено глобальною кризою[25]. Підприємства стикаються з більшою відповідальністю, але з меншою кількістю задіяних ресурсів.

Отже, зіткнувшись з безліччю перешкод нині, як організації мають ефективно управляти ризиками?

Ефективне управління ризиком кібербезпеки вимагає, щоб усі працівники в системі працювали з чітко визначеними ролями та відповідали за конкретні обов'язки. Сьогоднішня ситуація ризику рішуче вимагає уніфікованого, скоординованого, дисциплінованого та послідовного управлінського рішення. Нижче наведено кілька ключових компонентів дій щодо управління ризиками, про які повинні пам'ятати всі організації:

– Розробка надійної політики та інструментів для оцінки ризику постачальників;

– Виявлення внутрішніх слабких сторін, таких як відсутність двофакторної автентифікації, тощо;

– Зменшення IT-ризиків за допомогою навчальних програм або нових політик та внутрішнього контролю;

– Перегляд документації щодо управління ризиками безпеки для перевірок зі сторони регуляторних органів.

Що стосується безпосередньо управління ризиками, організації, як правило, дотримуються чотирьох етапів, починаючи з виявлення ризику. Далі ризик оцінюється на основі вірогідності загроз, що використовують вразливі місця, та потенційного

впливу. Ризики мають пріоритет, організації вибирають з різноманітних стратегій пом'якшення наслідків. Четвертий крок, моніторинг, побудований відповідно до реакції на ризик та контролює поточний стан, незважаючи на постійні зміни умов [35].

Умовний життєвий цикл управління ризиками на підприємстві можна подати у вигляді блок-схеми:

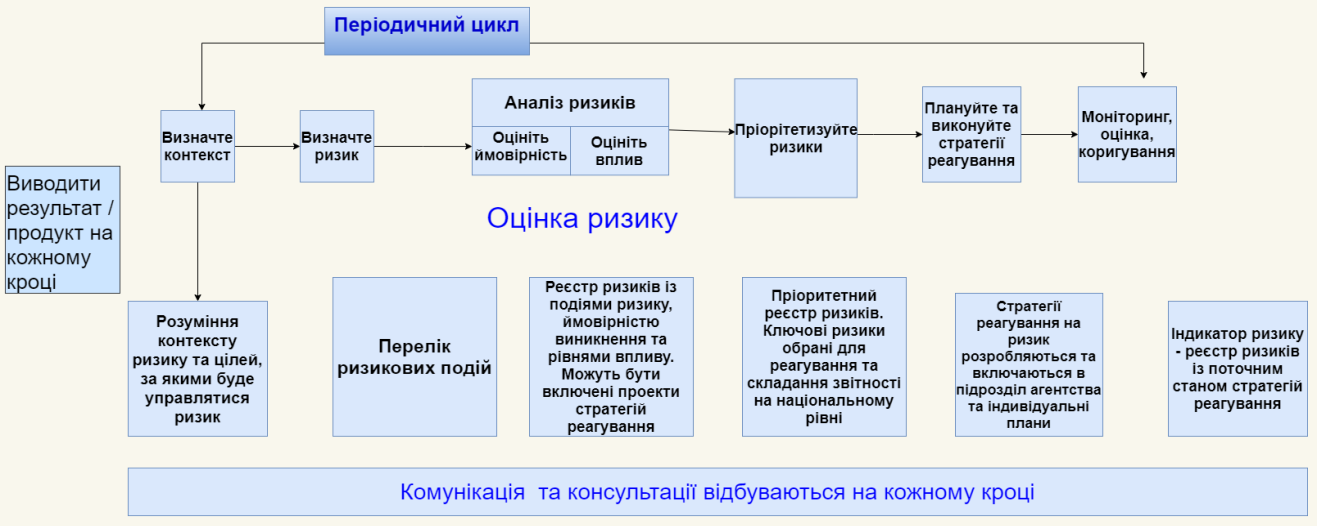


Рисунок 2.2- Умовний життєвий цикл управління ризиками на підприємстві

У верхньому рядку на рисунку 2.2 зображено шість кроків зі стрілками, що вказують послідовність. Нижній рядок пояснює результати кожного кроку. Об'єднуючим елементом є те, що спілкування та консультації між керівництвом і виконавцями (співробітниками організації) відбуваються на всіх етапах. Отже, послідовність є наступною:

1) Визначення контексту. Контекст - це середовище, в якому працює підприємство і на яке впливають ризики.

2) Визначення ризиків. Це означає виявлення всебічного набору позитивних та негативних ризиків - визначення того, які події можуть посилити або навпаки перешкодити досягнення цілей, включаючи ризики не реалізації можливості.

3) Аналіз ризиків. Це включає оцінку ймовірності настання кожної виявленої події ризику та потенційного впливу описаних наслідків.

4) Розміщення пріоритетів ризиків. Експозиція розраховується для кожного ризику, виходячи з вірогідності та потенційного впливу, а потім ризики визначаються пріоритетними на основі їх експозиції.

5) Планування та виконання стратегії реагування на ризик. Відповідна реакція визначається для кожного ризику, а рішення приймаються безпосередньо керівництвом щодо ризиків.

6) Моніторинг, оцінка та коригування. Постійний моніторинг гарантує, що умови ризику на підприємстві залишаються в межах визначених рівнів ризику, оскільки ризики кібербезпеки змінюються.

Для того, щоб допомогти професіоналам з кібербезпеки повідомити про значення превентивної безпеки своїм управлінським командам, нещодавно NIST – Національний Інститут стандартів та технологій США (The National Institute of Standards and Technology) опублікував документ під назвою «Інтеграція кібербезпеки та управління ризиками підприємств» (NISTIR 8286). Основна мета його керівництва зосереджена на просуванні інновацій та використанні реєстру ризиків, який описується як «сховище інформації про ризики», для ефективної інтеграції управління ризиками кібербезпеки в загальну програму ERM з метою підвищення економічної безпеки та покращення якості життя підприємства[44].

ERM (Enterprise risk management – керування ризиками підприємства): концепція, що описує методики та процеси впроваджені організаціями для управління ризиками та можливостями, пов’язаними з досягненням поставлених задач та цілей. Вона дозволяє закласти фундамент ризик- менеджменту, в тому числі виявленні конкретних події або обставин, що впливають на досягнення завдань компаній(загрози та можливості), також дають оцінку масштабам уразливостей, розробляють стратегії реакції та підсліджують ефективність.

Управління в ERM сконцентровано на 4 основних задачах:

- повне розуміння ризиків усіх співробітників компанії від генерального директора до молодшого менеджера;
- координація управління ризиками (задля підвищення економічної доцільності усього підприємства, а не окремої ланки);
- узгодження оцінки ризиків дозволяє сконцентрувати ризики з усіх дільниць підприємства;
- загальна відповідальність за ризики, що розподіляються між усіма співробітниками компанії.

Отже, що саме являє собою реєстр ризиків, яку інформацію слід відслідковувати в ньому та які стратегічні переваги від його оновлення? Як визначено в керівництві NISTIR 8286, реєстр ризиків - це «сховище інформації про ризики», що містить опис певного ризику, ймовірність його виникнення, його потенційний вплив з точки зору витрат, яке він займає місце в першочерговості по своєму впливу щодо інших ризиків [44]. Це корисна конструкція збору інформації: вони допомагають організації ефективно інтегрувати управління ризиками кібербезпеки в загальну програму управління ризиками на підприємстві.

Реєстр ризиків може бути інтегрований у будь-яку методологію управління ризиками, яку використовує організація. Можна відслідкувати також подібність у підходах для ведення реєстру ризиків у всіх організаціях: визначення контексту, ідентифікування ризиків, аналіз ризиків, оцінка їх важливості, виконання контрвідповідей на ризик, а також реагування на зміни з часом. Тобто, реєстр ризиків є найважливішим інструментом, який організації повинні використовувати для відстеження та передачі інформації про ризик для всіх цих етапів на всьому підприємстві. Він служить ключовим фактором для прийняття рішень з питань управління ризиками.

Відзначимо, що документ про ризики NIST «Інтеграція кібербезпеки та управління ризиками підприємств» був оприлюднений завдяки багаторічному

спостереженню команди Національного інституту стандартів і технологій. Було зауважено, що більшість організацій не оцінюють і не вимірюють ризик кібербезпеки з такою ж суворістю або послідовними методами, як інші типи ризиків в організації. NIST намагається допомогти державному та приватному секторам в підвищенні якості інформації про кіберризики, яку вони збирають та надають своїм управлінським групам та особам, що приймають рішення. У свою чергу, така практика сприятиме кращому управлінню кібербезпекою на рівні підприємства та підтримуватиме основні цілі фірми[45].

Національний інститут стандартів також створив незалежну систему управління ризиками, відому як Спеціальна публікація NIST 800-30 для керівництва оцінками ризиків у федеральній інформаційній системі. Структура 800-30 розширюється за вказівкою Спеціальної публікації 800-39- механізмом управління ризиками, який забезпечує каталог контролю безпеки та конфіденційності для федеральних інформаційних систем. Хоча NIST SP 800-30 не є обов'язковим у приватному секторі, він надає корисну інформацію як посібник для всіх організацій, які мають оцінювати свій ризик [45].

На основі цього було складено результуючу таблицю подібності міжнародних стандартів щодо управління ERM та управління ризиками:

Таблиця.1.1

Подібність міжнародних стандартів щодо управління ERM та управління ризиками

		NIST Risk Management Documents		
ERM	**ISO 31000:2018**	**SP 800-30 Rev. 1**	**SP 800-37 Rev.2**	**SP 800-39**

Визначте контекст		Встановіть зовнішній/ внутрішній контекст	Підготовка до оцінки ризику	Підготувати стратегію управління ризиками	Обрамлення ризику

Продовження таблиці 1.1

Визначте ризики	Оцінка ризику	Визначення ризику	Завдання 2-1: Визначити та охарактеризувати джерела загрози, що викликають загрозу; Завдання 2-2: Визначити потенційні події загроз, джерела загроз; Завдання 2-3: Визначення вразливостей / схильних умов	Підготуйте завдання Р-3, Р-14: звіт про оцінку ризику	
Проаналізуйте ризики		Аналіз ризиків	Завдання 2-5: Визначити несприятливий вплив від загрозливих подій, Завдання 2-6: Визначити ризик для організації Звіт про оцінку		Оцінка ризику SP800-30
Оцініть ймовірність		Розрахувати рівень ризику			
Оцініть вплив					
Пріоритети ризиків					
Розрахувати експозицію					
Плануйте та виконуйте стратегії реагування/ Моніторинг, оцінка та коригування		Оцінка ризику/ Моніторнг та огляд	Завдання 3-1: Повідомлення результатів оцінки ризиків; Завдання 3-2: Поділитися інформацією, пов’язаною з	Відповідь на ризик R-3	Відповідь на ризик/ моніторинг ризиків
				Класифікувати, впровадити,	

			ризиками/ Завдання 4-1: Проводити постійний моніторинг факторів ризику. Оновлення оцінки ризику	санкціонувати (R-4), Завдання А-6 План дій та етапи/ моніторинг	

Отже, узагальнена методика аналізу щодо захищеності інформаційних ресурсів установи включає:

- аналітичний збір по вихідних даних в інформаційній системі загалом;
- проведення оцінки ризиків по загрозами безпеці інформаційним ресурсам підприємства;
- постійний моніторинг механізмів безпеки організаційного рівня, огляд політики безпеки підприємства і організаційно-розпорядчої документації щодо забезпечення режиму ІБ на оцінку їх відповідності вимогам затвердженим нормативним документам, а також їх адекватності у відношенні до вже існуючих ризиків;
- ручний аналіз конфігураційних файлів маршрутизаторів і проксі-серверів, поштових і DNS-серверів;
- сканування зовнішніх мережевих адрес локальної мережі;
- сканування ресурсів локальної мережі внутрішньо в організації;
- аналіз конфігурації серверів і робочих станцій за допомогою спеціалізованих програмних агентів [46].

Описані вище технічні методи включають в себе як активне, так і пасивне тестування системи захисту. Передбачає конкретне відтворення дій потенційного порушника інформаційної безпеки- активне тестування; пасивне тестування - аналіз конфігурації ОС і додатків по шаблонах з використанням списків перевірки. Дані види перевірки можна виконувати вручну або з використанням спеціалізованих програмних засобів [47].

Таким чином, серед основних методів по оцінюванню стану захищеності інформаційних ресурсів головними є метод моніторингу несанкціонованих дій та криптографічні методи захисту даних [36].

Метод моніторингу несанкціонованих дій. Як було описано вище, на підприємстві має діяти чітка політика інформаційної безпеки, яка має виконувати контроль діяльності комп'ютерної системи та її функціональних складових і фіксувати будь-які зміни в журналах аудиту із метою подальшого аналізу подій аудитором або адміністратором. В журналі повинні фіксуватися наступні моменти:

–Log in/ log out користувачів з системи;

–Підозріле додавання нових користувачів до вже існуючого списку;

–спроби зміни політики безпеки.

Криптографічні методи захисту даних. Дані методи захисту даних на підприємстві вважаються найбільш ефективними. Перевіркою надійності криптографічного покриття інформації є його кількісний показник - стійкість.

Висновки за розділом 2

Підсумовуючи розділ II можна стверджувати, що забезпечення інформаційним захистом стало головним пріоритетом в діяльності організацій та установ. Сьогоднішня ситуація по оцінці ризиків рішуче вимагає уніфікованого, скоординованого, дисциплінованого та послідовного управлінського рішення.

В роботі було розглянуто ERM - концепцію, що описує методики та процеси впроваджені організаціями та установами для управління ризиками та можливостями, пов’язаними з досягненням поставлених задач та цілей. Саме вона дозволяє закласти фундамент ризик - менеджменту, в тому числі виявленні конкретних події або обставин, що впливають на досягнення завдань компаній(загрози та можливості), також дають оцінку масштабам уразливостей, розробляють стратегії реакції та досліджують ефективність підприємства.

Було відзначено, що реєстр ризиків може бути інтегрований у будь-яку методологію управління ризиками, яку використовує організація.

Встановлено, що серед основних методів по оцінюванню стану захищеності інформаційних ресурсів головними є метод моніторингу несанкціонованих дій та криптографічні методи захисту даних.

РОЗДІЛ 3. ДОСЛІДЖЕННЯ РОЗРОБЛЕННОЇ МЕТОДИКИ І СКЛАДАННЯ РЕКОМЕНДАЦІЙ ЩОДО ЇЇ ВИКОРИСТАННЯ

3.1. Формування звіту оцінки ризиків інформаційної безпеки по бізнес-діяльності

Керуючись настановами NIST у документі NISTIR 8286 «Integrating Cybersecurity and Enterprise Risk Management (ERM) » (Інтеграція кібербезпеки та управління ризиками підприємств) [44], було складено реєстр ризиків, попередньо врахувавши, що кожен ризик, внесений до відповідного реєстру, повинен містити опис ризику, вплив на ведення бізнесу, причину та ймовірність його виникнення, власника (-ів) ризику, як він класифікується загалом щодо всіх інших ризиків та відповіді на них. NIST зазначив, що компанії можуть додавати більше полів даних, як вважають за потрібне, але кожен реєстр ризиків повинен розвиватися в міру зміни поточних та майбутніх ризиків[44], про що детально йдеться у Додатку А.

Вибір методів реагування повинен бути детально відкоректованим, а відповідно розроблені заходи сприяти приведенню виявлених ризиків у відповідність з допустимим рівнем загрози. В таблиці 1.2 вказано на основні моменти реагування: прийняття – передача – пом’якшення – уникнення.

Таблиця 1.2

Типи реагування на ризики інформаційної безпеки по бізнес діяльності

Тип	Опис
Прийняття	Прийміть ризик кібербезпеки в межах рівня допуску до ризику. Ніяких додаткових дій щодо реагування на ризик не потрібно, крім моніторингу.

Продовження таблиці 1.2

Передача	Щодо ризиків кібербезпеки, які виходять за межі допустимого рівня, зменшіть їх до прийнятного рівня, поділившись частиною наслідків з іншою стороною (наприклад, 3 сторони, які займаються страхуванням). Хоча деякі фінансові наслідки можуть бути переданими, часто є наслідки, які неможливо передати, наприклад, втрата довіри споживачів.
Пом'якшенння	Застосовуйте дії, що знижують загрози, вразливості та наслідки даного ризику до прийнятного рівня. Можна включати відповіді, наприклад, як запобігти втраті (тобто зменшити ймовірність виникнення або ймовірність того, що подія загрози матеріалізується або досягне успіху), або як обмежити такі втрати, зменшуючи розмір шкоди та відповідальності.
Уникнення	Застосовуйте відповіді, щоб переконатися, що ризик не виникає. Уникнення ризику може бути найкращим варіантом, якщо немає економічно ефективного методу зниження ризику кібербезпеки до прийнятного рівня. Слід також враховувати вартість втраченої можливості, пов'язаної з таким рішенням.

Окремим етапом необхідно визначити цінність активів (Далі - ЦА) організації, в даному випадку буде розглянута чотирьохбальна система оцінки цінності:

1 - реалізація ризику, спрямованого на конфіденційність, цілісність і / або доступність активу не буде мати наслідків, як для організації в цілому, так і бізнес-процесів, зокрема.

2 - реалізація ризику, спрямованого на конфіденційність, цілісність і / або доступність активу призведе до незначних втрат для організації, в умовах, коли відновлення колишнього стану системи можливо без зупинки бізнес-процесів.

3 - реалізація ризику, спрямованого на конфіденційність, цілісність і / або доступність активу призведено значних фінансових втрат і / або зробить істотний негативний вплив на престиж організації, в умовах, коли відновлення

колишнього стану системи вимагає великих тимчасових і / або надалі постійних фінансових ресурсів.

4 - реалізація ризику, спрямованого на конфіденційність, цілісність і /або доступність активу може привести повної зупинки бізнес-процесів, великих фінансових втрат і / або матиме значний негативний вплив на престиж організації.

Так як бізнес-процесом є сукупність різних видів діяльності, в результаті якої створюється продукт або послуга, то в переліку актуальних загроз і існуючих вразливостей інших цінних активів будуть міститися загрози і вразливості актуальні і для бізнес-процесів. Особливістю даної категорії підприємств є те, що основний збиток бізнес-процесів організації здатні завдати загрози доступності мережевого обладнання та програмно-апаратного комплексу, а не загрози, спрямовані на порушення конфіденційності інформаційних ресурсів підприємства[48]. На це вказує таблиця 1.3, де пояснюється шкала оцінки цінності активів організації.

Таблиця 1.3

Шкала оцінки цінності активів організації

Ідентифікатор	**Актив організації**		**Конфіденційність**	**Цілісність**	**Доступність**	**Цінність активу**
А.	Основні активи Інформація	Інформація, необхідна для реалізації призначення або бізнесу організації	2	4	4	**4**

Продовження таблиці 1.3

B.		Інформація особистого характеру, яка визначена особливим чином, відповідним національним законам про недоторканність приватного життя	3	1	1	**3**
C.		Стратегічна інформація, необхідна для досягнення цілей організації	2	2	1	**2**
D.		Інформація, обробка якої вимагають тривалого часу і / або пов'язані з великими витратами на її придбання	3	2	2	**3**
E.	Апаратно-програмний комплекс		-	3	4	**4**
F.	Носії інформації		-	1	2	**2**
G.	Мережа		-	3	4	**4**
H.	Співробітники		-	1	1	**1**
I.	Місце функціонування підприємства		-	1	1	**1**

Таким чином, загальний рівень ризику ІБ для кожного з найцінніших активів організації розраховується за формулою (1.1) по критеріям, наведених в Додатку А і представляється результат для активів *A, E, G*, де *A- Основні активи, E - апаратно-програмний комплекс, G*- Мережа:

$$P = ЦН \times СВ \times Й \qquad (1.1),$$

де *Р- ризик; ЦН- цінність активів; СВ - ступінь вразливості кожного з найцінніших активів організації; Й- оцінка ймовірності реалізації загроз ІБ.*

Прийнятним ризиком вважається ризик, чиє числове значення знаходиться в проміжку від 1 до 10, такий ризик вважається незначним, і обробка такого ризику не потрібна. Середній ризик, чиє числове значення знаходиться в діапазоні від 11 до 21 рекомендований до обробки з метою його мінімізації. [49] Високим є ризик, чиє числове значення знаходиться в діапазоні від 22 до 64, даний ризик вважається істотним, і його обробка є обов'язковою.

Звіт оцінки ризиків інформаційної безпеки по бізнес-діяльності підприємства в цілому та критичним бізнес-процесам надається у вигляді таблиці, розрахункові дані якої наведені в Додатку Б. На рисунку 3.1 представлена діаграма розрахунків по таблиці 1.3 та із Додатку Б, окремо було вирахувано потенційно бажаний рівень оцінки ризиків інформаційної безпеки по бізнес-діяльності та порівняно вже з наявним.

Можемо зробити висновок, що на підприємстві загалом зависокий рівень ризику цілісності та доступності, тому всі заходи безпеки, включаючи додаткові, мають бути направлені на управління інформаційною безпекою. Таким чином, згідно з розрахунками, проведеними відповідно до методики аналізу, оцінки та обробки ризиків інформаційної безпеки на підприємстві, загальний ризик по бізнес-діяльності в цілому має рівень ризиків - «Середній».

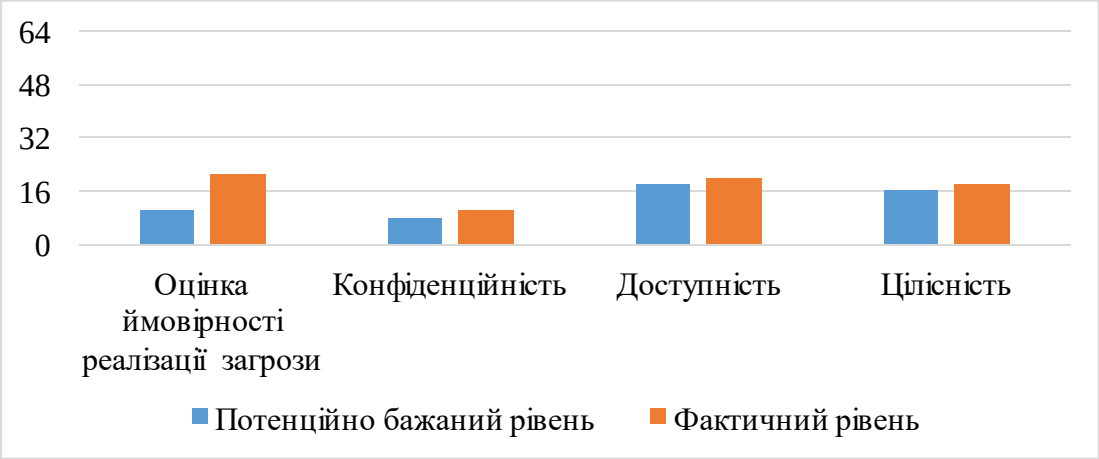


Рисунок 3.1- Порівняльний графік рівня ризиків інформаційної безпеки по бізнес-діяльності підприємства

3.2 Функціональні можливості використання SIEM-систем

Інформаційні технології стабільно розвиваються щороку. Позитивною стороною даного процесу стає спрощення ведення бізнесу. Але є і негативні наслідки прогресу - збільшення числа інформаційних потоків не дає проконтролювати все вручну, в тому числі забезпечити інформаційну безпеку організації на належному рівні. Без надійним чином вибудуваної системи відстеження всіх дій, що мають місце в мережі, вона знаходиться під постійною загрозою.

Системи захисту просто зобов'язані відповідати всім вимогам часу, розробники антивірусів створюють свої рішення SIEM - вони дають можливість забезпечити додатковий рівень мережевого захисту[50].

Інформація про безпеку та управління подіями (SIEM) – це набір інструментів та послуг, що пропонують цілісне уявлення про інформаційну безпеку організації.

Інструменти SIEM забезпечують:

– Огляд у реальному часі в системах інформаційної безпеки організації.

– Управління журналом подій, яке консолідує дані з численних джерел.

– Співвідношення подій, зібраних з різних журналів або джерел безпеки, використовуючи правила if-then (конструкція, що забезпечує виконання певної команди тільки за умови істинності деякого логічного виразу), які додають інтелект до необроблених даних.

– Автоматичні сповіщення про події безпеки. Більшість систем SIEM надають інформаційні панелі для питань безпеки та інших методів прямого повідомлення[51].

SIEM працює, поєднуючи дві технології: a) управління інформацією про безпеку (SIM), яка збирає дані з файлів журналів для аналізу та звітів про загрози та події безпеки, і b) управління подіями безпеки (SEM), що здійснює моніторинг системи в режимі реального часу, повідомляє адміністраторів мережі про важливі проблеми та встановлює співвідношення між подіями безпеки.

Інформацію про безпеку та процес управління подіями можна розділити наступним чином:

–Збір даних - всі джерела інформації про мережеву безпеку, наприклад, сервери, операційні системи, брандмауери, антивірусне програмне забезпечення та системи запобігання вторгненню налаштовані для подачі даних про події в інструмент SIEM. Більшість сучасних інструментів SIEM використовують агенти для збору журналів подій з корпоративних систем, які потім обробляються, фільтруються та надсилаються до SIEM.

–Політики - адміністратор SIEM створює профіль, який визначає поведінку систем підприємства як за звичайних умов, так і під час попередньо визначених випадків безпеки. SIEM надають правила за замовчуванням, попередження, звіти та інформаційні панелі, які можна налаштувати та налаштувати відповідно до конкретних потреб безпеки.

–Консолідація та кореляція даних - рішення SIEM консолідують, аналізують та аналізують файли журналів. Потім події класифікуються на основі вихідних даних та застосовують правила кореляції, які поєднують окремі події даних у значущі проблеми безпеки.

–Сповіщення - якщо подія або набір подій викликає правило SIEM, система повідомляє персонал служби безпеки.

Джерелами даних для SIEM-систем зазвичай служать системи виявлення та запобігання вторгнень, журнали серверів і призначених для користувача комп'ютерів, комутатори, маршрутизатори, системи СКУД, антивірусні платформи, системи віддаленого доступу, DLP-системи, а також файлові сервери[50].

SIEM має важливе значення, оскільки полегшує підприємствам управління безпекою, фільтруючи величезні обсяги даних безпеки та надаючи пріоритети попередженням про безпеку, які генерує програмне забезпечення.

Програмне забезпечення SIEM аналізує записи в журналі для виявлення ознак шкідливої діяльності. Крім того, оскільки система збирає події з різних джерел у

мережі, вона може відтворити часову шкалу атаки, що дозволяє компанії визначити природу атаки та її вплив на бізнес.

Система SIEM також може допомогти організації виконати вимоги відповідності, автоматично створюючи звіти, які включають усі зареєстровані події безпеки серед цих джерел. Без програмного забезпечення SIEM компанії довелося б збирати дані журналів та складати звіти вручну.

Оскільки SIEM система на підприємстві призначена для підтримки моніторингу та аналітичних функцій у режимі реального часу, вона буде аналізувати вміст файлу журналу, зберігаючи опрацьовану інформацію в якомусь структурованому сховищі даних підприємства, в базі даних [52]. Саме для аналітики даних зручною є покрокова блок-схема, як показано на малюнку 3.2 :

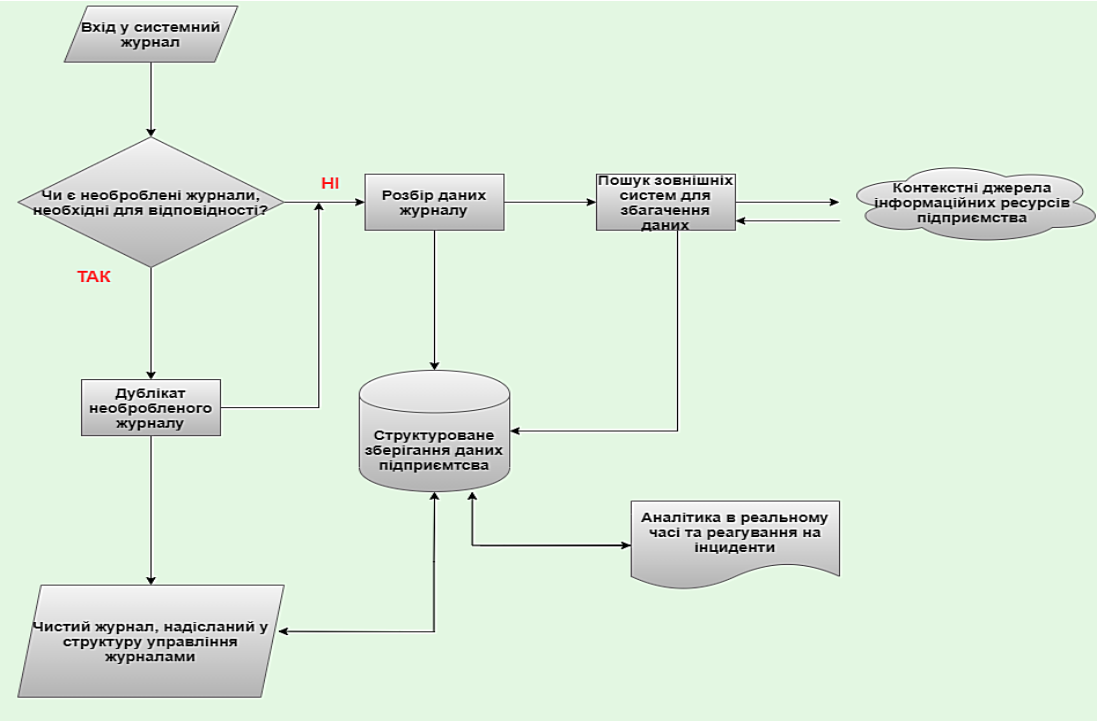


Рисунок 3.2 -Принцип SIEM аналізу даних по вмісту файлу журналу в структурованому сховищі даних підприємства

Система SIEM також покращує управління інцидентами, дозволяючи команді безпеки компанії розкрити маршрут, яка атака проходить по мережі, визначити

джерела, які були скомпрометовані, та забезпечити автоматизовані інструменти для запобігання триваючим атакам[53].

Для прикладу наведемо деякі ключові переваги SIEM-системи:

–скорочує час, необхідний для значного виявлення загроз, мінімізуючи шкоду від цих загроз;

–пропонує цілісне уявлення про середовище інформаційної безпеки організації, що полегшує збір та аналіз інформації про безпеку, щоб забезпечити безпеку систем – усі дані організації надходять у централізоване сховище, де вони зберігаються та легко доступні;

–може використовуватися компаніями для різноманітних випадків використання, які обертаються навколо даних або журналів, включаючи програми безпеки, аудит та звітність про відповідність, довідкову службу та усунення несправностей мережі;

–підтримує великі обсяги даних, щоб організації могли продовжувати масштабувати та збільшувати свої дані;

–забезпечує виявлення загроз та попередження безпеки;

–може проводити детальний покроковий аналіз у разі серйозних порушень безпеки.

Потрібно розуміти, що SIEM система безпосередньо не буде протидіяти хакерам, вона тільки аналізує велику кількість вхідної інформації і надає звіт про небезпеку певної області, повідомляючи користувача.

Таким чином, SIEM потрібно додавати в комплексний підхід для забезпечення безпеки мережі. Обов'язково в компанії повинен бути фахівець, який зможе відреагувати на повідомлення системи і в найкоротші терміни вжити заходів для запобігання зараження або крадіжки конфіденційної інформації.

Крім усього іншого, впроваджуючи SIEM систему, потрібно особливо ретельно ознайомитися з інфраструктурою компанії в кожному конкретному випадку, враховуючи встановлену систему безпеки, архітектуру мережі [51]. Правильно налаштована система дозволяє адміністратору реагувати тільки на дійсно важливі події

та інциденти. Основною ідеєю таких систем є можливість передачі на них все рутинні процеси і можливість приймати рішення за рівнем загрози події для мережі.

Сьогодні на ринку України функціонують ряд рішень щодо захисту інформації та управління подіями. Назвемо найбільш перспективні та популярні з них : Arcsight ESM, IBM Qradar, Splunk та Fortinet FortiSIEM.

3.3 Практичне впровадження роботи FortiSIEM від Fortinet

Для виконання практичних досліджень було обрано програмне забезпечення від Fortinet як світового лідера в області IT-безпеки, місією якого є доставка інтегрованих і високопродуктивних рішень для захисту IT-інфраструктури. Fortinet успішно оперує по всьому світу. За останні 18 років вона перетворилася в мільярдний компанію, яка постачає на ринок передові технології захисту для мереж, IT-інфраструктури, IoT і хмарних обчислень [54].

Бізнес компанії росте рік від року. За останній рік дохід компанії досяг 1,8 млрд. дол. Вона має 340 тис. замовників по всьому світу, що є більше, ніж у інших виробників в цьому сегменті. Частка ринку Fortinet по мережевих пристроїв становить майже 30%. а кількість встановлених пристроїв - понад 3,6 млн. Інноваційність технологій компанії підтверджується 467 виданими їй патентами і 291 заявкою на патент, які чекають затвердження.

Fortinet займає лідируючі позиції в правому верхньому квадранті Gartner по ряду продуктів для корпоративного сектора. Компанія поставляє на ринок високоінтегровані і автоматизовані рішення. Серед українських замовників компанії - Державна міграційна служба, Прикордонні війська, Lifecell, Астарта, ряд сервіс-провайдерів.

За словами пані Аксой (регіонального віце-президента компанії Fortinet), ринок України є дуже важливим для компанії. Зростання бізнесу тут в минулому році склав 72%. Fortinet буде продовжувати інвестувати в ринок України, проводячи тренінги та підтримуючи партнерів у процесі сертифікації [55].

FortiSIEM - це комплексний та масштабований засіб управління безпекою, продуктивністю і забезпеченням відповідності вимогам всіх компонентів інфраструктури, здатний працювати як з хмарами, так і з інтернетом речей (IoT). Рішення FortiSIEM направлено на зниження складності виявлення загроз при підвищенні ефективності системи безпеки. SIEM-система такого рівня спрямована на захист не тільки інформації, а й репутації клієнтів, знижуючи негативні наслідки від загроз і протидіючи виникненню нових атак [54].

Fortinet додала до класичної SIEM-системи ряд своїх запатентованих технологій: розподілену кореляцію подій в режимі реального часу; автоматизоване виявлення інфраструктури і додатків (CMDB); обробка журналів, що налаштовується [56].

FortiSIEM підтримує інтеграцію зі сторонніми пристроями, опитуючи інфраструктуру про виникаючі події безпеки, логах, продуктивності і т. д. При цьому FortiSIEM дозволяє спілкуватися із зовнішніми системами управління вразливостями і оповіщує про їх виявлення і, таким чином, дозволяє розширювати можливості з протидії та захисту від вразливостей.

Серед основних можливостей FortiSIEM виділяють:

–Підтримка широкого безлічі сторонніх пристроїв і додатків.

–Масштабований і гнучкий збір журналів:

–збір, обробка, зберігання, нормалізація, індексування та кореляція подій безпеки з підтримкою десятків тисяч подій в секунду;

–підтримка великої кількості систем безпеки і API постачальників (локальних і хмарних);

– збір подій за допомогою агентів Windows/ Linux, моніторинг цілісності файлів, змін встановлених програм і змін реєстру;

– створення і зміна засобів синтаксичного аналізу (шаблонів XML) в рамках графічного інтерфейсу і надання доступу іншим користувачам за допомогою функції експорту / імпорту[57].

–Повідомлення і управління інцидентами:

–побудова інфраструктури повідомлення про інциденти на основі політик;

– можливість запуску сценарію поновлення в разі виникнення зазначеного інциденту;

–Надання користувачеві повнофункціональних панелей моніторингу:

–панелі моніторингу з функцією прокручування слайд-шоу для демонстрації ключових показників ефективності в режимі реального часу;

–генерація звітів і аналітичних даних, доступних для колективного використання співробітниками організацій і користувачами;

– кольорове маркування для оперативного виявлення критичних проблем;

–Інтеграція зовнішніх даних про загрози:

–надання API для інтеграції зовнішніх джерел даних про загрози - доменах з шкідливими програмами, IP-адреси, URL-адреси, хешах, вузлах Tor;

–інтеграція популярних джерел даних про загрози - ThreatStream, CyberArk, SANS, Zeus;

–технологія обробки великих обсягів даних про загрози - зіставлення шаблонів з мережевим трафіком в режимі реального часу.

–Надання функцій аналізу:

–пошук подій в режимі реального часу та в історії;

–пошук за ключовим словом і обробленим атрибутам події;

–фільтрація в залежності від часу доби, зіставлення регулярних виразів, обчислювані вирази - графічний інтерфейс і API;

–тригер для шаблонів складних подій в режимі реального часу;

–використання виявлених об'єктів CMDB, даних користувача / посвідчення і відомостей про розташування в процесі пошуку і створення правил;

–планування складання звітів і доставка результатів ключовим співробітникам за допомогою електронної пошти;

–пошук подій в рамках всієї корпоративної мережі або фізичного/ логічного домену складання звітів;

–динамічно змінювані списки відстеження, призначені для виявлення критичних порушень;

–можливість розгортання функції визначення пріоритету в процесі складання звітів про інциденти за допомогою критичних бізнес-служб.

–задання базових показників і виявлення статистичних аномалій поведінки кінцевої точки / сервера / користувача.

–інтеграція зовнішніх технологій:

– інтеграція з будь-яким зовнішнім веб-сайтом з метою пошуку IP-адреси;

– інтеграція на основі API для зовнішніх джерел даних про загрози;

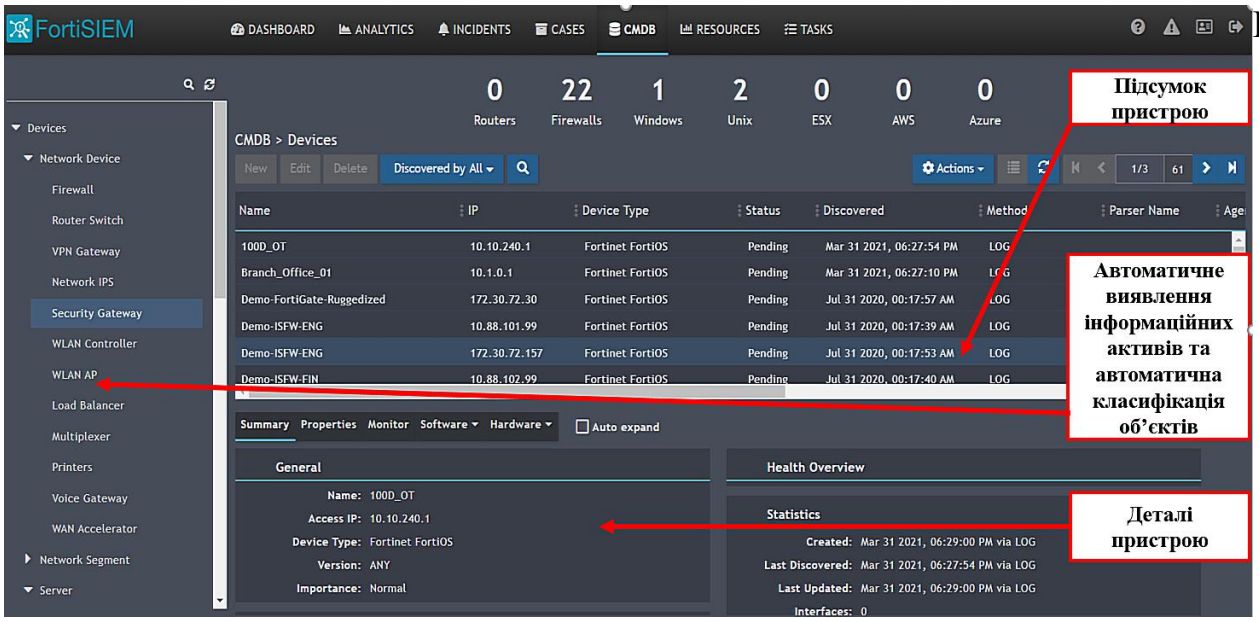
– надання API для додавання організацій, створення облікових даних, ініціалізації виявлення, внесення змін в процес моніторингу подій[57].

Отже, зараз буде продемонстровано функціонал FortiSIEM. Це є робочим процесом: початок із стандарного меню і подальша робота від моніторингу подій до розуміння того, який саме вплив на систему організації має дане середовище в деталях.

FortiSIEM надає два типи інтерфейсів. Перший містить ієрархічну структуру розділів і робочу область для відображення інформації. Такий інтерфейс дозволяє здійснювати адміністрування FortiSIEM і управління інформаційною безпекою, налаштовувати взаємодію з елементами інфраструктури підприємства, отримувати інформацію про виникаючі інциденти.

Зауважемо, що по кожному пристрою можна отримати розгорнуті звіти, що містять детальну інформацію про події безпеки.

Рисунок



3.3- Інтерфейс системи FortiSIEM від Fortinet

Другий інтерфейс дозволяє здійснювати поточний моніторинг подій на будь-якому пристрої. Відображення виконується по панелям (Dashboard) або інцидентів (Incidents) і різними критеріями.

Серед функціоналу FortiSIEM є зручна можливість налаштування в режимі реального часу панелі моніторингу, які можуть відображатися з функцією прокручування слайд-шоу для демонстрації ключових показників.

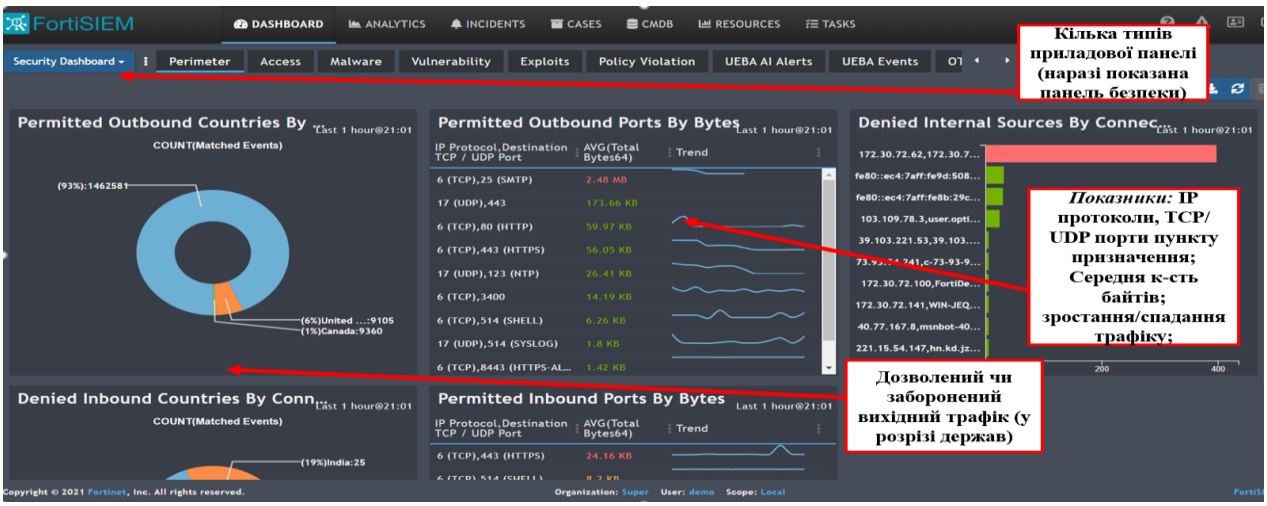


Рисунок 3.4 - Інтерфейс приладової панелі та її функціонал у FortiSIEM від Fortinet

FortiSIEM підтримує автоматизацію виявлення пристроїв, додатків і конфігурацій, дозволяючи зіставляти топологію фізичних і віртуальних інфраструктур, локальних і загальнодоступних / приватних хмар за допомогою облікових даних. Для пристроїв, розташованих на периметрі мережі, таких як міжмережеві екрани і маршрутизатори, важливо володіти інформацією, які інтерфейси зайняті і який трафік споживає більшість ресурсів пристроїв.

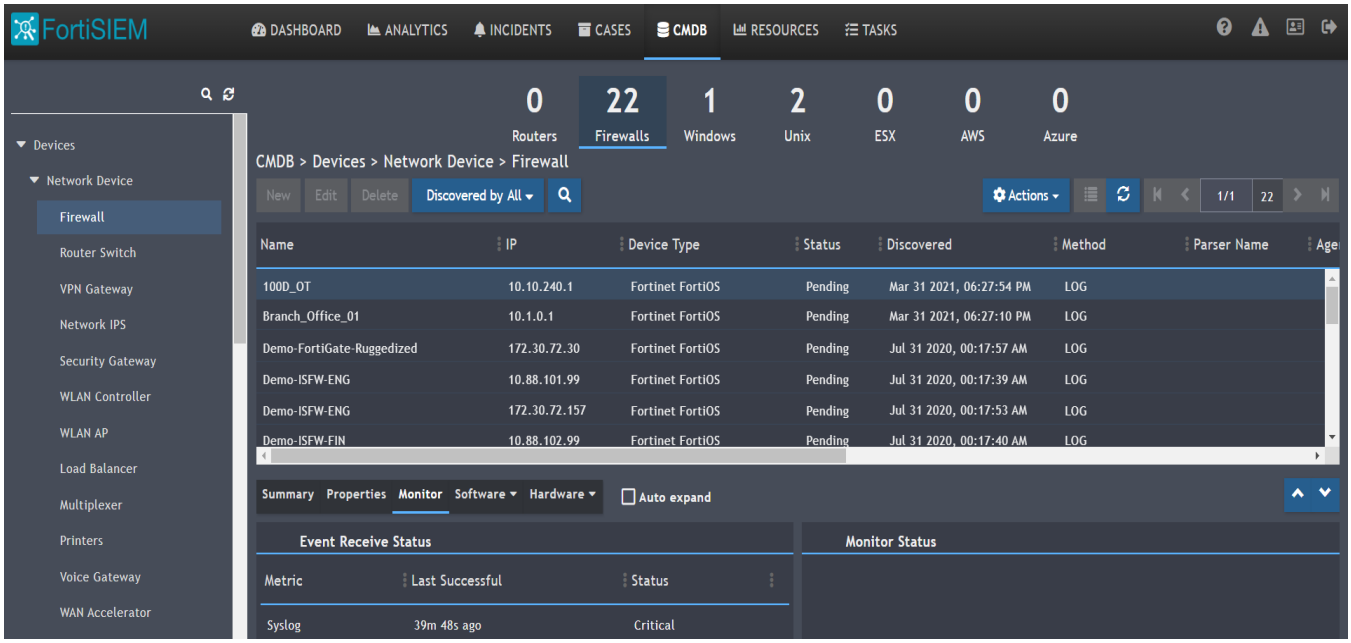


Рисунок 3.5 - Моніторинг станів міжмережевих екранів в інтерфейсі адміністратора у FortiSIEM від Fortinet

Виявлені засобами FortiSIEM пристрої будуть постійно відстежуватися, а зібрані дані дозволяють виконувати аналіз продуктивності інфраструктури. Для зручності адміністратор може налаштувати панель моніторингу продуктивності того або іншого пристрою/сервісу. Контрольований стан відстежується, корелюється, і можуть видаватися відповідні інциденти в залежності від заданих в FortiSIEM налаштувань.

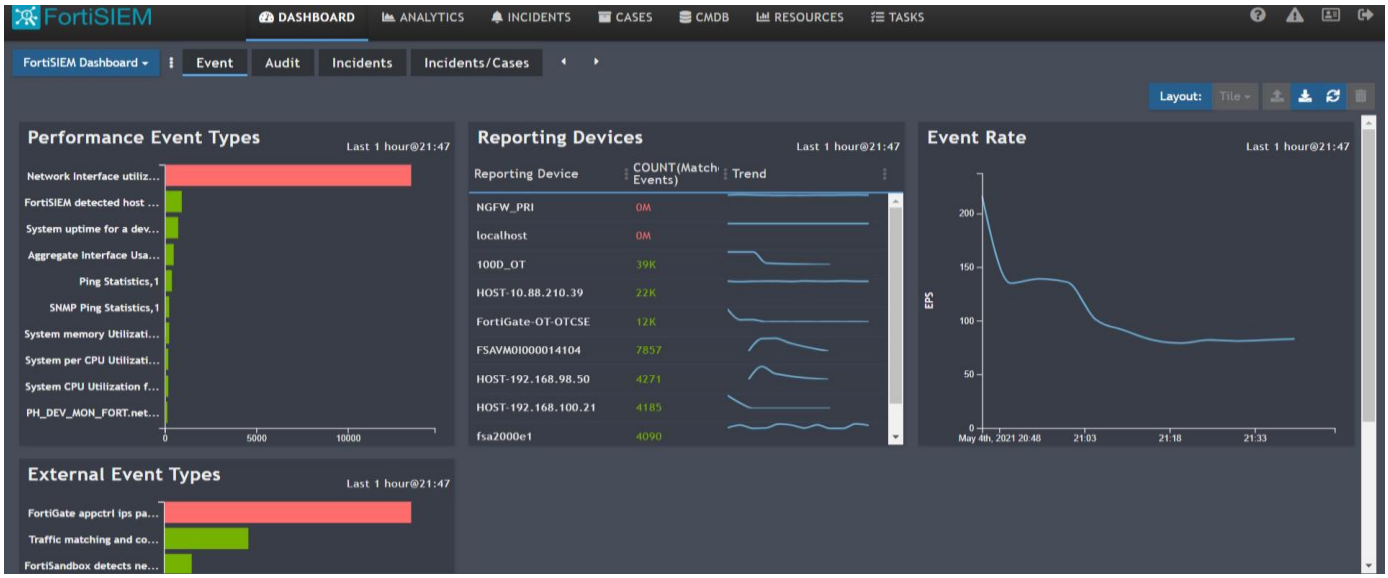


Рисунок 3.6 - Аналіз продуктивності інфраструктури за типом подій у FortiSIEM від Fortinet

FortiSIEM постійно відстежує інфраструктуру і надає інформацію, яку можна використовувати для аналізу продуктивності, доступності та безпеки. Для оперативного реагування на події безпеки необхідно своєчасно отримувати попередження про виникнення виняткових, підозрілих або потенційних несправностей і порушень. Для цього використовуються правила, що визначають умови, на які слід звернути увагу і які ініціюють інцидент. FortiSIEM включає в себе більше 600 вбудованих системних правил і понад 2000 створених звітів, а також редактор для генерації власних правил.

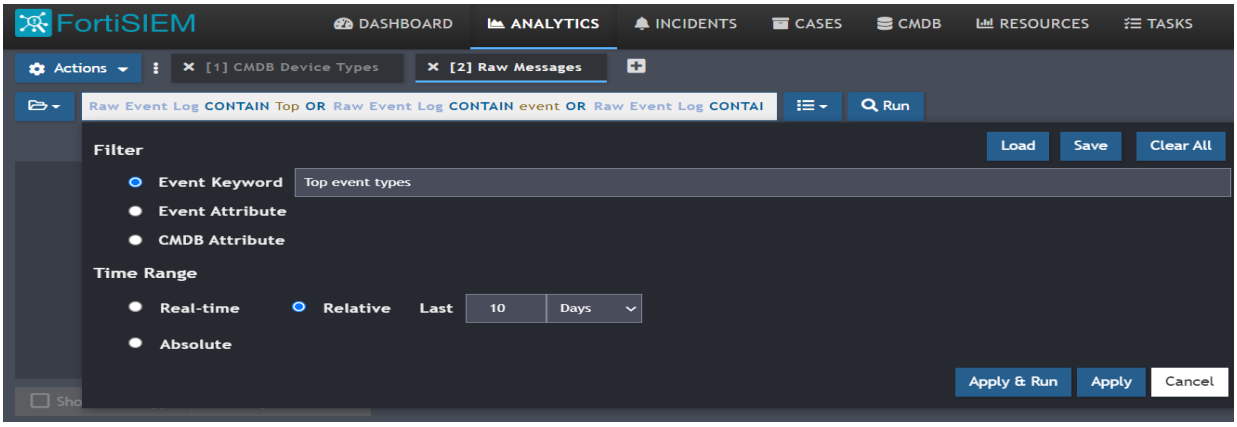


Рисунок 3.7 - Приклад створення системного правила у FortiSIEM від Fortinet

Функція пошуку FortiSIEM включає в себе пошук в реальному часі і історичний пошук інформації, зібраної з IT-інфраструктури. При пошуку в реальному часі відображаються події в міру їх виникнення, в той час як історичний пошук заснований на інформації, що зберігається в базі даних подій. Обидва типи пошуку включають простий пошук за ключовими словами і структуровані пошукові запити, які дозволяють виконувати пошук на основі певних атрибутів і значень подій, а потім групувати результати по атрибутам.

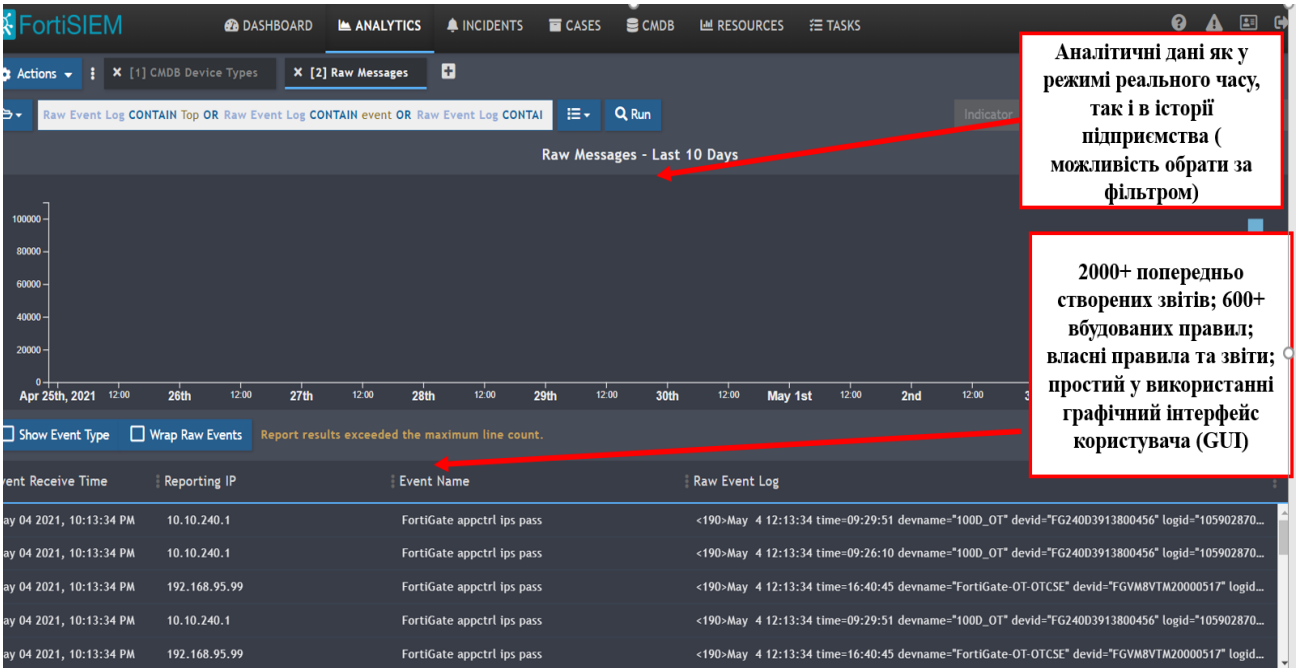


Рисунок 3.8 - Інтерфейс аналітичних даних підприємства у режимі реального часу та в історії у FortiSIEM від Fortinet

FortiSIEM надає можливість категоріювання інцидентів за рівнем критичності для інформаційних ресурсів підприємства- «високий», «середній» та «задовільний» з окремою змогою фільтрації по історії інцидентів ІБ в організації, що дозволяє прописати їх в політиці безпеки та запобігати їх вже за першими ознаками:

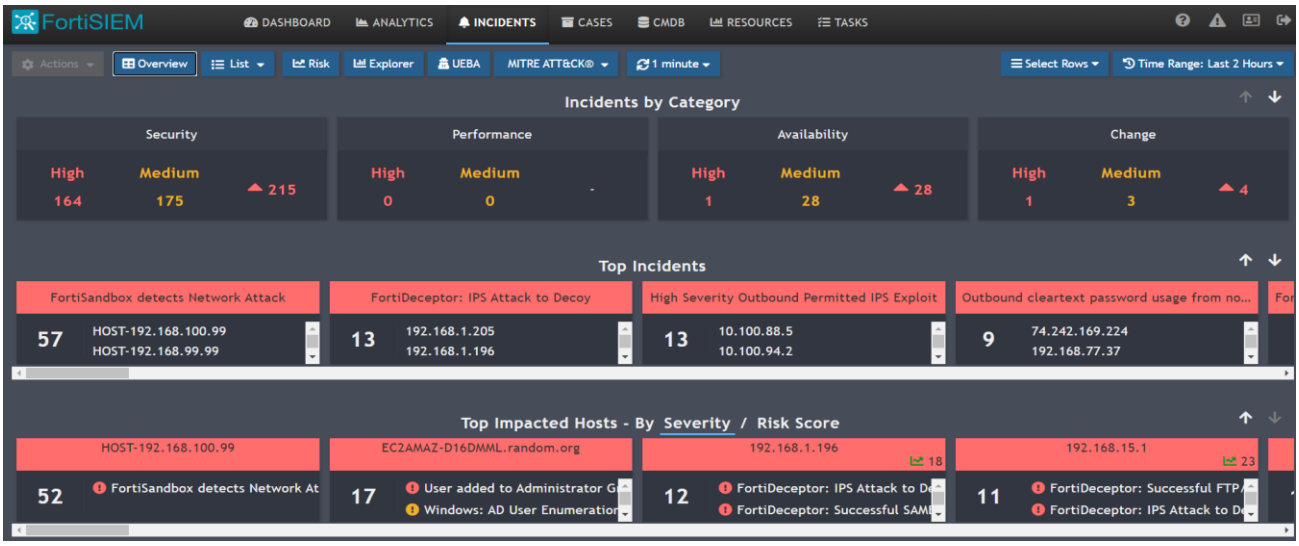


Рисунок 3.9 - Автоматичне категоріювання інцидентів інформаційної безпеки підприємства у FortiSIEM від Fortinet

По кожному інциденту інформаційної безпеки підприємства у FortiSIEM доступна детальна інформація, де можна переглянути детальний хід дій зловмисника, його програмно-апаратні засоби для здійснення правопорушення. Відзначимо, що автоматично прописується який ризик представляє зловмисник для інформаційних активів підприємства.

Рисунок 3.10 - Суб'єкти, що створили ризик для підприємства та відображення звіту їхніх дій у FortiSIEM від Fortinet

Для прикладу пропонується розглянути конкретне втручання зловмисника у роботу інформаційної системи підприємства за допомогою FortiSIEM - у вигляді успішного проходження процедури аутентифікації з декількох міст/країн одночасно за допомогою підбору паролю методом «грубої сили» (ризик автоматично оцінено як «високий»). Завдяки функціоналу FortiSIEM є можливість генерації повного звіту в pdf-форматі (наведено у Додатку В).

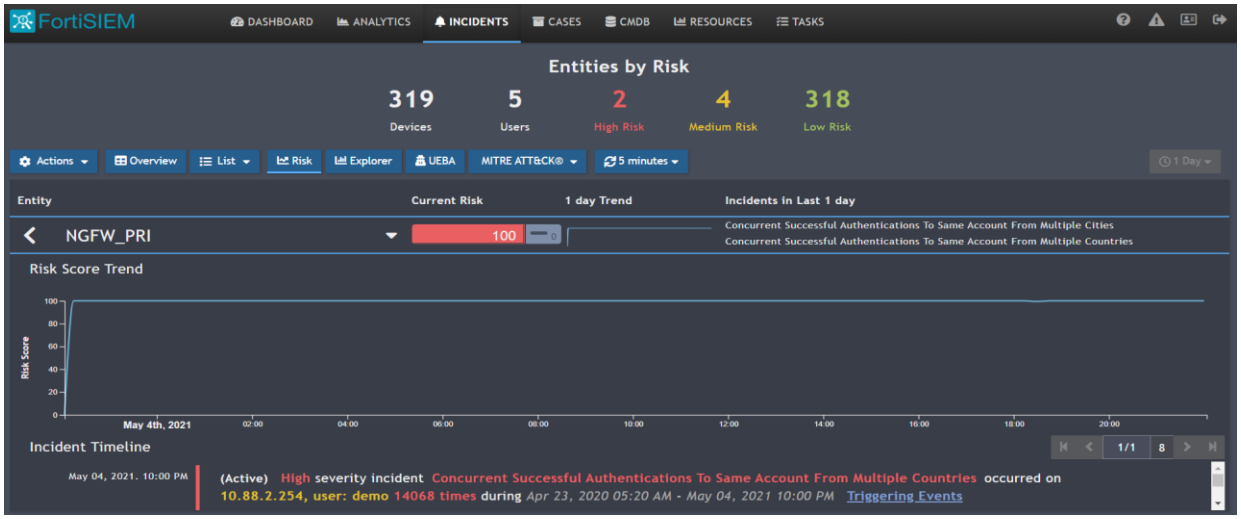


Рисунок 3.11 - Приклад № 1 конкретного втручання у інформаційну безпеку підприємства та відображення звіту дій порушника у FortiSIEM від Fortinet

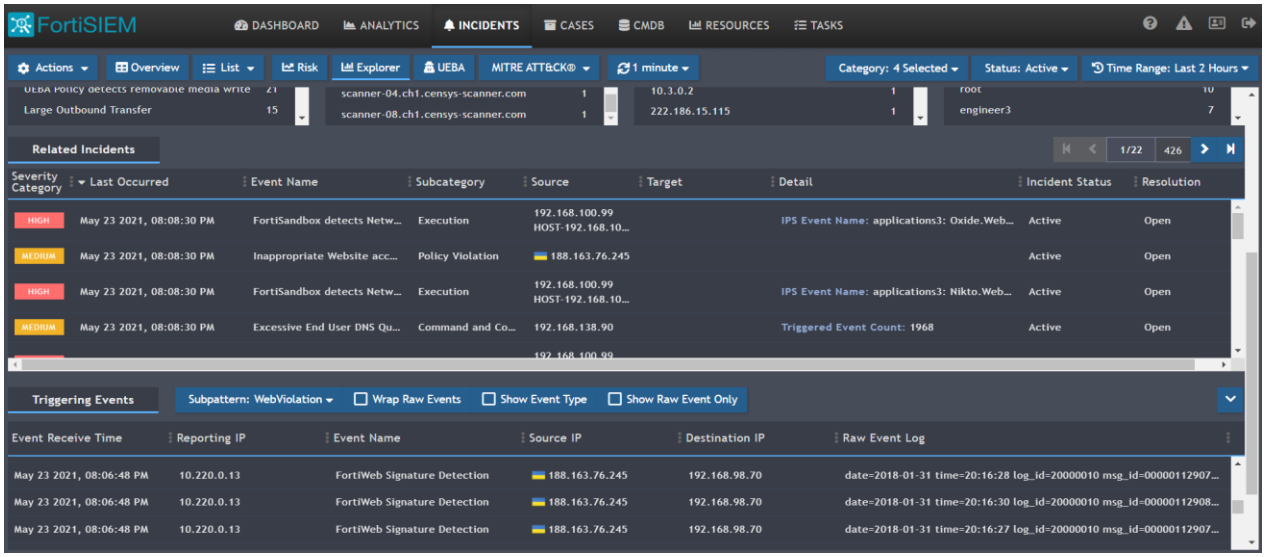


Рисунок 3.12 - Приклад № 2 конкретного втручання у інформаційну безпеку підприємства та відображення звіту дій порушника у FortiSIEM від Fortinet

Зауважимо, що у FortiSIEM надається можливість детального перегляду деталей про правопорушника, а саме джерела його походження: 1) точне місце розташування - (країна, місто, окремо - географічна широта і довгота); 2) IP-адреса; 3) ім'я хоста; 4) назва провайдера.

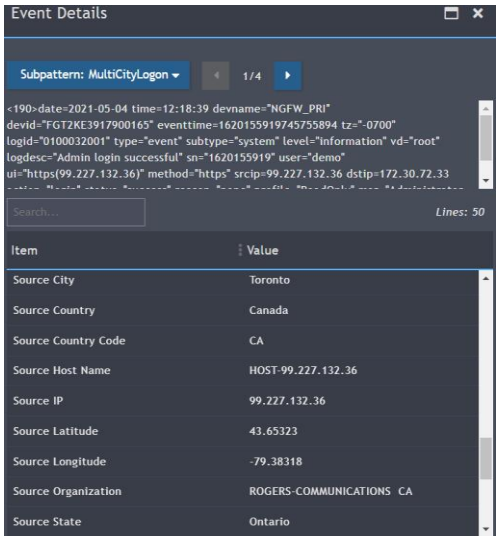


Рисунок 3.13- Детальна інформація зразка №1 про порушників інформаційної безпеки підприємства у FortiSIEM від Fortinet

Рисунок 3.14 - Детальна інформація зразка №2 про порушників інформаційної безпеки підприємства у FortiSIEM від Fortinet

Висновки за розділом 3

Підсумовуючи розділ III можна стверджувати, що цифрові перетворення торкнулися кожну галузь, кількість напрямків атак істотно зростає і це значно ускладнює управління системами безпеки. Фахівці із забезпечення кібербезпеки прагнуть надати повний захист інфраструктури, додатків і кінцевих точок (включаючи пристрої IoT). Для цього їм потрібно мати у своєму розпорядженні дані про всі пристрої та інфраструктуру підприємства загалом в режимі реального часу. Крім того, організації повинні мати своєчасне сповіщення про небезпеки для інформаційних ресурсів підприємства і джерела їх походження для швидкого реагування і мінімізації наслідків негативного впливу на роботу установи.

Таким чином, виявлення, пріоритизація і управління інцидентами безпеки можливе за допомогою одного рішення SIEM - системи управління інформацією про безпеку та подій безпеки.

FortiSIEM забезпечує можливості SIEM наступного покоління, так як являє собою єдине масштабоване рішення, яке об'єднує функції забезпечення доступності даних, кореляції, автоматичного реагування і виправлення. Вона спрощує управління операціями мережі і безпеки, що дозволяє ефективно вивільнити ресурси, поліпшити систему виявлення порушень і навіть запобігти порушенням.

Більш того, FortiSIEM дозволяє уніфікувати збір відомостей і аналітичні дані від різних джерел інформації, включаючи журнали, показники продуктивності, попередження системи безпеки і зміни конфігурації. Рішення FortiSIEM використовують для отримання більш цілісного уявлення про систему безпеки і конфіденційності, цілісності та доступності інформаційних ресурсів підприємства.

ВИСНОВКИ

Підсумовуючи кваліфікаційну роботу можна наголосити, що застосування сучасних систем інформаційної безпеки вимагає відстеження швидких змін в інформаційних технологіях і постійних загрозах, однак, повинні враховуватися реальні характеристики апаратного й програмного забезпечення корпоративних мереж і систем. Кінцевим результатом є визначення балансу між ймовірним збитком від несанкціонованого витоку інформації та розміром витрат для забезпечення захищеності інформаційних ресурсів. Задля підвищення ефективності захисту інформаційних ресурсів, необхідно досліджувати підходи щодо оцінки рівня захищеності систем захисту, які залежать від багатьох факторів (вартості інформації, статусу організації, важливості інформації, якості апаратного та програмного забезпечення тощо).

В ході роботи зроблено наступні висновки :

–на основі ряду опрацьованих джерел та літератури, як сучасних українських науковців, так і зарубіжних дослідників, визначено склад і зміст поняття захищеності інформаційних ресурсів та класифікації даних;

– проаналізовано принципи ефективного управління ризиками на підприємстві у контексті системи управління безперервністю бізнесу, яка охоплює кілька цілеспрямованих планів і гарантує, що організації зможуть продовжувати працювати незважаючи на різні типи збоїв або катастроф: втрату об’єкта, порушення безпеки, пандемію тощо, у тому числі навіть перебуваючи під значним тиском на IT-системи, будуть стійкими в ділових операціях.

–проведено якісну та кількісну оцінку стану захищеності ІР на основі дослідження джерел загроз.

–охарактеризовано процеси управління інформаційними ризиками та методологію їх застосування. Доведено, що методологія оцінки ризиків на

підприємстві стала усталеним підходом до виявлення та управління системним ризиком для організації.

–досліджено загальні принципи роботи SIEM-систем, які безпосередньо управляють інформацією про безпеку та мають надважливе значення, оскільки полегшують підприємствам управління безпекою, фільтруючи величезні обсяги даних та надаючи пріоритети попередженням про безпеку, які генерує програмне забезпечення.

–визначено на практиці основні переваги впровадження роботи FortiSIEM від Fortinet в роботу організації та установи: це є SIEM наступного покоління, єдине масштабоване рішення для об'єднання функції забезпечення доступності даних, кореляції, автоматичного реагування і виправлення інформації. FortiSIEM спрощує управління операціями мережі і безпеки, що дозволяє ефективно вивільнити ресурси, поліпшити систему виявлення порушень і запобігти їм. Дане рішення використовують для отримання більш цілісного уявлення про систему безпеки і конфіденційності, цілісності та доступності інформаційних ресурсів підприємства.

Результати даних досліджень апробовані у наступних тезах: «Аналіз методів та засобів оцінки стану захищеності інформаційних ресурсів, процеси управління безперервністю бізнесу» IV міжнародної науково-практичної конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)» 15-16 квітня 2021 року, м. Київ; «Сучасні технології оцінювання стану захищенності інформаційних ресурсів на основі досліджень джерел загроз інформаційній безпеці» науково-практичної конференції “Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання” (ITCTK-2020) СЗЗІ КПІ ім. Ігоря Сікорського, 18-19 листопада 2020, м. Київ; «Управління захистом інформації в інформаційних установах України» Міжнародного круглого столу «Інформація та соціальні комунікації сучасного світу: тренди глобалізації» 12 травня 2021 р., м. Київ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ:

1. Councilof Europe, Avenuedel 'Europe F-67075 Strasbourg Cedex, France [Electronic resource] – Режим доступу: https://www.coe.int/en/web/ cybercrime /-/ cybercrime-and-covid-19.

2. Mark Carney, Executive Vice President, Coalfire [Electronic resource] – Режим доступу: https://www.coalfire.com/the-coalfire-blog.

3. Довгаль Ю.С. Особливості побудови захисту інформаційних систем// Науковий вісник публічного та приватного права. 2016 – №4. – С.111-115.

4. Курило А.П. Аудит інформаційної безпеки / [Курило А. П., Зефіров С.Л., Голованов В.Б. та ін.] Аудит інформаційної безпеки. – М.: Видавнича група «БДЦ-прес», 2006. – 420 с.

5. Закон України про захист інформації в інформаційно-телекомунікаційних системах від 05.07.1994 № 80/94-ВР [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/80/94-вр.

6. М. Браіловський, О. Качмала «Аналіз методів та засобів оцінки стану захищеності інформаційних ресурсів, процеси управління безперервністю бізнесу» - IV Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS)” 15 - 16 квітня 2021, Київ

7. Стратегія кібербезпеки України: Указ Президента України від 15 березня 2016 року № 96/2016: URL: [Електронний ресурс]. Режим доступу: https: //www.president. gov. ua/ documents /962016.

8. Стратегія національної безпеки України : Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 вересня 2020№ 392 [Електронний ресурс] https://zakon.rada.gov.ua/laws/show/392/2020#Text

9. Бурячок, В. Л Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа].– К.: ДУТ, 2015.–288 с.

10. Гладких Д. М. Банківська безпека держави в умовах розвитку інформаційної економіки (трансформації банківських операцій) / Д.М. Гладких. К.: НУОУ, 2019. – 392 с.

11. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В. Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний Н.В. Лукова-Чуйко/ – К. : ДУТ - КНУ, 2016. – 178 с.

12. С. В. Толюпа Оценка защищённости информации в автоматизированных информационных системах с помощью Общих критериев / С. В. Толюпа, В. С. Наконечный, Ю. М. Якименко // Наук. зап. Укр. н.-д. ін-ту зв'язку. - 2015. - № 6. - С. 27-31. - Библиогр.: 5 назв. - рус.

13. Рамазанов С.К. Інноваційні технології антикризового управління економічними системами: монографія / [С.К. Рамазанов, Г.О. Надьон, Н.І. Кришталь, О.П. Степаненко, Л.А. Тимашова].– Луганськ-Київ: вид-во СНУ ім. В. Даля, 2009. – 584 с.

14. Dustin Heath Enterprise Security [Electronic resource] – Режим доступу: https://www.linkedin.com/in/dustin-heathb2aa112b#:~:text=Dustin%20Heath%20 is%20the%20co ,IT%20systems%20for%20the%20DoD.

15. Закон України про інформацію документ 2657-XII, чинний, поточна редакція — Редакція від 16.07.2020, підстава - 692-IX.

16. Jingcong Zhao Conductingan Information Security Risk Assessment: a PrimerNov 22, 2019 [Electronic resource] – Режим доступу: // https:// hyperproof.io/ resource/ information-security-risk-assessment-a-primer/

17. Єрмошин В. В., Невойт Я. В. Аналіз і оцінка ризиків інформаційної безпеки для банківських та комерційних систем // Науково-технічний журнал Державного

університету телекомунікацій «Сучасний захист інформації».– 2014 р. – № 4. – С. 14-25.

18. Аналіз підходів та програмних рішень оцінки і контролю інформаційних ризиків в комп'ютеризованих системах// А.В. Чунарьова, І.І. Пархоменко, І.І. Сащук - Вісник Інженерної академії України, 2014

19. Gartner Security & Risk Management Summit // Middle East | Virtual [Electronic resource] – Режим доступу: https://www.gartner. com/en/newsroom/press-releases/gartner-announces-gartner-security-risk-management-summit-2020

20. Герасимович І.А. Фінансовий інжиніринг як об'єкт обліку інновацій / І.А. Герасимович // Науковий вісник Ужгородського університету, 2015. Серія "Економіка". Випуск 1 (45). Т.2.– С.20-23.

21. Robert Giffin The Ultimate Guide to the Business Impact Analysis [Electronic resource] – Режим доступу: https://avalution.com/business-impact-analysis/

22. Виталий Москвин // RTO и RPO. Или о чем нужно помнить при резервировании данных // [Електронний ресурс] – Режим доступу: https://www. ukrinform.ru/rubric-technology/2281679-rto-i-rpo-ili-o-cem-nuzno-pomnit-pri-rezervirovanii-dannyh.html

23. Нетепчук В.В. Управління бізнес-процесами: навч.посібник / В.В. Нетепчук – Рівне: НУВГП, 2014. -158 с.

24. Домарацький М. Б. Забезпечення безпеки та підвищення ефективності

захисту критично важливихоб'єктів на державному рівні / М. Б. Домарацький // Публічне управління і адміністрування в Україні. – 2019. – Вип. 14. – С. 82–85.

25. Alexander Hiznay, Candice Moschell Cybersecurity Watch 5/14/2020 [Electronic resource] https://www.crowe.com/cybersecurity-watch/business-continuity-management-during-covid-19?utm_content=buffer3120b&utm_medium= social&utm_source=twitter.com&utm_campaign=buffer.

26. Орлова К.Є. Управління бізнесом: підручник [Електронне видання] / К.Є. Орлова. – Житомир: Державний університет «Житомирська політехніка», 2019. –319 с.

27. IBM Services Adapt and respond to risks with a business continuity plan (BCP) /25 November 2020/ [Electronic resource] – https://www. ibm. com/ services /business-continuity/plan.

28. Kim Lindros, Ed Tittel How to create an effective business continuity plan /JUL 18, 2017// [Electronic resource] – https://www.cio.com/article/2381021/best-practices-how-to-create-an-effective-business-continuity-plan.html

29. Michael Herrera A Business Impact Analysis Guide / March 7, 2017/- / [Electronic resource] - https://bcmmetrics.com/business-impact-analysis-thorough-definition/

30. Steven A. Taddonio, CBCI Massachusetts Institute of Technology MIT Emergency Management [Electronic resource] – https://prepared. mit.edu/preparedness/dlcs/epp/.

31. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України "Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України" від 03.03.2011 N 24-112/365.

32. В.П. Пасько, В.А. Гасанов, А.С. Гришко, А.В. Максимюк Інтер операбельність матриці прийняття рішень для оцінювання ризиків інформаційної безпеки : / Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління».– 2018.– № 2’ (33).– 86 с.

33. Ситник Г.П., Абрамов В.І.. Глобальна та національна безпека: підручник / [авт. кол. :В.І. Абрамов, Г.П. Ситник, В.Ф. Смолянюк та ін.] / за заг. ред. Г.П.Ситника. – Київ : НАДУ, 2016. – 784 с.

34. Посохов І. М. Управління ризиками у підприємництві: навчальний посібник / І. М. Посохов. – Харків : НТУ «ХПІ», 2015. – 220 с.

35. COSO Enterprise Risk Management–Integrated Framework Executive Summary [Electronic resource] http:// www.coso.org/Publications/ERM/COSO_ERM_ ExecutiveSummary.pdf

36. Вишня В. Б. Основи інформаційної безпеки: навч. посіб. / [В.Б. Вишня, О.С. Гавриш, Е.В. Рижков]. – Дніпро : ДДУВС, 2020. – 128 с.

37. Maciej Kiedrowicz1, Jerzy Stanik / Method for assessing efficiency of the management system Military University of Technology, Faculty of Cybernetics/ CSCC 2018 [Electronic resource] https://www.matec-conferences.org /articles/ matecconf/pdf/2018/69/matecconf_cscc2018_04011.pdf

38. Виноградова Н.В. Методи управління ризиками в підприємницькій діяльності /[Електронний ресурс] http://enalp.edu.ua:8080/bitstream/ntb/9668/1/93.pdf.

39. Нормативний документ системи технічного захисту інформації «Типове положення про службу захисту інформації в автоматизованій системі».

40. Kevin Stine, Stephen Quinn, Greg Witte R. K. Gardner NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management (ERM).

41. ISO/IEC 27035. Information technology. Securitytechniques. Information security incedent management. – 2011. – 78 с.

42. Dave Hatter Intrust IT-support, cyber security [Electronic resource] https://www.intrust-it.com/dave-hatter/.

43. Ponemon institute: Advancing Responsible Information Management [Electronic resource] https://www.ponemon.org/

44. Kevin Stine (NIST), Stephen Quinn (NIST), Gregory Witte (Huntington Ingalls Industries), Robert Gardner (New World Technology Partners) NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Managemen (ERM) [Electronic resource] https://csrc.nist.gov/publications/detail/nistir/8286/final.

45. NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments

46. Internationalstandard ISO/IEC 17799:1999, “Information technology – Code of practice for information security managment”.

47. International standard ISO/IEC 15408:1999, “Information technology – Security techniques –Evaluation criteria for IT security – Part 1- Part 3”.

48. Шаго Ф.Н., Зикратов И.А. Методика оптимизации планирования аудита системы менеджмента информационной безопасности // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 2 (90). – С. 111–117.

49. Лютова И.И. Моделирование уровня приемлемого риска информационной безопасности // Вестник государственного университета. Серия 5: Экономика. 2014. – № 2 (141). – С. 175–180.

50. Imperva blog: Securityinformationandeventmanagement (SIEM) // [Electronic resource] https://www.imperva.com/learn/application-security/siem/

51. Ю. Самохвалов Корреляция событий в SIEM-системах на основе немонотонного вывода / Ю. Самохвалов, С. Толюпа // Захист інформації. - 2017. - 19, № 1. - С. 5-9. - Библиогр.: 9 назв. - рус.

52. Linda Rosencrance. Security information and event management (SIEM) // [Electronic resource] //https://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

53. Jeff Petters What is SIEM? A Beginner’s Guide// [Electronic resource] // https://www.varonis.com/blog/what-is-siem/

54. Fortinet // [Electronic resource] //https://www.fortinet. com/ru/products/ siem /fortisiem

55. Леонид Бараш. Fortinet Security Day 2018 в Украине // [Електронний ресурс] – Режим доступу: // https://ko.com.ua/fortinet _security_day_ 2018_v_ ukraine_ 124500

56. Forti SIEM Технические данные // [Electronic resource]// https://www.fortinet. com/content/dam/fortinet/assets/datasheets/ru_ru/FortiSIEM.pdf

57. Gartner peerin sights Forti SIEM Reviews// [Electronic resource] //

https://www.gartner. com/reviews/market/security-information-event-management/vendor/fortinet/product/fortisiem

ДОДАТОК А

Формування реєстру ризиків інформаційної безпеки по бізнес діяльності

Реєстраційний елемент	**Опис**
Ідентифікатор (ідентифікатор ризику)	Послідовний числовий ідентифікатор для посилання на ризик у реєстрі ризиків
Пріоритет	Відносний показник критичності цього запису в реєстрі ризиків, виражений або в порядковому значенні (наприклад, 1, 2, 3), або у посиланні на дану шкалу (наприклад, високий, помірний, низький)
Опис ризику	Коротке пояснення сценарію ризику кібербезпеки (потенційно), що впливає на організацію та підприємство. Описи ризиків часто пишуться у причинно-наслідковому форматі, наприклад, "якщо виникає X, то трапляється Y"
Поточна оцінка - ймовірність	Оцінка ймовірності виникнення цього сценарію до будь-якої реакції на ризик. На першій ітерації циклу ризику це також можна вважати початковою оцінкою.
Поточна оцінка - вплив	Аналіз потенційних вигод або наслідків, які можуть виникнути внаслідок цього сценарію, якщо додаткові відповіді не надаються. На першій ітерації циклу ризику це також можна вважати початковою оцінкою.

Поточна оцінка - Рейтинг впливу	Розрахунок ймовірності впливу ризику на основі оцінки ймовірності та визначених переваг або наслідків ризику. Інші загальні рамки використовують для цієї комбінації різні терміни, такі як *рівень ризику (* наприклад, ISO 31000, NIST SP 800-300 Rev. 1). На першій ітерації циклу ризику це також можна вважати початковою оцінкою.
Тип відповіді на ризик	Реакція на ризик (іноді її називають «лікуванням» ризику) для управління виявленим ризиком.
Опис реакції на ризик	Короткий опис реакції на ризик. Наприклад, «Впровадити програму управління програмним забезпеченням XYZ для забезпечення інвентаризації програмних платформ та додатків», або «Розробити та впровадити процес, щоб забезпечити своєчасне отримання інформації про загрози від [назва конкретних форумів та джерел обміну інформацією].
Власник ризику	Призначена сторона, відповідальна і відповідальна за забезпечення збереження ризику відповідно до вимог підприємства. Власник ризику може працювати з призначеним менеджером з управління ризиками, який відповідає за управління та моніторинг обраної реакції на ризик
Статус	Поле для відстеження поточного стану ризику.

ДОДАТОК Б

Шкала оцінки цінності активів організації включно з оцінкою ризику

Цінний актив організації	**Загрози**	**ЦН**	**СВ**	**Й**	**Р**	**Числове значення оцінки ризику**
Інформація, необхідна для реалізації призначення або бізнесу організації	Загроза завантаження нештатної операційної системи	4	1	1	4	Низький
	Загроза використання інформації ідентифікації / аутентифікації, заданої за замовчуванням	4	2	1	8	Низький
	Загроза дослідження механізмів роботи програми	4	1	2	8	Низький
	Загроза несанкціонованого видалення	4	3	4	48	Високий
	Загроза пошкодження системного реєстру	4	2	2	16	Середній
	Загроза подолання фізичного захисту	4	1	3	12	Середній
	Загроза програмного виведення з ладу засобів зберігання, обробки і (або) введення / виведення / передачі інформації	4	3	2	24	Високий
	Загроза втрати обчислювальних ресурсів	4	1	2	8	Низький
	Загроза втрати носіїв інформації	4	3	4	48	Високий
	Загроза форматування ня носіїв інформації	4	1	3	12	Низький
	Загроза розкрадання коштів зберігання, обробки і (або) введення / виведення / передачі інформації	4	1	3	12	Низький
	Загроза неправомірного шифрування інформації	4	2	2	16	Низький
	Загроза впровадження шкідливого коду через рекламу, сервіси та контент	4	2	3	24	Високий

Апаратно-програмний комплекс	Загроза тривалого утримання обчислювальних ресурсів користувачами	4	2	2	16	Середній
	Загроза завантаження нештатної операційної системи	4	3	1	12	Середній
	Загроза надлишкового виділення оперативної пам’яті	4	2	2	16	Середній
	Загроза зміни компонентів системи	4	3	3	36	Високий
	Загроза використання інформації ідентифікації / аутентифікації, заданої за замовчуванням	4	1	1	4	Низький
	Загроза дослідження механізмів роботи програми	4	1	2	8	Низький
	Загроза перезавантаження апаратних і програмно-апаратних засобів обчислювальної техніки	4	2	2	16	Середній
	Загроза пошкодження системного реєстру	4	2	2	16	Середній
	Загроза підвищення привілеїв	4	2	2	16	Середній
	Загроза подолання фізичного захисту	4	3	3	36	Високий
	Загроза приведення системи в стан «відмова в обслуговуванні	4	3	2	24	Високий
	Загроза програмного виведення з ладу засобів зберігання, обробки і (або) введення / виведення / передачі інформації	4	2	2	16	Середній
	Загроза втрати обчислювальних ресурсів	4	3	2	24	Високий
	Загроза фізичного виведення з ладу засобів зберігання, обробки і (або) введення / виведення / передачі інформації	4	1	3	12	Середній

	Загроза розкрадання коштів зберігання, обробки і (або) введення / виведення / передачі інформації »	4	2	3	24	Високий
	Загроза фізичного старіння апаратних компонентів	4	1	3	12	Середній
	Загроза маскування дій шкідливого коду	4	1	2	8	Низький
Мережа	Загроза надлишкового виділення оперативної пам’яті	4	2	2	16	Середній
	Загроза використання слабкостей протоколів мережевого / локального обміну даними	4	1	2	8	Низький
	Загроза дослідження механізмів роботи програми	4	1	2	8	Низький
	Загроза приведення системи в стан «відмова в обслуговуванні	4	3	2	24	Високий
	Загроза втрати обчислювальних ресурсів	4	3	2	24	Високий
	Загроза поширення електронною поштою «черв’яків»	4	2	2	16	Середній
	Загроза фізичного старіння апаратних компонентів	4	1	3	12	Середній
	Загроза впровадження шкідливого коду через рекламу, сервіси та контент	4	2	3	24	Високий
	Загроза маскування дій шкідливого коду	4	1	2	8	Низький

ДОДАТОК В

Розгорнутий звіт про втручання в інформаційну безпеку підприємства

FortiSIEM

Incident Report
Organization: Super
User Notes

Incident: 13

Event Severity Category	HIGH	Incident Last Occurrence Time	02:25:00, Sun, May 09 2021	Event Name	Concurrent Successful Authentications To Same Account From Multiple Cities
PhIncidentTactics	Credential Access	PhIncidentTechniques	[{"name": "Brute Force: Password Guessing", "techniqueid": "T1110.001"}]	Incident Reporting Device	NGFW_PRI
Incident Source		Incident Target	destName:NGFW_PRI, destIpAddr:10.88.2.254, user:demo,	Incident Detail	
Incident Status	Active	Incident Resolution	Open	Incident ID	13
Event Type	PH_RULE_CONCURRENT_SUCCESS_AUTH_MULTI_CITY	Incident Ticket Status	None	Business Service Name	
Count	12647	Incident Cleared Time		Incident Ticket User	
Incident Notification Recipients		Incident Cleared Reason		Incident Comments	
Event Severity	9	Incident First Occurrence Time	19:23:00, Wed, Apr 22 2020	Incident Reporting IP	10.88.2.254
Incident Ticket ID		Organization Name	Super	Incident Notification Status	
Incident Cleared User		Incident Externally Assigned User		Incident Externally Cleared Time	
Incident External Ticket ID		Incident External Ticket State		Incident External Ticket Type	
Incident View Status	Read			Incident Category	Security
Incident Subcategory	Credential Access			Incident Reporting Device Status	Pending

IP Address	Host Name	Organization ID	Country	State	City	Region	Building	Floor
Incident Reporting IP: 10.88.2.254	NGFW_PRI	1						

Total Number Records: 2

Rank	Event Receive Time	Event Type	Event Name	Source IP	Source Country	Source City	User	Reporting Device	Reporting IP
1	02:24:01, Sun, May 09 2021	FortiGate-event-admin-login-success	Admin logged in successfully	121.7.77.171	Singapore	Singapore	demo	NGFW_PRI	10.88.2.254
2	02:22:22, Sun, May 09 2021	FortiGate-event-admin-login-success	Admin logged in successfully	103.75.29.64	India	Aurangabad	demo	NGFW_PRI	10.88.2.254