МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

На рецензію
Завідувач кафедри УІКБ
Доктор економічних наук, доцент
_____ С.В. Легомінова
«___»_____2021 р.

До захисту
Завідувач кафедри УІКБ
Доктор економічних наук, доцент
_____ С.В. Легомінова
«___»_____2021 р.

ДИПЛОМНА РОБОТА

на тему:

ДОСЛІДЖЕННЯ ПРОЦЕСУ ОРГАНІЗАЦІЇ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

СТУДЕНТ: Голіненко Артем Олегович _____
(підпис)

КЕРІВНИК: к.в.н., доцент, Якименко Юрій Михайлович _____
(підпис)

НОРМОКОНТРОЛЕР: _____ _____
(підпис)

Київ — 2021

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

Освітньо-кваліфікаційний рівень — магістр
Галузь знань — «12 Інформаційні технології»
Спеціальність — «125 Кібербезпека»
Спеціалізація — «Управління інформаційною безпекою»

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____Легомінова С. В.
“___”_____ 2021р.

ЗАВДАННЯ
на магістерську атестаційну роботу
Студенту **Голіненко Артему Олеговичу**

1.Тема роботи “Дослідження процесів управління інцидентами інформаційної безпеки на підприємстві”, затверджена наказом по університету від “13” жовтня 2020 р. №.230

2. **Термін здачі** студентом закінченої дипломної роботи 25 грудня 2020р.

3. **Вихідні дані до роботи**:

- дослідити організаційно-правові вимоги до забезпечення інформаційної безпеки підприємства,
- проаналізувати організацію управління інцидентами в системі забезпечення інформаційної безпеки підприємства,
- провести дослідження процесів організації управління інцидентами в системі забезпечення інформаційної безпеки на прикладі підприємства,
- розробити рекомендації щодо вдосконалення процесів управління інцидентами інформаційної безпеки на підприємстві (для вибраного прикладу).

4. **Склад розрахунково-пояснювальної записки** (перелік питань до розробки).

1. Аналіз організаційно-правових вимог до забезпечення інформаційної безпеки підприємства.
2. Аналіз організації управління інцидентами в системі забезпечення інформаційної безпеки підприємства.
3. Дослідження процесів організації управління інцидентами в системі забезпечення інформаційної безпеки на прикладі підприємства.

5. **Перелік обов’язкових демонстраційних креслень**:

1. Схема системи забезпечення інформаційної безпеки підприємства.
2. Схема системи управління інцидентами інформаційної безпеки підприємства.
3. Схема алгоритму дій керівництва щодо організації процесів управління інцидентами інформаційної безпеки на підприємстві.
4. Рекомендації щодо вдосконалення процесів організації управління інцидентами на підприємстві (для вибраного прикладу).
5. Презентація доповіді, виконана в Microsoft PowerPoint.

6. **Термін виконання дипломної роботи**:
   подання закінченої роботи керівнику 22 грудня 2020 року.
   подання роботи на рецензію 23 грудня 2020 року.
7. **Дата видачі завдання** 26.10.2020 року.

Календарний план

№ з/п	Назва етапів магістерської атестаційної роботи	Термін виконання етапів	Відмітка про виконання
1.	Підбір науково-технічної літератури.	29.10.2020 р.	
2.	Аналіз та систематизація матеріалу. Вступ	5.11.2020 р.	
3.	Аналіз організаційно-правових вимог до забезпечення інформаційної безпеки підприємства.	13.11.2020 р.	
4.	Аналіз організації управління інцидентами в системі забезпечення інформаційної безпеки підприємства.	11.12.2020 р.	
5.	Дослідження процесів організації управління інцидентами в системі забезпечення інформаційної безпеки на прикладі підприємства.	15.12.2020 р.	
6.	Оформлення та друк пояснювальної записки	25.12.2020 р.	
7.	Отримання відгука та рецензії на роботу	29.12.2020 р.	
8.	Оформлення презентацій	4.01.2021 р.	
9.	Попередній захист на кафедрі	8.01.2021 р.	
10.	Захист в ДЕК	20.01.2021 р.	

Керівник _____ Якименко Юрій Михайлович
(підпис) (прізвище, ім’я, по-батькові)

Завдання прийняв
для виконання _____ Голіненко Артем Олегович
(підпис) (прізвище, ім’я, по-батькові)

РЕФЕРАТ

Дипломна робота присвячена дослідженню методів організації управління інцидентами інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 20 рисунків, 2 таблиці, висновків та списку використаних джерел, що містить 39 найменувань. Загальний обсяг роботи становить 88 аркушів, з яких 5 аркушів займають перелік умовних скорочень та список використаних джерел.

Об'єктом дослідження в роботі є система управління інцидентами інформаційної безпеки.

Предметом дослідження є організація управління інцидентами інформаційної безпеки в діяльності підприємства.

Метою роботи є дослідження організаційно-правових вимог та методологічних підходів до організації управління інцидентами інформаційної безпеки, а також розробка рекомендацій щодо вдосконалення процесів управління інцидентами інформаційної безпеки на підприємстві. Для цього в роботі використовуються найпоширеніші підходи до організації управління інцидентами в системі забезпечення інформаційної безпеки.

Як результат у роботі проведено аналіз досвіду країн у використанні підходів до створення ефективної системи управління інцидентами інформаційної безпеки, а також розроблено методику впровадження системи управління інцидентами інформаційної безпеки на прикладі підприємства.

Ключові слова: ІНЦИДЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ПРОЦЕС РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АСУ — автоматизована система управління.

ВПЗ — вірусне програмне забезпечення.

ГРІІБ — група реагування на інциденти інформаційної безпеки.

ЗМІ — засоби масової інформації.

ІБ — інформаційна безпека.

ІС — інформаційна система.

СКД — система контролю доступу.

СУІІБ — система управління інцидентами інформаційної безпеки.

ШПЗ — шкідливе програмне забезпечення.

APT — advanced persistent threat (розвинена стійка атака).

OWASP — Open Web Application Security Project (Відкритий проект з безпеки веб-застосунків).

SIEM — Security Information and Event Management (Управління інформаційною безпекою та подіями інформаційної безпеки).

ВСТУП

Актуальність теми. Сьогодні будь-яка організація незалежно від виду діяльності та форми власності не в змозі успішно розвиватися й вести господарську або управлінську діяльність без створення належних умов для надійного функціонування системи захисту власної інформації. Всі організації за умов конкурентного середовища, що формується, стикаються з такими негативними явищами, як підслуховування, викрадення конфіденційної інформації на матеріально-речових носіях, зняття інформації з технічних каналів через комп'ютерні мережі. Всі ці інциденти повинні бути швидко проаналізовані та закриті, з метою забезпечення безперервності роботи бізнесу та уникнення великих як матеріальних так і ресурсних втрат. Для цього всі процеси управління інцидентами повинні бути добре налагоджені і організовані. Тому, нині перед суб'єктами підприємницької діяльності стоїть необхідність організації ефективного управління інцидентами інформаційної безпеки.

Мета і завдання дослідження. Мета роботи полягає у дослідженні організаційно-правових вимог та методологічних підходів до організації управління інцидентами інформаційної безпеки, а також розробці рекомендацій щодо вдосконалення процесів управління інцидентами інформаційної безпеки на підприємстві. Для досягнення цієї мети в роботі необхідно вирішити такі завдання:

- проаналізувати досвід країн у використанні підходів до створення ефективної системи управління інцидентами інформаційної безпеки;
- розробити методику впровадження системи управління інцидентами інформаційної безпеки на прикладі підприємства.

Виходячи з цього *об'єктом дослідження* є система управління інцидентами інформаційної безпеки. *Предмет дослідження* — організація управління інцидентами інформаційної безпеки в діяльності підприємства.

Методи дослідження. Для вирішення зазначеного вище наукового завдання в роботі використані методи системного аналізу та теорії інформаційної безпеки, теорії та практики організації управління інцидентами інформаційної безпеки.

Розділ 1
АНАЛІЗ ОРГАНІЗАЦІЙНО-ПРАВОВИХ ВИМОГ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

В даному розділі буде проаналізовано організаційно-правові вимоги до забезпечення інформаційної безпеки підприємства. Для цього необхідно розкрити основні характеристики забезпечення інформаційної безпеки, роль управління інцидентами інформаційної безпеки, а також проаналізувати основні вимоги стандартів цієї сфери.

1.1 Основні характеристики забезпечення інформаційної безпеки

Розвиток глобального процесу інформатизації суспільства, що спостерігається в останні десятиліття, спричинив нову глобальну проблему — інформаційну безпеку. Багато найважливіших інтересів підприємства в даний час значною мірою визначається станом навколишнього інформаційного середовища. Цілеспрямовані або ненавмисні впливи на інформаційну сферу з боку зовнішніх або внутрішніх джерел можуть завдавати серйозної шкоди цим інтересам і становлять загрози та ризики для безпеки. Тому інформаційна безпека в сучасних умовах є однією з необхідних умов нормального функціонування підприємства. Не випадково питання інформаційної безпеки вже давно входять до головних пріоритетів практично всіх великих компаній. Останнім часом більше керівників середнього і малого вітчизняного бізнесу починають усвідомлювати реальну небезпеку інцидентів, пов'язаних з інсайдерською інформацією, системами її обробки і співробітниками, що беруть участь у цьому процесі.

Питання інформаційної безпеки знайшли відображення у законах України [1-4]: «Про національну безпеки України», «Про концепцію національної програми інформатизації», «Про національну програму інформатизації», а також у Стратегії національної безпеки України, яка затверджена Указом Президента.

Найбільш актуальним сьогодення є Закон «Про основи національної безпеки України», яким надано офіційну оцінку значущості й системної сутності інформаційної безпеки як невід'ємної складової національної безпеки України. У Стратегії національної безпеки, присвяченій стану інформаційної безпеки в нашій державі, зазначено: посилюється негативний зовнішній вплив на інформаційний простір України, що загрожує розмиванням суспільних цінностей і національної ідентичності; недостатніми залишаються обсяги вироблення конкурентоспроможного національного інформаційного продукту; наближається до критичного стан безпеки інформаційно-комп'ютерних систем у фінансовій і банківській сфері, сфері державного управління, енергетики, транспорту, внутрішніх та міжнародних комунікацій тощо [4, п. 2.8].

Поняття інформаційної безпеки можна розглядати у декількох ракурсах [5-8]. По-перше, це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави. По-друге, це стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їх існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.

Зі зростанням науково-технічного прогресу буде зростати важливість питання інформаційної безпеки. Інформація стала чинником, який може призвести до значних технологічних аварій, військових та політичних конфліктів, дезорганізувати державне управління, фінансову систему [9]. Чим вищий рівень інтелектуалізації та інформатизації суспільства, тим потрібнішою стає надійна інформаційна безпека, оскільки реалізація інтересів, людей та держав усе більше здійснюється за допомогою інформатизації. Ураховуючи той факт, що під впливом інформаційних інцидентів може цілеспрямовано змінюватися кругозір та

мораль як окремих осіб, так і суспільства в цілому, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності та форм проявів сучасних методів скритого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і суперечать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямах.

Як показує практична діяльність організацій (господарюючих суб’єктів) інформаційна безпека для підприємства полягає у певних діях щодо вияву, усунення та нейтралізації негативних джерел, причин і умов впливу на інформацію [9]. При цьому поняття «інформаційна безпека» характеризує стан інформаційного захисту господарюючого суб’єкта, в умовах якого можлива дія загроз. Досягається це системою заходів, спрямованих на попередження, вияв та ліквідацію інформаційних загроз. Погіршення на підприємстві таких параметрів інформації, як конфіденційність, цілісність, доступність, вірогідність тощо, може призвести до досить негативних наслідків: збоїв у функціонуванні систем управління технологічними процесами й іншими критичними системами; розголошення відомостей, що становлять комерційну й інші види таємниць; порушення вірогідності фінансової документації; несанкціонованого доступу до персональних даних фізичних осіб тощо. Результатом перерахованого можуть стати: погіршення ділових відносин із партнерами; зриви переговорів, втрата вигідних контрактів; невиконання договірних зобов'язань; необхідність проведення додаткових ринкових досліджень; відмовлення від рішень, що стали неефективними через розповсюдження інформації, і, як наслідок, — фінансові втрати, пов'язані з новими розробками; втрата можливості запатентувати результат науково-технічної діяльності або продати ліцензію; зниження цін або обсягів реалізації; втрати ділової репутації; більш жорсткі умови одержання кредитів; труднощі в постачанні і придбанні устаткування тощо. У визначених ситуаціях зневага питаннями захисту інформації може призвести до повного банкрутства. Тому питання управління інцидентами є визначальним при побудові ефективної системи захисту інформації.

Основними постулатами (принципами) інформаційної безпеки є конфіденційність, цілісність та доступність (рис. 1.1). Кожен елемент програми інформаційної безпеки повинен бути розроблений для досягнення одного або кількох із цих принципів.

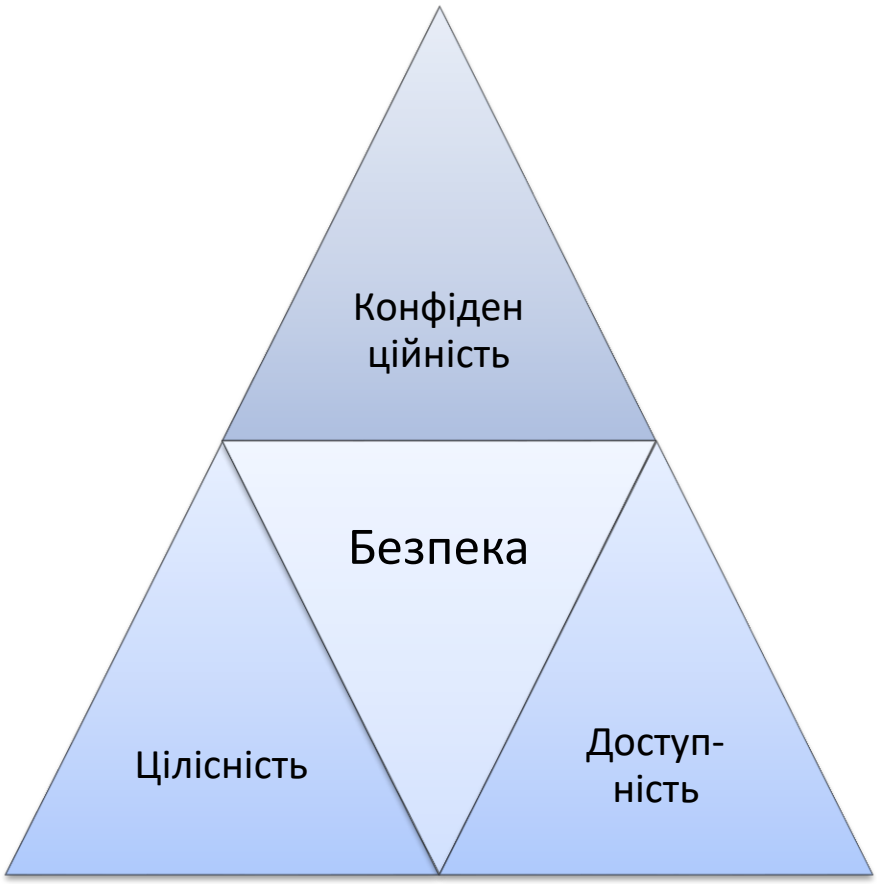

Рис.1.1 Принципи інформаційної безпеки [12]

Заходи щодо конфіденційності призначені для захисту від несанкціонованого розголошення інформації. Мета принципу конфіденційності полягає у забезпеченні того, щоб приватна інформація залишалася приватною та щоб її могли переглядати або отримувати доступ лише особи, яким ця інформація потрібна для виконання своїх службових обов'язків.

Цілісність передбачає захист від несанкціонованих модифікацій (наприклад, додавання, видалення або зміни) даних. Принцип цілісності розроблений для того, щоб гарантувати, що дані можуть бути достовірними і що вони не були неналежним чином змінені.

Доступність захищає функціональність систем підтримки та забезпечує повну доступність даних у той момент часу (або вимоги періоду), коли вони потрібні її користувачам. Мета доступності — забезпечити доступність даних для використання, коли це потрібно для прийняття рішень.

Ефективне виконання всіх трьох принципів створює ідеальний результат з точки зору інформаційної безпеки. Розглянемо такий приклад: організація отримує або створює фрагмент конфіденційних даних, який буде використовуватися в ході її господарських операцій. Оскільки дані є конфіденційними, ці дані можуть бачити лише ті люди в організації, яким потрібно їх бачити для того, щоб виконувати свою роботу. Вони повинні бути захищені від доступу сторонніх осіб. Це приклад принципу конфіденційності.

Коли особа, якій потрібні ці дані для виконання службового обов’язку, готова використовувати їх, вони повинні бути доступні своєчасно та надійно, щоб завдання можна було виконати вчасно і компанія могла працювати безперервно. Це описує принцип доступності. І нарешті, дані будуть використані при розрахунках, які впливають на ділові рішення та інвестиції, які буде здійснено організацією. Тому точність даних є критично важливою для забезпечення належних розрахунків та результатів, за якими будуть прийматися рішення. Гарантія того, що дані не були якимсь чином підроблені, і тому їм можна довіряти під час розрахунків та прийнятих рішень є принципом цілісності.

Існує три основні галузі або класифікації засобів контролю безпеки. Сюди входять безпека управління, оперативна безпека та контроль фізичної безпеки.

Фізична безпека — це захист персоналу, даних, апаратних засобів тощо від фізичних загроз, які можуть завдати шкоди, пошкодити або порушити ділові операції або вплинути на конфіденційність, цілісність або доступність систем та / або даних. Це може бути, наприклад, забезпечення засобами безперебійного живлення інфраструктури компанії, фізична охорона і т.д.

Управління безпекою — це загальний план всіх елементів і процесів інформаційної безпеки. Сюди входять вказівки, правила та процедури для

забезпечення безпечного середовища функціонування підприємств. Наприклад, вимоги до використання і роботи з корпоративною інформацією, парольні політики, навчання співробітників принципам інформаційної безпеки і т.д.

Операційна безпека — це ефективність всіх елементів інформаційної безпеки. Сюди входять технічні засоби контролю, до яких належать засоби контролю доступу, аутентифікації та топології безпеки, що застосовуються до мереж, систем та програм. Наприклад, забезпечення антивірусного захисту, постійний моніторинг корпоративної мережі та всіх її елементів, використання тільки ліцензованого програмного забезпечення та своєчасне його оновлення і т.д.

На рис. 1.2 показано, що система забезпечення інформаційної безпеки складається з трьох основних елементів:

- Організаційна;
- Технічна;
- Правова.

Рис. 1.2 Основні елементи системи забезпечення інформаційної безпеки [37]

Організаційна — наявність політик безпеки підприємства, ретельний підбір персоналу, фінансування, необхідне і достатнє фінансування, наявність

ефективних систем управління інцидентами, забезпечення кваліфікованими кадрами і т.д.

Технічна — захищеність організації від несанкціонованого доступу до системи шляхом використання парольної політики, шифрування файлів, резервне копіювання, використання систем контролю доступу, пожежогасіння, резервні системи живлення, тощо;

Правова — відповідність міжнародним та державним стандартам, захист авторських прав, юридична підтримка політик, договори про нерозголошення конфіденційної безпеки, тощо.

Таким чином, система забезпечення інформаційної безпеки підприємства є необхідною і достатньо багатогранною. Задля того, щоб полегшити компаніям процес створення чи впровадження системи забезпечення інформаційної безпеки були розроблені різноманітні загальноприйняті міжнародні стандарти, які необхідно детально розглянути.

1.2 Вимоги стандартів до забезпечення управління інцидентами інформаційної безпеки

Стандарти є однією з форм накопичення знань на процедурному та програмно-технічному рівнях інформаційної безпеки. Вони також включають тестування, якісні рішення та методології, розроблені кваліфікованими фахівцями.

Найбільш поширеною і загальновизнаною у світі збіркою рекомендацій в сфері захисту інформації є серія стандартів ISO / IEC 27k. В Україні аналогом цих стандартів є стандарти ДСТУ ISO/IEC 27к, які розробляються Українським науково-дослідним центром проблем стандартизації, сертифікації та якості.

Серія містить рекомендації щодо найкращих практик щодо управління інформаційною безпекою — управління інформаційними ризиками за допомогою засобів контролю інформаційної безпеки — в контексті загальної системи управління інформаційною безпекою (СУІБ), яка в тому числі включає систему управління інцидентами інформаційної безпеки.

Серія стандартів дуже широка і охоплює не лише приватність та конфіденційність, а й питання інформаційної та кібербезпеки. Ці стандарти застосовуються до організацій будь-якої форми та розміру. Всім організаціям пропонується оцінити свої інформаційні ризики, а потім управляти ними (як правило, використовуючи засоби захисту інформації) відповідно до своїх потреб, використовуючи вказівки та пропозиції, де це доречно. З огляду на динамічний характер інформаційного ризику та безпеки, концепція СУІБ включає постійні заходи зворотного зв'язку та вдосконалення для реагування на зміни в загрозах, вразливостях або наслідках інцидентів.

Відповідно до рекомендацій стандарту, СУІБ включає в себе повний комплекс дій по забезпеченню інформаційної безпеки, в тому числі організацію діяльності та управління ризиками, а також безпосереднє застосування заходів захисту інформації. Робити вибір тих чи інших способів захисту інформації слід на основі оцінки ризиків ІБ, тобто розміру можливих збитків від реалізації загроз конфіденційності, цілісності та доступності інформації. І, звичайно, виходячи з необхідності виконання нормативних зобов'язань перед державою, партнерами та іншими зацікавленими сторонами. Таким чином, пропонований підхід дозволяє застосовувати стандарт для реалізації СУІБ в організаціях будь-якого масштабу і рівня нормативної зарегульованості.

Безпосередньо питання управління інцидентами інформаційної безпеки описане в стандартах ISO/IEC 27035-1 — Information security incident management — Part 1: Principles of incident management та ISO/IEC 27035-2 — Information security incident management — Part 2: Guidelines to plan and prepare for incident response. На даний момент діючими в Україні є стандарти ДСТУ ISO/IEC

27035-1:2018 (ISO/IEC 27035-1:2016, IDT) Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами та ДСТУ ISO/IEC 27035-2:2018 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти.

ISO / IEC 27035 забезпечує структурований та запланований підхід до:

- виявлення, повідомлення та оцінки інцидентів інформаційної безпеки;
- реагування на інциденти інформаційної безпеки та управління ними;
- виявлення, оцінки та управління вразливостями інформаційної безпеки;
- постійного вдосконалення інформаційної безпеки та управління інцидентами.

ISO / IEC 27035 надає вказівки щодо управління інцидентами в галузі інформаційної безпеки для великих та середніх організацій. Менші організації можуть використовувати базовий набір документів, процесів та процедур, описаних у цьому міжнародному стандарті, залежно від їх розміру та типу бізнесу відповідно до ризику інформаційної безпеки. Він також надає вказівки для зовнішніх організацій, що надають послуги з управління інцидентами в галузі інформаційної безпеки.

На рис. 1.3 показано, що згідно з ISO/IEC 27035-2 основними етапами управління інцидентами інформаційної безпеки є:

1. Планування і підготовка;
2. Виявлення та звітність;
3. Оцінка та прийняття рішень;
4. Реагування;
5. Діяльність після інциденту;
6. Аналіз отриманого досвіду.

Рис. 1.3 Етапи управління інцидентами інформаційної безпеки

В ході планування та підготовки впроваджується політика реагування на інциденти, оновлюються політики ІБ і управління ризиками, як на корпоративному рівні так і на рівні систем, створюється план реагування на інциденти ІБ, створюється ГРІІБ, налагоджується взаємодія з внутрішніми і зовнішніми організаціями і технічна підтримка.

На етапі виявлення і звітності відбувається моніторинг безперервності системних і мережевих процесів, виявлення і сигналізація про аномальну, підозрілу або шкідливу активність, узагальнення звітів про події ІБ від клієнтів, постачальників, інших ГРІІБ або відповідних організацій, звітність по подіям ІБ.

Етап оцінки та прийняття рішень включає в себе загальну оцінку ІБ, її стану та ситуації, крім того відбувається визначення інциденту та його класифікація.

Реагування інциденту включає в себе впровадження дій для визначення місця знаходження інциденту, його локалізація та ліквідація, відновлення діяльності після інциденту ІБ, визначення висновків та закриття інциденту. Після

чого за необхідності відбувається розслідування інциденту на етапі діяльності після інциденту.

Останній етап — це узагальнення та аналіз отриманого досвіду в результаті інциденту. На цьому етапі також відбувається визначення та удосконалення ІБ підприємства, визначення та удосконалення систем визначення та управління ризиками ІБ, визначення та удосконалення плану управління ІБ та також оцінюється ефективність ГРІІБ.

Крім стандартів серії ISO/IEC 27k існують вимоги OWASP. Це онлайн-спільнота, яка створює вільно доступні статті, методології, документацію, інструменти та технології в галузі безпеки веб-застосунків [38].

Основними проектами OWASP є:

- Проект OWASP Топ Десять: Проект «Top 10», вперше опублікований у 2003 і регулярно оновлюється. Він спрямований на підвищення обізнаності про безпеку застосунків шляхом виявлення деяких найбільш критичних ризиків для організацій Багато стандартів, книг, інструментів та організацій посилаються на OWASP Топ Десять, включно з MITRE, PCI DSS, Defense Information Systems Agency (DISA-STIG), Федеральна торговельна комісія США та багато інших.
- Настанова з тестування OWASP: Настанова з тестування включає найкращі практики з тестування на проникнення, які користувачі можуть впровадити у своїх організаціях, та настанову з низькорівневого тестування на проникнення, яка описує методики перевірки найбільш загальних проблем безпеки веб-застосунків та веб-сервісів. Версія 4 була опублікована 4 вересня 2014 із внеском від більш ніж 60 осіб.
- Стандарт перевірки безпеки застосувань OWASP (Application Security Verification Standard, ASVS): стандарт перевірки безпеки на рівні застосунків;
- Настанова OWASP з реагування на інциденти. Цей проект надає проактивний підхід до планування реагування на інциденти. Документ

призначений для аудиторії, що включає власників бізнесу, інженерів з безпеки, розробників, аудиторів, керівників програм, правоохоронців та юристів.

Щодо управління інцидентами спільнотою OWASP було розроблено топ 10 правил для реагування на інциденти інформаційної безпеки (рис. 1.4).

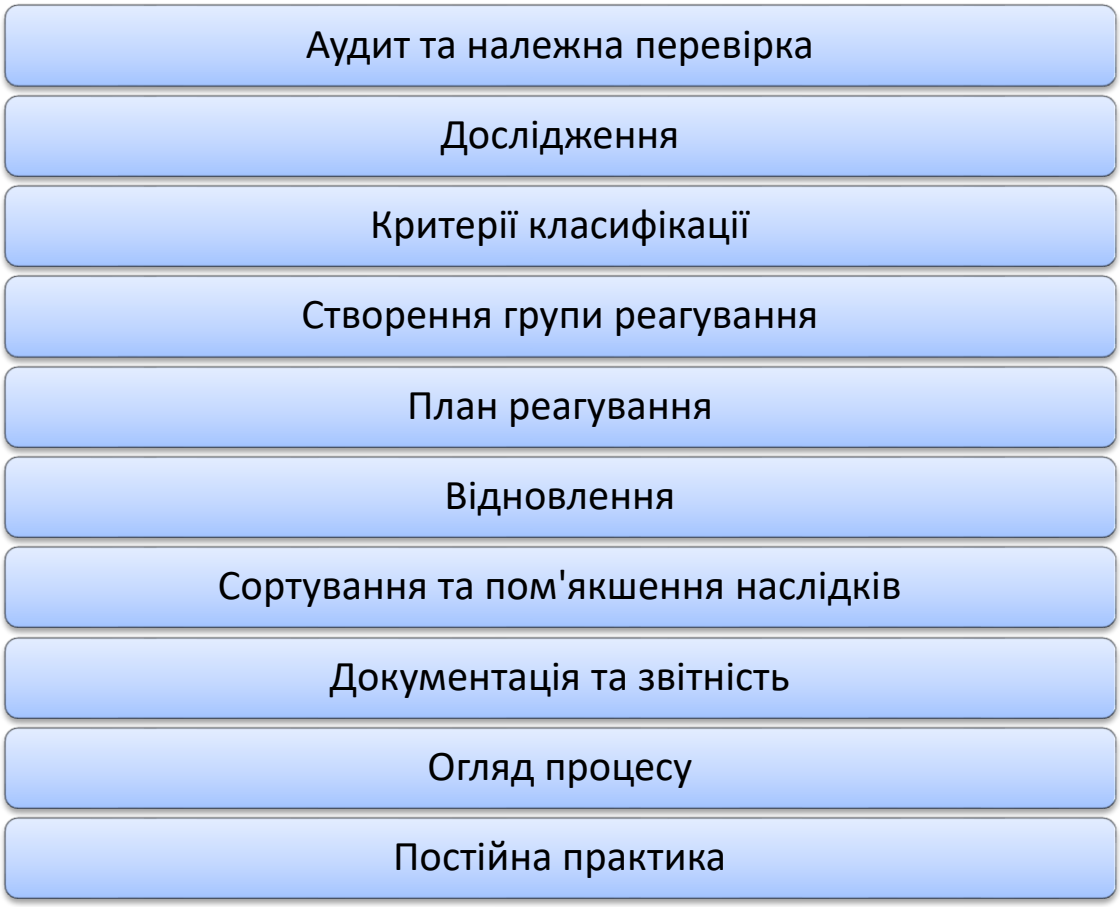

Рис. 1.4 10 правил OWASP [30]

Розглянемо кожне з правил детальніше:

– Аудит та належна перевірка. Проведення аудиту дасть вам зрозуміти, наскільки організація добре підготовлена до реагування на аварії з точки зору людей, процесів та обладнання;
– Створення групи реагування. Запобігання атакам та інцидентам, які можуть статися без попереднього повідомлення, та управління ними найкраще проводити експертам, які входять до групи реагування на інциденти. Але

потрібно переконатись в компетентості команди та її керівника, а також задокументувати та донести ролі та обов’язки кожного члена команди;

- Створіть документований план реагування на інциденти. Організація повинна мати добре задокументований план реагування на аварії, який би керував командою реагування на аварії під час інциденту. Комплексний план, як мінімум, повинен охоплювати ролі та обов'язки, розслідування, сортування та пом'якшення наслідків, процес відновлення та документування;
- Визначте свої критерії. Необхідно визначити, що можна класифікувати як інцидент у вашій організації, наскільки важливими чи вагомими є фактори, які можуть спричинити інцидент;
- Дослідіть проблему. Для ретельного розслідування буде потрібно залучення групи реагування на інциденти, а також може знадобитися внесок із зовнішніх ресурсів. Необхідно задокументувати всі подробиці інциденту, зокрема, на що слід звернути увагу, кого залучити та як задокументувати знайдене;
- Сортування та пом'якшення наслідків. Розслідування повинно включати процес сортування та вирішення проблем. Оскільки група виявляє потенційний вплив, їм слід відповідно планувати та виконувати ефективне пом'якшення наслідків за пріоритетами;
- Відновлення. Повне відновлення функціонування є важливим для будь-яких послуг чи процесів, які могли постраждати під час інциденту;
- Документація та звітність. Звітування та документація — це критично важлива дія, яка завжди відбуватиметься до, під час та після реагування на аварії. Необхідний вичерпний звіт про інцидент відповідно до найкращих практик та плану реагування на аварії. Тип звітів, які можуть знадобитися, може відрізнятися, але основною його ціллю є допомога ефективно керувати та уникати в подальшому подібних інцидентів;

- Огляд процесу. Обов’язково потрібно постійно контролювати інциденти та навантаження / ефективність роботи команди або спеціаліста з обробки інцидентів. Це допоможе визначити необхідність збільшення команди реагування на інциденти, необхідність автоматизації процесів та визначити на що потрібно звернути більш уваги;
- Практика, практика і ще раз практика. Не чекайте, поки трапиться інцидент, перш ніж почати щось робити. Важливо, щоб ваша команда реагування на інциденти розуміла, наскільки важливі фіктивні тренування та практика для фірми. Іноді ви можете практикувати імітацію реального сценарію. Цей тест може бути таким простим, як, наприклад, підкинута флешка на підлогу офісу та спостерігання за тим, що відбувається, для імітації порушення даних або фішингової атаки.

Реагування на інциденти охоплює всю організацію і не повинно обмежуватися лише IT-відділом чи окремими підрозділами. Слід чітко розуміти до яких наслідків може призвести той чи інший інцидент.

Також існує серія американських стандартів NIST Cybersecurity Framework. Це стандарти Національного інституту стандартів і технологій США. Це набір керівних принципів для компаній приватного сектору, які мають бути краще підготовленими до виявлення, ідентифікації та реагування на кібератаки. Ним визначено п’ять основних елементів забезпечення кібербезпеки (рис. 1.5):

- Виявлення;
- Ідентифікація;
- Захист;
- Реагування;
- Відновлення.

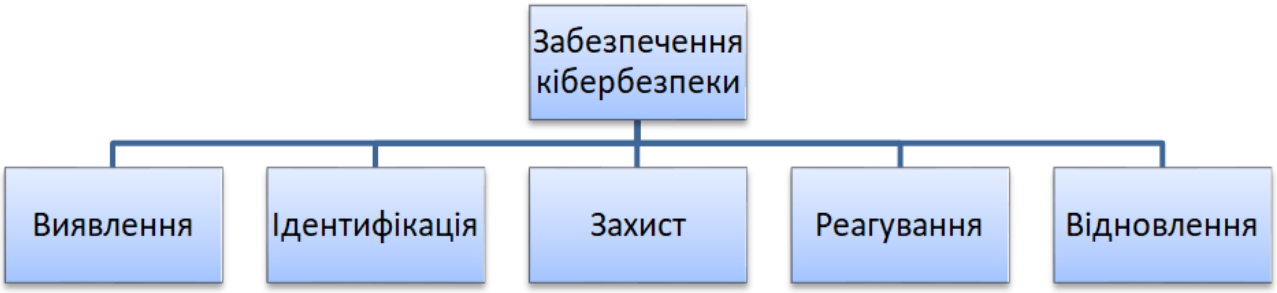

Рис. 1.5 Основні елементи забезпечення кібербезпеки

Управління інцидентами виділено в окремий документ під назвою «Computer Security Incident Handling Guide» [27]. Цим стандартом визначено основні дії необхідні для створення та управління системою реагування на інциденти:

- Створення політики та плану реагування на аварії;
- Розробка процедур для обробки інцидентів та звітування;
- Встановлення вказівок для спілкування із сторонніми сторонами щодо інцидентів;
- Вибір структури команди реагування та кадрової моделі;
- Встановлення стосунків та ліній зв'язку між командою реагування на події та іншими групами, як внутрішніми (наприклад, юридичний відділ), так і зовнішніми (наприклад, правоохоронні органи);
- Визначення, які дії повинна виконувати команда реагування на інциденти;
- Кадрове забезпечення та навчання групи реагування на події.

Такі дії повинні призвести до зменшення частоти інцидентів, завдяки ефективному захисту мережі, системи та додатків. Організації, як правило, повинні бути готовими вирішити будь-який інцидент, але перш за все необхідно зосередитись на тому, щоб бути готовими до інцидентів, що використовують загальні вектори атак, а саме:

- Зовнішні / знімні носії;
- Надмірне навантаження системи;
- Веб-застосунки;

- Електронна пошта;
- Ненавмисні дії працівників;
- Викрадення або втрата обладнання.

1.3 Підходи до побудови та функціонування системи управління інцидентами інформаційної безпеки

На рис. 1.6 показані основні підходи до управління інформаційною безпекою підприємства:

- Процесний;
- Системний;
- Ситуаційний.

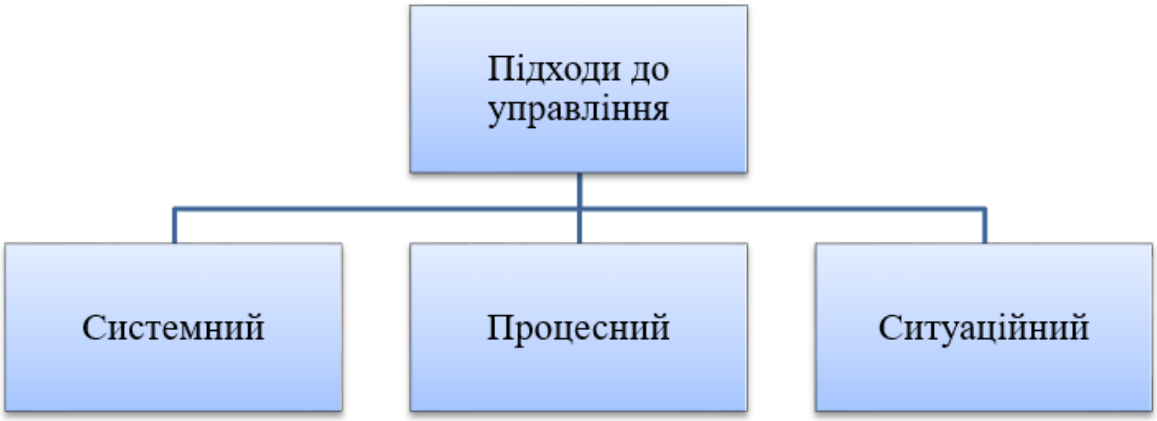

Рис. 1.6 Підходи до управління інформаційною безпекою [16]

Процесний підхід трактує управління як серію безпосередніх взаємопов'язаних дій. Ці дії, кожна з яких сама по собі вже є процесом, значною мірою визначають успіх діяльності організації. Вони дістали назву "управлінські функції". Кожна управлінська функція — це також процес. Отже, процес управління являє собою суму всіх функцій.

Процес управління містить функції планування, організації, мотивації, контролювання та регулювання (рис. 1.7).

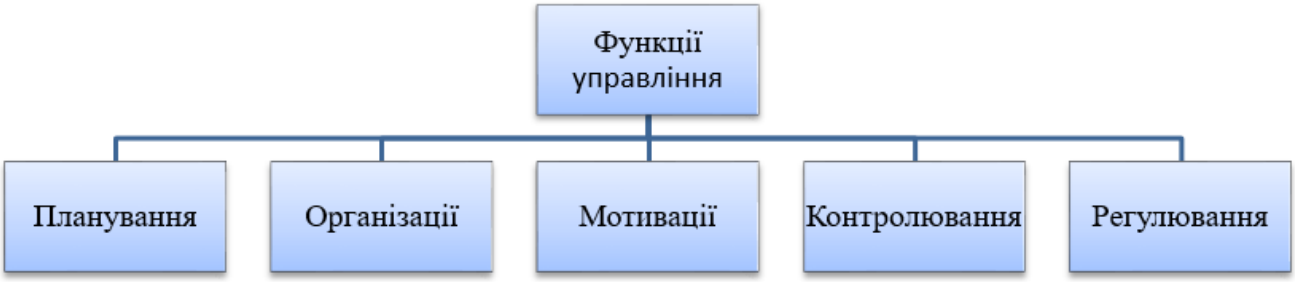

Рис. 1.7 Функції управління в процесному підході

Цих п’ять основних функцій управління поєднані з процесами комунікацій та прийняття рішень. Керівництво (лідерство) — це самостійна діяльність.

Функція планування передбачає рішення про те, якими мають бути цілі організації (підприємства) і що слід зробити, щоб досягти їх. Передусім треба відповісти на такі питання: стан справ, бажані результати, шляхи досягнення їх. Планування — це один з способів, за допомогою якого керівництво спрямовує зусилля всіх членів колективу на досягнення його загальних цілей.

Функція організації. Організувати — означає створити деяку структуру з метою досягнення певної мети. Сюди входить розподіл робіт між працівниками, делегування завдань і повноважень. Функція організування забезпечує організованість, дисципліну, відповідальність за доручену справу.

*Функція мотивування***.** Керівник має завжди пам'ятати, що навіть прекрасно складений план, найдосконаліша структура організації втрачають зміст, якщо працівники не виконують доручену їм роботу або виконують її неякісно, безініціативно. Функція мотивування спрямована на забезпечення виконання працівниками підприємства делегованих їм обов'язків. Для цього в організації мають бути створені умови для матеріальної та моральної зацікавленості працівників у виконанні робіт.

Функція контролювання — це процес забезпечення досягнення організацією своїх цілей. Існує три аспекти управлінського контролю: встановлення стандартів, зміни того, що було фактично досягнуто за відповідний період, порівняння досягнутого з очікуваним результатом.

Розглянуті функції управління мають дві загальні характеристики: всі вони потребують прийняття рішення. Тому прийняття рішення і комунікації належать до сполучних процесів управління.

Функція регулювання — вид управлінської діяльності, спрямований на усунення відхилень, збоїв, недоліків тощо в керованій системі шляхом розроблення і впровадження керуючою системою відповідних заходів.

Регулювання покликане усунути всі недоліки, відхилення, збої, виявлені у процесі контролювання. При цьому регулювальні заходи можуть застосовуватись на всіх попередніх етапах технології менеджменту (планування, мотивування, організування). Для цього вдаються до коригуючих дій, що базуються на виборі таких рішень:

- Усунення відхилень;
- Перегляд стандартів і критеріїв;
- Усунення відхилень з переглядом стандартів і критеріїв.

Особливість регулювання полягає в тому, що, на відміну від функцій планування, організації та мотивування, які удосконалюються безпосередньо в керуючій системі організації, регулювання, як і контролювання, вдосконалюється в керуючій та керованій системах.

Системний підхід. Система — це якась цілісна структура, яка складають взаємозалежні частини, кожна з яких певною мірою характеризує ціле. Згідно з системним підходом керівник має розглядати організацію як сукупність взаємопов'язаних елементів, таких як люди, структура, завдання, технологія, що орієнтовані на досягнення певних цілей і тісно переплетені з зовнішнім світом. Дещо спрощено організацію як систему можна описати так. Організація отримує з зовнішнього середовища інформацію, капітал, матеріали, трудові ресурси. Ці

компоненти мають назву "входи". У процесі перетворення ці входи перетворюються на підприємстві у продукцію або послуги. Вони і є виходами організації. Якщо організація управління ефективна, то в процесі перетворення утворюється додаткова вартість. За цих умов збільшується обсяг продажу, зростають прибуток, задоволення працівників результатами своєї праці.

Ситуаційний підхід ґрунтується на тому, що пріоритетність методів управління визначається ситуацією. Через те що існує безліч факторів як у самій організації, так і у зовнішньому середовищі, не існує єдиного "кращого" методу управління. Щодо конкретної ситуації найефективнішим є той, що найбільш повно відповідає її суті.

Таким чином, серед розглянутих підходів найефективнішим в області управління інформаційною безпекою є процесний підхід, який реалізується в міжнародних стандартах і рекомендаціях.

Висновки до першого розділу.

Таким чином, проаналізувавши організаційно-правові вимоги до забезпечення інформаційної безпеки підприємства можна виділити кілька найпоширеніших вимог до системи управління інцидентами:

- Необхідний чіткий план дій в разі виникнення інциденту;
- Необхідна компетентна команда реагування на інциденти, з чітко визначеними ролями і обов’язками;
- Необхідна якісна обробка та розслідування інцидентів з метою не тільки усунення та мінімізації наслідків, а й подальшого уникнення подібних інцидентів.

Розглянуті в першому розділі основні характеристики та стандарти забезпечення інформаційної безпеки дають розуміння як мінімально повинна забезпечуватись організація управління інцидентами інформаційної безпеки, та дозволяють провести дослідження процесів організації управління інцидентами в

системі забезпечення інформаційної безпеки підприємства. Для цього необхідно проаналізувати методичні підходи, концепції та міжнародний досвід організації системи управління інцидентами інформаційної безпеки в системі забезпечення інформаційної безпеки підприємства.

Розділ 2
АНАЛІЗ ОРГАНІЗАЦІЇ УПРАВЛІННЯ ІНЦИДЕНТАМИ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

В даному розділі буде проаналізовано методичні підходи та міжнародний досвід організації управління інцидентами та її роль в системі забезпечення інформаційної безпеки підприємства.

2.1 Роль організації управління інцидентами в системі забезпечення інформаційної безпеки

Організація управління інцидентами в системі забезпечення інформаційної безпеки є одним з найважливіших етапів забезпечення інформаційної безпеки підприємства (рис. 2.1).

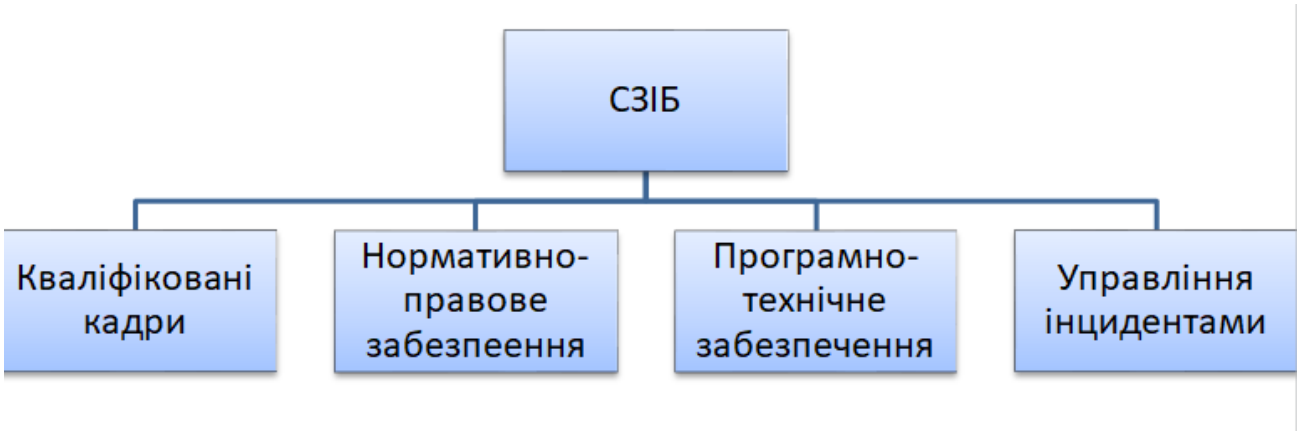

Рис. 2.1 Система забезпечення інформаційної безпеки підприємства

Управління інцидентами — це збірний термін, який охоплює всю діяльність протягом усього життєвого циклу інциденту; від планування, навчання та підвищення обізнаності, до виявлення, реагування та вивчення випадків. Можливість управління інцидентами включає політику управління подіями, план

та процедури, які повинні бути пристосовані до потреб конкретної організації. Крім того, важливим є планомірний підхід до повідомлення про вразливості, які ще не використані. Також існують настанови щодо встановлення пріоритетів інцидентів, а також їх оцінки для отримання досвіду від попередніх інцидентів. Управління інцидентами — це не суто проблема, пов’язана з ІТ, оскільки інциденти інформаційної безпеки загрожують організації в цілому.

Основною метою забезпечення інформаційної безпеки (ІБ) організації є зниження ризиків, які діють щодо інформаційних ресурсів, і в кінцевому рахунку запобігання або мінімізація шкоди від можливих інцидентів ІБ.

Останніми роками повідомляється про все більшу кількість інцидентів інформаційної безпеки. Кілька великих інцидентів привернули увагу ЗМІ та привернули увагу до цієї теми. Типові випадки включають як загальні, так і цільові атаки, спричинені шкідливим програмним забезпеченням, крім незначних помилок із серйозними наслідками. Незважаючи на те, що організації застосовують політику та засоби захисту інформації, неминуче періодично виникають нові уразливості та інциденти інформаційної безпеки. Неможна вважати, що всі інциденти можна запобігти. Це також економічно недоцільно. Отже, очевидно, що організаціям потрібні плани та процедури для обробки інцидентів, коли вони трапляються. Наявність у організації можливості реагування на інциденти може допомогти їм швидко виявити інциденти, мінімізувати втрати та руйнування, пом'якшити слабкі місця, які були використані, і відновити обчислювальні ресурси.

Як показано на рис.2.2 статистика у сфері інформаційної безпеки свідчить, що близько 80% зловмисників належить до інсайдерів [5]. На їх дії припадає близько 90% фінансових утрат. Людський фактор завжди був і є одним із найважливіших ризиків будь-якого бізнесу, оскільки більшість інцидентів відбуваються саме з вини співробітників.

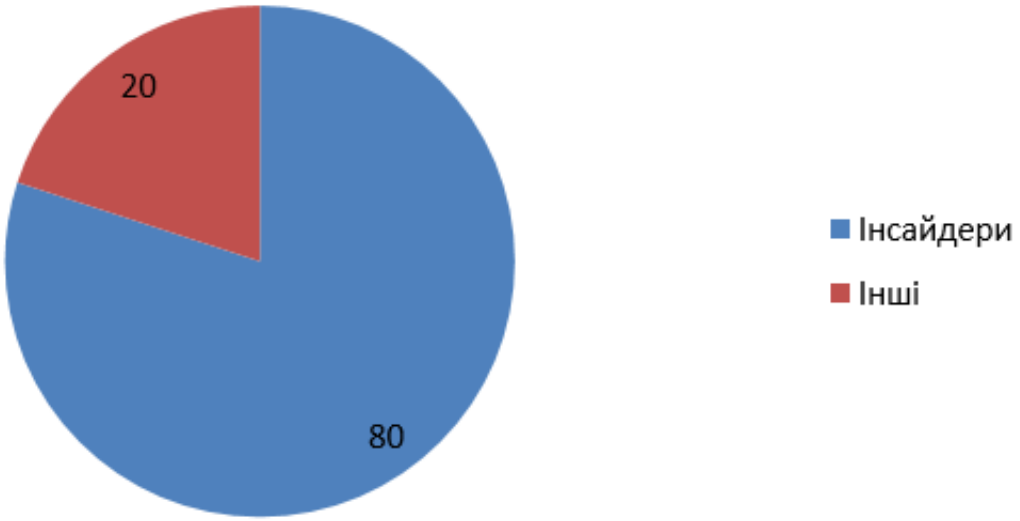

Рис. 2.2 Статистика причин інцидентів

Найбільш частими та небезпечними є ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи. Іноді такі помилки є загрозами (невірно введені дані, помилка в програмі, котра викликає колапс системи), іноді вони створюють ситуації, якими не лише можуть скористатися зловмисники, а які самі по собі становлять безпосередню небезпеку об'єкта.

За результатами проведених фахівцями з інформаційної безпеки досліджень, понад 65 % шкоди, яка завдається інформаційним ресурсам, є наслідком ненавмисних помилок [5]. Пожежі та землетруси, тобто інциденти природного характеру, трапляються набагато рідше. Саме тому, доцільним є акцентування уваги на більшому впровадженні комп'ютерних систем для забезпечення безпеки.

Наступними, за розміром шкоди, можна виділити крадіжки. У більшості випадків, суб'єктами вчинення даних дій були штатні працівники цих організацій, які є добре обізнаними у роботі інформаційної системи, а також заходів безпеки. У цьому аспекті дуже небезпечними є співробітники, які є незадоволеними або не поділяють цінностей тієї організації, де вони працюють.

У загальному плані діями ображених співробітників керує намагання нанести шкоду організації, в якій вони працювали, і яка, на їхню думку, їх образила. Така образа може знайти відображення у вчиненні наступних дій:

- пошкодження обладнання;
- вбудовування логічної бомби, яка з часом руйнує програми і дані;
- введення невірних даних;
- знищення даних;
- зміна даних;
- модифікація даних;
- надання доступу до даних із обмеженим доступом тощо.

Ображені співробітники обізнані з порядками в організації і здатні нашкодити вельми ефективно. Необхідно слідкувати за тим, щоб при звільненні співробітника його права доступу до інформаційних ресурсів були повністю обмежені, а після його звільнення змінені всі паролі доступу до внутрішньої мережі. Більш того, слід обмежити його спілкування із особами, які мають доступ до важливої інформації.

Окрім антропогенних, слід виділяти інциденти природного характеру. Інциденти природного характеру характеризуються великим спектром. По-перше, можна виділити порушення інфраструктури: аварії електроживлення, тимчасово відсутній зв'язок, перебої із водопостачанням тощо. Небезпечними також є стихійні лиха, землетруси, урагани, смерчі, бурани, тайфуни тощо. Загальна процентна кількість інформаційних загроз природного характеру за даними американських аналітиків становить приблизно 14 відсотків від загальної кількості.

Безперечно певну частку інцидентів становлять собою хакери, водночас їхня діяльність більше носить міфічний характер, а самі можливості хакерів є більше їхньою ж продукцією, яка лякає необізнаних. Насправді, щодня сервери органів державного управління підлягають атакам хакерів, водночас їхній

загальний коефіцієнт шкоди порівняно зі шкодами іншого характеру вельми маленький.

Таким чином, можна виділити основні та найпоширеніші інциденти інформаційної безпеки (табл. 2.1).

Таблиця 2.1

Види інцидентів

Види інцидентів	Опис
Відмова в обслуговуванні	Атаки типу DoS (denial of service, відмова в обслуговуванні) і DDoS (Distributed denial of service; розподілена відмова в обслуговуванні) - великі категорії інцидентів, які мають загальну спрямованість. Такого роду інциденти є причиною припинення роботи системи, служби або мережі в повному обсязі всіх можливостей, найчастіше з повною відмовою в доступі авторизованим користувачам.
Несанкціонований доступ	В цілому, ця категорія інцидентів складається зі спроб несанкціонованого доступу і використання системи, служби або мережі.

Продовження табл. 2.1

Впровадження шкідливого коду	Шкідливий код визначається як програма або частина програми, вбудована в іншу програму з метою зміни її початкової моделі поведінки, як правило, для виконання потенційно небезпечних видів діяльності, таких як крадіжка інформації та персональних даних, знищення інформації і ресурсів, DoS-атаки, спамінг та ін.
Зловживання	Інцидент подібного роду відбувається, коли користувач порушує політику безпеки інформаційної системи організації. Подібні інциденти не є атаками в строгому сенсі цього слова, але часто відображаються в звітах як інциденти і повинні управлятися ГРІБ
Зловживання	Інцидент подібного роду відбувається, коли користувач порушує політику безпеки інформаційної системи організації. Подібні інциденти не є атаками в строгому сенсі цього слова, але часто відображаються в звітах як інциденти і повинні управлятися ГРІБ

Продовження табл. 2.1

Збір інформації	У загальних рисах, категорія інцидентів збору інформації включає в себе види діяльності, пов'язані з виявленням потенційних цілей і розумінням принципу роботи служб, спрямованих на досягнення цих цілей
Соціальна інженерія	В загальному розумінні це злочинні психологічні маніпуляції над співробітниками компанії, з метою примушення виконання якихось дій.
Стихійні лиха	Природні явища, наслідками яких можуть бути перебої у живленні електромереж, виведення з ладу систем, втрата інформації і т.д.
Ненавмисні дії	Ненавмисні дії, як рядових співробітників компанії, так і системних адміністраторів, які призводять до втрати інформації, ресурсів, чи порушення нормальної роботи бізнесу

Кожен з основних видів інцидентів бувають як технічного так і нетехнічного характеру:

1. DOS атаки технічного характеру бувають двох видів: ліквідація джерела або зависання джерела.

Деякі типові приклади навмисних технічних інцидентів DoS і DDoS включають в себе:

- перевірку за допомогою пінг-запитів мережевої передачі з метою заповнення мережевого діапазону відповідним трафіком;
- відправку даних в невідомому форматі в систему, службу або мережу, з метою її виходу з ладу або переривання нормального функціонування;
- відкриття декількох санкціонованих сесій з конкретною;
- системою, службою або мережею, з метою вичерпання її ресурсів (тобто, уповільнення, закриття або збій).

Такі атаки часто здійснюються за допомогою ботів, керованих ботнетом — комп'ютерною мережею, яка запускає шкідливий код. Ботнет — це централізована командна і керуюча ботами мережу, регульована людьми. Ботнети можуть складатися з сотень і мільйонів заражених комп'ютерів.

Причинами інцидентів DoS нетехнічного характеру, що закінчуються втратою інформації, служби та / або матеріальних коштів, можуть бути:

- порушення заходів фізичної безпеки, що закінчуються крадіжкою, навмисним пошкодженням або виведенням з ладу обладнання;
- випадкові пошкодження апаратних засобів (і / або місць їх розташування) в результаті пожежі або повені;
- надзвичайні умови навколишнього середовища, наприклад, висока робоча температура (в результаті збою роботи кондиціонера);
- системні збої або перезавантаження;
- неконтрольовані зміни системи;
- збої програмного забезпечення або апаратних засобів.

2. Деякі приклади інцидентів несанкціонованого доступу технічного характеру включають в себе:
   - спроби відновити файли паролів;

- атаки переповнення буфера обміну для отримання привілейованого (наприклад, на рівні системного адміністратора) доступу до об'єкта;
- використання вразливостей протоколу для захоплення або перенаправлення санкціонованих підключень до мережі;
- спроби підвищення існуючого рівня привілеїв на доступ до ресурсів або інформації, якими на законних підставах володіє користувач або адміністратор.

Інциденти несанкціонованого доступу нетехнічного характеру, що виникають в результаті прямого або непрямого розкриття або модифікації інформації, порушень підзвітності або неправильного використання інформаційних систем, можуть бути викликані:

- порушеннями заходів фізичної безпеки в результаті несанкціонованого доступу до інформації;
- поганий і / або неправильно вибраний параметр конфігурації операційних систем через неконтрольовані системні зміни або збої програмного забезпечення або апаратних засобів.

3. Інциденти з впровадженням шкідливого коду бувають тільки технічного характеру. Вони можуть бути розділені на п'ять категорій: віруси, черв'яки, трояни, мобільні коди і змішані категорії. Спочатку віруси писалися для отримання вразливої зараженої системи, проте в даний час для виконання цільових атак використовуються і інші шкідливі коди. Іноді це відбувається шляхом зміни існуючого шкідливого коду і створення такого його різновиду, який часто не розпізнається технологіями виявлення шкідливого коду.
4. Зловживаннями можуть бути:
   - завантаження і установка засобів злому;
   - використання корпоративної електронної пошти для спамінг або просування особистого бізнесу;
   - використання корпоративних ресурсів для створення

- несанкціонованого веб-сайту;
- використання децентралізованої піринговой мережі для придбання або поширення піратських файлів (музика, відео, програмне забезпечення).

5. Збір інформації передбачає ознайомлення з інформацією, з метою визначення:
   - наявності мети і розуміння топології навколишнього її мережі, і того, з ким ціль регулярно взаємодіє;
   - потенційних вразливостей в цільовому середовищі або безпосередньо в мережевому середовищі, які можуть бути використані.

Типові приклади атак збору інформації технічного характеру включають в себе:

- скидання записів DNS (Domain Name System, система доменних імен) для цільового інтернет-домену (передача зон DNS);
- пінг-запити мережевих адрес для пошуку діючих систем;
- перевірку цільової системи для ідентифікації (наприклад, за допомогою відбитків пальців) хостингової операційної системи;
- сканування доступних мережевих портів системи з метою виявлення мережевих служб (наприклад, електронна пошта, протокол передачі файлів, веб-служби та ін.) і версій програмного забезпечення цих служб;
- сканування однієї або декількох відомих уразливих служб в діапазоні мережевих адрес (горизонтальне сканування).

6. Соціальна інженерія являє собою маніпулятивні дії психологічного характеру, метою яких є змусити співробітника компанії виконати якісь дії, необхідні зловмиснику. Це може бути як просто прохід на територію компанії так і отримання якоїсь конфіденційної інформації.
7. Стихійні лиха це також інциденти інформаційної безпеки. Вони можуть призвести, наприклад, як до перебоїв з живленням електроенергії, так і до

неможливості ключових співробітників виконувати свої обов’язки (прибути на роботу наприклад).

8. З технічної сторони ненавмисні дії співробітників можуть, наприклад, призвести до критичних помилок системи, чи до зараження мережі вірусом, або, наприклад, пожежа з нетехнічної сторони.

В більшості великих і середніх компаній створені підрозділи інформаційної безпеки, які планують і реалізують комплекс заходів щодо захисту своїх інформаційних ресурсів. Доброю практикою організації діяльності по захисту інформації є проходження моделі PDCA (Plan — плануй, Do — дій, Check — перевіряй, Act — впливай). На рис. 2.3 показані 4 взаємопов'язані процеси моделі PDCA: розробка, впровадження, моніторинг та розвиток.

Рис. 2.3 Модель PDCA

Всі чотири перерахованих процеси є критично важливими. Виняток або недостатня опрацьованість одного з них може істотно вплинути на захищеність інформаційних ресурсів компанії.

Управління інцидентами інформаційної безпеки — процес або набір процесів, на вхід яких подаються дані, отримані в результаті збору і

протоколювання даних про події, які зачіпають інформаційні системи, а на виході цих процесів отримують інформацію про причини інциденту, про збитки, завдані компанії, і заходи, які необхідно прийняти для того, щоб інцидент не повторився. Таким чином, організація управління комп'ютерними інцидентами направлено на вдосконалення підсистеми забезпечення безпеки компанії. Крім того, одержувані на виході дані є, по суті, єдиним об'єктивним свідченням у визначенні ймовірності реалізації загроз при аналізі ризиків.

У більшості організацій процес управління комп'ютерними інцидентами побудований таким чином (рис. 2.4):

- отримання інформації про інцидент;
- отримання додаткової інформації, пов'язаної з виявленими порушенням;
- аналіз ситуації, локалізація порушення і оперативне застосування контрзаходів;
- встановлення причин, за якими стало можливим те, що трапилося порушення і, може бути, визначення відповідальних осіб (розслідування);
- проведення профілактичних заходів, розробка і впровадження заходів по недопущенню повторного порушення.

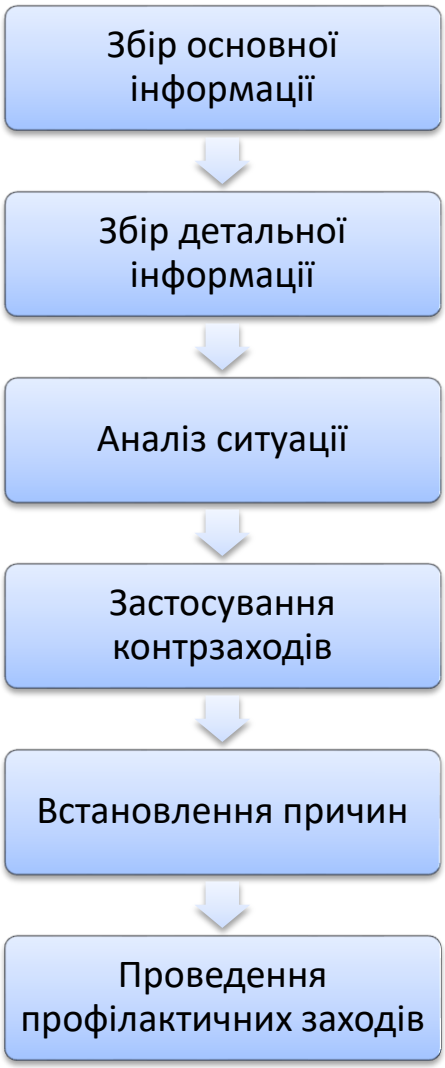

Рис. 2.4 Послідовність дій при управлінні інцидентами

Використовувані для виявлення інцидентів процедури збору інформації можуть забезпечуватися як технічними, так і організаційними заходами; наприклад, відповідно до вимог політики безпеки співробітник, який знайшов порушення, зобов'язаний повідомити про нього в підрозділ інформаційної безпеки. Потім інформація про виявлені інциденти фіксується в спеціальних журналах (в паперовому або електронному вигляді).

Результати аналізу, розслідувань і профілактичних заходів зазвичай оформляються у вигляді довідок, звітів і аналітичних записок і зберігаються в підрозділі ІБ. Однак якщо в компанії ефективно реалізована реєстрація подій, а її інформаційна інфраструктура характеризується значним розміром і територіально розподілена, то рано чи пізно настає момент, коли інформацію, пов'язану з

інцидентами і ходом їх розслідувань, стає важко обробляти без допомоги спеціального інструментарію. Ще проблематичніше стає підготовка і аналіз статистики по комп'ютерним інцидентів, в той час як ця статистика є одним з ключових показників ефективності діючої підсистеми безпеки компанії. Очевидно, що в результаті цього падає ефективність процесу управління інформаційними інцидентами, що в кінцевому рахунку негативно впливає на забезпечення ІБ компанії в цілому.

Яким же чином можна істотно підвищити ефективність процесу організації управління комп'ютерними інцидентами? Перш за все необхідно визначити показники ефективності. Ефективність процесу організації управління інцидентами залежить від:

- координації та узгодженості дій всіх залучених в нього осіб;
- наявних можливостей щодо отримання та аналізу інформації, пов'язаної з інцидентом;
- оперативності та коректності отриманих результатів.

Підвищення кожного з перерахованих показників помітно підніме ефективність всього процесу організації управління інцидентами і тим самим дозволить підрозділу інформаційної безпеки домогтися більш значних результатів.

Радикально змінити ситуацію з організації управління інцидентами можна, використовуючи систему управління інформаційними інцидентами. Ця система дозволить:

- консолідувати всю інформацію про комп'ютерні інциденти в єдиному сховищі;
- створити єдиний центр управління інцидентами ІБ з метою забезпечення контролю і координації дій по локалізації та розслідувань;
- підвищити швидкість реагування і оперативність виявлення причин інциденту;

- підвищити достовірність отриманих результатів з виявлення причин інциденту, відповідальних осіб і визначенням необхідних дій, усунення наслідків інциденту і застосування контрзаходів;
- формувати статистику по інцидентах ІБ, виявляти тенденції її зміни і аналізувати динаміку цих змін;
- автоматизувати застосування контрзаходів для зниження ризику ІБ при виявленні типових інцидентів.

Таким чином, більшість інцидентів відбуваються з провини співробітників компанії. Система управління інцидентами ІБ фактично буде системою, яка об’єднає процеси з управління інцидентами ІБ, за допомогою інтеграції людей і апаратно-програмного забезпечення моніторингу та захисту, а також інформаційної інфраструктури організації. Гарним рішенням буде впровадження єдиної ефективної системи управління інцидентами, для цього необхідно дослідити методичні підходи до її впровадження.

2.2 Методичні підходи до організації управління інцидентами в системі забезпечення інформаційної безпеки підприємства

Сучасна система забезпечення інформаційної безпеки підприємства — це комплекс заходів за засобів, спрямованих на захист та забезпечення безперебійної роботи всієї інформаційної інфраструктури компанії. Вона включає в себе нормативно-правове забезпечення, організаційні методи, загальну політику інформаційної безпеки, політику реагування на інциденти ІБ, систему управління інцидентами ІБ, програмні і технічні засоби забезпечення захисту інформації, програмно-апаратне забезпечення управління інцидентами інформаційної безпеки.

Відповідно до найкращих світових практик можна сформулювати методику організації управління інцидентами інформаційної безпеки, використовуючи яку організація забезпечить ефективну політику реагування на інциденти інформаційної безпеки. Можна представити систему управління інцидентами інформаційної безпеки у вигляді схеми (рис. 2.5)

Рис 2.5 Схема системи управління інцидентами інформаційної безпеки

Виходячи з цього, процес організації управління інцидентами інформаційної безпеки повинен включати в себе наступні дії:

- розробка нормативно-правового забезпечення (процедури, політики і т.д.);
- виділення та навчання кваліфікованих кадрів;
- вибір та впровадження систем моніторингу подій інформаційної безпеки;
- розробка системи розслідування інцидентів;

– впровадження інтелектуальної системи обробки та обліку всіх інцидентів ІБ.

Алгоритм дій керівництва щодо організації процесів управління інцидентами інформаційної безпеки можна представити у вигляді схеми (рис. 2.6).

Рис. 2.6 Алгоритм дій керівництва щодо організації процесів управління інцидентами інформаційної безпеки

Розробляючи політики та процедури управління інцидентами ІБ керівництво організації повинно сприяти створенню необхідних умов для їх впровадження всередині організації, а саме:

– створення формалізованої політики реагування на інциденти;
– розробці процедур обробки інцидентів;

- врегулювання юридичних аспектів обігу інформації в процесі розслідування;
- налагодженню внутрішніх організаційних контактів команди з розслідування інцидентів з профільними фахівцями (юристи, кадри, служба сприяння бізнесу, інформаційна безпека і т.д.)
- визначенню зон відповідальності команди розслідування, навчання і технічного оснащення команди розслідування.

Політика в сфері реагування на інциденти інформаційної безпеки розробляється з урахуванням специфіки організації, профілю її діяльності. Разом з тим, існують обов'язкові елементи політики, що не залежать від того чи є організація закритого (банки, держустанови, і т.д.) або публічного (ЗМІ, рекламні агентства, і т.д.) типу. До даних елементів відносяться:

- розуміння керівництвом організації необхідності реагування на інциденти інформаційної безпеки;
- управління процедурою розслідування інцидентів інформаційної безпеки;
- визначення цілей і місця політики розслідування інцидентів в загальній структурі процесів управління безпекою та організацією в цілому (політика розслідування інцидентів є частиною процесу забезпечення безперервності функціонування організації);
- визначення понять "інцидент інформаційної безпеки" і "наслідки інциденту інформаційної безпеки" в контексті сфери діяльності організації;
- опис складу, структури, функціональних обов'язків, зон відповідальності, ролей, правил внутрішньої організації взаємодії, порядку зовнішніх відносин команди з розслідування інцидентів інформаційної безпеки;
- порядок встановлення пріоритетів інцидентів і оцінки серйозності наслідків інцидентів інформаційної безпеки;
- оцінка критеріїв якості роботи команди з розслідування інцидентів;
- розробка форм звітності та регламенту сповіщень про інцидент;

- розробка набору процедур, що описують дію співробітників організації в разі інциденту інформаційної безпеки (виділений телефон, адреса електронної пошти);
- розробка стандартних операційних процедур (SOPs — Standard Operating Procedures), докладно описують дії співробітників команди реагування в процесі обробки інциденту інформаційної безпеки;
- порядок перегляду, тестування та актуалізації стандартних операційних процедур.

Скорочення інцидентів інформаційної безпеки шляхом ефективного використання сучасних засобів захисту мереж, комп'ютерних систем, програмного забезпечення і додатків повинно враховувати, що:

- превентивні заходи (запобігання проблем до настання події інциденту) є менш дорогими, ніж роботи по ліквідації наслідків інцидентів, отже, превентивні заходи є невід'ємною частиною політики реагування на інциденти інформаційної безпеки;
- процедура реагування на інциденти і розслідування за фактом їх події буде більш ефективною, якщо певним видам інформаційних ресурсів будуть поставлені у відповідність адекватні засоби технічного захисту інформації.

Всі процеси управління інцидентами інформаційної безпеки повинні бути детально описані і задокументовані.

Всі події інформаційної безпеки повинні бути формалізовані згідно з принципами пріоритетності. Дієвою методикою є використання принципу пріоритетності інцидентів інформаційної безпеки, заснованого на визначенні ступеня критичності розглянутого ресурсу і ступеня критичності впливу на аналізований ресурс, тобто, так званий, ефект інциденту. Важливо, також, враховувати популярність ресурсу, тобто наскільки ресурс затребуваний. Подібні припущення повинні бути оформлені у вигляді методики, і увійти, як складова частина, в формалізовану політику розслідування інцидентів інформаційної

безпеки. Зручною формою подання подібної методики є уявлення припущень про критичність активів в матричній формі:

- дії команди з розслідування інцидентів повинні бути формалізовані і представлені у вигляді Угоди про рівень обслуговування (SLA — Service Level Agreement), де докладно визначаються дії кожного співробітника і час реакції на певні події.

Крім того, дієвою методикою є аналіз інцидентів та обробка результатів з метою отримання практичного досвіду:

- після обробки інциденту, результати розслідування повинні бути задокументовані і внесені в базу даних інцидентів інформаційної безпеки. Завершення розслідування повинно супроводжуватися спільним обговоренням його результатів з усіма залученими і зацікавленими сторонами. Команда розслідування інцидентів повинна зробити відповідні висновки про уразливість, класифікувати їх і вжити заходів до недопущення в подальшому інцидентів подібного виду. Гарною практикою є проведення подібних обговорень на регулярній основі;
- розуміння причинно-наслідкових зв'язків в процесі розслідування складних інцидентів;
- до розслідування складних інцидентів залучаються фахівці з різних підрозділів організації, вирішальним фактором проведення успішного розслідування складного інциденту є консолідація дій співробітників і впровадження практики рольового управління розслідуванням.

Можливим є використання зовнішніх експертів для реагування та усунення наслідків інцидентів. Але будь-яка організація повинна мати у своєму штаті мінімум двох фахівців, здатних забезпечити працездатність системи в процесі обробки інциденту. Даний персонал покликаний здійснювати зв'язок з постачальником послуг, оцінювати якість їх роботи, знати систему і бути здатним відновити в короткий термін її працездатність.

Від компетентності фахівців підтримки залежить працездатність процедури обробки інцидентів в організації. Гарною якістю є комунікабельність, оскільки розслідування інциденту пов'язано зі спілкуванням з персоналом, в тому числі, керівництвом організації.

Для підтримки процедури обробки інцидентів інформаційної безпеки організація повинна проводити таку політику щодо команди реагування на інциденти:

- фінансування процедури обробки інцидентів;
- навчання співробітників профілюючих і суміжних дисциплін, зокрема юридичним аспектам діяльності команди реагування;
- залучення фахівців до процесу навчання співробітників, написання нормативної та технічної документації;
- штат команди повинен бути повністю укомплектований, повинен дотримуватися принцип сегрегації обов'язків;
- повинна підтримуватися практика ротації персоналу;
- перманентне залучення до процесу експертів з профілюючих областям діяльності з метою підняття рівня компетенції співробітників;
- проведення тренінгів та тестування сценаріїв обробки інцидентів;
- залучення до процесу розслідування інцидентів фахівців інших підрозділів: управління, інформаційна безпека, телекомунікації, IT підтримка, юристи, відділ зі зв'язків з громадськістю та ЗМІ, відділ по роботі з персоналом, відділ планування безперервності функціонування організації, служба сприяння бізнесу і т.д.

Процедура реагування на інциденти інформаційної безпеки складається з кількох фаз, починаючи з навчання персоналу і збору необхідного інструментарію, до виходу з інциденту (завершення розслідування і усунення наслідків). У процесі підготовки організація повинна прагнути обмежити потенційне число підозрілих подій, налаштовуючи систему кореляції і ретельно опрацьовуючи процедури ходіння інформації всередині організації та зовні. В

процесі підготовки, організація оцінює ризики інформаційної безпеки. Гарною практикою є впровадження Системи Менеджменту Інформаційної Безпекою (СМІБ), яка суттєво полегшить процес обробки інцидентів. Розслідування інциденту завершується процедурою оцінки залишкових ризиків та отримання практичної користі для подальшої роботи.

Для впровадження процедури реагування на інциденти інформаційної безпеки в структуру допоміжних процесів, що забезпечують супровід і підтримку процесу управління організації, потрібно переглянути підхід до проблеми забезпечення інформаційної безпеки в рамках організації, заручившись відповідною підтримкою керівництва.

Після виявлення, аналізу та класифікації інциденту, важливим етапом є процедура протидії його поширенню. Дії з протидії поширенню в чому залежать від того, наскільки якісно команда розслідування відпрацювала попередні етапи життєвого циклу процесу розслідування. Взаємодія підрозділів організації, правильна класифікація і глибина аналізу можливих наслідків, відіграють вирішальну роль і істотного скорочують час реагування. Кращою практикою підготовки до протидії поширення інциденту є заздалегідь підготовлений сценарій дій, проведений аналіз ризиків і класифіковані події по кожному основному класу інцидентів.

Процедура протидії поширенню інциденту будується окремо для кожного конкретного інциденту і залежить від його типу. Критерії стратегії протидії повинні бути формалізовані і доступні для всіх учасників команди реагування. Критерії визначення стратегії включають такі основні позиції:

- потенційне можливе пошкодження або крадіжка активу;
- потреба в безпеці даних інциденту;
- доступність активу;
- кількість часу і необхідні ресурси для реалізації протидії;
- ефективність стратегії протидії (часткове або повне вирішення проблеми);
- термін дії стратегії (тиждень, місяць, квартал, і т.д.).

У ряді випадків, для вивчення зловмисника і збору необхідних свідчень інциденту може бути застосована стратегія відкладеного (контрольованого) стримування, суть якої полягає у виявленні, аналізі, класифікації та контролі (стеження) за діями порушника. Дана методика, має нарівні з високим ступенем ефективності, високий рівень ризику, оскільки зловмисник може використовувати дискредитований ресурс як майданчик для атаки на інші активи організації. Контрольоване стримування можливо за умови наявності в організації висококваліфікованих експертів команди реагування і пропрацювала політики реагування на інциденти інформаційної безпеки.

Збір даних інциденту інформаційної безпеки є процедурою збору фактів зловмисних дій з метою завдати шкоди організації або окремим співробітникам. Причини, за якими необхідний збір свідчень, розглядаються як отримання законних підстав для притягнення до відповідальності особи або групи осіб за умисне або ненавмисну дію або спробу дії, спрямовану на нанесення шкоди організації, збір фактів для залучення осіб, які вчинили діяння, до відповідальності. Інша причина — формування пакету для аналізу уразливості і ліквідації наслідків інциденту інформаційної безпеки. Реєстраційні дані інциденту повинні містити наступні основні позиції:

- ідентифікація джерела (місце розташування, ID, ім'я хоста, MAC — address, IP — address, і.т.д.);
- персональні дані співробітників, які зверталися за допомогою;
- дата і час кожної події;
- місце розташування ресурсу зберігання даних.

Процедура збору даних інциденту інформаційної безпеки повинна бути представлена у вигляді внутрішнього регламенту і доведена до відома всіх учасників команди реагування і фахівців підрозділів, що залучаються до процедури розслідування інцидентів.

Процедура ліквідації наслідків інциденту інформаційної безпеки повинна бути оформлена у вигляді внутрішнього регламенту і безпосередньо залежить від

особливості функціонування інформаційної системи організації і способу атаки, який був застосований зловмисником. Дії персоналу в процесі ліквідації наслідків інциденту повинні бути узгоджені як з технічними фахівцями, які здійснюють підтримку системи, так і керівниками підрозділів, чия інформація стала об'єктом зловмисника.

На практиці, не існує універсальної методики, яка б однозначно визначала набір ефективних дій команди реагування при ліквідації наслідків інцидентів. Масштаби відновлення можуть бути різні, від лікування заражених вірусом файлів і відновлення операційного середовища з резервних копій, до відстоювання репутації організації в суді. Кращою практикою, на сьогоднішній день, є наявність в організації плану по відновленню функціонування бізнесу, підтримуваного постійно діючим колегіальним органом управління.

Вся інформація, яка була зібрана в процесі обробки і розслідування інциденту повинна бути структурована, проаналізована і збережена в спеціально створених і підтримуваних базах даних.

Таким чином, на основі розглянутих методичних підходів до організації управління інцидентами інформаційної безпеки необхідно проаналізувати міжнародний досвід останніх років в цій сфері.

2.3 Міжнародний досвід організації управління інцидентами в системах управління підприємств

Кожного дня організації по всьому світу стикаються з безліччю різних інцидентів інформаційної безпеки. Більшість з них не несуть великої загрози підприємству. Але все частіше трапляються випадки, коли наслідки інциденту несуть величезні матеріальні і репутаційні втрати не тільки для якоїсь однієї

організації, а й для великої кількості її клієнтів і партнерів, серед яких часто опиняються не тільки якісь гіганти IT сфери, а й цілі країни.

За останні роки найбільш поширеними типами атак є (рис. 2.7):

– використання шкідливого ПЗ;
– фішинг;
– атака через посередника;
– відмова в обслуговуванні;
– впровадження SQL-коду;
– експлойт нульового дня;
– інсайдерські атаки;
– APT атаки.

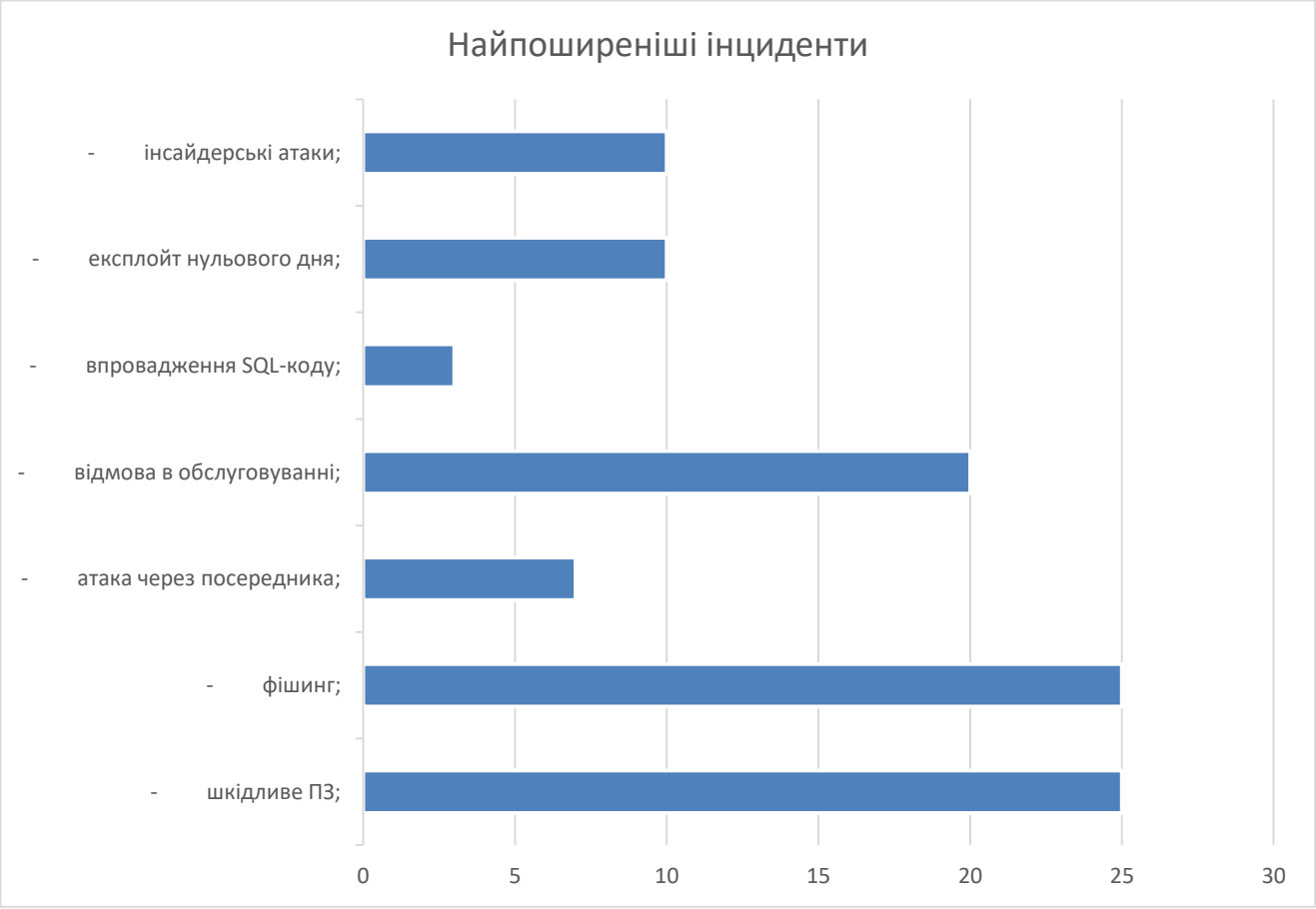

Рис. 2.7 Найпоширеніші типи атак за 2019 рік [24]

Термін «шкідливе ПЗ» вживається, коли мова йде про шпигунське ПЗ, програми-вимагачі, віруси і інтернет-хробаки. Шкідливе ПЗ проникає в мережу

через вразливість, як правило, коли користувач переходить по небезпечній посиланням або відкриває вкладення в електронній пошті, що призводить до встановлення такого ПЗ. Опинившись всередині системи, шкідливе ПЗ може:

- блокувати доступ до ключових компонентів мережі (віруси-вимагачі);
- встановлювати шкідливі програми або додаткове шкідливе ПЗ;
- приховано збирати дані з жорсткого диска і відправляти їх зловмисникові (шпигунське ПЗ);
- порушувати роботу деяких компонентів і виводити систему з ладу.

Фішинг — це розсилка, як правило, по електронній пошті, шахрайських повідомлень, які виглядають так, ніби вони відправлені надійним адресатом. Метою цієї діяльності є крадіжка конфіденційних даних, наприклад про кредитні картки або облікових записах, або встановлення зловмисного програмного забезпечення на комп'ютері жертви. Фішинг стає все більш поширеною кіберзагрозою.

Атаки через посередника (MitM) виникають, коли хакери впроваджуються у взаємодію двох сторін. Отримавши доступ до трафіку, хакери можуть фільтрувати і красти дані.

Атака типу «відмова в обслуговуванні» переповнює системи, сервери або мережі трафіком, що призводить до вичерпання ресурсів і пропускної здатності. В результаті система втрачає здатність виконувати нормальні запити. Хакери також можуть використовувати скомпрометовані пристрої для організації атак. Це називається розподіленою атакою типу «відмова в обслуговуванні» (DDoS-атака).

SQL ін'єкція — це передача шкідливого SQL-коду на сервер, що обробляє SQL-запити, в результаті чого сервер розкриває дані, що не передбачалося розкривати. Щоб впровадити SQL-код, іноді досить ввести шкідливий код в поле пошуку уразливого веб-сайту.

Експлойт нульового дня виникає після розкриття уразливості мережі і до створення виправлення або вирішення цієї проблеми. У цей часовий інтервал

хакери атакують з використанням відкритої уразливості. Для виявлення загроз, пов'язаних з уразливістю нульового дня, потрібен постійний моніторинг.

Інсайдерські інциденти виникають через умисні або ненавмисні випадкові дії зі сторони співробітників компанії.

APT атаки — це добре організована, ретельно спланована кібератака, яка спрямована на конкретну компанію або цілу галузь. За APT-атакою, як правило, стоять злочинні угруповання, які мають значні фінансові ресурси і технічні можливості.

Пандемія коронавірусної інфекції також вплинула на кіберзлочинність. Зловмисники намагаються використовувати і звернути її в свою користь, так само як і будь-який інший гучний інфопривід. Поширення коронавірусной хвороби COVID-19 вплинуло на зростання кіберзлочинності і на весь IT-світ.

Про різке зростання кількості інцидентів ІБ дослідники говорять вже кілька місяців. Спеціалісти з нформаційної безпеки заявляють, що число інцидентів збільшилося на 20-25% з приходом пандемії COVID-19 [38]. Це пояснюється тим, що в період пандемії люди почали тісніше спілкуватися з цифровим простором. Наприклад, студентів і учнів перевели на дистанційне навчання, організації та підприємства швидко розгортають віддалені системи і мережі для підтримки співробітників, що працюють з дому, з'являється все більше нових сервісів з доставки їжі і т. д. Злочинці ж використовують підвищену вразливість систем безпеки в мінливих умовах, щоб викрасти дані, отримувати прибуток і порушувати нормальну роботу сервісів. У березні 2020 року, наприклад, фахівці фіксували 2500 інцидентів за добу.

Зловмисники почали використовувати новий інфопривід, у вигляді COVID-19, у своїх фішингових атаках. Тепер вони використовують тему Covid-19 у своїх фішингових розсилках, часто видаючи себе за органи охорони здоров’я. Була, наприклад, серія фішингових атак, імітуючих листи від Всесвітньої організації охорони здоров’я, з метою переконати людей, стурбованих вірусом, зробити

потрібні зловмисникам дії. Сама ВООЗ піддалася кібератакам, спрямованим на її персонал і системи.

Злочинці також використовували COVID-19 для шахрайства з підприємствами та державними установами. Компанії, які дозволяють екстрені транзакції, були атаковані за допомогою методу BEC (Business Email Compromise, компрометація корпоративних ящиків електронної пошти). Одна французька фармацевтична фірма відправила 7,25 мільйона доларів США фальшивому постачальнику, який стверджував, що він продає дезінфікуючий засіб для рук і захисні маски [38]. В інших випадках кіберзлочинці застосовували вкрадені персональні дані для подачі шахрайських заяв на допомогу з безробіття в США і інших країнах.

Кіберзлочинці все частіше використовують шкідливі програми проти критично важливих об'єктів інфраструктури та медичних установ — через величини потенційного впливу і можливої фінансової вигоди. У перші два тижні квітня 2020 року спостерігався сплеск кількості інцидентів з використанням програм-вимагачів з боку декількох хакерських угруповань, які протягом кількох попередніх місяців були відносно неактивні.

Сектор охорони здоров'я виявився особливо вразливим для кібератак в силу своєї критичної важливості (адже представники цієї сфери борються за лікування пацієнтів з COVID-19 і женуться за розробкою успішної вакцини) і специфічних особливостей того, як в ньому застосовуються інформаційні технології. Хоча деякі злочинні групи пообіцяли утриматися від атак на лікарні та медичні установи під час пандемії, сімейство шифрувальників Maze, наприклад, було націлене на Hammersmith Medicines Research — фірму, яка проводить клінічні випробування ліків і вакцин. В рамках іншої кампанії, описаної експертами Check Point, зловмисники видавали себе за представників фармацевтичних підприємств з метою поширення програм-вимагачів в Італії.

Поширення шкідливих засобів збору даних, таких як програми для віддаленого доступу або крадіжки інформації, шпигунські програми та банківські

«трояни», також зростає. Використовуючи пов'язані з COVID-19 відомості в якості приманки, зловмисники проникають в інформаційні системи, щоб зламати мережі, вкрасти дані або гроші, створити ботнети.

Скориставшись підвищеним попитом на медичне приладдя та інформацію про COVID-19, кіберзлочинці почали реєструвати доменні імена, що містять такі ключові слова, як «коронавірус», «COVID» і т. д. Ці шахрайські веб-сайти служать основою для самих різних кіберзлочинних дій, включаючи управління ботнетами (C2C), поширення шкідливих програм і фішинг. З лютого по березень 2020 року партнер Інтерполу з приватного сектора виявив помітне зростання числа зловмисних реєстрацій: по шкідливим програмам — на 569 відсотків, по фішингу — на 788 відсотків, про що і повідомив прес-секретар міжнародної поліції [37].

З введенням політики соціального дистанціювання і карантину багато організацій змушені були перевести співробітників на віддалену роботу. Але, звичайно ж, цей перехід дав кіберзлочинцям ще одну область для шкідливої активності. Використовуючи додатки для віртуальних зустрічей і відеодзвінків, багато хакерів намагалися зірвати збори в Zoom і на інших платформах. Інші створювали підроблені домени, шкідливі програми і служби для спуфінга (імітації) в рамках фішингових кампаній, спрямованих проти користувачів того ж Zoom або Microsoft Teams.

Що ще більш тривожно, хакери побачили привабливу мету в активізації використання VPN-з'єднань і засобів віддаленого управління. Оскільки організації поспішили впровадити протокол віддаленого робочого стола Microsoft (RDP), належні вимоги безпеки не завжди дотримувалися, що зробило облікові записи RDP уразливими. Кіберзлочинці за допомогою атак методом перебору намагаються отримати реєстраційні дані користувачів таких акаунтів. У разі успіху вони можуть отримати доступ до серверів та інших важливих систем і навіть взяти під контроль мережу.

Внаслідок нових проблем, що виникли, було випущено безліч рішень в області інформаційної безпеки і міжнародних / державних рекомендацій. Як приклад можна привести керівництво NIST «Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security».

В останні кілька років парадигма забезпечення інформаційної безпеки почала змінюватися і все більше компаній приходять до розуміння, що побудова захисту, яку не можна зламати, — утопічна за своєю суттю. Левова частка систем або вже зламана, або може виявитися зламаною, і головне завдання будь-якої системи безпеки — максимально швидко виявити інцидент і джерело інциденту в системі, скоротити можливості настільки, щоб він не встиг завдати непоправної шкоди. У зв'язку з цим спостерігається зростання затребуваності високоінтелектуальних засобів захисту, що дозволяють вирішувати завдання по своєчасному виявленню атак і інцидентів. Зокрема, мова йде про системи класу security information and event management (SIEM), network traffic analysis (NTA) та комплексних анти-APT рішеннях.

Як зазначають спеціалісти «Positive technologies» в 2019 році кількість APT-атак і злочинних угрупувань, які займаються цими атаками, сильно зросла (рис. 2.8). Ріст цілеспрямованих атак стабільно швидкий, внаслідок чого за результатами досліджень кількість APT-атак перевищує кількість масових. Кількість цілеспрямованих атак зросла з 59% у першому кварталі 2019 року, до 65% у третьому.

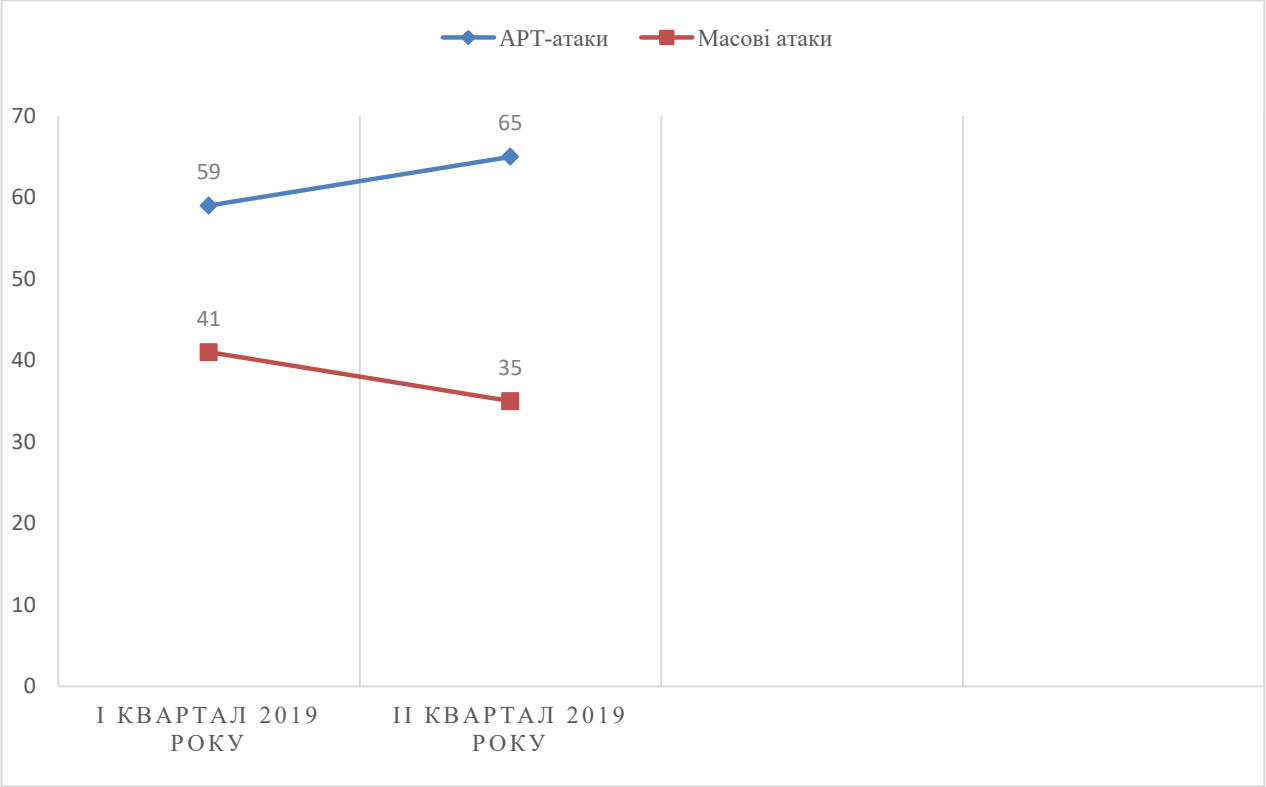

Рис. 2.8 Збільшення кількості APT-атак у 2019 році [34]

Організації рік за роком беруть на озброєння все більш ефективні методи захисту, тому масові атаки просто перестають працювати. Така тенденція з великою ймовірністю збережеться і в майбутньому.

Якщо ж говорити про таргетовані атаки, то ситуація інша: середня швидкість реакції великих компаній на сучасні загрози — близько трьох років. Тобто з моменту усвідомлення необхідності покупки рішення щодо виявлення інциденту і протидії зловмисникам до його реального застосування в компаніях проходить близько трьох років, присвячених бюджетування, тендерів, пілотним впровадженням, закупівлю, впровадження, навчання та ін.

При цьому зловмисники активно використовують новітні вразливості (в 2019 році APT-угруповання використовували в своїх атаках чотири вразливості нульового дня), діють дуже швидко, а головне — часто змінюють свій інструментарій і тактики. Наприклад, угруповання RTM протягом року використовувало три різні способи отримання інформації про контрольні сервери: через namecoin, через Tor, через bitcoin [32]. Разом з тим в 2019 році було три різні

версії дроппера (установщика основного модуля ШПЗ), одну версію завантажувача і три різних версій трояна.

У зв’язку з швидким розвитком нових видів інцидентів, організації вимушені використовувати максимально ефективні системи як для моніторингу систем так і для швидкого реагування на інциденти (IDS та IPS системи). Найбільш поширеними системами виявлення і реагування на інциденти є [19]:

- IBM Security Network Intrusion Prevention System;
- Suricata;
- McAfee Network Security Platform;
- StoneGate Intrusion Prevention System;
- Samhain;

А також із відкритим кодом:

- Zabbix;
- Wazuh.

IBM Security Network Intrusion Prevention System — система запобігання інцидентів, розроблена IBM, використовує запатентовану технологію аналізу протоколів, яка забезпечує превентивний захист в тому числі і від 0day-загроз. Як і у всіх продуктів серії IBM Security, його основою є модуль аналізу протоколів — PAM (Protocol Analysis Module), що поєднує в собі традиційний сигнатурний метод виявлення інцидентів (Proventia OpenSignature) і поведінковий аналізатор. При цьому PAM розрізняє 218 протоколів програм (атаки через VoIP, RPC, HTTP і т. д.). І такі формати даних, як DOC, XLS, PDF, ANI, JPG, щоб передбачати, куди може бути впроваджений шкідливий код. Для аналізу трафіку використовується більше 3000 алгоритмів, 200 з них «відловлюють» DoS. Функції брандмауера дозволяють дозволити доступ тільки по певних портів і IP, виключаючи необхідність залучення додаткового пристрою. Технологія Virtual Patch блокує віруси на етапі поширення і захищає комп'ютери до установки оновлення, що усуває критичну вразливість. При необхідності адміністратор сам може створити і використовувати сигнатуру. Модуль контролю додатків дозволяє управляти P2P,

IM, ActiveX-елементами, засобами VPN і т.д. І при необхідності блокувати їх. Реалізовано модуль DLP, що відслідковує спроби передачі конфіденційної інформації та переміщення даних в мережі, що захищається, що дозволяє оцінювати ризики і блокувати витік. За замовчуванням розпізнається вісім типів даних (номери кредиток, телефони ...), решту специфічну для організації інформацію адмін задає самостійно за допомогою регулярних виразів. В даний час велика частина вразливостей доводиться на веб-додатки, тому в продукт IBM входить спеціальний модуль Web Application Security, який захищає системи від поширених видів інцидентів: SQL injection, LDAP injection, XSS, JSON hijacking, PHP file-includers, CSRF і т. д.

Передбачено кілька варіантів дій при виявленні інциденту — блокування хоста, відправлення попередження, запис трафіку (в файл, сумісний з tcpdump), приміщення вузла в карантин, виконання настроюється користувачем дії і деякі інші. Політики прописуються аж до кожного порту, IP-адреси або зони VLAN. Режим High Availability гарантує, що в разі виходу з ладу одного з декількох пристроїв IPS, наявних в мережі, трафік піде через інше, а встановлені з'єднання не урвуться. Всі підсистеми всередині залізяки — RAID, блок живлення, вентилятор охолодження — дубльовані. Налаштування, що виробляється за допомогою веб-консолі, максимально проста (курси навчання тривають всього один день). При наявності декількох пристроїв зазвичай отримується IBM Security SiteProtector, який забезпечує централізоване управління, виконує аналіз логів і створює звіти.

Передбачено кілька варіантів дій при виявленні інциденту — блокування хоста, відправлення попередження, запис трафіку (в файл, сумісний з tcpdump), приміщення вузла в карантин, виконання настроюється користувачем дії і деякі інші. Політики прописуються аж до кожного порту, IP-адреси або зони VLAN. Режим High Availability гарантує, що в разі виходу з ладу одного з декількох пристроїв IPS, наявних в мережі, трафік піде через інше, а встановлені з'єднання не урвуться.

Stonegate IPS

В основі роботи StoneGate IPS закладена функціональність виявлення і запобігання вторгнень, яка використовує різні методи виявлення вторгнень: сигнатурний аналіз, технологія декодування протоколів для виявлення вторгнень, що не мають сигнатур, аналіз аномалій протоколів, аналіз поведінки конкретних хостів, виявлення будь-яких видів сканування мереж, адаптивне застосування сигнатур (віртуальне профілювання). StoneGate IPS надає величезну кількість можливостей по налаштуванню і управлінню. Володіючи найсучаснішими можливостями з управління політиками виявлення вторгнень, система дозволяє складати карти мережі і проводити аналіз мережевої активності в наочному вигляді. Зручна централізована система управління дозволяє управляти величезною кількістю сенсорів одному адміністратору. Система безпечних оновлень дозволяє централізовано керувати оновленнями ПЗ і сигнатур, і в разі невдалого оновлення повернутися до попередньої успішно працювала версії ПЗ.

Zabbix — опенсорсне повністю безкоштовне рішення, яке підходить як для великого бізнесу так і для малих компаній. Підходить для всіх платформ і систем. Основні можливості:

- Розподілений моніторинг аж до 1000 вузлів. Конфігурація молодших вузлів повністю контролюється старшими вузлами, розташованих на вищому рівні ієрархії;
- Сценарії на основі моніторингу;
- Автоматичне виявлення;
- Централізований моніторинг лог-файлів;
- Веб-інтерфейс для адміністрування і налаштування;
- Звітність і тенденції;
- SLA моніторинг;
- Підтримка високопродуктивних агентів (zabbix-agent) практично для всіх платформ;
- Комплексна реакція на події;

- Підтримка SNMP пасток;
- Розширення за рахунок виконання зовнішніх скриптів;
- Гнучка система шаблонів і груп;
- Автоматичне виявлення за діапазоном IP-адрес, доступним сервісам і SNMP перевірка;
- Автоматичний моніторинг виявлених пристроїв;
- Автоматичне видалення відсутніх хостів;
- Розподіл за групами та шаблонами в залежності від повернутого результату;
- виявлення файлових систем;
- виявлення мережевих інтерфейсів.

Таким чином, за останній час не тільки збільшилась кількість інцидентів а і їх тип. Збільшилась кількість цілеспрямованих атак, що вимушує організації збільшувати витрати та підходи до забезпечення ефективного управління інцидентами інформаційної безпеки.

2.4 Концепція та структура автоматизованої системи управління інцидентами інформаційної безпеки

Організація процесу обробки подій без використання засобів автоматизації являє собою складну і трудомістку задачу [31]. Необхідно збирати і консолідувати велику кількість даних в різних форматах, вести центральний архів. Для ручної обробки подій потрібна велика кількість висококваліфікованих фахівців-аналітиків. В силу великого обсягу рутинної ручної роботи обробка подій часто буває неповною, яка не відбиває всю повноту поточної ситуації. При цьому можлива ситуація, коли події, критичні для надійного і захищеного функціонування бізнес-систем, виявляться поза увагою аналітиків, і щодо них не будуть прийняті відповідні превентивні заходи.

Процес управління інцидентами — найважливіший аспект комплексної СУІБ організації. Організувати цей процес без використання засобів автоматизації представляється важко розв'язуваним завданням, особливо, в великих інформаційних системах, в яких, постійно відбувається величезна кількість подій, оскільки, необхідно збирати і консолідувати велику кількість даних. В силу великого обсягу ручної роботи і відомого людського фактора обробка інцидентів найчастіше може бути неповною, і не відображати всю повноту і критичність ситуації.

При автоматизації процесів управління інцидентами в першу чергу необхідно приділяти увагу автоматизованій обробці подій інформаційної безпеки — основі практично будь-якого інциденту. На підставі подій проводяться коригувальні дії, оцінка поточної захищеності системи, ефективності функціонування СУІБ. Тільки володіючи повним і достовірним набором подій, можна провести належне розслідування інцидентів, отримати уявлення про динаміку розвитку СУІБ. Можна сказати, що події — основний канал зворотного зв'язку для керуючих впливів в рамках СУІБ. Важливим є і те, що події легко документовані і відтворювані.

Автоматизована система моніторингу й управління інцидентами ІБ включає себе наступні основні компоненти (рис. 2.9):

- інтеграційну платформу;
- апаратно-програмні засоби моніторингу та аудиту;
- апаратно-програмні засоби захисту інформації;
- сховище інформації про інциденти ІБ;
- аналітичні інструменти і засоби генерації звітів;
- засоби управління і інтерфейси взаємодії з користувачами.

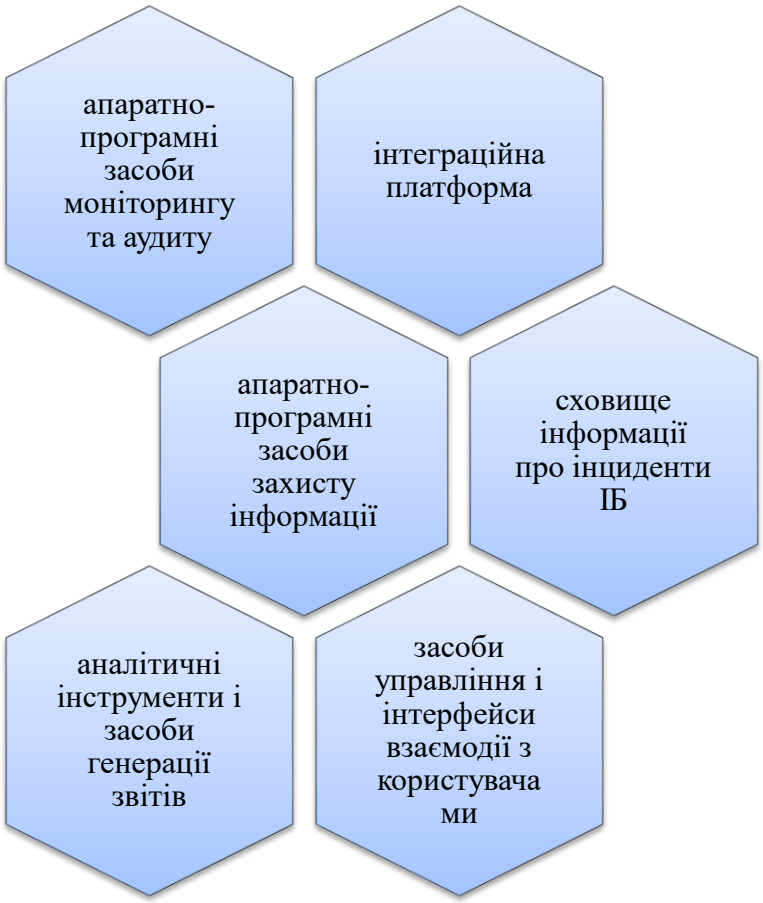

Рис. 2.9 Елементи автоматизованої системи моніторингу та управління інцидентами інформаційної безпеки [39]

Для підтримки процесу обробки подій на рівні, відповідному сучасним вимогам в кращих світових практиках застосовуються концепція SIEM систем. SIEM системи — це засоби, призначені для управління інформаційною безпекою в організаціях в цілому і управління подіями, отриманими з різних джерел. SIEM-системи здатні в режимі реального часу аналізувати події, що надходять від мережевих пристроїв і різних додатків.

Термін SIEM вперше з'явився в 2005 році і мав на увазі під собою систему збору даних від пристроїв, розміщених в мережі підприємства, і пристроїв безпеки, різних сервісів, призначених для управління обліковою інформацією і управління доступом, а також операційних систем, наявних баз даних та встановлених в мережі додатків для відстеження вразливостей, і подальшого аналізу отриманих відомостей.

SIEM системи повинні забезпечувати наступний функціонал:

- дозволяти збирати події від всіх технічних засобів забезпечення захищеності, використовуваних в рамках СУІБ;
- виробляти нормалізацію подій, приводячи їх до єдиного формату;
- здійснювати зберігання подій способом, що дозволяє зберігати необхідні обсяги даних;
- надавати інструментарій для пошуку в сховище даних;
- надавати механізми формування звітів різного роду;
- повинна бути розширюваною і масштабуватися;
- опціонально здійснювати кореляцію зібраних подій.

Процес обробки подій автоматизованими системами включає наступні основні кроки: нормалізація (приведення до єдиного формату) даних, агрегування (накопичення), кореляція і візуалізація. На перших двох стадіях інформація про події безпеки збирається практично з усіх використовуваних в рамках СУІБ засобів захисту: міжмережевих екранів, систем виявлення атак, антивірусних систем, операційних систем і додатків різних виробників, засобів контролю фізичного доступу, і перетвориться в єдиний, зручний для розуміння формат. Зібрані дані піддаються кореляції і виводяться на консоль оператора системи.

Розвинені засоби пошуку дозволяють проводити оперативне та всебічне розслідування інцидентів, забезпечувати свідчення наявності і функціонування засобів захисту в рамках СУІБ при проведенні різних аудитів.

Джерелами даних для SIEM-систем зазвичай служать системи виявлення та запобігання вторгнень (IDS та IPS системи), журнали серверів і призначених для користувача комп'ютерів, комутатори, маршрутизатори, системи СКД, антивірусні платформи, системи віддаленого доступу, DLP-системи, а також файлові сервери. З огляду на різноманіття можливих джерел подій в компанії, при виборі SIEM необхідно враховувати, від яких джерел система здатна приймати і обробляти дані. В даний час SIEM-системи повинні виробляти поведінковий

аналіз і порівняння даних в режимі реального часу. Крім цього платформа повинна мати функції нормалізації і можливістю фільтрації інцидентів.

Однією з таких систем є програмно-апаратний комплекс — OSSIM (Open Source Security Information Management) — програмне рішення від компанії AlienVault — комплексна система управління, контролю і забезпечення ІБ — забезпечує аналіз в реальному часі різних загроз та інцидентів за допомогою пристроїв та додатків (проводить моніторинг інцидентів та подій, збирає і оброблює ці дані та представляє їх графічно.

OSSIM включає в себе такий функціонал як:

- Збір, аналіз і кореляція подій;
- Хостова система виявлення вторгнень (HIDS);
- Мережева система виявлення вторгнень (NIDS);
- Бездротова система виявлення вторгнень (WIDS);
- Більше 200 плагінів для парсинга і кореляції логів;
- Набір шаблонів для загроз.

SIEM системи в тому числі збирають інформацію від систем виявлення аномальної активності [32] (рис. 2.11):

- IDS системи;
- IPS системи.

IDS система — Intrusion detection system, система виявлення вторгнень. Це система, яка реєструє якусь аномальну активність і надсилає сповіщення адміністратору.

IPS система — Intrusion prevention system, система протидії вторгненням. Це система яка не тільки виявляє вторгнення, а й застосовує алгоритми дій спрямовані на протидію атаці, розрив з’єднання, наприклад, або виконання скрипту встановленого адміністратором.

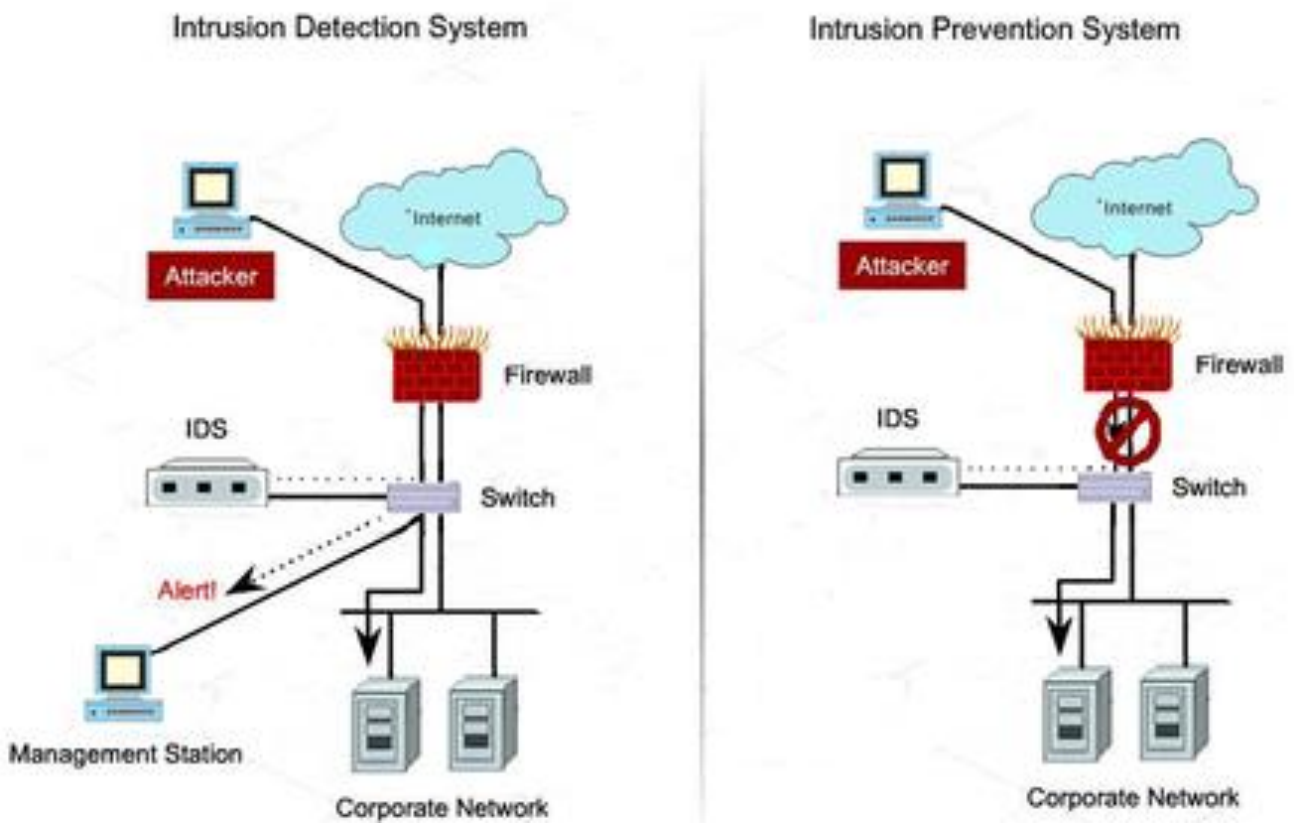

Рис. 2.10 Порівняння IDS та IPS систем

Таким чином, впровадження автоматизованої системи управління інцидентами інформаційної безпеки допоможе швидше виявляти інциденти інформаційної безпеки, скоротити витрати часу на реагування та аналіз інциденту.

Висновки до другого розділу:

Проаналізувавши організацію управління інцидентами в системі забезпечення інформаційної безпеки підприємства на основі методичних підходів і міжнародних практик можна дійти висновку, що добре організований процес управління інцидентами в підрозділах служби інформаційної безпеки це:

- чітке визначення для всіх фахівців ролей і відповідальності за якісне і своєчасне реагування на інциденти;
- оперативна інформація для моніторингу ефективності прийнятих захисних заходів;
- прозорість контролю за ефективністю роботи співробітників підрозділу;

– підвищення якості взаємодії фахівців в суміжних IT-та бізнес-підрозділах.

Крім того впровадження системи автоматизації процесу управління інцидентами додатково дозволить:

– обробляти і зберігати інформацію про події та інциденти інформаційної безпеки, а також про всі дії по їх усуненню;
– оперативно приймати рішення щодо усунення виниклого інциденту, грунтуючись на аналізі інформації про попередні інциденти;
– проводити аналіз накопичених даних.

Розглянувши як саму систему управління інцидентами інформаційної безпеки, так і її основні елементи та методичні підходи організації та впровадження слід поєднати всю проаналізовану інформації та розробити рекомендації щодо вдосконалення процесів організації управління інцидентами в системі забезпечення інформаційної безпеки підприємства.

Розділ 3
ДОСЛІДЖЕННЯ ПРОЦЕСІВ ОРГАНІЗАЦІЇ УПРАВЛІННЯ ІНЦИДЕНТАМИ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПРИКЛАДІ ПІДПРИЄМСТВА

Результати, отримані в першому і другому розділі, пропонується перевірити на прикладі функціонування підприємства ТОВ «АБВ геймс ентертейнмент». Для цього необхідно провести якісну підготовку підприємства щодо проведення дослідження процесів управління інцидентами інформаційної безпеки, визначення їх місця в системі забезпечення інформаційної безпеки та провести дослідження, що дозволить розробці рекомендацій щодо вдосконалення цих процесів організації управління інцидентами на підприємстві.

3.1 Підготовка підприємства щодо проведення дослідження процесів управління інцидентами інформаційної безпеки на підприємстві

З огляду на вище сказане, необхідно розробити рекомендації щодо організації системи управління інцидентами інформаційної безпеки в системі забезпечення інформаційної безпеки підприємства. Зробимо це на прикладі ТОВ «АБВ геймс ентертеймент». Це продуктова IT компанія. Основним напрямком діяльності якої є видання комп’ютерних ігор.

Графік роботи підприємства по буднім дням з 8 ранку до 8 вечора, технічна підтримка клієнтів працює цілодобово. Штат співробітників складається з 117 осіб, серед яких (рис. 3.1):

- Рада директорів — 3 особи;
- Керівники департаментів — 4 особи;

- Бухгалтер — 5 осіб;
- Юрист — 4 особи;
- Секретар — 1 особа;
- Системний адміністратор 1 лінії підтримки — 3 особи;
- Програмісти — 50 осіб;
- Дизайнери — 20 осіб;
- Тестувальники — 7 осіб;
- Спеціаліст відділу інформаційної безпеки — 1 особа;
- Фахівці відділу маркетингу — 10 осіб;
- Охоронець — 5 осіб;
- Прибиральниця — 2 особи.

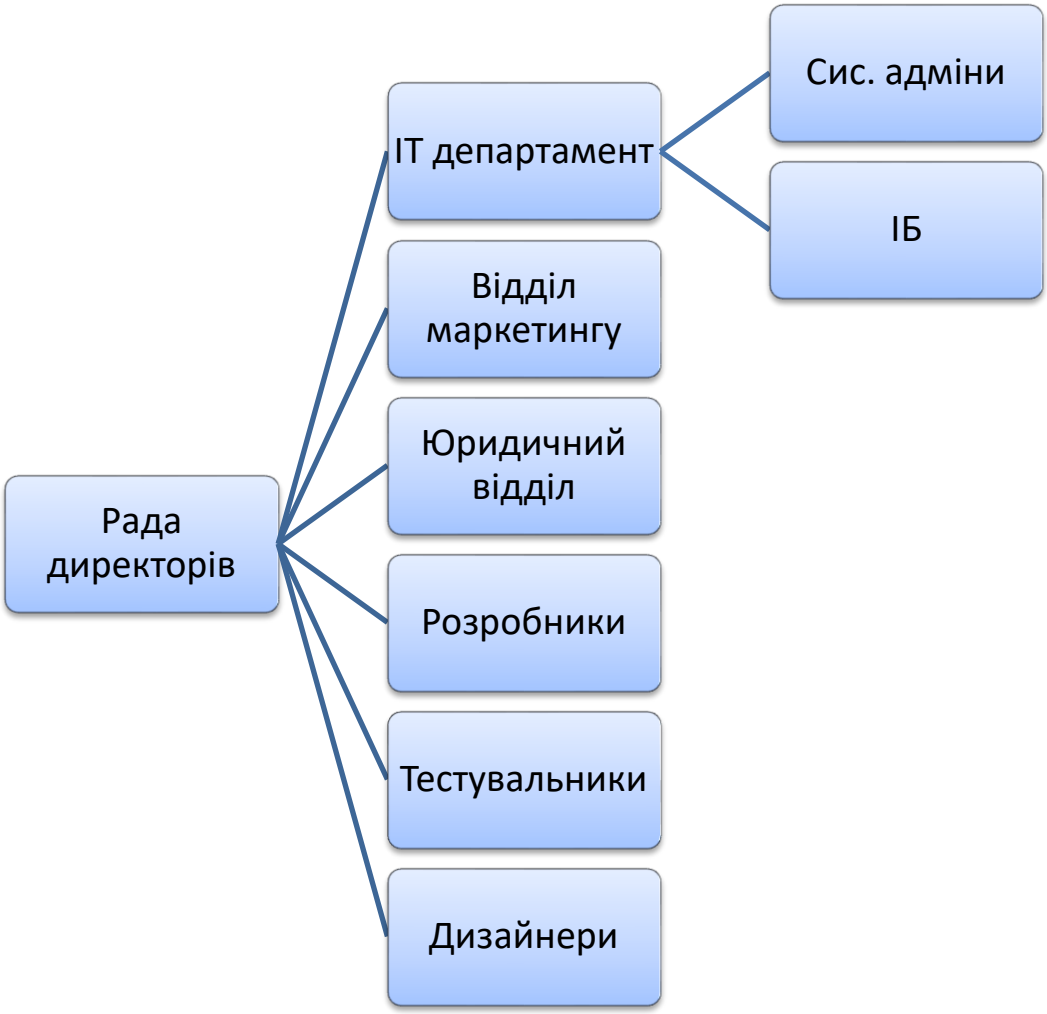

Рис. 3.1 Організаційна структура ТОВ «АБВ геймс ентертейнмент»

ТОВ «АБВ геймс ентертеймент» має локальну обчислювальну мережу, яка включає 104 одиниці обчислювальної техніки (97 комп’ютерів, 5 FTP серверів, 1 поштовий сервер та 1 сервер віддаленого управління), та має вихід в мережу Інтернет, автоматизована система (АС) відноситься до класу АС 3.

В комп’ютерній мережі підприємства використовується топологія «ієрархічна зірка». Її відмінністю від «зірки» є використання декількох центральних вузлів, ієрархічно з'єднаних між собою зв'язками типу «зірка». Для зв’язку комп’ютерів локальної мережі використовується стек протоколів TCP/IP. Для зв’язку з віддаленими офісами партнерів та державних структур на контролері домену налаштований VPN-сервер. На підприємстві діє система охоронно-пожежної сигналізації та організована система відеоспостереження. Для доступу на територію підприємства встановлена СКД.

Крім того, на даному підприємстві вивчені можливості існуючої системи забезпечення інформаційної безпеки, процесів організації реагування на інциденти інформаційної безпеки, з яких актуальними є використання структурованої побудови мережі, забезпечення швидкості реагування на виявлений інцидент і відповідальних осіб, наявність загальної політики інформаційної безпеки і використання антивірусного захисту. Проте проблемними місцями є політика інформаційної безпеки, процедури і порядок дій при виявленні інциденту, система реагування на інциденти не достатньо автоматизована і деякі інциденти залишаються без уваги, на підприємстві не використовуються системи постійного моніторингу та протидії інцидентам, недостатня забезпеченість людськими ресурсами, через що при критичних інцидентах збільшується час обробки інцидентів.

Виявлено, що першим етапом організації управління інцидентами інформаційної безпеки в системі забезпечення інформаційної безпеки є планування та підготовка.

Досліджено, що даний етап є підготовчим і призначений для організації та регламентування діяльності з реагування на інциденти. На цьому етапі:

- виділяють людські і матеріальні ресурси;
- розробляється схема реагування на інциденти;
- розробляється і затверджується ряд організаційно-регламентуючих документів;
- проводиться необхідне навчання персоналу і апробація обраної схеми реагування на інциденти.

Відповідно до ISO / IEC 27035 в компанії створена група з розслідування інцидентів ІБ. Відмічено, що головними цілями є:

- забезпечення компанії кваліфікованим персоналом для обліку, реагування та аналізу інцидентів;
- забезпечення необхідної координації і управління процесом реагування на інциденти;
- забезпечення належного рівня інформування керівництва і зацікавлених осіб;
- забезпечення максимального зниження наслідків інцидентів як в матеріальній сфері, так і для підтримки репутації організації.

До складу групи входять включити представники наступних підрозділів організації:

- служба інформаційної безпеки: забезпечення координаційної, адміністративної, експертної та технологічної діяльності;
- служба інформаційних технологій: забезпечення експертної та технологічної діяльності;
- служба персоналу: забезпечення адміністративної та процедурної діяльності;
- юридична служба: забезпечення експертної та нормативно-правої діяльності;

- бізнес-менеджери профільних підрозділів: залучаються на тимчасовій основі для підтримки забезпечення адміністративної, експертної та технологічної діяльності;
- зовнішні експерти: забезпечення консультативної, експертної та технологічної діяльності.

Виявлено, що основними процесами підготовчого етапу є:

- виділення людських і матеріальних ресурсів;
- розробка та затвердження організаційно-розпорядчої документації;
- навчання персоналу;
- тестування схеми реагування на інциденти.

Досліджено, що перш за все, було донесено бізнесу важливість і необхідність впровадження ефективної системи управління інцидентами інформаційної безпеки, зважаючи на всі ризики, а також виділити доцільну кількість матеріальних та людських ресурсів.

Також, на даному етапі було розподілено ролі між членами групи реагування на інциденти, також визначено основні обов’язки кожної особи. Крім того, потрібно провести навчання як самої групи реагування на інциденти в рамках їх обов’язків, так і решти персоналу на предмет порядку необхідних дій при виявленні ними інциденту.

Визначено, що ще однією важливою дією є визначення всіх можливих інцидентів, їх опис, аналіз, категоризація і пріоритизація. А також впровадження дій для попередження і усунення кожного з інцидентів.

Прикладом інцидентів для даного підприємства є:

- втрата співробітником магнітної картки СКД;
- викрадення конфіденційної інформації;
- викрадення техніки;
- проникнення зловмисників в мережу компанії;
- фішингова атака;
- DDOS атака;

– компрометація облікових записів працівників компанії;
– і т. д.

Крім того було визначено критичність кожного з інцидентів. Для цього створено шкалу критичності (табл. 3.1).

Таблиця 3.1

Шкала критичності інцидентів

Інцидент	Критичність
Компрометація облікових записів	4
Викрадення конфіденційної інформації	5
Втрата магнітної картки СКД	1
Викрадення техніки	4
Фішингова атака	2

Проаналізовано, що наступним етапом є експлуатація.

На даному етапі здійснюється: виявлення інциденту ІБ, його ідентифікація, попередній аналіз і реагування на інцидент.

Основні процеси етапу:

– виявлення та ідентифікація інциденту;
– попередній аналіз інциденту;
– початкове реагування на інцидент;
– реагування на інцидент.

Враховуючи дані отримані з попереднього етапу можна одразу класифікувати знайдений інцидент, визначити його критичність і дії необхідні для його усунення.

Наприклад, інцидент з втратою магнітної картки СКД одним з дизайнерів. Інформація про інцидент була отримана в понеділок вранці, коли співробітник прийшов на роботу, але не зміг потрапити в офіс без магнітної картки і повідомив про це свого начальника, який у свою чергу передав інформацію до відділу інформаційної безпеки. Критичність інциденту за шкалою, визначеною на минулому етапі дорівнює 1. Але через те, що співробітник не знає коли загубив картку існує ймовірність, що її викрав зловмисник і незаконно потрапив на територію офісу. Перш за все дану картку потрібно заблокувати. Після цього необхідно провести розслідування і перевірити останні використання заблокованої картки. Якщо нею останній раз користувався працівник, то інцидент можна вважати вичерпаним.

Виявлено, що далі йде етап аналізу.

Для проведення поглибленого аналізу інциденту була створена група з реагування на інциденти, на основі результатів аналізу робляться висновки і складаються рекомендації щодо поліпшення процесу забезпечення ІБ і реагування на інциденти. Формується звіт про інцидент.

Основним процесом етапу є поглиблений аналіз інциденту.

На прикладі інциденту з втраченою карткою на даному етапі групі реагування на інциденти необхідно проаналізувати причини виникнення інциденту, можливі наслідки, а також розробити рекомендації для уникнення подібних інцидентів у майбутньому. В даному випадку можна рекомендувати провести поштову розсилку з нагадуванням про відповідальне ставлення до магнітних карток СКД, а також не буде зайвим нагадати, що при втраті необхідно одразу повідомити про це у відділ інформаційної безпеки. Після цього всі дані про інцидент оформювалися в єдиний звіт.

Також визначено, що останнім етапом є поліпшення.

На даному етапі здійснюється реалізація рекомендацій щодо поліпшення процесів забезпечення ІБ і реагування на інцидент. Затверджені уповноваженою особою компанії рекомендації передаються на виконання відповідальним особам.

Таким чином, організація «АБВ геймс ентертейнмент» має достатньо ефективну систему управління інцидентами інформаційної безпеки. Але на основі отриманих данних необхідно розробити рекомендації щодо вдосконалення основних процесів управління та забезпечення інформаційної безпеки.

3.2 Рекомендації щодо вдосконалення процесів організації управління інцидентами на підприємстві

Для того щоб система управління інцидентами інформаційної безпеки була ефективною до неї необхідний комплексний підхід. Починаючи з організаційних моментів, таких як створення повноцінної політики інформаційної безпеки підприємства, в яку також повинні бути включені процеси управління інцидентами і доповнені пунктами для їх попередження. Наприклад, політикою інформаційної безпеки може бути заборонено використовувати особисту техніку для роботи з корпоративною інформацією, а також підключати особисті носії інформації до корпоративної техніки. Такі вимоги зменшили б ризики викрадення конфіденційної інформації, і покращили б контроль за нею. Окрім того дані вимоги можна підкріпити програмними засобами моніторингу систем працівників на предмет підключення зовнішніх носіїв інформації.

Крім того, в компанії обов’язково необхідна кваліфікована група реагування на інциденти, або внутрішня, або аутсорс команда. Але в другому випадку обов’язково всередині компанії повинні бути кваліфіковані спеціалісти, які зможуть швидко відновити мережу у випадку якогось інциденту.

Всі системи повинні постійно моніторитись і оновлюватись. Задля уникнення вразливостей в використовуваному ПЗ. Цим повинні займатись або фахівці відділу інформаційної безпеки підприємства, або системні адміністратори.

Потрібно враховувати недостатнє фінансування ІТ та ІБ і відсутність у відповідальних осіб чіткого розуміння, що потрібно впроваджувати першочергово для захисту ключових інформаційних активів. Саме тому всі рішення інформаційної безпеки повинні бути детально фінансово обґрунтовані.

Можна виділити кілька основних рекомендацій щодо вдосконалення процесів управління інцидентами інформаційної безпеки:

1) Керівництво організації повинно сприяти створенню необхідних умов для впровадження процедури розслідування інцидентів інформаційної безпеки всередині організації;
2) Скорочення інцидентів інформаційної безпеки шляхом ефективного використання сучасних засобів захисту мереж, комп'ютерних систем, програмного забезпечення і додатків;
3) Документування керівних принципів і процедур розслідування інцидентів інформаційної безпеки для забезпечення внутрішньої організації взаємодії і формування уявлень в органи державної влади;
4) Інформування про результати розслідування інциденту своїх співробітників і партнерів;
5) Структуризація і пріоритезація потоку інформації про можливі інциденти інформаційної безпеки, що надходить від технічних засобів моніторингу і збору даних;
6) Формалізація принципів пріоритетності подій інформаційної безпеки;
7) Аналіз інцидентів та обробка результатів з метою отримання практичного досвіду.

Щодо вдосконалення процесів управління інцидентами інформаційної безпеки можна також виділити кілька рекомендацій:

1) Для зменшення навантаження на системних адміністраторів та фахівців з інформаційної безпеки доцільним буде впровадження автоматизованої системи управління інцидентами інформаційної безпеки, наприклад, Zabbix;
2) Частіше проводити навчання персоналу організації, а також відповідальних фахівців.

Висновки до третього розділу:

Отже, інформаційна безпека підприємства є однією з найактуальніших проблем сьогодення. Технології розвиваються з кожним днем все швидше і швидше, через що з'являються нові загрози для підприємств. Для організації ефективної системи управління інцидентами в системі забезпечення інформаційної безпеки підприємства, на прикладі ТОВ «АБВ геймс ентертейнмент», можна виділити такі основні рекомендації:

- необхідний комплексний обґрунтований підхід до організації управління інцидентами в системі забезпечення інформаційної безпеки підприємства;
- необхідно створити групу реагування на інциденти інформаційної безпеки в кількості мінімум 5 людей, в яку повинні входити спеціалісти з різних відділів компанії (Системні адміністратори, фахівці ІБ, Юридичний відділ, керівник ІТ департаменту), крім того необхідно налагодити комунікацію між відділами;
- всі інциденти повинні бути детально оброблені, усунуті, задокументовані та проаналізовані, для подальшого їх уникнення та мінімізації наслідків.

Задля пришвидшення обробки та реагування на інциденти доцільно на підприємстві поліпшити автоматизовану систему управління інцидентами. Вона не тільки дозволить економити час, а й допомогти у розслідуваннях інцидентів, а також, звести ймовірність деяких видів інцидентів до мінімуму.

Використовуючи інформацію, проаналізовану в минулому розділі можна запропонувати один найпоширеніших у світі систем. Зважаючи на невеликий розмір підприємства і відносно невелику кількість працівників доцільним буде використання опенсорсної системи Zabbix, яка ідеально підійде під потреби підприємства.

ВИСНОВКИ

Таким чином мета роботи досягнута: досліджено методи побудови системи управління інцидентами інформаційної безпеки. Проаналізовано найпоширеніші стандарти в сфері управління інформаційною безпекою, це:

- Стандарти серії ISO/IEC 27k;
- OWASP Incident response guidance;
- NIST 800-53 Incident response.

На основі цих стандартів, а також світових практик було визначено основні вимоги до системи управління інцидентами інформаційної безпеки:

- в компанії обов’язково повинна бути кваліфікована група реагування на інциденти інформаційної безпеки. Крім того повинні бути чітко визначені ролі і обов’язки всіх членів групи;
- необхідна якнайшвидша реакція на інциденти для забезпечення безперервної роботи бізнесу;
- всі інциденти повинні бути детально задокументовані, оброблені і проаналізовані;
- в результаті обробки кожного інциденту повинні бути створені рекомендації для подальшого не повторення такого ж інциденту та мінімізації наслідків;
- всі клієнти, партнери та співробітники, на яких міг вплинути інцидент повинні бути поінформовані про результати розслідування.

Як було з`ясовано у роботі, забезпечення інформаційної безпеки підприємства — це низка певних методологій та засобів, направлених на всебічне системне підтримання та вдосконалення рівня захисту інформаційних ресурсів за допомогою виконання відповідними підрозділами системи безпеки завдань щодо забезпечення конфіденційності, цілісності та доступності інформації.

Також було розроблено рекомендації щодо організації управління інцидентами в системі забезпечення інформаційної безпеки підприємства.

Результати дослідження підтверджені на прикладі підприємства ТОВ «АББ геймс ентертейнмент», для якого було досліджено процеси організації управління інцидентами та розроблено рекомендації щодо покращення цих процесів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про концепцію національної програми інформатизації: Закон України від 4 лютого 1998 року № 75/98-ВР. *Відомості Верховної Ради України*. 1998. № 27-28. Ст. 182.

2. Про національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-В. *Відомості Верховної Ради України*. 1998. № 27-28. Ст. 181.

3. Про національну безпеки України: Закон України від 21 червня 2018 року № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

4. Про Стратегію національної безпеки України: Указ Президента України від 14 вересня 2020 року № 1392/2020. *Офіційний вісник України*. 2020. № 11. Ст. 389.

5. Коваленко Ю.О. Забезпечення інформаційної безпеки підприємства. URL: http://nbuv.gov.ua/UJRN/econpr_2015_3_20

6. Швець Ю. О. Ризики в діяльності промислових підприємтсв, види, методи оцінки та заходи подолання ризику. *Науковий вісник Ужгородського Національного університету*. 2017. №6. С.15-28.

7. Семенютіна Т.В. Концептуальні основи формування національного стандарту ризик-менеджменту діяльності підприємств в Україні. *Сталий розвиток економіки*. 2015. № 4(21). С. 140–144.

8. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах Євроінтеграції. URL: https://pidruchniki.com/1584072028356/politologiya/informatsiyna_bezpeka_ukrayini_v_umovah_yevrointegratsiyi

9. Борсуковський Ю.В., Борсуковська В.Ю. Прикладні аспекти захисту інформації в сучасних умовах. *Сучасний захист інформації.* 2018. №2. URL: journals.dut.edu.ua/index.php/dataprotect/article/view/1893/1796

10. Борсуковський Ю.В. Борсуковська В.Ю. Рекомендації по категоріюванню інформації з обмеженим доступом. *Сучасний захист інформації*. 2017. №4. С. 9-17. URL: journals.dut.edu.ua/index.php/dataprotect/article/view/1743/1665

11. Борсуковський Ю.В., Борсуковська В.Ю. Базові напрямки забезпечення кібербезпеки державного та приватного секторів. *Сучасний захист інформації*. 2017. №2. С. 85-89 URL: journals.dut.edu.ua/index.php/dataprotect/article/view/1494/1426

12. Олійник О. В. Принципи забезпечення інформаційної безпеки України. 2016. URL: http://jrnl.nau.edu.ua/index.php/UV/article/11123/14773

13. Кірейцев. Г.Г. Фінансовий менеджмент. 2015 URL: https://buklib.net/books/21874/

14. Велігура А.В. Оцінювання стану інформаційної безпеки підприємства. Управління проектами та розвиток виробництва. 2014. № 4. С. 28-39.

15. Рулєв В.А Гуткевич С.О. Менеджмент. 2016 URL: https://pidru4niki.com/1584072022660/menedzhment/menedzhment

16. Dess, Gregory. *Strategic Management*. United States: McGraw-Hill. 2018 с. 73.

17. Гловацький В.В. Методи оцінювання стану безпеки та загроз інформаційних ресурсів. *Зв'язок* .2016. №5. URL: http://nbuv.gov.ua/UJRN/Zvjazok_2016_5_5

18. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

19. Мєшков В. І. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах. 2015 URL: https://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf

20. NIST Computer Security Incident Handling Guide. 2017 URL: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

21. OWASP Incident response. 2018 URL: https://owasp.org/www-project-incident-response

22. Maria Bartnes, Karin Bernsmed Information Security Incident Management: Identified Practice in Large Organizations. 2017 URL: https://www.researchgate.net/publication/269304347_Information_Security_Incident_Management_Identified_Practice_in_Large_Organizations

23. Axelsson, S. Intrusion Detection Systems: A Survey and Taxonomy. 2017 URL: http://neuro.bstu.by/ai/To-dom/My_research/Paper-0-again/For-research/D-mining/Anomaly-D/Intrusion-detection/taxonomy.pdf

24. Кибербезопасность 2019-2020. Тренды и прогнозы. 2020. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020

25. Методи виявлення інцидентівю *Ukrainian Information Security journal. №2. 2015* URL: http://jrnl.nau.edu.ua/index.php/ZI/article/view/8798

26. NIST SP 800-61 Rev. 2 Computer Security Incident Handling. 2016 URL: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

27. Julia Jisielius «Automated Incidednt Response Explained». 2018URL: https://cybersecurity.att.com/blogs/security-essentials/automated-incident-response-in-action-7-killer-use-cases

28. Гнатюк С.О. Теоретичні основи побудови та функціонування систем управління інцидентами інформаційної безпеки. 2012.

29. Computer Security Incident Response team (CSIRT). 2017 URL: https://whatis.techtarget.com/definition/Computer-Security-Incident-Response-Team-CSIRT

30. Управління інцидентами інформаційної безпеки. *SearchInform КІБ.* 2018. URL: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/upravlenie-intsidentami-informatsionnoj-bezopasnosti/

31. Эксперты PT Expert Security Center предсказывают атаки кибергруппировки RTM. *Блог Positive technologies.* 2020. URL: https://www.ptsecurity.com/ru-ru/about/news/eksperty-pt-expert-security-center-predskazyvayut-ataki-kibergruppirovki-rtm/?sphrase_id=68372

32. Системи IDS/IPS. 2019. URL: https://www.anti-malware.ru/security/ids-ips

33. Аналіз загроз інформаційної безпеки. 2019. URL: https://www.anti-malware.ru/analytics/Threats_Analysis

34. APT-атаки. *Блог Positive technologies.* 2020. URL: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-finance-2019/#id1

35. Поповський В.В., Лемешко О. В. Телекомунікаційні системи та мережі. Основні підходи до забезпечення інформаційної безпеки. 2015. URL: https://www.znanius.com/3533.html

36. Who is OWASP foundation. 2017 URL: https://owasp.org/

37. Актуальні кіберзагрози на 3 квартал 2020 року. *Блог Positive technologies*. 2020 URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q3/

38. Нові виклики для інформаційної безпеки підприємства». *Блог ESET.UA.* 2019 URL: https://eset.ua/ua/blog/view/67/novyye-vyzovy-dlya-informatsionnoy-bezopasnosti-predpriyatiya-kak-minimizirovat-potentsialnyye-riski

39. Корченко О.Г. Аудит управління інцидентами інформаційної безпеки. навч. посібник. *НАСБУ*, 2017. с.147.