ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи

на тему:

«ТЕХНОЛОГІЯ ПОБУДОВИ СИСТЕМ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)

Поліщук Д.В.
(прізвище та ініціали)

Керівник Борсуковський Ю.В.

Рецензент

Нормоконтролер Чумак Н.С
(прізвище та ініціали)

КИЇВ – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“___”_____ 2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ
СТУДЕНТУ

Поліщуку Денису Вікторовичу
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: «Технологія побудови систем управління інцидентами інформаційної безпеки»

керівник магістерської роботи Борсуковський Юрій Володимирович, к.т.н,доцент.
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «12» жовтня 2022 року № 122.

2. Строк подання студентом магістерської роботи 15.12.2022 р.

3. Вихідні дані до магістерської роботи Результати власних спостережень автора процесів які досліджувалис
Побудова системи управління інцидентами інформаційної безпеки
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Визначити поняття та класифікацію джерел інцидентів інформаційної

безпеки

2. Окреслити сучасні підходи до управління інцидентами інформаційної безпеки

3. Запропонувати практичні рекомендації з побудови та функціонування систем управління інцидентами інформаційної безпеки

5. Перелік графічного матеріалу

1. Презентація PowerPoint

6. Дата видачі завдання 26.09.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Уточнення постановки завдання	26.09.2022 р.	
2.	Аналіз літератури	29.10.2022 р.	
3.	Збір даних	02.11.2022 р.	
4.	Дослідження систем управління інцидентами інформаційної безпеки	09.11.2022 р.	
5.	Виконання теоретичної та практичної частини	26.11.2022 р.	
6.	Створення рекомендацій щодо систем управління інцидентами інформаційної безпеки	03.12.2022 р.	
7	Оформлення презентації	07.12.2021 р.	
8	Підготовка до захисту	15.12.2022 р.	

Студент _____ Поліщук Д.В.
(підпис) прізвище та ініціали

Керівник магістерської роботи _____ Борсуковський.Ю.В
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА

на бакалаврську роботу

студента Поліщука Дениса Вікторовича

на тему: «Технологія побудови систем управління інцидентами інформаційної безпеки»

Актуальність: Управління інцидентами є однією з найважливіших процедур управління інформаційною безпекою (ІБ). Основною метою створення системи інформаційної безпеки (ІБ) організації є зниження ризиків щодо інформаційних активів і зменшення негативних наслідків від можливих інцидентів ІБ. Процес управління інцидентами інформаційної безпеки (УІІБ) – ключовий процес у системі інформаційної безпеки. Він включений до рекомендацій ITIL (Information Technology Infrastructure Library) і стандарту ISO/IEC 27002. Тому тема магістерської роботи, є дослідження теоретичних, науково-методичних та розроблення організаційно-економічних основ управління інцидентами інформаційної безпеки та моделювання її системи. Наукові положення, викладені в магістерській роботі, висновки та рекомендації мають теоретичне обґрунтування. Проведені дослідження свідчать про вміння автора працювати з науково-технічною літературою, проводити інженерний аналіз та узагальнювати матеріал.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми побудови систем управління інцидентами інформаційної безпеки
2. Було досліджено методи та засоби за якими можна створити власну SIEM систему.
3. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. Наведений приклад у третій частині достатньо примітивний і не відображує багатьох архітектурних та функціональних особливостей SIEM системи.
2. Фінальне рішення більше схоже на WAF(Web Application Firewall) ніж на SIEM систему.

Висновок: Враховуючи недоліки, магістерська робота заслуговує оцінку **добре**, а студент **Поліщук Денис Вікторович** – присвоєння кваліфікації: магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую

Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Поліщук Д.В. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія побудови систем управління інцидентами інформаційно безпекою».

Магістерська робота і рецензія додаються.

Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Поліщук Д.В за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2021 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту, факультету (відділення) _____ Бреславська О.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент ***Поліщук Д.В.*** обрав тему роботи, метою якої було дослідити технологію побудови систем управління індицентами інформаційної безпеки. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Поліщук Д.В. показав хорошу теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану магістерську роботу студента Поліщука Дениса Вікторовича на оцінку **«добре»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник бакалаврської роботи _____ Борсуковський Ю.В.
(підпис) (прізвище та ініціали)
“____” _____ 2021 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Поліщук Д.В.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина бакалаврської роботи: 88 сторінок, 1 таблиця, 26 рисунків, 33 джерел.

Об'єкт дослідження – побудова системи управління інцидентами інформаційної безпеки.

Предмет дослідження – теоретичні засади, методичні підходи та науково-практичні рекомендації щодо процесу управління інцидентами інформаційної безпеки на підприємствах.

Мета роботи – дослідження теоретичних, науково-методичних та розроблення організаційно-економічних основ управління інцидентами інформаційної безпеки та моделювання її системи.

Методи дослідження – опрацювання літератури за цією темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, проведення експерименту.

В роботі розглянуто теоретичні, практичні, науково-методичні та організаційно-функціональні основи побудови системи управління інцидентами інформаційної безпеки. Окреслено інструментарій наукового пізнання інформаційної безпеки та процесу її забезпечення. Узагальнено класифікаційні ознаки джерел інцидентів інформаційної безпеки. Визначено сучасні підходи до управління інцидентами інформаційної безпеки. Наведено методичні підходи до формування концепції та структури автоматизованої системи управління інцидентами інформаційної безпеки. Проаналізовано стандарти, рекомендації, етапи та світові практики щодо управління інцидентами інформаційної безпеки. Створено систему управління інцидентами інформаційної безпеки та наведено методику розслідування інцидентів інформаційної безпеки. Розроблено та обґрунтовано практичні рекомендації з побудови та функціонування систем управління інцидентами інформаційної безпеки.

Галузь використання – управління інцидентами інформаційної безпеки на підприємствах.

ІНФОРМАЦІЙНА БЕЗПЕКА, ІНЦИДЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ТЕХНОЛОГІЯ ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНЦИДЕНТАМИ.

ABSTRACT

Master's thesis: 88 pages, 1 tables, 26 figures, 33 sources.

Object of research – construction of information security incident management system.

Subject of research – theoretical principles, methodological approaches and scientific and practical recommendations regarding the process of managing information security incidents at enterprises.

The aim of research – theoretical, scientific-methodical research and development of organizational and economic foundations of information security incident management and modeling of its system.

Research methods – study of the literature on this topic, analysis of operating documentation, international standards and their comparison, conducting an experiment.

The paper examines the theoretical, practical, scientific-methodical, and organizational-functional foundations of building an information security incident management system. The toolkit of scientific knowledge of information security and the process of its provision is outlined. The classification features of the sources of information security incidents are summarized. Modern approaches to information security incident management are defined. Methodical approaches to the formation of the concept and structure of the automated information security incident management system are presented. The standards, recommendations, stages and global practices regarding the management of information security incidents were analyzed. The information security incident management system was created and the method of investigation of information security incidents was given. Practical recommendations for the construction and operation of information security incident management systems have been developed and substantiated.

Field of use – management of information security incidents at enterprises.

INFORMATION SECURITY, INFORMATION SECURITY INCIDENT, INFORMATION SECURITY INCIDENT MANAGEMENT SYSTEM, TECHNOLOGY OF BUILDING INCIDENT MANAGEMENT SYSTEM.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ…….. 10

ВСТУП ……..……. 11

1 ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ ЗАСАДИ УПРАВЛІННЯ ІНЦИНДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ……...……. 13

1.1. Поняття інформаційної безпеки та процес її забезпечення…… 13

1.2. Класифікація джерел інцидентів інформаційної безпеки……... 15

1.3. Сучасні підходи до управління інцидентами інформаційної безпеки……. 21

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ……... 31

2.1. Аналіз стандартів, рекомендацій та світових практик щодо управління інцидентами інформаційної безпеки…… 31

2.2. Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035……..……... 34

2.3. Методичні підходи до формування концепції та структури автоматизованої системи управління інцидентами інформаційної безпеки……. 40

3 ОРГАНІЗАЦІЙНО - ТЕХНОЛОГІЧНІ ПІДХОДИ ДО УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ……. 47

3.1. Побудова системи управління інцидентами інформаційної безпеки …… 47

3.2. Перевірка працездатності розробленої системи управління інцидентами інформаційної безпеки ……... 67

3.3. Практичні рекомендації з побудови та функціонування систем управління інцидентами інформаційної безпеки ……... 72

ВИСНОВКИ……. 81

ПЕРЕЛІК ПОСИЛАНЬ..... 84

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)..... 88

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ

DDoS – Denial-of-Service Attack розподілена атака на відмову в обслуговуванні

DNS – Domain Name System – система перетворення імен хоста

DoS – Denial of Service – атака на відмову в обслуговуванні

HTML – HyperText Markup Language мова розмітки гіпертекстових документів

HTTP – Hyper Text Transfer Protocol – протокол передачі гіпертекстових документів

IP – Internet Protocol – протокол мережевого рівня

IT – інформаційна технологія

ІБ – інформаційна безпека

TCP/I – набір протоколів мережі інтернет

TLS – Transport Layer Security – криптографічний протокол

ПЗ – програмне забезпечення

DLP – data leak prevention, система захисту від витоку конфіденційних даних

FTP – file transfer protocol, протокол передачі файлів

IMAP – Internet message access protocol, протокол доступу до Інтернет-повідомлень

SIEM – security information and event management, управління інформаційною безпекою та подіями безпеки

УІІБ – управління інцидентами інформаційної безпеки

ІКС – інформаційно-комунікаційні системи

СУІІБ – система управління інцидентами інформаційної безпеки

СМІІБ – система менеджменту інцидентами інформаційної безпеки

ВСТУП

Актуальність дослідження. Управління інцидентами є однією з найважливіших процедур управління інформаційною безпекою (ІБ). Основною метою створення системи інформаційної безпеки (ІБ) організації є зниження ризиків щодо інформаційних активів і зменшення негативних наслідків від можливих інцидентів ІБ. Процес управління інцидентами інформаційної безпеки (УІІБ) – ключовий процес у системі інформаційної безпеки. Він включений до рекомендацій ITIL (Information Technology Infrastructure Library) і стандарту ISO/IEC 27002.

У бібліотеці кращих IT-практик ITIL під поняттям «інцидент» розуміється будь-яка подія, що не є елементом нормального функціонування певного сервісу і при цьому впливає, або здатна вплинути, на роботу цього сервісу шляхом його переривання або зниження якості. Відповідно до діючих міжнародних та вітчизняних стандартів у галузі управління інцидентами інформаційної безпеки (УІІБ), першим і найважливішим кроком є своєчасне та коректне усунення наслідків інциденту. Далі, необхідно розслідувати інцидент, виконати оцінку необхідності дій щодо усунення причин інциденту, якщо потрібно – реалізувати їх, а також виконати дії щодо попередження повторного виникнення інциденту (превентивні заходи). Окрім цього, важливо зберігати всі дані про інциденти ІБ, адже за допомогою статистики інцидентів можна визначити найбільш актуальні загрози для організації і, відповідно, максимально точно планувати заходи щодо підвищення рівня захищеності інформаційно-комунікаційних систем (ІКС) організації. Саме цей факт і визначає актуальність побудови та дослідження ефективності роботи систем управління інцидентами інформаційної безпеки (СУІІБ).

Аналіз та узагальнення публікацій з даної проблематики дали можливість зробити висновки про те, що, незважаючи на постійні глибокі, обґрунтовані дослідження за інформаційною тематикою, яка є надзвичайно важливою для розвитку сфери IT, вивчення кола проблем щодо формування інформаційних

ресурсів не можна визнати завершеним через їх стрімкий розвиток. Цей факт підтверджує необхідність здійснення й надалі досліджень, підходів і методів управління інформаційних ресурсів, розроблення питань подальшого вдосконалення системи управління інцидентами інформаційної безпеки на підприємствах. Саме цим зумовлені теоретична значущість, практична спрямованість та новизна теми диплому, його мета і сукупність завдань.

Об'єкт дослідження – побудова системи управління інцидентами інформаційної безпеки.

Предмет дослідження – теоретичні засади, методичні підходи та науково-практичні рекомендації щодо процесу управління інцидентами інформаційної безпеки на підприємствах.

Мета роботи – дослідження теоретичних, науково-методичних та розроблення організаційно-економічних основ управління інцидентами інформаційної безпеки та моделювання її системи.

Наукові завдання:

визначити поняття та класифікацію джерел інцидентів інформаційної безпеки.

окреслити сучасні підходи до управління інцидентами інформаційної безпеки;

запропонувати практичні рекомендації з побудови та функціонування систем управління інцидентами інформаційної безпеки.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів полягає у використанні теоретичних та методичних положень, що сприятиме підвищенню ефективності управління інцидентами інформаційної безпеки підприємств та їх функціонуванню загалом, а також створення системи управління інцидентами інформаційної безпеки.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ ЗАСАДИ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Поняття інформаційної безпеки та її забезпечення

Поняття інформаційної безпеки, залежно від його використання, розглядається у декількох ракурсах. У найзагальнішому випадку інформаційна безпека — це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

Під інформаційним середовищем розуміють сферу діяльності суб'єктів, пов'язану зі створенням, перетворенням і споживанням інформації. Інформаційне середовище умовно поділяється на три основні предметні частини:

- створення і розповсюдження вихідної та похідної інформації;
- формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг;
- споживання інформації;
- та дві забезпечувальні предметні частини:
- створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення;
- створення і застосування засобів і механізмів інформаційної безпеки.

Більш розгорнуте формулювання інформаційної безпеки — це стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.

Слід відзначити, що задоволення в будь-якій мірі потреб в інформації призводить до оволодіння відомостями про навколишній світ та процеси, що протікають в ньому, тобто інформованості особистості, суспільства та держави. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами

навколишньої дійсності і як наслідок — обґрунтованість рішень та дій, що приймаються.

В залежності від виду загроз інформаційній безпеці інформаційну безпеку можна розглядати наступним чином :

- як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації;
- інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;
- інформаційних прав і свобод людини і громадянина.

В інформаційному праві інформаційна безпека — це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

У тих випадках, коли йдеться про безпеку щодо інформації та інформаційно-обчислювальних систем, застосовуються загальноприйняті терміни про властивості цих об'єктів – категорії (рис. 1.1).

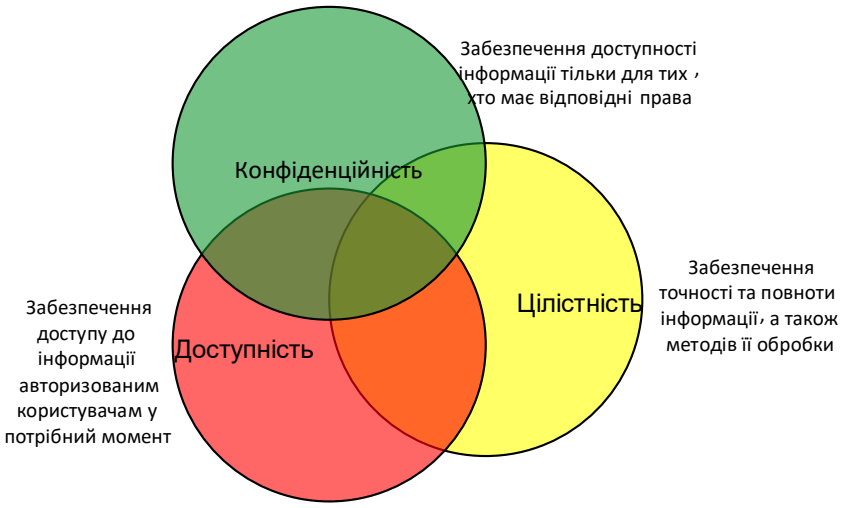

Рис. 1.1. Властивості ІБ

Інформація з точки зору інформаційної безпеки має наступні категорії:

- конфіденційність – гарантія того, що конкретна інформація доступна тільки тому колу осіб, для якого вона призначена; Контроль за станом здоров'я людини – це і є моніторинг системи/організму або самоконтроль.

- цілісність – гарантія того, що інформація зараз існує в її початковому вигляді, тобто при її зберіганні або передачі не було проведено несанкціонованих змін; порушення цієї категорії називається фальсифікацією повідомлення;
- автентичність – гарантія того, що джерелом інформації є саме та особа, яка заявлена як її автор, порушення цієї категорії також називається фальсифікацією, але вже автора повідомлення;

Відносно інформаційних систем застосовуються інші категорії:

- надійність – гарантія того, що система в нормальному і позаштатному режимах поводиться так, як заплановано;
- точність – гарантія точного і повного виконання всіх команд;
- контроль доступу – гарантія того, що різні групи осіб мають різний доступ до інформаційних об'єктів, і ці обмеження доступу постійно виконуються;
- можливість контролю – гарантія того, що в будь-який момент може бути проведена повноцінна перевірка будь-якого компонента програмного комплексу;
- контроль ідентифікації – гарантія того, що клієнт, підключений в даний момент до системи, є саме тим, за кого себе видає;
- стійкість до навмисних збоїв – гарантія того, що при навмисному внесенні помилок в межах заздалегідь обговорених норм система буде поводитися так, як це було обумовлено заздалегідь.

1.2 Класифікація інцидентів інформаційної безпеки

У міжнародній практиці розроблено достатню кількість нормативних документів, що регламентують питання управління ІІБ. Для управління ІІБ необхідно організувати комплекс методів та засобів управління інцидентами (УІ), забезпечити його належними ресурсами, відповідною нормативно-розпорядчою і робочою документацією, технічними засобами забезпечення механізмів контролю. Проте, перш ніж організовувати такий комплекс, потрібно мати повне розуміння поняття інциденту. Крім того, останні зміни у міжнародній

нормативній базі у рамках інформаційної безпеки (ІБ) її складову – кібернетичну безпеку (кібербезпеку), яка відповідно до [17] охоплює кіберпростір, що знаходиться в межах інформаційного простору. Зважаючи на це, доцільно було б розмежувати поняття ІІБ та інцидент кібербезпеки (кіберінцидент). Для цього необхідно провести аналіз поняття «інцидент» та інтерпретувати його в інформаційному та кіберпросторі.

Проведений аналіз показав, що різноманітні трактування інциденту мають спільну множину базових характеристик, а саме:

1) подія;

2) порушення комп'ютерної безпеки;

3) порушення політики безпеки;

4) порушення діяльності;

5) загроза ІБ;

6) підклас кризових і надзвичайних ситуацій;

7) випадок;

8) пригода;

9) відмова;

10) зниження якості послуги.

З урахуванням цього, доцільно буде запропонувати узагальнене визначення поняття «інцидент ІБ»: подія, яка може порушити діяльність, пов’язану із використанням ІС, повноту, своєчасність та вірогідність оброблюваної інформації, а також її конфіденційність, цілісність та доступність. Відповідно до роботи [8] кіберпростір – це віртуальний простір, отриманий у результаті взаємодії користувачів, програмного та апаратного забезпечення, мережевих технологій (у т.ч. Інтернет) для підтримки та управління процесами перетворення інформації з метою забезпечення інформаційних потреб суспільства. Крім того, у стандарті [17] під кібербезпекою розуміється забезпечення конфіденційності, цілісності та доступності інформації у кіберпросторі. Зважаючи на це, можна дійти висновку, що будь-яка діяльність у кіберпросторі забезпечується із використанням ІС.

Таблиця 1

Аналіз дефініцій поняття інцидент за базовими характеристиками

№	Дефініція	Базові характеристики інциденту									
		1	2	3	4	5	6	7	8	9	10
1.	Стандарт ISO / IEC 20000:2005	+									+
2.	Стандарт ISO / IEC 27000:2009 & ISO / IEC 27035	+				+					
3.	Стандарт ISO / IEC 13335-1:2004	+		+	+	+				+	
4.	Стандарт ISO / IEC TR 18044:2004	+				+					
5.	Стандарт ISO / IEC 27002	+									
	Стандарт BS 25999-1:2006	+									
6.	Національний інститут стандартів і технології NIST		+	+							
7.	Бібліотека інфраструктури інформаційних технологій ITIL (v3) Велика Британія										+
8.	Керівництво по обробці інцидентів інформаційної безпеки (Гонконг, КНР)	+	+			+					
9.	Процедура реагування на інциденти Мічиганського технологічного університету(США)		+	+							
10.	Керівні принципи з управління інцидентами інформаційної безпеки	+		+		+				+	
11.	Державний департамент закордонних справ США			+							
12	Центр CMS департаменту охорони здоров'я та соціальних служб (США)			+		+					
13.	Поштова служба США	+				+					
14.	ГОСТ Р ІСО / МЕК 27001-2006	+			+	+					
15.	Стандарт ЦБ РФ СТО БР Іббс-1.0-2010	+				+					
16.	Інструкція з реагування на інциденти, пов'язані з системами ДБО	+		+							
17.	С. Гладиш						+				
18.	П. Хусаінов	+				+					
19.	А. Голов	+		+							
20.	В. Кононович, С. Гладиш	+	+			+					
21.	Нове в українській лексиці: Словник-довідник Д. Мазурик	+						+	+		
22.	Словник Ожегова							+			
26.	Словник екологічних термінів і визначень									+	
30.	Електронний словник	+									
31	Глосарій інформаційної безпеки	+				+					
32.	Словник української мови	+						+	+		
33.	Матеріали із Вікіпедії	+						+		+	

Таким чином, під кіберінцидентом необхідно розуміти подію, яка може порушити кібербезпеку (конфіденційність, цілісність та доступність інформації у кіберпросторі).

Інцидент інформаційної безпеки (information security incident) – одинична подія або ряд небажаних і непередбачених подій інформаційної безпеки, через

які існує ймовірність компрометації бізнес-інформації і загрози інформаційній безпеці.

Загрози інформаційній безпеці — сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері. Основні загрози інформаційній безпеці можна розділити на три групи:

- загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;
- загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);
- загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі та гідності тощо).

Фактори загроз за видовою ознакою поділяються на політичні, економічні та організаційно-технічні.

Під політичними факторами загроз інформаційній безпеці розуміють:

- зміни геополітичної обстановки внаслідок фундаментальних змін у різноманітних регіонах світу, зведення до мінімуму ймовірності світової ядерної війни;
- інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів, та розповсюджують інформацію з метою здобуття односторонніх переваг;
- становлення нової державності в пострадянських країнах на основі принципів демократії, законності, інформаційної відкритості;
- знищення колишньої командно-адміністративної системи державного управління, а також системи забезпечення безпеки;

- порушення інформаційних зв'язків унаслідок утворення на території колишнього СРСР нових держав;
- прагнення пострадянських країн до більш тісного співробітництва із закордонними країнами в процесі проведення реформ на основі максимальної відкритості сторін;
- низька загальна правова та інформаційна культура сторін.

Основними економічними факторами загроз безпеці інформації є:

- перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур — виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин;
- критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації;
- розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.

Основними організаційно-технічними факторами загроз інформаційній безпеці є:

- недостатня нормативно-правова база у сфері інформаційних відносин, у тому числі в галузі забезпечення інформаційної безпеки;
- недостатнє регулювання державою процесів функціонування та розвитку ринку засобів інформатизації, інформаційних продуктів та послуг;
- широке використання у сфері державного управління та кредитно-фінансової сфери незахищених від витоку інформації імпортних технічних та програмних засобів для зберігання, обробки та передавання інформації;
- зростання обсягів інформації, яка передається відкритими каналами зв'язку;
- загострення криміногенної обстановки, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері.

Ієрархічна класифікація загроз інформаційній безпеці.

Глобальні фактори загроз інформаційній безпеці:

- недружня політика іноземних держав у галузі глобального інформаційного моніторингу, розповсюдження інформації, розповсюдження інформації та нових інформаційних технологій;
- діяльність іноземних розвідувальних та спеціальних служб;
- діяльність іноземних політичних та економічних структуру, спрямована проти інтересів держави;
- злочинні дії міжнародних груп, формувань та окремих осіб.

Регіональні фактори загроз інформаційній безпеці:

- використання інформаційної інфраструктури колишнього СРСР для передавання конфіденційної інформації;
- невідповідність інформаційного забезпечення державних та суспільних інститутів сучасним вимогам управління економічними, політичними та соціальними процесами;
- відставання від розвинених країн світу з темпів та масштабів розробки та впровадження нових інформаційних технологій;
- недопустимо високий рівень технологічної залежності держави від зарубіжних держав у зв'язку з широким використанням імпортних засобів обчислювальної техніки, систем телекомунікації, зв'язку та інформаційних технологій;
- розвиток зарубіжних технічних засобів розвідки, та промислового шпигунства, що дозволяє одержати несанкціонований доступ до конфіденційної інформації, у тому числі такої що складає державну таємницю;
- зростання злочинності в інформаційній сфері;
- використання старих методів та засобів захисту національних інформаційних мереж, широке розповсюдження комп'ютерних вірусів, призначених для ураження систем управління та зв'язку;
- відсутність ефективної системи забезпечення цілісності, незмінності та схоронності нетаємної інформації, у тому числі такої, що є інтелектуальною власністю.

Локальні фактори загроз інформаційній безпеці:

- перехоплення електронних випромінювань;
- застосування підслуховуючих пристроїв або закладок;
- дистанційне фотографування;
- розкрадання носіїв інформації та промислових відходів;
- копіювання носіїв інформації з подоланням заходів захисту;
- незаконне приєднання до апаратури та ліній зв'язку;
- упровадження та використання комп'ютерних вірусів і т. ін.

1.3.Сучасні підходи до управління інцидентами інформаційної безпеки

Підприємства, що відповідально ставляться до питань забезпечення інформаційної безпеки, необхідно вирішити такі завдання:

- виявлення, інформування та облік ІІБ;
- реагування на ІІБ, зокрема застосування необхідних засобів для запобігання, зменшення і відновлення після завданого збитку;
- аналіз ІІБ, що відбулися, з метою планування превентивних заходів захисту і поліпшення процесу забезпечення інформаційної безпеки в цілому.

Вирішити ці завдання покликана система менеджменту інцидентами інформаційної безпеки (СМІІБ).

Управління інцидентами інформаційної безпеки (УІІБ) є важливим процесом, який забезпечує організацію можливістю своєчасного виявлення інциденту та якомога швидшого реагування на нього за допомогою коректно обраних засобів підтримки. Основна задача УІІБ – оперативно відновити нормальну роботу служб і звести до мінімуму негативний вплив інциденту на діяльність організації з метою підтримки якості і доступності служб (сервісів) на максимально можливому рівні.

Нормальною вважається робота служб, що не виходить за межі угоди про рівень обслуговування (т. зв. Service-Level Agreement, SLA).

Цілі управління інцидентами:

- відновлення нормальної роботи служб в найкоротші терміни;
- зведення до мінімуму впливу інцидентів на роботу організації;
- забезпечення злагодженої обробки всіх ІІБ і запитів обслуговування;
- зосередження ресурсів підтримки на найбільш важливіших напрямках;
- надання відомостей, які надають можливість оптимізувати процеси підтримки, зменшити кількість інцидентів і спланувати управління.

Управління інцидентами і проблемами ІБ є комплексним рішенням, що оптимізує управління всіма аспектами обслуговування і підтримки, необхідними для підприємства. Використовуючи кращі, перевірені часом, напрацювання і відновлення ІТ-процесів після збоїв будь-яких видів, рішення з УІІБ дозволяють використовувати ресурси залежно від пріоритетів бізнес-діяльності, управляти рівнями обслуговування, а також краще контролювати витрати ІТ-служб. Рішення з УІІБ прискорює процеси реагування на ІІБ на всіх етапах: від первинного виявлення і діагностики проблем та основних причин до остаточного їх усунення.

Основними заходами створення СМІІБ є:

1. Виділення ресурсів для розробки та впровадження СМІІБ.
2. Визначення сфери функціонування СМІІБ.
3. Розробка комплексу процесів СМІІБ.
4. Навчання персоналу.
5. Впровадження процесів УІІБ та їх інтегрування з функціонуючими процесами управління інформаційної безпекою, такими як, інвентаризація активів, аналіз ризиків та оцінка ефективності.
6. Розробка архітектури і комплексу технічних засобів з автоматизації процесів УІІБ і моніторингу подій інформаційної безпеки.
7. Впровадження комплексу програмно-технічних засобів автоматизації УІІБ.

Результатом зазначених заходів буде впровадження СМІІБ**,** яка буде вирішувати такі завдання*:*

1. Оперативний моніторинг стану інформаційної безпеки в межах обраної сфери дії СМІБ.

2. Виявлення, облік, реагування, розслідування та аналіз ІІБ.

3. Інформування вищого керівництва і зацікавлених осіб про поточний стан інформаційної безпеки.

Також, слід зазначити, що при експлуатації різного роду СМІБ процес УІІБ є одним з найважливіших постачальників даних для аналізу функціонування подібних систем, оцінки ефективності використовуваних заходів зниження ризиків і планування удосконалення роботи системи.

Міжнародні стандарти ISO/IEC 27001 та ISO/IEC 27035 вводять такі визначення основних понять у галузі УІІБ:

- подія інформаційної безпеки – ідентифікований випадок стану системи або мережі, що вказує на можливе порушення політики інформаційної безпеки чи відмову засобів захисту, або раніше невідому ситуацію, яка може істотно впливати на безпеку;

- інцидент інформаційної безпеки – одинична подія або низка небажаних і непередбачених подій інформаційної безпеки, через які існує ймовірність компрометації бізнес-інформації (бізнес-процесів) і загроза інформаційній безпеці.

Серед інших дефініцій поняття ІІБ також можуть бути корисними такі:

- будь-яка небажана та непередбачена подія, яка може порушити діяльність чи інформаційну безпеку. Відповідно до стандарту ISO13335-1:2004 ІІБ вважається: втрата надання послуг обладнанням чи пристроями; системні збої чи перевантаження; помилки користувачів; недотримання політик і рекомендацій; порушення фізичних заходів захисту; неконтрольовані зміни систем; збої ПЗ і відмови технічних засобів; порушення правил доступу тощо;

- незапланованe переривання послуги або зниження якості послуги (відповідно до ITIL);

- будь-яка подія, яка не є частиною стандартної роботи служби і яка завдає або може спричинити переривання або зниження якості цієї послуги (відповідно до ISO/IEC 20000:2005).

Стандарт ISO/IEC 27001 накладає низку загальних вимог до побудови процесів управління інформаційною безпекою, до складу яких входить і процес УІБ. Такими вимогами є:

- використання вже згадуваної вище моделі PDCA для забезпечення планування процесів, впровадження процесів, контролю й аналізу процесів, удосконалення процесів;
- належне документування процесів і процедур;
- своєчасне виявлення невдалих і успішних спроб порушення безпеки та ІІБ;
- своєчасне повідомлення про ІІБ в установленому порядку;
- встановлення відповідальності керівництва і процедур для забезпечення швидкого й ефективного реагування на ІІБ;
- наявність механізмів вимірювання і відстежування типів, обсягів і вартості ІІБ;
- збирання, збереження і надання доказів відповідно до вимог локального законодавства;
- забезпечення підтримки процесів УІБ керівництвом;
- безперервний аналіз і удосконалення процесів управління інцидентами.

Стандарт ISO/IEC 27035 визначає формальну модель процесу реагування на

ІІБ. Цілями впровадження цієї моделі є впевненість у тому, що:

- події та ІІБ виявляються і обробляються ефективним чином, особливо в частині класифікації подій;
- виявлені ІІБ враховуються і обробляються найбільш відповідним і ефективним чином;

- наслідки ІІБ можуть бути мінімізовані у процесі реагування, можливо із залученням процесів відновлення після збоїв та аварій (BCP/DRP, Business Continuity Planning / Disaster Recovery Plan).

Шляхом аналізу інцидентів та подій ІБ підвищується ймовірність запобігання майбутнім ІІБ, удосконалюються механізми і процеси забезпечення ІБ. З огляду на це, для УІІБ необхідно організувати комплекс процесів управління інцидентами, забезпечити його належними ресурсами, відповідною нормативнорозпорядчою і робочою документацією, технічними засобами контролю.

Окреслимо основні питання, пов’язані з управлінням інцидентами інформаційної безпеки. Більшість ІТ-служб організації вирішує ті, чи інші питання, пов’язані з інцидентами ІБ. Служба технічної підтримки (т. зв. Service Desk) відповідає за моніторинг процесу усунення всіх зареєстрованих інцидентів, оскільки є власником усіх таких інцидентів. Цей процес є дуже швидким, а для ефективного реагування на інциденти слід визначити формальний метод дій співробітників, що передбачає використання необхідного ПЗ. Ті ІІБ, які не можуть бути вирішені безпосередньо службою Service Desk, повинні переадресовуватись відповідним фахівцям. Спосіб розв'язання інциденту або варіант його обходу має бути встановлений і доведений до користувачів якнайшвидше. Це випливає з головної цілі – мінімізації негативного впливу на основну діяльність користувачів. Після усунення причини інциденту і відновлення служби до обумовленого в SLA рівня інцидент закривається.

Частота появи і кількість інцидентів, пов'язаних з інформаційною безпекою, – один з наочних показників того, чи правильно функціонує система управління безпекою.

Стандарт ISO/IEC 27001 звертає особливу увагу на необхідність створення процедури УІІБ – очевидно, що без своєчасного реагування на інциденти безпеки й усунення їх наслідків неможливе ефективне функціонування системи УІБ. На жаль, в процесі аудиту різних інформаційних систем доводиться стикатися з

безліччю проблем реєстрації і розслідування інцидентів, що свідчать про те, що впровадженню стандартів на підприємствах приділяється дуже незначна увага.

Управління інцидентами інформаційної безпеки – це процес або набір процесів, на вхід яких подаються дані, отримані в результаті збору і протоколювання даних про події, що стосуються інформаційних систем, а на виході цих процесів одержують інформацію про причини інциденту, що відбувся, про збиток, нанесений організації, і заходи, які необхідно вжити для того, щоб інцидент не повторився у майбутньому. Таким чином, УІІБ спрямовано на вдосконалення системи забезпечення безпеки організації. Крім того, одержувані на виході дані є, по суті, єдиною об'єктивною інформацією для визначення ймовірності реалізації загроз при аналізі ризиків.

У більшості організацій процес УІІБ побудований таким чином:

- отримання інформації про інцидент;
- отримання додаткової інформації, пов'язаної з виявленим порушенням;
- аналіз ситуації, локалізація порушення і оперативне застосування контрзаходів;
- встановлення причин, через які стало можливим порушення, що трапилося, і, можливо, визначення відповідальних осіб (розслідування);
- проведення профілактичних заходів, розробка і впровадження заходів з недопущення повторного порушення.

Використовувані для виявлення інцидентів процедури збору інформації можуть забезпечуватися як технічними, так і організаційними заходами. Наприклад, відповідно до вимог політики безпеки, співробітник, що виявив порушення, зобов'язаний повідомити про нього в підрозділ інформаційної безпеки. Потім інформація про виявлені інциденти фіксується у спеціальних журналах (в паперовому або електронному вигляді). Таким чином збирається статистика про ІІБ.

Результати аналізу, розслідувань і профілактичних заходів зазвичай оформляються у вигляді довідок, звітів і аналітичних записок та зберігаються в

підрозділі ІБ. Проте якщо в організації ефективно реалізована реєстрація подій, а її інформаційна інфраструктура характеризується значним розміром і територіально розподілена, то рано чи пізно наступає момент, коли інформацію, пов'язану з інцидентами і станом їх розслідування, стає важко обробляти без допомоги спеціального інструментарію. Ще більшою проблемою стає підготовка і аналіз статистики, тоді як ця статистика є одним з ключових показників ефективності діючої підсистеми безпеки компанії. Як наслідок, знижується ефективність процесу УІІБ, що негативно впливає на забезпечення ІБ компанії в цілому.

Яким же чином можна істотно підвищити ефективність процесу УІІБ? Перш за все, необхідно визначити показники ефективності. Ефективність процесу управління інцидентами залежить від:

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

Підвищення кожного з наведених показників буде сприяти зростанню ефективності усього процесу УІІБ. Радикально змінити ситуацію з управління інцидентами можна, використовуючи СМІБ.

Ця система надає можливість:

- консолідувати всю інформацію про інциденти в єдиному сховищі;
- створити єдиний центр УІІБ з метою забезпечення контролю і координації дій з локалізації і розслідування;
- підвищити швидкість реагування і оперативність виявлення причин інциденту;
- підвищити достовірність одержуваних результатів з виявлення причин інциденту, відповідальних осіб і визначення необхідних дій, усунення наслідків інциденту і застосування контрзаходів;
- формувати статистику інцидентів ІБ, виявляти тенденції її змін і аналізувати динаміку цих змін;

- автоматизувати застосування контрзаходів для зниження ризику ІБ з виявлення типових інцидентів.

Таким чином, система фактично буде системою колективної роботи, яка автоматизує процеси з УІІБ, за допомогою інтеграції людей і апаратно-програмного забезпечення моніторингу і захисту, а також інформаційної інфраструктури організації.

Опишемо ознаки інциденту інформаційної безпеки. Припущення про те, що в організації стався ІІБ, має базуватися на трьох основних групах порушень:

1) Можливі порушення вимог конфіденційності:

- інциденти, через які отримано несанкціонований доступ до інформації;
- втрата носіїв інформації за межами приміщення;
- втрата або крадіжка ноутбука;
- спроби персоналу організації отримати доступ вище наданого рівня;
- спроби зсередини або ззовні отримати доступ до систем (злам).

2) Можливі порушення вимог цілісності:

- втрата даних або незавершені транзакції;
- віруси, «троянські коні» (зловмисне ПЗ);
- пошкоджені сектори на жорстких дисках, помилки парності і пам'яті;
- невірні контрольні суми або значення хеш-функцій.

3) Можливі порушення вимог доступності:

- зупинка роботи протягом неприйнятного періоду часу. Якщо зупинка триває довше, ніж обумовлено в SLA, і не може бути усунена протягом певного часу, набирає чинності надзвичайний план;
- віруси, «троянські коні»;
- крадіжка ноутбуків, комплектуючих або носіїв інформації.

Проаналізуємо інциденти інформаційної безпеки. Інцидент назавжди відбувається відкрито. Навпаки, зловмисники намагаються зробити все, щоб не залишити в системі слідів своєї діяльності. Прийняття рішення про настання події інциденту багато в чому залежить від компетентності експертів команди

реагування. Необхідно відрізняти випадкову помилку оператора від зловмисного цілеспрямованого впливу на інформаційну систему. Керівництво організацій повинно звернути увагу на цю обставину і надати експертам команди реагування певну свободу дій.

Складання діагностичних матриць служить для візуалізації результатів аналізу подій, що відбуваються в інформаційний системі. Така матриця формується з рядків потенційних ознак інциденту та стовпців – типів інцидентів. Дається оцінка події за шкалою пріоритетів «високий», «середній» та «низький». Діагностична матриця покликана документувати процес логічних висновків експертів під час прийняття рішення і, поряд з іншими документами, використовується для розслідування інциденту.

При аналізі ІІБ організація повинна виконати таке:

- своєчасно ідентифікувати невдалі та успішні порушення безпеки і інциденти безпеки;
- допомогти у виявленні подій безпеки, таким чином запобігти інцидентам безпеки шляхом використання індикаторів.

Таким чином, УІІБ передбачає проведення таких заходів:

1) Повідомлення про події інформаційної безпеки. Ці повідомлення повинні якомога швидше поширюватися належними управлінськими каналами.

2) Повідомлення про уразливості захисту. Необхідно зобов'язати всіх співробітників, підрядчиків і користувачів із сторонніх організацій, що використовують інформаційні системи та сервіси, відмічати і повідомляти про всі спостережувані або передбачувані уразливості захисту систем або сервісів.

3) Відповідальність і процедури. Необхідно встановити відповідальність керівників та визначені процедури для забезпечення швидкого, ефективного і правильного реагування на інциденти інформаційної безпеки.

4) Навчання інцидентам ІБ. Повинні бути реалізовані механізми, які надають можливість виміряти та відстежувати типи, об'єми і вартість ІІБ.

5) Збір доказів. Якщо в результаті аналізу ІІБ встановлено, що дії осіб потребують правової кваліфікації, то необхідно зібрати, зберегти та надати

докази такої протиправної діяльності у встановленому правовою системою певної країни порядку.

Отже, підсумовуючи все, наведене вище, можна зробити висновок про важливість дослідження теоретичних та прикладних засад управління інцидентами інформаційної безпеки. Нами визначено поняття інформаційної безпеки та процес її забезпечення, наведено класифікацію джерел інцидентів інформаційної безпеки, на окреслено сучасні підходи до управління інцидентами інформаційної безпеки.

РОЗДІЛ 2.
АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Аналіз стандартів, рекомендацій та світових практик щодо управління інцидентами інформаційної безпеки

На сьогодні у міжнародній практиці є достатня кількість нормативних документів, якими регламентуються питання УІІБ. Варто відзначити, що питання УІІБ виникає не тільки в процесі забезпечення інформаційної безпеки, але й при управлінні IT-сервісами у цілому. Серія міжнародних стандартів ISO 20000 у розділі Service Delivery & Support описує низку вимог до організації процесу управління інцидентами в IT-інфраструктурі. Специфічні питання УІІБ розглядаються та регламентуються такими міжнародними та національними нормативними документами.

ISO 20000. Як уже зазначалось, у розділі «Service Delivery & Support» цього стандарту описується низка вимог до організації процесу управління інцидентами в IT-інфраструктурі. Слід зазначити, що у новій версії цього стандарту ISO 20000:2011 було істотно переопрацьовано розділ управління інцидентами, визначено стандартний перелік процедур. Розділ розширився і став більш подібним до ITIL v3. Управління інцидентами тепер охоплює ще й управління запитами на обслуговування (Service Request).

ISO/IEC 27001. У цьому стандарті розглядаються загальні вимоги до створення, впровадження, експлуатації, моніторингу, аналізу, підтримки і вдосконалення документованої СМІБ, що стосуються зокрема й процесів управління інцидентами. Він визначає вимоги до здійснення контролю безпеки та призначений для задоволення потреб окремих організацій або їх структур.

ISO/IEC 27035 (який замінив свого попередника **ISO/IEC 18044** у 2011 р.).

Документ описує інфраструктуру управління інцидентами в рамках циклічної моделі PDCA. Наводяться детальні специфікації для етапів планування, експлуатації, аналізу й удосконалення процесів. Розглядаються питання забезпечення нормативно-розпорядчою документацією, ресурсами, надаються детальні рекомендації щодо необхідних процедур.

CMU/SEI-2004-TR-015. Цей документ описує методологію планування, впровадження, оцінки й удосконалення процесів управління інцидентами. Основний наголос робиться на організації роботи CISRT (Critical Incident Stress Response Team) – групи або підрозділів, які забезпечують сервіс і підтримку запобігання, обробки і реагування на ІІБ. Вводиться низка критеріїв, на підставі яких можна оцінювати ефективність цих сервісів, надаються детальні моделі процесів.

NIST SP 800-61. Цей стандарт містить збірку «кращих практик» щодо побудови процесів управління інцидентами і реагування на них. Детально розбираються питання реагування на різні типи загроз, такі як розповсюдження шкідливого ПЗ, несанкціонований доступ та ін.

ITU-T X-1051. У розділі «Information Security Incident Management» цього стандарту містяться вказівки щодо визначення слабких сторін в інформаційній безпеці та удосконалення УІІБ.

ITU-T E.409. Метою цих рекомендацій є аналіз, структурування методів для створення підрозділу управління інцидентами всередині підприємства електрозв'язку, що бере участь у забезпеченні міжнародного електрозв'язку (в центрі уваги цього підрозділу знаходяться перебіг і структура інциденту). Поняття «потік» і «обробка» використовуються у випадку необхідності класифікувати яку-небудь подію як «подія», «інцидент», «інцидент безпеки» або «криза». Ці рекомендації містить огляд і рамкові положення, які є дороговказом для планування діяльності щодо реагування на інциденти та обробки інцидентів безпеки. Варто також зауважити, що ці рекомендації мають загальний характер, у них не визначаються і не розглядаються вимоги для конкретних мереж і підприємств.

ГОСТ Р ІСО/МЕК 18044. Цей стандарт РФ визначає рекомендації з УІБ для керівників підрозділів інформаційної безпеки. Фактично повністю відповідає міжнародному стандарту ISO/IEC 18044, про який уже йшла мова, що у міжнародній практиці був замінений стандартом ISO/IEC 27035.

Зауважимо, що всі ISO/IEC серій 9000, 14000, 20000, 27000 та інші стандарти ISO/IEC, що описують правила створення систем управління різними процесами, гармонійно поєднуються один з одним. Всі вони ґрунтуються на процесному підході, який розглядає управління як процес, а саме як набір взаємозв'язаних безперервних дій. Процесний підхід акцентує увагу на досягненні поставлених цілей, а також на ресурсах, витрачених для цього. Крім цього, стандарти вказаних серій використовують модель PDCA як структуру життєвого циклу всіх процесів системи управління.

Тому природно, що ISO 20000, описує як систему управління IT-сервісами, так і процедуру управління інцидентами, але також розглядає IT-інциденти. Сама процедура управління інцидентами IT дуже близька до процедури УІБ з тією лише різницею, що в останньому випадку більше акцент робиться на його розслідуванні, збиранні доказів, покаранні винних (або звернення до суду). Це ще раз свідчить про те, що доцільно розробляти одну систему управління всіма процесами в компанії, оскільки управління схожими процесами в різних сферах діяльності однієї компанії часто відбувається за однією схемою.

Варто також зазначити, що неможливо провести вичерпний аналіз усіх наявних рекомендації щодо УІБ, оскільки їх дуже багато на різних рівнях і в різних галузях промисловості. Цілком ймовірно, що найбільш ефективним для конкретної організації буде використання якої-небудь іншої методології, у тому числі і розробленої самостійно (IT-департаментом чи департаментом інформаційної безпеки). Але будь-яка використовувана методологія не повинна суперечити вимогам сучасних міжнародних нормативних документів.

2.2. Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035

Як зазначалося вище, особливістю інцидентів інформаційної безпеки є те, що вони не завжди помітні (не завжди заважають роботі користувачів), проте можливий збиток від таких інцидентів складно недооцінити. Тому важливо, щоб жоден ІІБ не залишився непоміченим, було проведено розслідування, виявлені винні, і, найголовніше, проведені корегувальні і запобіжні заходи. Отже, необхідна чітка процедура реєстрації та розслідування інцидентів безпеки, а також інформування користувачів про правила виявлення інцидентів.

Необхідно усвідомлювати, що УІІБ не запобігає нанесенню збитку компанії (як правило, компанія вже понесла збиток, пов'язаний з інцидентом), проте розслідування інциденту і своєчасне впровадження превентивних та корегувальних заходів знижує ймовірність його повторення (і, отже, ймовірність повторного нанесення збитку). Відзначимо також, що статистика інцидентів інформаційної безпеки має особливу цінність для компанії як показник ефективності функціонування системи управління інформаційною безпекою. Статистику інцидентів слід регулярно аналізувати під час аудиту системи управління інформаційною безпекою.

Опишемо дії, які необхідно виконати для розробки ефективної процедури УІІБ. Насамперед необхідно, щоб процес розробки процедури (як і всіх процедур в компанії) був ініційований її керівництвом. Як правило, процедура управління інцидентами розробляється в межах загальної системи управління інформаційною безпекою, тому важлива позиція керівництва з питань створення та функціонування такої системи. На даному етапі важливо, щоб всі співробітники компанії розуміли, що забезпечення інформаційної безпеки в цілому і управління ІІБ зокрема є основними бізнес-цілями компанії.

На другому кроці розробляють необхідні нормативні документи з УІІБ. Як правило, такі документи повинні описувати:

- визначення ІІБ, перелік подій, що є інцидентами (які є інцидентом саме в цій компанії);

- порядок оповіщення відповідальних осіб про виникнення інциденту (необхідно визначити формат оповіщення, а також відобразити контактну інформацію осіб, яких треба оповіщати про інцидент);
- порядок усунення наслідків і причин ІІБ;
- порядок розслідування ІІБ (визначення причин інциденту, винних у виникненні інциденту, порядок збору та збереження доказів);
- накладання дисциплінарних стягнень;
- реалізацію необхідних корегувальних і превентивних заходів.

Визначення переліку подій, що є інцидентами, є важливим етапом розробки процедури УІІБ. Адже всі події, які не увійдуть до зазначеного переліку, будуть розглядатися як штатні (навіть якщо вони складають загрозу інформаційній безпеці). Зокрема, ІІБ в компанії можуть бути:

1) відмова в обслуговуванні сервісів, засобів обробки інформації, обладнання;
2) порушення конфіденційності та цілісності цінної інформації;
3) недотримання вимог інформаційної безпеки, прийнятих в компанії (порушення правил обробки інформації);
4) незаконний моніторинг інформаційної системи;
5) виявлення шкідливих програм;
6) компрометація інформаційної системи (наприклад, розголошення пароля користувача).

Іншими прикладами інцидентів є неавторизована зміна даних на сайті компанії, залишення комп'ютера незаблокованим без нагляду, пересилання конфіденційної інформації за допомогою корпоративної або особистої пошти.

Оскільки інцидентом, насамперед, вважається недозволена подія, вона має бути кимось заборонена. Отже, необхідно мати документи, які чітко описують всі дії, які можна виконувати в системі і які виконувати заборонено. Наприклад, в одній з компаній співробітник зберігав на мобільному комп'ютері конфіденційні відомості компанії без застосування засобів шифрування. Після роботи він забрав комп’ютер додому і забув його в машині, яку залишив під

вікнами будинку, а вночі машину зламали, і комп'ютер був вкрадений. Зловмисники отримали доступ до конфіденційної інформації компанії і могли продати її конкурентам. Крім цього, на комп'ютері зберігалася цінна інформація, яка не була зарезервована на іншому носії. Такий інцидент міг статися внаслідок того, що в компанії не були розроблені процедури поводження з мобільними комп'ютерами та порядок зберігання на них інформації. Переміщення комп'ютера за межі офісу, відсутність засобів шифрування і резервного копіювання інформації - можливі порушення, а отже, причини інцидентів. Однак поки документально не зафіксовано, що це порушення (тобто у відповідних документах не описано, що це заборонено), співробітника неможливо притягнути до відповідальності і запобігти повторному виконанню неправомірних дій.

Важливо, щоб були налагоджені такі процедури, як моніторинг подій, своєчасне видалення облікових записів, що не використовуються контроль і моніторинг дій користувачів, контроль над діями системних адміністраторів та інше.

В одній з компаній був зафіксований такий інцидент. При звільненні з роботи системний адміністратор вкрав розроблений в компанії програмний продукт і передав його конкурентам, які випустили програму на ринок під своїм товарним знаком. Крім цього, він вніс зміни в інформаційну систему, внаслідок яких після його звільнення функціонування певних її компонентів було порушено. Залучити адміністратора до відповідальності в даному випадку виявилося неможливо, оскільки, по-перше, не виконувалася реєстрація його дій, по-друге, адміністратор міг видалити всі докази своїх неправомірних дій і, потретє, не була налагоджена процедура збору доказів про інцидент. Крім цього, в компанії просто не знали, як слід чинити в таких випадках (зокрема, можна було звернутися в спеціалізовану компанію з розслідування інцидентів або подати заяву до суду).

Для опису процесу формування СМІБ використовується класична модель безперервного удосконалення процесів (рис. 4.1), що отримала назву від циклу

Шухарта-Демінга - модель PDCA (Плануй, Plan - Виконуй, Do - Перевіряй, Check - Дій, Act).

Рис.2.1. Етапи формування СМІІБ відповідно до моделі PDCA

Стандарт ISO/IEC 27001 описує модель PDCA як основу функціонування всіх процесів системи управління інформаційною безпекою. Природно, що і процес управління інцидентами підпорядковується моделі PDCA (рис. 4.2) – це чітко задекларовано в стандарт ISO/IEC 27035. Розглянемо цю модель для УІІБ більш детально.

1. Виявлення та реєстрація інциденту. Інцидент інформаційної безпеки може помітити користувач або адміністратор системи. Як правило, адміністратори знають, що слід робити у випадку виявлення інцидентів, чого не завжди можна сказати про користувачів. Для користувачів доцільно розробити інструкцію, яка буде містить опис, в якому вигляді співробітник повинен повідомити про виникнення інциденту, координати відповідальних осіб, а також перелік дій, які співробітник може виконати самостійно (або попереджений, що виконувати будь які дії самостійно заборонено).

Звіт користувача про інцидент повинен містити його детальний опис, перелік співробітників, залучених до інциденту, прізвище співробітника, який виявив інцидент, дату виникнення та реєстрації інциденту. Таким чином, кожен співробітник отримує інструкцію, що визначає, як діяти, наприклад, у випадку, якщо він продовжив роботу з документом і помітив, що з минулого разу в його документ були внесені зміни, які не відповідають дійсності, при цьому автору зміни невідомі.

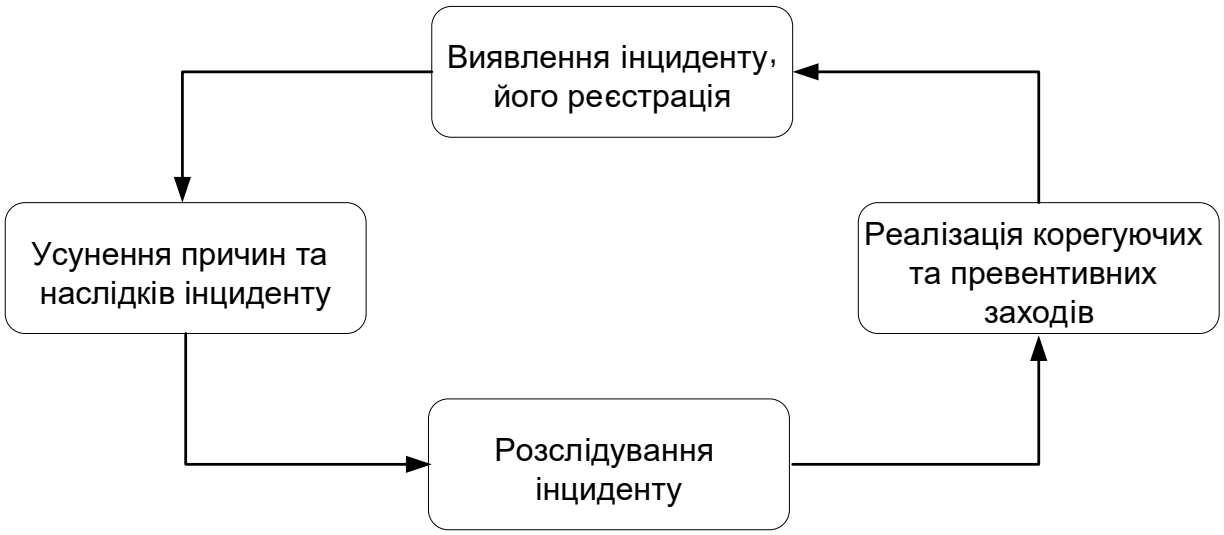

Рис. 2.2. Модель життєвого циклу процесу УІІБ

Також необхідно розробити інструкцію для фахівця, обов'язком якого є реєстрація інцидентів. Співробітник, який виявив інцидент, зв'язується зі співробітником, відповідальним за реєстрацію інцидентів і виконання подальших дій. У невеликих компаніях співробітники звертаються безпосередньо до фахівця, який може усунути наслідки і причини інциденту (наприклад, до системного адміністратора або адміністратора безпеки). У досить великих компаніях, як правило, виокремлюють співробітника, який реєструє інцидент і передає інформацію про інцидент відповідним фахівцям. Така інструкція може містити, наприклад, правила і термін реєстрації інциденту, перелік необхідних первинних інструкцій для співробітника, що виявив інцидент, крім того, опис порядку передачі інформації про інцидент

відповідному фахівцю, порядок контролю над усуненням наслідків і причин інциденту.

2. Усунення причин, наслідків інциденту і його розслідування. Інструкція щодо усунення причин та наслідків інциденту включає загальний опис заходів, які необхідно вжити (конкретні дії для кожного виду інциденту визначати складно і не завжди доцільно), а також терміни, протягом яких слід усунути наслідки і причини інциденту. Терміни усунення наслідків і причин інциденту залежать від рівня інциденту. Доцільно розробити класифікацію інцидентів, визначити кількість рівнів критичності інцидентів, описати інциденти кожного рівня і терміни їх усунення. Документ, що визначає, які події в компанії слід вважати інцидентом, також може описувати рівні інцидентів. Таким чином, інструкція з усунення наслідків і причин інциденту може містити: опис заходів, які вживаються для усунення наслідків і причин інциденту, терміни усунення і відомості про відповідальність за недотримання інструкції.

3. Розслідування інциденту Цей етап передбачає визначення винних у його виникненні, збір доказів інциденту, накладення відповідних дисциплінарних стягнень. У великих компаніях, як правило, виділяють комісію з розслідування інцидентів інформаційної безпеки (до складу якої може входити співробітник, який реєструє інциденти). Інструкція з розслідування інцидентів повинна описувати: заходи щодо розслідування інциденту (у тому числі визначення винних), правила збору і зберігання доказів (особливо у випадку, якщо ситуація потребує використання доказів у судових органах) і правила накладення дисциплінарних стягнень.

4. Корегувальні та запобіжні заходи. Після усунення наслідків інциденту і відновлення нормального функціонування бізнес-процесів компанії, доцільним є проведення заходів щодо запобігання повторного виникнення інциденту. Для визначення необхідності реалізації таких заходів слід провести аналіз ризиків, в рамках якого визначається доцільність корегувальних і превентивних дій. У деяких випадках наслідки інциденту будуть незначними у

порівнянні з корегувальними і запобіжними заходами, і тоді доцільно не здійснювати подальших кроків після усунення наслідків інциденту.

Для того, щоб процедура УІІБ було ефективною, всі ці етапи моделі PDCA повинні безперервно і послідовно повторюватися. Через певний час (як правило, через півроку або рік) необхідно знову переглянути перелік подій, названих інцидентами, форму звіту та ін., впровадити оновлену процедуру, перевірити її функціонування і ефективність, реалізувати запобіжні заходи. Таким чином, цикл моделі PDCA буде безперервно повторюватися і гарантувати чітке функціонування процедури управління інцидентами і, головне, її постійне удосконалення.

2.3. Методичні підходи до формування концепції та структури автоматизованої системи управління інцидентами інформаційної безпеки

Для ефективного функціонування СМІБ необхідно на стадії її впровадження забезпечити вирішення низки ключових питань. Насамперед, СМІБ повинна бути забезпечена вхідним потоком подій інформаційної безпеки, що адекватно відображав би стан ІБ сфери, на яку поширюється дія СМІБ. При виявленні і реагуванні на інцидент, необхідно мати дані щодо задіяних активів, їх власників і ступеню критичності. При розслідуванні інцидентів необхідно мати доступ до подій інформаційної безпеки, що вплинули на інцидент, таких як дані аудиту дій користувачів і адміністраторів. При аналізі інцидентів, наданні звітів керівництву необхідно мати можливість зіставлення активів, що потрапили під вплив інциденту, і ризиків для основних бізнес-процесів організації.

Таким чином, визначаючи сферу дії СМІБ і черговості етапів її впровадження, необхідно вибирати звернути увагу насамперед на такі процеси:

- інвентаризацію активів;
- аналіз ризиків;
- моніторинг подій інформаційної безпеки;

– аудит дій користувачів і адміністраторів в інформаційних системах.

Опишемо концептуальні засади впровадження СМІБ. Впровадження СМІБ відбувається у декілька етапів. На першому етапі проводиться обстеження об'єкту. На цьому етапі здійснюється збір й аналіз інформації щодо наявних та використовуваних на цей момент регламентів, процедур і засобів забезпечення інформаційної безпеки, управління інцидентами. Виявляються джерела подій інформаційної безпеки, збираються відомості щодо використовуваних інформаційних систем і технологій обробки інформації. Визначається сфера, на яку буде поширюватись дія системи управління інцидентами інформаційної безпеки. Розробляються документи «Завдання щодо розробки системи управління інцидентами інформаційної безпеки» і «Технічне завдання на автоматизовану систему моніторингу й управління інцидентами інформаційної безпеки».

На другому етапі здійснюється розробка процесів СМІБ, написання відповідних документів (перелік яких обумовлений «Завданням…»). На цьому етапі здійснюється ескізне проектування автоматизованої системи, визначаються основні технічні рішення, розробляється перелік необхідного програмного і апаратного забезпечення.

На третьому етапі здійснюється впровадження СМІБ. Проводиться навчання персоналу, розподіл ролей, інтеграція системи управління з іншими процесами управління інформаційною безпекою. На цьому етапі здійснюється техніко-робоче проектування автоматизованої системи.

На четвертому етапі здійснюється впровадження автоматизованої системи моніторингу й управління інцидентами інформаційної безпеки..

Перший крок побудови процесно-ролевої моделі управління системою ІБ – це складання та/або аналіз бази елементарних одиниць, що містить активи системи інформаційної безпеки – ПЗ, апаратне забезпечення, співробітники і процедури (Configuration Management Database, CMDB). Насамперед, необхідно визначити існуючі активи та процеси в організації, а потім проаналізувати ключові з них, які потребують удосконалення. Як правило, більшість

організацій починають з організації служби Service Desk і впровадження процесу УІІБ. Необхідно зосередити пріоритети впровадження процесів і співвіднести їх з планами створення СМІБ. Всі послуги повинні забезпечувати дотримання суворих корпоративних стандартів захисту інформації.

З часом у процесі розширення сфери використання інформаційних систем та їх ускладнення, проблема забезпечення інформаційної безпеки загострюється. Безпеку вже неможливо забезпечити одним лише набором технічних засобів і підтримувати тільки силами підрозділу безпеки. Відсутність систематичного оцінювання інформаційних ризиків, недостатня поінформованість співробітників про правила роботи з інформацією, що потребує захисту, недотримання режиму інформаційної безпеки, відсутність формалізованої класифікації інформації за ступенем її критичності і вартістю інформаційних активів – все це може звести нанівець зусилля організації щодо забезпечення інформаційної безпеки. Із зростанням ролі інформаційних систем у підтримці основних бізнес-процесів організації до цих проблем додаються питання забезпечення безперервності функціонування бізнесу в критичних ситуаціях.

Завданням СМІБ є систематизація процесів забезпечення інформаційної безпеки, розташування пріоритетів організації в галузі інформаційної безпеки, досягнення адекватності системи ІБ існуючим ризикам, досягнення її прозорості. Останнє набуває особливої важливості, оскільки дозволяє чітко визначити, як взаємозв'язані процеси і підсистеми ІБ, хто за них відповідає, які фінансові і кадрові ресурси необхідні для їх забезпечення та ін.

У цілому, процес управління безпекою відповідає за планування, виконання, контроль і технічне обслуговування всієї інфраструктури безпеки. Організація цього процесу ускладнюється також тією обставиною, що забезпечення інформаційної безпеки компанії пов'язане не тільки із захистом інформаційних систем і бізнес-процесів, які підтримуються цими інформаційними системами.

При цьому виникають такі питання. Як побудувати ефективну СМІБ, яка б інтегрувалася в загальну систему управління ІТ? Як виділити і описати процеси забезпечення інформаційної безпеки? Як забезпечити виявлення інцидентів (нештатних ситуацій) в системі інформаційної безпеки і як на них реагувати? Як визначити, чи вплине цей інцидент на інші процеси і працездатність інформаційних систем і яким буде цей вплив? Що зробити, щоб в майбутньому ця ситуація не повторилася?

У світовій практиці для відповіді на ці питання розроблені моделі СМІБ, наприклад, «Information Security Management Maturity Model» (ISM3 від ISECOM) або Systems Security Engineering Capability Maturity Model» або стандарт NIST SP 800-33. Існує також низка міжнародних стандартів, про які вже згадувалось.

Проте пряме використання цих моделей і стандартів ISO/IEC 27001 та ISO/IEC 27002 для побудови СМІБ досить складне. Вони або дуже

конкретизовані, а в будь-якій організації, як правило, вже існує певна система процесів, ролей, організаційно-розпорядчих документів інформаційної безпеки, які необхідно інтегрувати в систему управління інформаційною безпекою. Або, навпаки, рекомендації мають дуже загальний характер.

Підхід до побудови СМІБ, зокрема й розробку процесів УІБ, може грунтуватися на таких методичних рекомендаціях і директивах:

рекомендаціях ITIL, а також моделі управління ІТ-ресурсами та ІТсервісами Microsoft Operations Framework (MOF);

рекомендаціях Microsoft Service Management Function (SMF); - стандарті ISO/IEC 27001.

Доцільність використання рекомендацій з управління ІТ-ресурсами та ІТпослугами (і, насамперед, управління інцидентами, змінами) при побудові СМІБ обумовлена тим, що процеси забезпечення інформаційної безпеки нерозривно пов'язані з процесами захисту, а тому управління інформаційними системами має бути тісно пов’язане з процесами управління ІТ.

Інтеграція процесу управління безпекою в систему процесів управління ІТресурсами та ІТ-послугами і застосування сервісно-ресурсного підходу при побудові СМІБ (коли забезпечення інформаційної безпеки розглядається як сервіс з певним рівнем якості, надання якого забезпечується певними фінансовими, технічними, людськими ресурсами) надає цілу низку переваг.

При цьому процесна модель СМІБ передбачає три рівні процесів:

процеси стратегічного рівня – управління ризиками, управління безперервністю ведення бізнесу, розробка і розвиток політики інформаційної безпеки верхнього рівня;

тактичні процеси – розробка і розвиток процедур інформаційної безпеки, технічної архітектури системи інформаційної безпеки, класифікація ІТресурсів, моніторинг і управління інцидентами;

процеси операційного рівня – управління доступом, управління мережевою безпекою, перевірка відповідності та ін.

Структура автоматизованої системи моніторингу й управління інцидентами інформаційної безпеки

До складу автоматизованої системи моніторингу й управління інцидентами інформаційної безпеки входять такі основні компоненти:

- інтеграційна платформа;
- апаратно-програмні засоби моніторингу і аудиту;
- апаратно-програмні засоби захисту інформації;
- сховище інформації про ІІБ;
- аналітичні інструменти і засоби генерації звітів;
- засоби управління і набуті інтерфейси з користувачами.

Інтеграційна платформа є ядром системи. Вона реалізує функції з інтеграції і взаємодії всіх компонент, що складають систему. Інтеграційна платформа надає:

- інтерфейси для інтеграції засобів моніторингу і аудиту, забезпечуючи збір даних;

- інтерфейси до засобів захисту інформації для оперативної зміни їх конфігурації в інтересах локалізації наслідків інцидентів ІБ;
- інтерфейс до сховища даних;
- сервіси щодо використання аналітичних функцій і засобів генерації звітів.

Основна ціль інтеграційної платформи полягає у забезпеченні чіткої і оперативної координації і взаємодії осіб, що відповідають за реагування на події, пов'язані з ІІБ. Такими особами можуть бути:

- користувачі інформаційних систем організації – повідомлення про ІІБ;
- адміністратори і персонал підрозділів автоматизації – інформування, реагування, локалізація, розбір інцидентів тощо;
- співробітники підрозділів безпеки – реагування, контроль, координація дій щодо усунення, розслідування причин, розробки пропозицій з недопущення повторення інцидентів.

Апаратно-програмні засоби моніторингу і аудиту – засоби, що виконують функції з протоколювання, збору, накопичення та обробки інформації про функціонування інформаційних систем організації. До таких засобів відносяться як вбудовані (штатні засоби операційних систем, додатків, мережевих пристроїв, засобів захисту і автоматизованих систем), так і спеціалізовані засоби (розроблені за технічними завданнями підрозділу інформаційної безпеки, а також спеціалізовані засоби аудиту – сканери безпеки, програмні агенти, сенсори, що збирають інформацію та ін.). Результатом роботи всіх наведених засобів є дані, на основі яких системою автоматично або після їх аналізу експертом приймається рішення щодо настання ІІБ. Дані засоби складають підсистему збору інформації про ІІБ.

Апаратно-програмні засоби захисту в контексті СМІІБ – засоби, які забезпечують локалізацію інцидентів або зменшення збитків. Ці засоби мають механізми, що дозволяють проводити швидку і дистанційну зміну своєї конфігурації або мати в своєму складі наперед розроблені автоматизовані сценарії дій з мінімізації можливого збитку від ІІБ.

Сховище інформації про ІІБ – це предметно орієнтований, інтегрований, незмінний набір даних, що підтримує хронологію і здатний бути комплексним джерелом достовірної інформації для оперативного аналізу та прийняття рішень щодо ІІБ.

Аналітичні інструменти і засоби генерації звітів – це інструментарій, що надає користувачам доступ до відповідних баз даних і виконують певний аналіз, формуючи звіти щодо ІІБ. Інструменти цієї категорії поєднують такі можливості: настільний генератор запитів; пакетна генерація регламентних звітів; розсилання звітів та їх оперативне оновлення.

Засоби управління і набуті інтерфейси з користувачами містять комплекс засобів для обробки та відображення інформації, максимально пристосованих для зручності користувачів (клієнтів системи).

РОЗДІЛ 3
ОРГАНІЗАЦІЙНО - ТЕХНОЛОГІЧНІ ПІДХОДИ ДО УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Побудова системи управління інцидентами інформаційної безпеки

Основне завдання SIEM системи – аналізувати реєстровані в інфраструктурі, що захищається, події що надходять від різних джерел, і виявляти атаки/сценарії атак/підозрілі дії/відхилення від норми, формуючи при необхідності відповідні інциденти безпеки.

Базові можливості системи SIEM повинні забезпечувати вирішення наступних завдань:

- збирання та зберігання подій безпеки, що надходять;
- обробка та аналіз зареєстрованих подій безпеки;
- виявлення атак та порушень політик безпеки у реальному часі (близькому до реального часу);
- виявлення та розбір інцидентів безпеки;
- формування звітів.

Крім того, до сучасних рішень класу SIEM пред'являються додаткові вимоги з метою забезпечення наступних функціональних можливостей:

- оцінка захищеності ресурсів контрольованої системи;
- перевірка відповідності системи управління ІБ існуючим вимогам та нормам;
- управління ризиками ІБ та ін.

У прикладі моделюється спрощений сценарій атаки типу «перебір пароля» щодо поставлених навчальних задач. Завдання SIEM системи, що

розробляється, - сповістити адміністратора безпеки про спробу реалізації такої атаки.

1.1 VirtualBox

Виконання цієї частини пропоную проводити на тестовому обладнанні “VirtualBox”.

Тут ми будемо проводити основну частину розробки SIEM системи.

Потрібно перейти на їх основний сайт та завантажити останню версію.

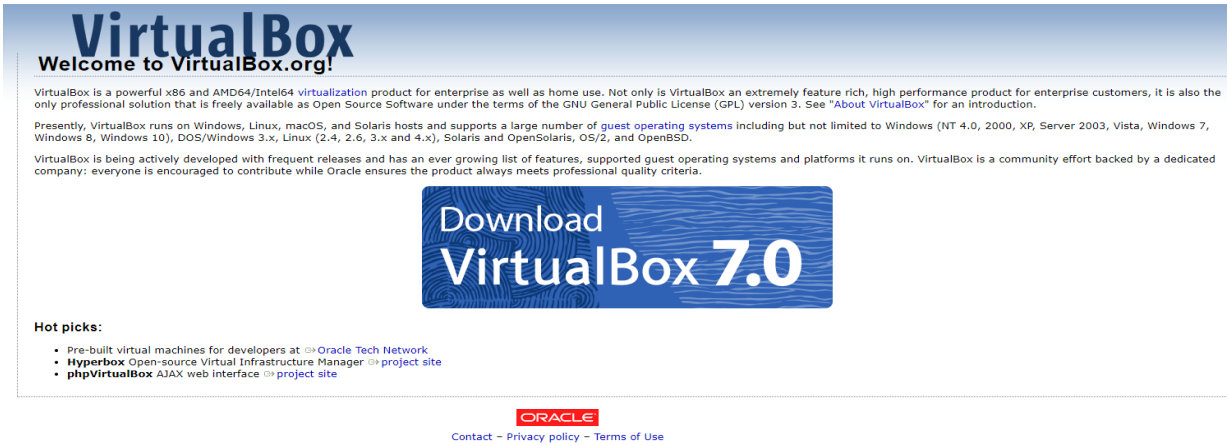

Рис.3.1. Вибір версії та інсталювання «VirtualBox»

Монтуємо образ Windows 7 та ставлю на тестове обладнання.

1.2 Встановлення та налаштування веб-сервера Apache.

Як веб-сервер пропоную використовувати збірку XAMPP for Windows, версія 7.1.9 (Apache 2.4.27 + PHP 7.1.9). Завантажуємо та встановлюємо XAMPP за допомогою інсталятора, обирайте папку для встановлення за замовчуванням – «c:xampp».

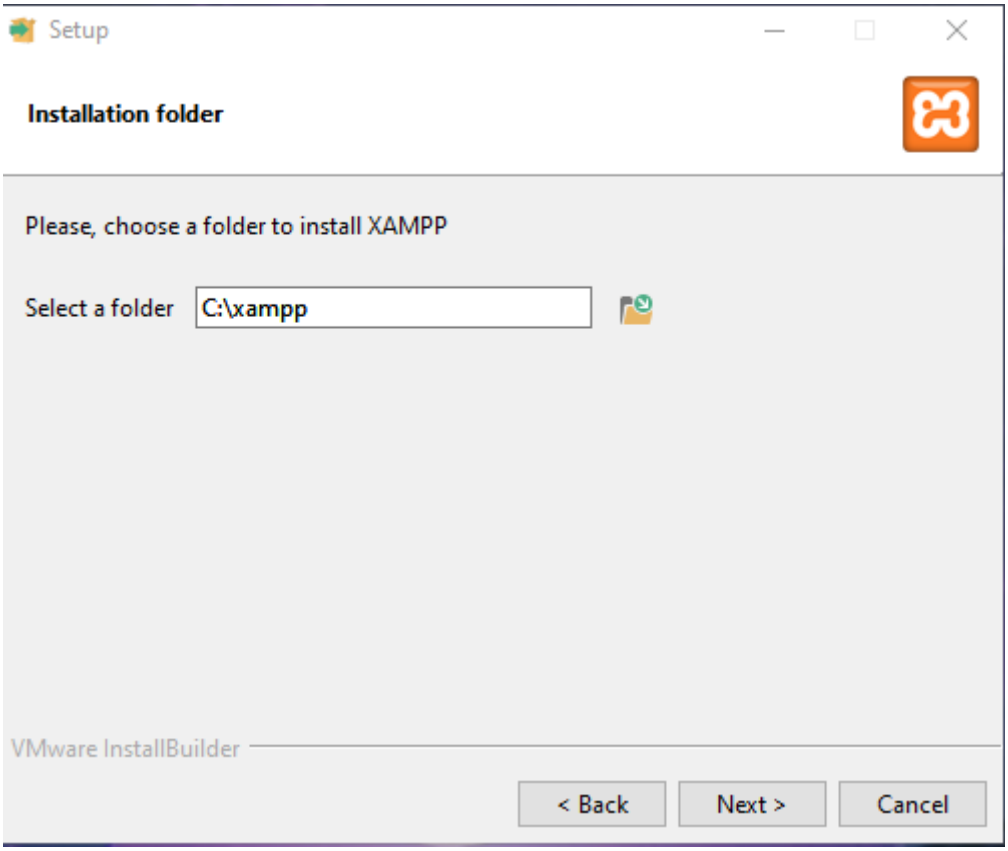

Рис.3.2. Вибір версії та інсталювання «VirtualBox»

Для перевірки правильності встановлення веб-сервера потрібно відкрити панель керування XAMPP Control Panel та запустити модуль Apache. Після цього у браузері за адресою «http://127.0.0.1/» має відкритись вітальна сторінка проекту XAMPP.

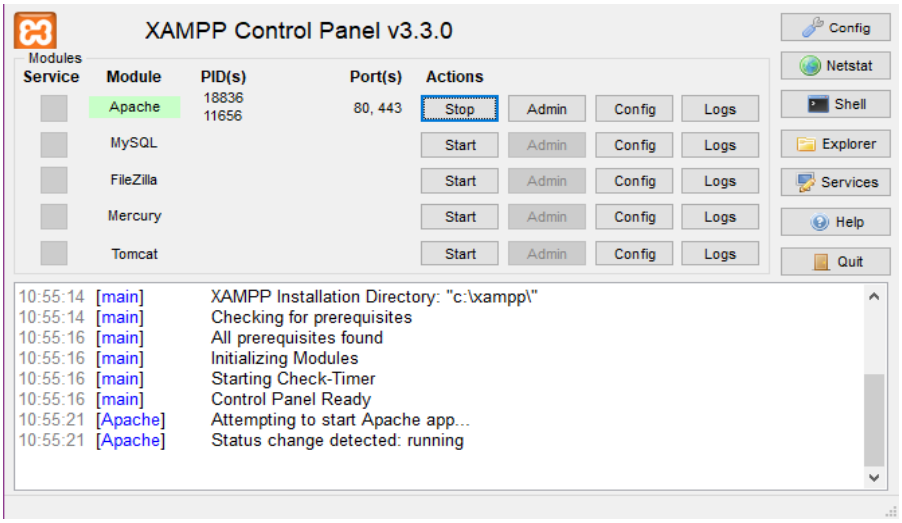

Рис.3.3. Панель керування «XAMPP»

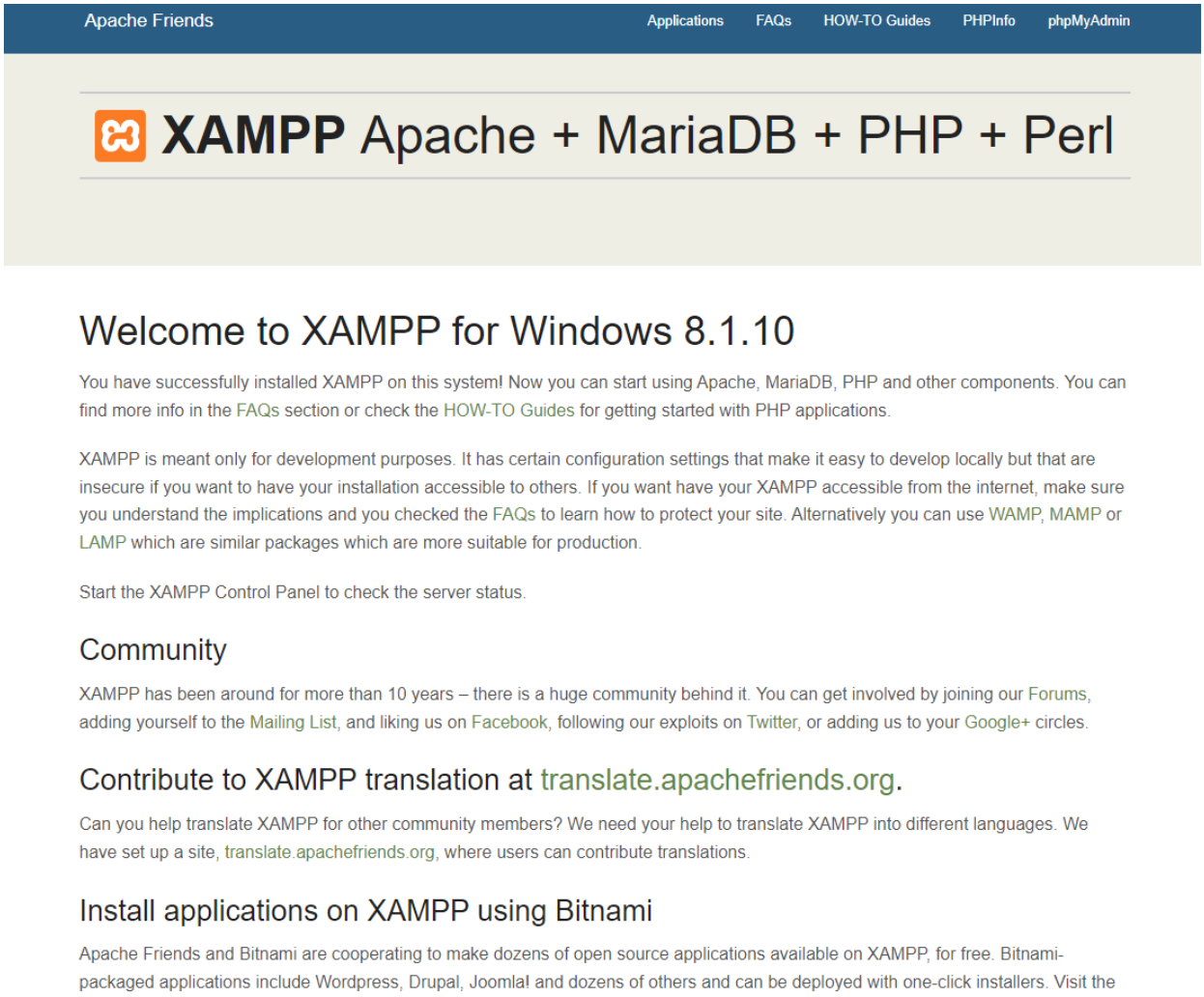

Рис.3.4. Вітальна сторінка «XAMPP»

1.3 Встановлення та налаштування сховища даних MongoDB

Для організації збереження інформації обрано документну базу даних MongoDB. Головною причиною такого вибору є вирішення освітнього завдання , бажання познайомитись з MongoBD а також знайомство з підходами NoSQL. Також прочитавши в інтернеті що більшість провідних виробників разом із традиційними SQL базами даних у своїх рішеннях застосовують технології No SQL/NewSQL.

Переходжу на офіційну сторінку продукту та обираю версію MongoBD Community Server 3.4.10.

Слідуючи інструкції все інсталюємо.

Додатково перевіримо працездатність чи все будо інстальовано без помилок,

створивши в колекції (collection) test новий документ (document) з полем (field) {a:1}.

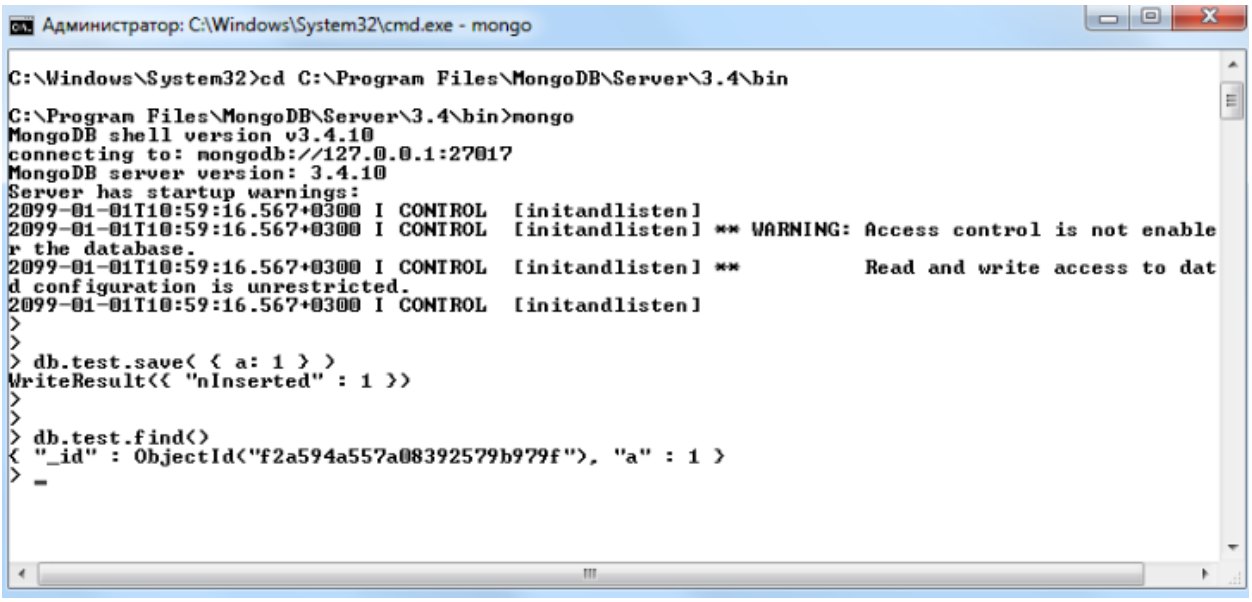

Рис.3.5. Створення тестової колекції

Як бачимо об’єкт знайдено, зробимо висновок що все працює правильно.

Але на всякий випадок давайте проведемо ще одну перевірку, аби унаочнити. Завантажуємо одне з доступних засобів адміністрування Robomongo 1.1.0-Beta, та підключаємо до серверу MongoDB.

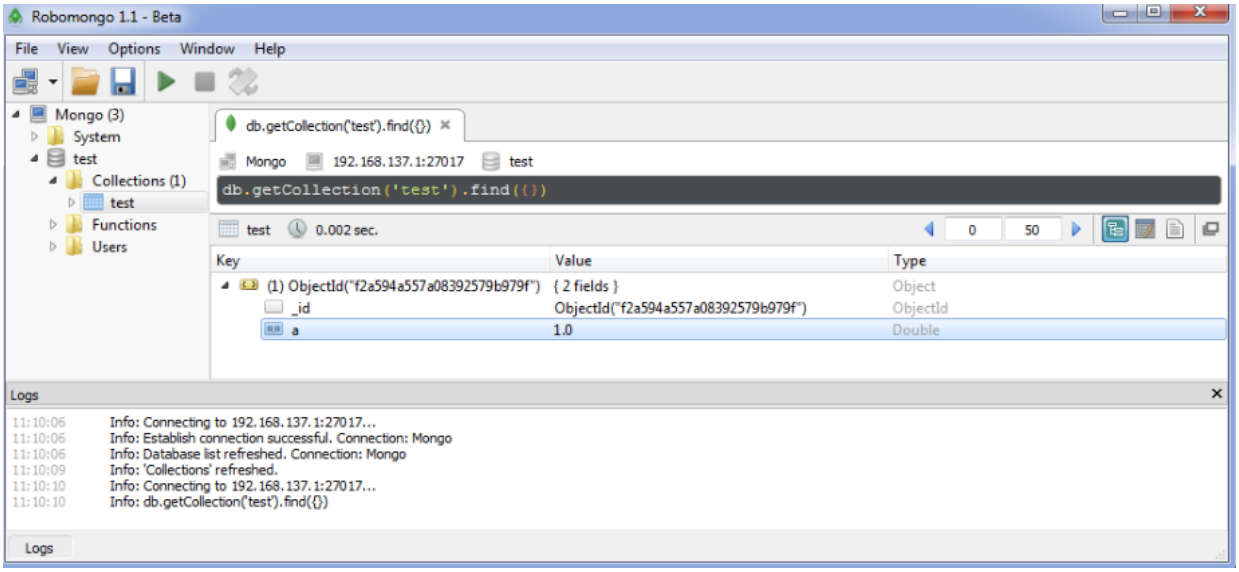

Рис.3.6. Результат створення тестової колекції

Як ви можете зазначити в колекції test є створений документ з полем { a:1 }.

1.4 Встановлення та налаштування брокера повідомлень RabbitMQ

Потрібно ще рішення для організації обміну даними між компонентами системи, тому будемо використовувати RabbitMQ.

Використовуйте офіційну інструкцію по інсталюванню RabbitMQ Server версії 3.7.2, додатково потрібно встановити Erlang версії 20.1.

Інсталятор налаштує RabbitMQ Server як службу. Для подальших перевірок перейдіть в каталог “C:\Program Files\RabbitMQServer\rabbitmq_server-3.7.2\sbin\”.

Для запуску служби використайте команду:

rabbitmq-service start

Та перевірте статус командою:

rabbitmqctl status

Для візуального контролю за функціонуванням брокера повідомлень підключіть відповідний плагін Management plugin:

rabbitmq-plugins enable rabbitmq_management

Після запуску плагіна в браузері за адресою "http://127.0.0.1:15672/" доступна панель адміністрування.

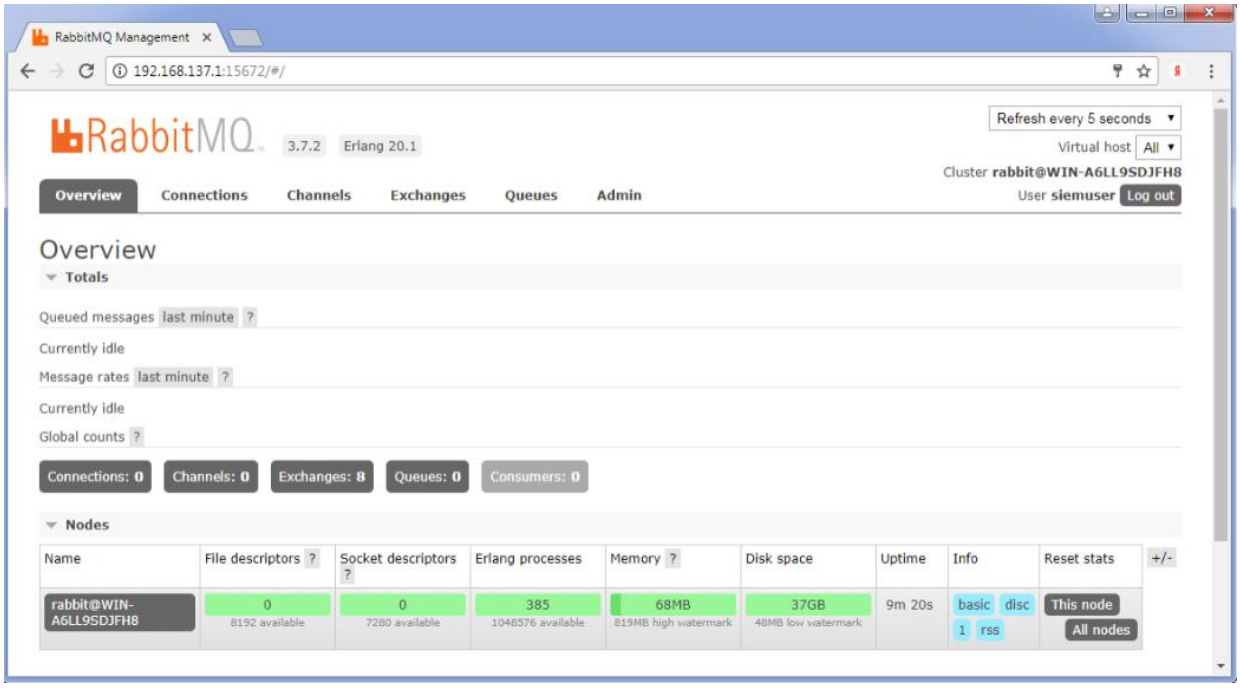

Рис.3.7. Панель адміністрування RabbitMQ

1.5 Встановлення та налаштування середовища розробки Visual Studio Code

Пропонується використовувати мову програмування C#, ця мова програмування легка для розуміння і якщо що можна буде знайти додаткові відповіді на ваші запитання в інтернеті.

Можна використати вже інстальований Visual Studio Code на основній робочій машині.

1.6 Розробка веб-додатку, що захищається Buggy Webapp

Наступним кроком потрібно розробити простенький веб додаток який буде реалізовувати функцію аутентифікації. Верстати макет пропоную за допомогою Bootstrap 4. Для реалізації мовою програмування обрано PHP.

admin.php

C: > Users > Ditolk > Desktop > admin.php

```php
<html>
  <head>
    <meta charset="utf-8">
    <title>Buggy Webapp</title>
    <meta name="viewport" content="width=device-width, height=device-height, initial-scale=1.0" />
    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-beta/css/bootstrap.min.css"
    <script src="https://code.jquery.com/jquery-3.2.1.slim.min.js"></script>
    <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.3/umd/popper.min.js"></script>
    <script src="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-beta.2/js/bootstrap.min.js"></script>
  </head>
  <body>

  <?php
  if (isset($_GET['logged'])) {
    $logged = $_GET['logged'];
  } else {
    $logged = 0;
  }

  $error = 0;
  if (isset($_GET['username']) && isset($_GET['password'])) {
    if (strcmp($_GET['username'], 'admin') == 0 && strcmp($_GET['password'], 'admin') == 0) {

      header('Location: admin.php?logged=1');
      die();
    } else {
      $error = 1;
    }
  }

  if ($logged != 1):
  ?>

    <div class="container py-5">
      <div class="row">
        <div class="col-md-6 mx-auto">

        <?php if ($error == 1): ?>
          <div class="alert alert-danger alert-dismissible fade show" role="alert">
            <strong>ERROR!</strong> Incorrect username or password.
            <button type="button" class="close" data-dismiss="alert" aria-label="Close">
              <span aria-hidden="true">&times;</span>
            </button>
          </div>
        <?php endif; ?>

          <div class="card rounded-0">
            <h3 class="card-header">Log In</h3>
            <div class="card-body">
              <form role="form" action="admin.php" method="get">
                <div class="form-group">
                  <label for="username">Username</label>
                  <input type="text" class="form-control rounded-0" name="username" id="username" placeholde
                </div>
                <div class="form-group">
                  <label for="password">Password</label>
                  <input type="password" class="form-control rounded-0" name="password" id="password" placeh
                </div>
                <button type="submit" class="btn btn-success rounded-0">Log In</button>
              </form>
            </div>
          </div>
        </div>
      </div>
    </div>

  <?php else: ?>

    <div class="container py-5">
      <div class="row">
        <div class="col-md-6 mx-auto">
          <div class="card rounded-0">
            <h3 class="card-header">Dashboard</h3>
            <div class="card-body">
              <p class="card-text">Howdy, <strong>admin</strong>!</p>
              <p class="card-text"><a href="admin.php">Log Out</a></p>
            </div>
          </div>
        </div>
      </div>
    </div>

  <?php endif; ?>

  </body>
</html>
```

Рис.3.8. Код веб-додатку для аутентифікації.

Скрипт admin.php запитує логін та пароль користувача та порівнює їх на відповідність з адміністратором облікового запису (admin\admin). Якщо логін та пароль не співпадають, виводиться повідомлення про помилку.

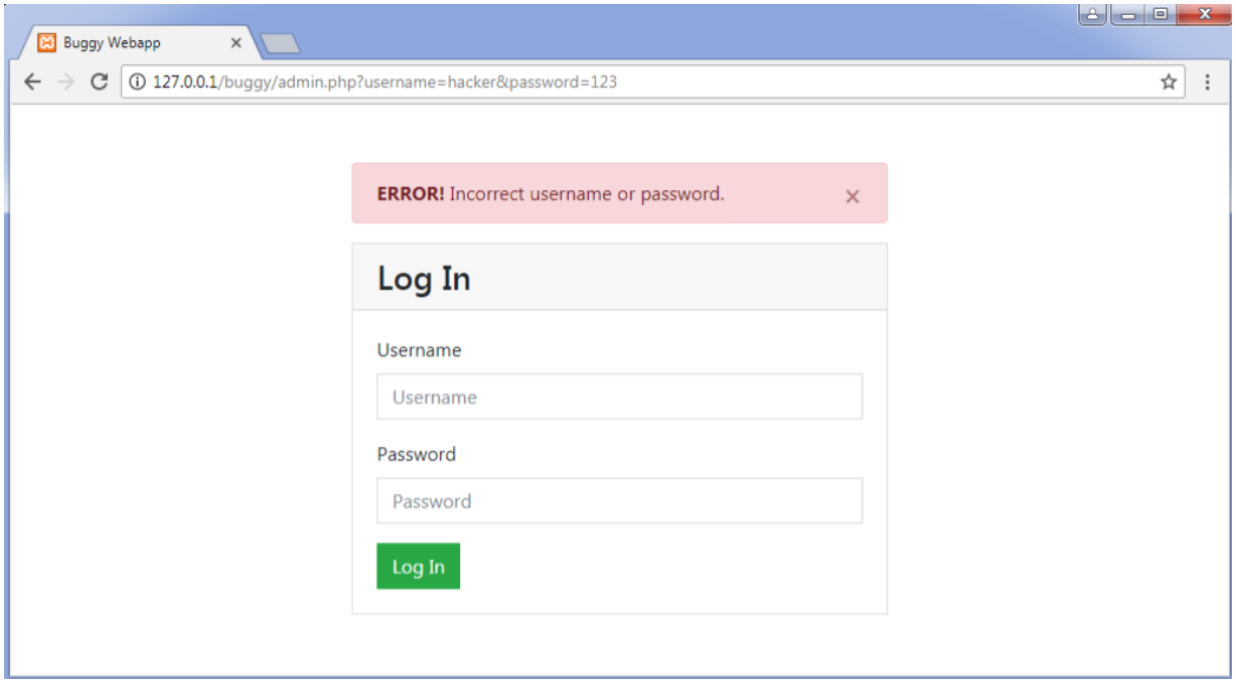

Рис.3.9. Прилад хибно введеного логіна на паролю

У випадку правильно введених логіна та пароля надається доступ до розділу адміністратора.

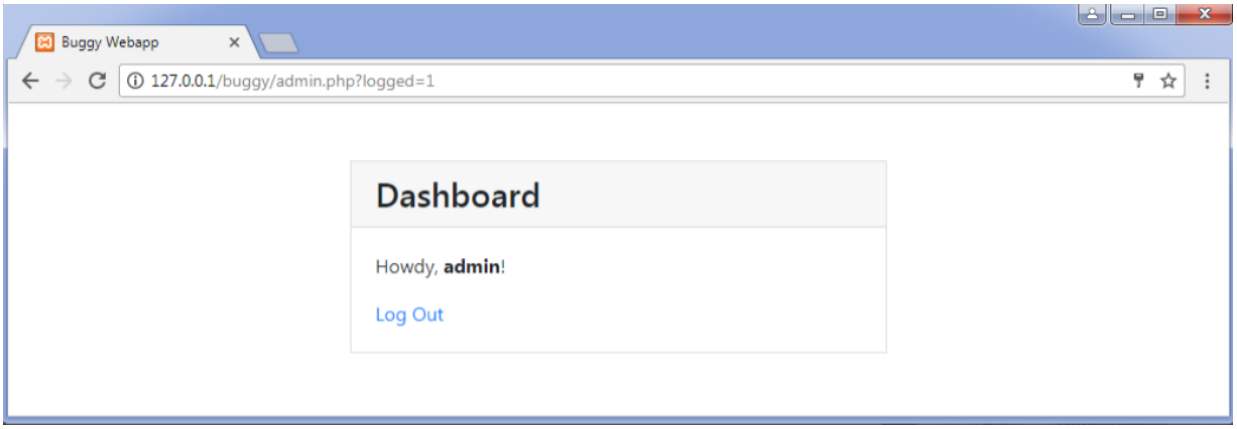

Рис.3.10. Результат правильного введеного логіна на паролю

Зберігаємо файл зі скриптом admin.php у відповідну папку збірки XAMPP

(C:\xampp\htdocs\buggy\admin.php). Після чого з панелі управління XAMPP запускаємо веб-сервер щоб перевірити працездатність та наявність помилок.

1.8 Розробка конектора для веб-сервера Apache

Тепер потрібно зробити журнал доступу до веб-сервера щоб відстежити звернення до веб-додатку, що захищається, щоб мати змогу виявити підозрілі дії користувачів.

Переходимо до журналу звернень до файлу access.log.

(C:\xampp\apache\ logs\access.log).

Після кількох завантажень веб-застосунку в браузері зверніться до вмісту файлу журналу:

127.0.0.1 - - [01/Jan/2099:12:30:39 +0300] "GET /buggy/admin.php?username=hacker&password=123 HTTP/1.1" 200 2040 "http://127.0.0.1/buggy/admin.php" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.91 Safari/537.36

Формат запису визначається у конфігураційному файлі httpd.conf веб-сервера Apache:

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined

CustomLog "logs/access.log" combined

Пропоную взяти вже готовий код конектора ApacheConnector:

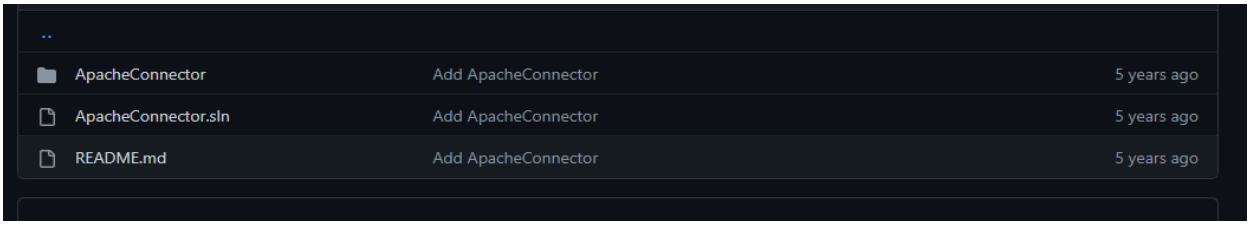

Рис.3.11. Готовий ApacheConnector:

1.На початковому етапі звертаємось до журналу доступу access.log та запам'ятовую розмір файлу.

2. Далі в нескінченному циклі з паузою між ітераціями відстежуйте зміни розміру файлу.

Для складання конектора підключіть до проекту бібліотеку .NET/C# RabbitMQ client library.

Виконаємо тестовий запуск конектора з одночасною перевіркою працездатності брокера повідомлень відповідно до наступного сценарію:

1. Запуск програми ApacheConnector. Конектор починає відстежувати зміни розміру файлу access.log.

2. У браузері кілька разів оновлюємо сторінку веб-програми Buggy Webapp, при цьому журнал доступу веб-сервера буде дописано рядки, що відповідають зверненням браузера до веб-сервера.

3.ApacheConnector виявить зміни розміру файлу і надішле останні рядки в чергу брокера повідомлень RabbitMQ.

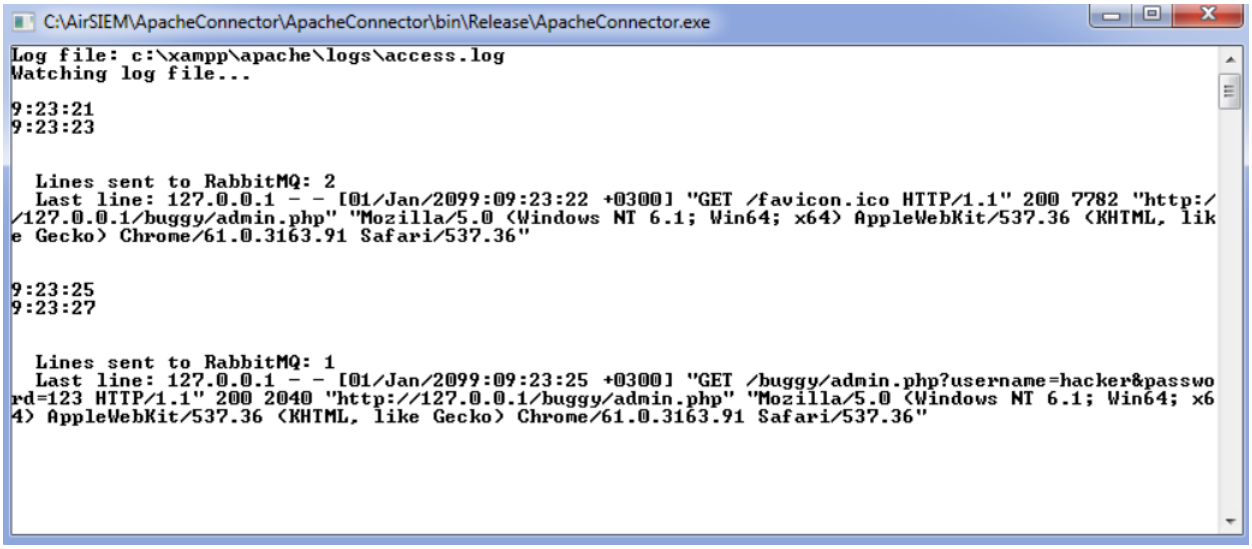

Рис.3.12. Результат зміни розміру файла

Все працює правильно та у панелі адміністрування RabbitMQ маємо виявити додану чергу AirSIEM_ConnectorQueue з ненульовим навантаженням:

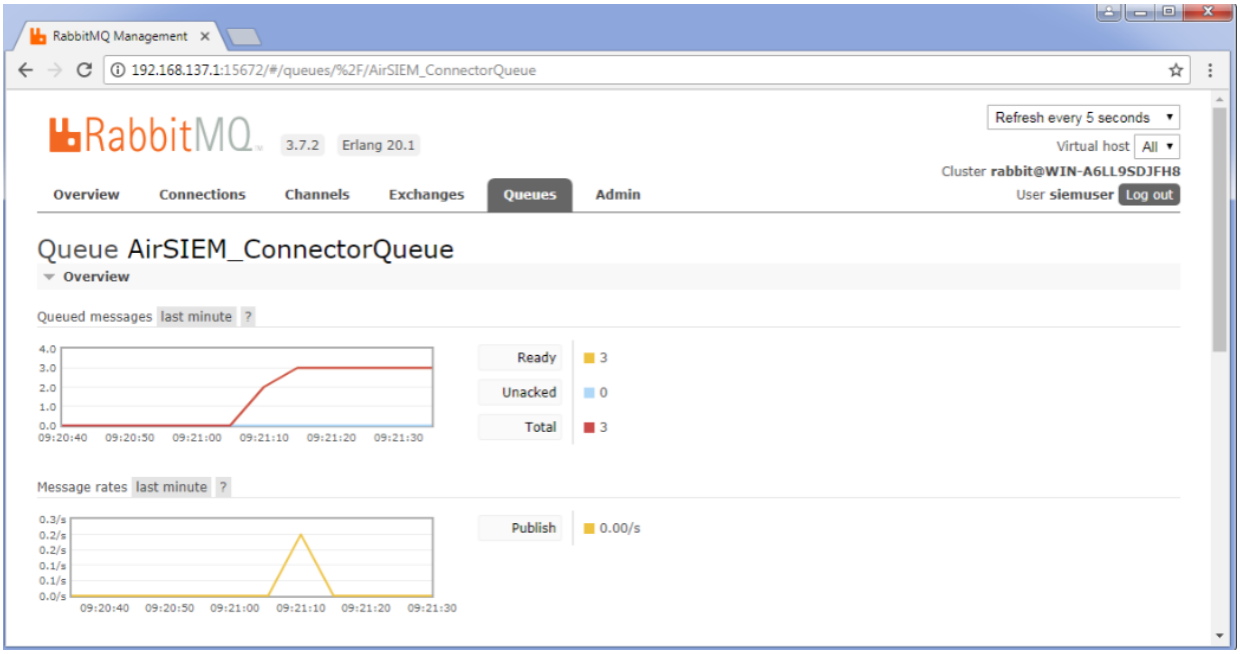

Рис.3.13. Результат запуску конектора на працездатність

1.9 Розробка ядра кореляції (обробника подій)

До цього етапу налаштовано підсистему збору подій безпеки від одного джерела – веб-сервера Apache. Конектор ApacheConnector відстежує зміни журналу звернень access.log і надсилає останні рядки в чергу брокера повідомлень RabbitMQ.

Наступний етап – розробка ядра кореляції (обробника подій). А також пропонуємо оцінити швидкість обробки запитів і читання зі сховища даних MongoDB

1.10 Оцінка продуктивності сховища даних MongoDB.

Тестування продуктивності виконайте простим методом - спочатку оцініть швидкість послідовного запису в сховищі (одиночні документи та

пакети документів), після цього оцініть швидкість випадкового читання документа з колекції. Для цього використаємо вже готовий додаток MongoBenchmark.

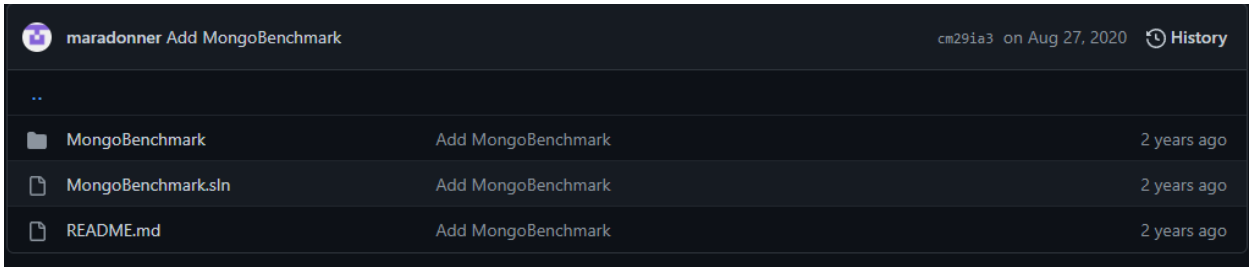

Рис.3.14. Готовий MongoBenchmark.

Додатково під’єднайте .NET driver for MongoDB для MongoDB.

Легше за все це зробити за допомогою спеціального пакету NuGet у консолі Package Manager Console за допомогою команди:
Install-Package MongoDB.Driver -Version 2.5.0

Після запуску програми оцінимо результати бенчмарку:

InsertMany by 1: 20000 ops in 13.52 seconds (1479.15 ops/sec) => 1479.15 docs/sec
InsertMany by 2: 10000 ops in 7.11 seconds (1406.24 ops/sec) => 2812.48 docs/sec
InsertMany by 5: 4000 ops in 3.20 seconds (1250.93 ops/sec) => 6438.66 docs/sec
InsertMany by 10: 2000 ops in 2.08 seconds (960.88 ops/sec) => 9907.78 docs/sec
InsertMany by 50: 400 ops in 1.15 seconds (347.68 ops/sec) => 18001.15 docs/sec
InsertMany by 100: 200 ops in 1.06 seconds (188.32 ops/sec) => 18685.26 docs/sec
InsertMany by 250: 80 ops in 0.95 seconds (83.87 ops/sec) => 21088.05 docs/sec
InsertMany by 500: 40 ops in 0.92 seconds (43.67 ops/sec) => 21521.64 docs/sec
InsertMany by 1000: 20 ops in 0.93 seconds (21.39 ops/sec) => 21521.22 docs/sec
InsertMany by 5000: 4 ops in 1.00 seconds (3.99 ops/sec) => 19856.32 docs/sec
InsertMany by 10000: 2 ops in 1.01 seconds (1.97 ops/sec) => 19260.96 docs/sec
InsertMany by 20000: 1 ops in 1.01 seconds (0.99 ops/sec) => 19789.80 docs/sec
Find: 10000 ops in 6.17 seconds (1620.21 ops/sec)

Розподілення відбувається на випадок випадкової відправки 500-ста подій в одному пакеті(блоці).

Швидкість поступового запису при цьому – 21961 документів в секунду.

Швидкість випадкового читання з колекції – 1620 документів в секунду.

З урахуванням того що це проходить на віртуальній машині яка має не повну швидкість основної машини, результат хороший. Скоріше за все отримані в ході експерименту значення швидкості запису і читання дозволять сховищу даних MongoDB обробити заплановане в прикладі навантаження, якщо це буде не так, експеримент проведемо на основній машині.

1.12 Формування набору правил кореляції

Сформуємо тестовий набір правил, який буде використовуватись надалі

Спробуємо змоделювати спрощений сценарій атаки “Перебір пароля” щодо веб-програми, що захищається, для цього зробімо відповідний набір правил test_webapp_rules.xml:

test_webapp_rules.xml

C: > Users > Ditolk > Desktop > test_webapp_rules.xml

```
<group name="web-app">

  <rule id="100000" level="0">
    <match>/buggy/</match>
    <description>Access to BUGGY webapp</description>
  </rule>

  <rule id="100001" level="0">
    <if_sid>100000</if_sid>
    <match>password</match>
    <description>Attempt to login to BUGGY webapp</description>
  </rule>

  <rule id="100002" level="1" frequency="3" timeframe="5">
    <if_matched_sid>100001</if_matched_sid>
    <same_source_ip/>
    <description>Brute force trying to login to BUGGY webapp</description>
  </rule>

</group>
```

Рис.3.15 Сформовані правила

Далі розглянемо окремо кожне правило та коротко пояснимо особливості синтаксису. Перше правило:

```
<rule id="100000" level="0">
  <match>/buggy/</match>
  <description>Access to BUGGY webapp</description>
</rule>
```

Рис.3.15 Перше сформоване правило

Елемент <rule> визначає правило.

Атрибут id елемента <rule> визначає ідентифікатор правила.

Атрибут level елемента <rule> визначає рівень значущості правила.

Елемент <match> задає підрядок для пошуку в рядку повідомлення, що обробляється.

Елемент <description> задає опис правила, яке відображатиметься як сповіщення для адміністратора безпеки.

Випадок спрацьовування такого правила перевіряється просто - якщо підрядок, вказаний в елементі <match>, буде виявлений у рядку повідомлення, що обробляється, ядро кореляції сформує оповіщення безпеки.

Логіка правила 100000 наступна: оповіщати систему безпеки про всі спроби звернення до веб-застосунку Buggy Webapp. Для цього відстежується підстрока /buggy/ у всіх зверненнях до веб-сервера. Рівень значущості у правила 100000 нульовий, критичність у відстежуваних зверненнях відсутня, спрацьовування правила використовуватимуться для побудови складніших ланцюжків правил.

Друге правило:

```
<rule id="100001" level="0">
  <if_sid>100000</if_sid>
  <match>password</match>
  <description>Attempt to login to BUGGY webapp</description>
</rule>
```

Рис.3.16. Друге сформоване правило

В описі правила 100001 є новий елемент <if_sid> з ідентифікатором правила 100000, який накладає додаткову умову спрацьовування - необхідно, щоб до цього спрацювало правило 100000.

Логіка правила 100001: якщо рядок, що обробляється, має відношення до доступу до веб-програми, що захищається (попередньо спрацювало правило 100000) і при цьому у зверненні до веб-сервера виявлено підрядок «password» (можливо свідчить про передачу пароля у форму введення імені користувача та пароля), то сповістити систему безпеки про спробу отримання адміністративного доступу - Attempt to login to BUGGY webapp.

Третє правило:

```
13
14    <rule id="100002" level="1" frequency="3" timeframe="5">
15      <if_matched_sid>100001</if_matched_sid>
16      <same_source_ip/>
17      <description>Brute force trying to login to BUGGY webapp</description>
18    </rule>
19
20  </group>
```

Рис.3.17. Третє сформоване правило

В описі правила 100002 є новий елемент <if_matched_sid> з ідентифікатором правила 100001, який накладає додаткову умову спрацьовування – необхідно, щоб правило 100001 спрацювало не менше 3 разів (атрибут frequency=«3» елемента <rule>) протягом останніх =«5»).

Порожній елемент <same_source_ip/> вказує на те, що при підрахунку спрацьовувань правила, заданого елементом <if_matched_sid>, враховуються лише спрацьовування з відповідними IP-адресами джерела.

Логіка правила 100002: якщо протягом останніх 5 секунд з однієї і тієї ж адреси зафіксовано безліч спроб (3 і більше) отримання доступу до веб-додатку, що захищається, то сформувати оповіщення з більш високим рівнем значущості level=«1» про спробу підбору пароля доступу – «Brute force trying to login to BUGGY webapp».

1.13 Реалізація ядра кореляції

Програмна реалізація ядра кореляції є найтяжчим етапом, визнаючи всю логіку обробки подій безпеки системи SIEM, що розробляється.

Логіка роботи ядра кореляції описується наступним чином:

1. Ядро кореляції "читає" чергу повідомлень AirSIEM_ConnectorQueue.

2. При надходженні чергового повідомлення (події) ядро намагається застосувати щодо нього заздалегідь завантажені правила обробки подій (правила кореляції).

3. У разі застосування одного з правил до дії, що надійшла, ядро при необхідності формує інцидент безпеки і зберігає його в колекції alerts сховища даних MongoDB.

Реалізація буде достатньо об'ємною, тому для зручності налагодження підключимо до проекту систему логування NLog. Найпростіше це зробити, встановивши відповідний пакет NuGet у консолі Package Manager Console за допомогою команди:

Install-Package NLog -Version 4.4.12

Ще для роботи з брокером повідомлень треба підключити пакет RabbitMQ.Client, а для взаємодії зі сховищем даних пакет – MongoDB.Driver:

Install-Package RabbitMQ.Client -Version 5.0.1

Install-Package MongoDB.Driver -Version 2.5.0

Інсталювання робити слід за інструкцією додаючи до проекту (Меню Project > Add Existing Item) файл конфігурації nlog.config. Вказуйте необхідність його копіювання у вихідний каталог.

Завантажуємо вихідний код проекту та перед запуском перевірте налаштування в конфігураційному файлі AirSIEM.exe.config, чи правильно вказані шлях до правил та рядки підключення до брокера повідомлень та сховища даних.

1.14 Розробка консолі адміністратора

Для зручності роботи передбачимо створення консолі керування. Фунціонал консолі обмежуємо переглядом сформованих інцидентів безпеки. Варіант реалізації – веб-додаток PHP.

Щоб PHP міг взаємодіяти з MongoDB підключіть до інтерпретатора PHP відповідне розширення, а до веб-додатку – відповідну бібліотеку.

index.php

C: > Users > Ditolk > Desktop > index.php

```php
<?php
  // Include Composer autoloader
  require __DIR__ . '/vendor/autoload.php';

  // Connect to MongoDB
  $database = (new MongoDB\Client("mongodb://192.168.137.1:27017"))->AirSIEM;
  $collection = $database->alerts;
  $cursor = $collection->find([]);
?>

<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8">
    <title>AirSIEM</title>
    <meta name="viewport" content="width=device-width, height=device-height, initial-scale=1.0" />
    <meta http-equiv="refresh" content="5; URL=index.php">
    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-beta/css/bootstrap.min.css"
    <script src="https://code.jquery.com/jquery-3.2.1.slim.min.js"></script>
    <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.3/umd/popper.min.js"></script>
    <script src="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-beta.2/js/bootstrap.min.js"></script>
  </head>
  <body class="p-5">
    <h1 class="mb-4">AirSIEM Dashboard</h1>
    <table class="table table-hover table-sm border">
      <thead>
        <tr class="table-success">
          <th scope="col">_id</th>
          <th scope="col">Timestamp</th>
          <th scope="col">Rule SID</th>
          <th scope="col">Level</th>
          <th scope="col">Source</th>
          <th scope="col">Destination</th>
          <th scope="col">Message</th>
        </tr>
      </thead>
      <tbody>

        <?php
          // Show alerts
          $counter = 0;
          foreach ($cursor as $alert)
          {
            $counter++;
            if ($counter > 100) $collection->drop();

            // Specify colors for critical alerts
            $color_class = "";
            if ($alert['level'] == '1') $color_class = ' class="table-warning"';
            if ($alert['level'] == '2') $color_class = ' class="table-danger"';
        ?>

        <tr<?php echo $color_class; ?>>
          <th scope="row"><?php echo $counter; ?></th>
          <td><?php echo $alert['timestamp']; ?></td>
          <td><?php echo $alert['matching_rule_SID']; ?></td>
          <td><?php echo $alert['level']; ?></td>
          <td><?php echo $alert['src_IP']; ?></td>
          <td><?php echo $alert['dest_IP']; ?></td>
          <td><span data-toggle="tooltip" data-placement="right" title="<?php echo htmlspecialchars($alert['
        </tr>

        <?php
          }
        ?>

      </tbody>
    </table>

    <script>
      $(function () {
        $('[data-toggle="tooltip"]').tooltip()
      })
    </script>
  </body>
</html>
```

Рис.3.18. Код консолі адміністратора

1.15. Підключення розширення php_mongodb.dll до веб-серверу

За умовчанням інтерпретатор PHP не знає про існування сховища MongoDB, тому виправимо це інсталяцією драйвера MongoDB PHP Driver on Windows.

Вирушайте на веб сайт pecl.php.net/package/mongodb у пошуках підходящої версії драйвера php_mongodb.dll. Пропоную обрати стабільну версію (1.3.0), Windows, PHP Version 7.1, thread safe, x86.

Зкопіюйте драйвер php_mongodb.dll в папку розширень PHP а також додайте у файл налаштувань PHP (за замовчуванням "c:\xampp\php\php.ini") рядок "extension=php_mongodb.dll" в розділ підключення розширень.

Перезапускаємо веб сервер Apache з панелі керування XAMPP.

1.16 Підключення до веб додатку бібліотеки MongoDB PHP Library

Далі необхідно підключити до проекту консолі адміністратора безпеки, бібліотеку MongoDB PHP Library.

В інструкції зауважено що легше за все це зробити за допомогою Composer, тому встановіть його.

Створіть папку для майбутнього проекту та виконайте в папці команду установки пакету mongodb:

composer require mongodb/mongodb

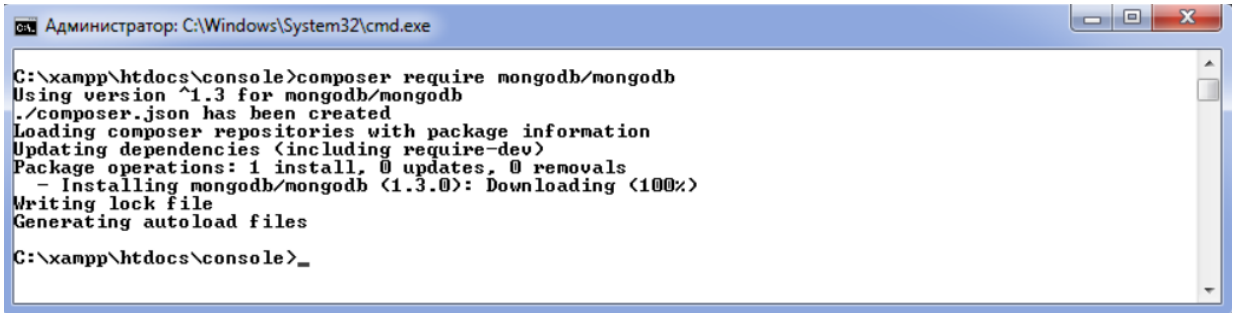

Рис.3.19. Результат виконання команди

Composer завантажив необхідні файли та додав їх у проект. Щоб проект міг використовувати функціонал бібліотеки MongoDB PHP Library, до коду потірбно додати один рядок:

require_once __DIR__ . "/vendor/autoload.php";

Збережіть код програми у файлі "c:\xampp\htdocs\console\index.php" та відкрийте у браузері.

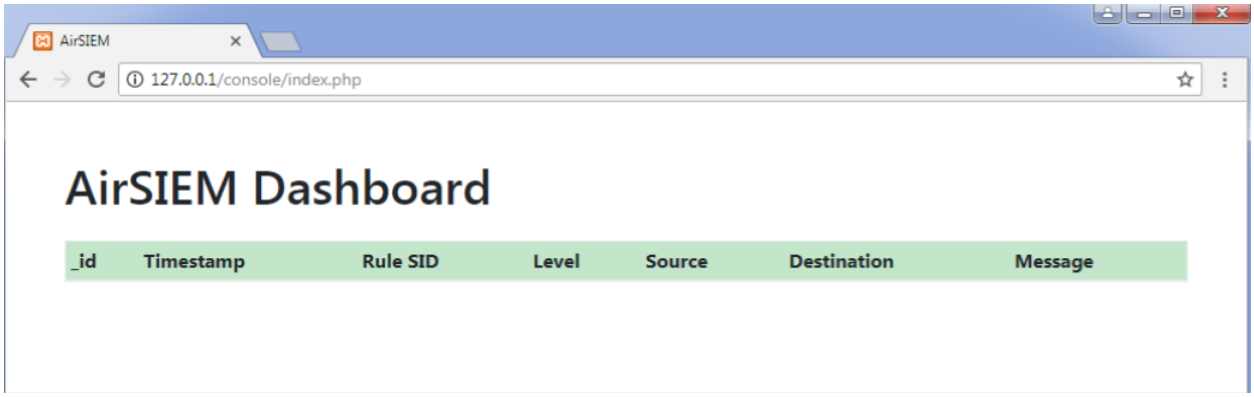

Рис.3.20. Перевірка працездатності бібліотеки MongoDB PHP Library

3.2 Перевірка працездатності розробленої системи управління інцидентами інформаційної безпеки.

На останньому етапі треба виконати налагодження ядра кореляції і переконатися в правильності роботи всього рішення в цілому.

Тестовий сценарій буде виглядати приблизно так:

1. Зловмисник відкриває сторінку admin.php веб-програми Buggy Webapp, що захищається, і кілька разів намагається підібрати ім'я користувача та пароль адміністратора.

2. Після кількох безуспішних спроб зловмисник підбирає облікові дані адміністратора – «admin/admin» – та отримує доступ до адміністративного розділу.

3. Розроблена SIEM система в результаті обробки зареєстрованих подій безпеки із застосуванням заданих правил кореляції виявляє реалізацію сценарію атаки, формує інцидент безпеки та сповіщає адміністратора.

Виконаємо тестовий сценарій та розглянемо послідовність дій SIEM системи.

1. Підключіться до MongoDB за допомогою Robomongo і видаліть базу даних AirSIEM. Далі відкрийте ApacheConnector.

2. Відкриваємо у браузері веб-додаток Buggy Webapp за адресою: http://127.0.0.1/buggy/admin.php

3. У вікні додатку ApacheConnector перевірте факт читання журналу звернень веб-сервера та передачу зареєстрованих подій безпеки у чергу брокера повідомлень. Перевірте на панелі адміністрування брокера повідомлень RabbitMQ («http://127.0.0.1:15672/») наявність навантаження: у черзі AirSIEM_ConnectorQueue має з’явились повідомлення.

4. Далі в процес обробки вступає ядро кореляції. Проведіть запуск AirSIEM.

На початковому етапі завантажуються правила кореляції:

```
----- AirSIEM start -----
ParseRuleDir start
ParseRulesFromXML handles file: test_webapp_rules.xml
  3 rules processed: 100000, 100001, 100002
ParseRuleDir: total 1 files processed
ParseRuleDir: total 3 rules processed
ParseRuleDir stop
```

Після загрузки правил виконується побудова низки правил:

```
CheckDependencies start
Dependencies:
  100000 children => 100001
  100001 children => 100002
  100002 children =>
CheckDependencies stop
```

Далі створюються черги для підрахунку спрацьовувань тих правил, ідентифікатори яких зустрічаються в елементах <if_matched_sid>:

```
GenerateQueueList start

Created 1 queues:
[100001, FireQueue object => ID=[100001], count=[0], timeFrame=[5 sec],
maxSize=[1000]]
GenerateQueueList stop
```

Потім ініціюється та запускається «підписник», який «слухає» чергу AirSIEM_ConnectorQueue і передає прийняті повідомлення обробникові:

RabbitMQConsumer init

RabbitMQConsumer start

Після першої спроби зловмисника підібрати логін користувача та пароль, ApacheConnector передає черговий рядок з журналу звернень access.log веб-сервера в чергу RabbitMQ, «підписник» отримує повідомлення та передає на обробку:

RMQ message received: ApacheConnector:127.0.0.1 - - [01/Jan/2099:16:24:57 +0300] "GET /buggy/admin.php?username=1&password...

З повідомлення формується нормалізована подія безпеки (екземпляр класу SecurityEvent):
SecurityEvent object => timestamp=[16:24:57], source=[127.0.0.1], destination=[], message=[GET /buggy/admin.php?username=1&password=1 HTTP/1.1]

Далі ядро кореляції застосовує завантажені правила до події яка обробляється. При першому «проході» проглядаються ті правила, спрацьовування яких залежить від інших правил:

Check rule 100000 - Access to BUGGY webapp
Check <match>/buggy/</match>
Rule 100000 matched
ALERT: LEVEL 0 - Access to BUGGY webapp

Правило 100 000 спрацьовує, формується інцидент безпеки, оповіщення передається в MongoDB і відображається в консолі адміністратора.

Далі рекурсивно проглядаються правила, спрацювання яких залежить від спрацьовування правила 100000:

Check the child rules
Check rule 100001 - Attempt to login to BUGGY webapp
Check <if_sid>100000</if_sid>
Check <match>password</match>
Rule 100001 matched
ALERT: LEVEL 0 - Attempt to login to BUGGY webapp
Matched rule is queue tracked

Enqueue item: FireQueueItem object => timestamp=[16:24:57], source=[127.0.0.1], destination=[]
FireQueue object => ID=[100001], count=[1], timeFrame=[5 sec], maxSize=[1000]
1: FireQueueItem object => timestamp=[16:24:57], source=[127.0.0.1], destination=[]
Check the child rules
Check rule 100002 - Brute force trying to login to BUGGY webapp
Check <if_matched_sid>100001</if_matched_sid>
QueueDictionary.CheckIfMatched start
counter++ => counter=[1]
counterSameSourceIP++ => counterSameSourceIP=[1]
Rule 100001 QueueDictionary.CheckIfMatched == FALSE
Rule 100002 not matched
Check rule 100002: OK
Check the child rules: OK
Check rule 100001: OK
Check the child rules: OK
Check rule 100000: OK

В результаті обробки спрацювало правило 100001, у чергу підрахунку FireQueue заноситься перше спрацювання. Коли кількість спрацювань дорівнюватиме 3, виконається одна з умов спрацювання правила 100002.

RMQ message received: ApacheConnector:127.0.0.1 - - [01/Jan/2099:16:25:02 +0300] "GET /buggy/admin.php?username=1&password...
SecurityEvent object => timestamp=[16:25:02], source=[127.0.0.1], destination=[], message=[GET /buggy/admin.php?username=1&password=1 HTTP/1.1]
Check rule 100000 - Access to BUGGY webapp
Check <match>/buggy/</match>
Rule 100000 matched
ALERT: LEVEL 0 - Access to BUGGY webapp
Check the child rules
Check rule 100001 - Attempt to login to BUGGY webapp
Check <if_sid>100000</if_sid>
Check <match>password</match>
Rule 100001 matched
ALERT: LEVEL 0 - Attempt to login to BUGGY webapp

У черзі підрахунку зафіксовано 3 спрацювання правила 100001 за інтервал часу timeframe (5 секунд). Обробка події безпеки продовжується:

```
Check the child rules
   Check rule 100002 - Brute force trying to login to BUGGY webapp
    Check <if_matched_sid>100001</if_matched_sid>
```

У цьому місці перевіряється кількість спрацювань правила 100001. Оскільки в описі правила був присутній елемент <same_source_ip/>, одночасно підраховуються спрацювання з однаковим значенням IP-адреси джерела:

```
QueueDictionary.CheckIfMatched start
        counter++ => counter=[1]
        counterSameSourceIP++ => counterSameSourceIP=[1]
        counter++ => counter=[2]
        counterSameSourceIP++ => counterSameSourceIP=[2]
        counter++ => counter=[3]
        counterSameSourceIP++ => counterSameSourceIP=[3]
      Rule 100001 QueueDictionary.CheckIfMatched == TRUE
     Rule 100002 matched
     ALERT: LEVEL 1 - Brute force trying to login to BUGGY webapp
   Check rule 100002: OK
   Check the child rules: OK
  Check rule 100001: OK
  Check the child rules: OK
Check rule 100000: OK
```

Правило 100002 спрацьовує, ядро кореляції виявляє сценарій атаки типу перебір пароля і формує відповідний інцидент безпеки. Відомості про інцидент надсилаються до сховища даних MongoDB.

5. Перевірте формування сповіщення у MongoDB за допомогою Robomongo та перегляньте колекцію документів alerts бази даних AirSIEM.

6. Відкриваємо у браузері консоль адміністратора безпеки за адресою: http://127.0.0.1/console/index.php. Якщо всі компоненти SIEM системи налаштовані правильно, після виконання тестового сценарію вікно консолі повинне мати приблизний вигляд:

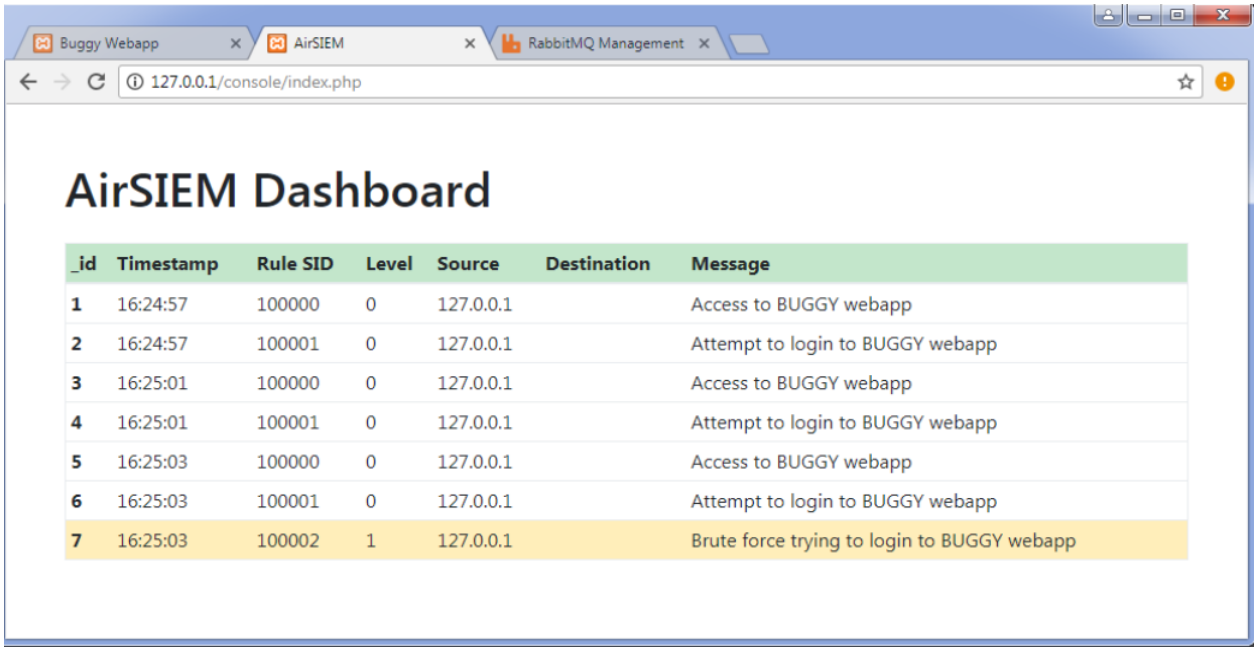

Рис.3.21. Успішне виявлення атаки типу «Перебір пароля»

Загалом виявлено не лише окремі події, а й виділено послідовність дій зловмисника та ідентифіковано сценарій атаки. У консолі адміністратора це рядок під номером 7 який виділений кольором, є повідомлення про виявлену реалізацію сценарію атаки типу «перебір пароля». Адміністратор безпеки успішно сповіщений про підозрілі дії зловмисника, тому розроблена SIEM система виконала своє поставлене завдання.

3.3. Практичні рекомендації з побудови та функціонування систем управління інцидентами інформаційної безпеки

Відповідно до [13] УІІБ – це процес або набір процесів, на вхід яких подаються дані, отримані в результаті збору і протоколювання даних про події, що стосуються ІКС, а на виході цих процесів одержують інформацію про причини інциденту, що відбувся, про збиток, нанесений організації, і заходах, які необхідно прийняти для того, щоб інцидент не повторився. Таким чином, УІІБ спрямовано на вдосконалення системи забезпечення безпеки організації. Крім того, вихідні дані є, по суті, єдиним об'єктивним параметром у визначенні ймовірності реалізації загроз при аналізі ризиків. Ефективність процесу УІІБ залежить від: координації і узгодженості дій всіх залучених до нього осіб;

наявних можливостей з отримання та аналізу інформації, пов'язаної з інцидентом; оперативності та коректності отриманих результатів. Підвищення кожного з наведених показників помітно підвищить ефективність всього процесу і, тим самим, дозволить підрозділу ІБ організації набути більш значних результатів. Використовуючи СУІБ можна радикально змінити ситуацію щодо ефективності управління інцидентами. Таким чином, СУІБ фактично буде системою колективної роботи, яка автоматизує процеси з УІБ за допомогою інтеграції людей і апаратно-програмного забезпечення моніторингу і захисту, а також інформаційної інфраструктури організації.

Припущення про те, що в організації стався інцидент ІБ, має базуватися на трьох основних чинниках [13]:

1) Повідомлення про інцидент ІБ надходять одночасно з декількох джерел (користувачі, IDS, файли журналів тощо);

2) IDS сигналізують про багаторазове повторення певних подій;

3) Аналіз файлів журналів автоматизованої системи (АС) дає підставу для висновку про можливість настання інциденту.

У загальному випадку, ознаки інциденту поділяються на дві основні категорії – повідомлення про те, що інцидент відбувається в даний момент і повідомлення про те, що інцидент, можливо, відбудеться у майбутньому.

Прийняття рішення про настання інциденту багато в чому залежить від компетентності експертів команди реагування. Вони мають чітко відрізняти випадкову помилку оператора, наприклад, від зловмисного цілеспрямованого впливу на ІКС. У документах [4, 25] наведено основні принципи організації та функціонування команд (груп) реагування на інциденти ІБ CERT/CSIRT, а рис. 3.4 містить перелік і місцерозташування діючих команд CERT/CSIRT за даними Європейського агентства з питань мереж та ІБ [6].

Як показав проведений аналіз [11, 22, 37], сьогодні у міжнародній практиці розроблено достатню кількість нормативних документів різного характеру (стандарти, рекомендовані практики, керівництва тощо), що регламентують питання УІБ. Відповідно до [3] для ефективного УІБ необхідно організувати

комплекс процесів управління інцидентами, забезпечити його належними ресурсами, відповідною нормативно-розпорядчою і робочою документацією, технічними засобами забезпечення механізмів контролю. Для обробки подій та інцидентів ІБ необхідно організувати процес реагування на інциденти. Потім слід розробити необхідні нормативні документи щодо управління інцидентами.

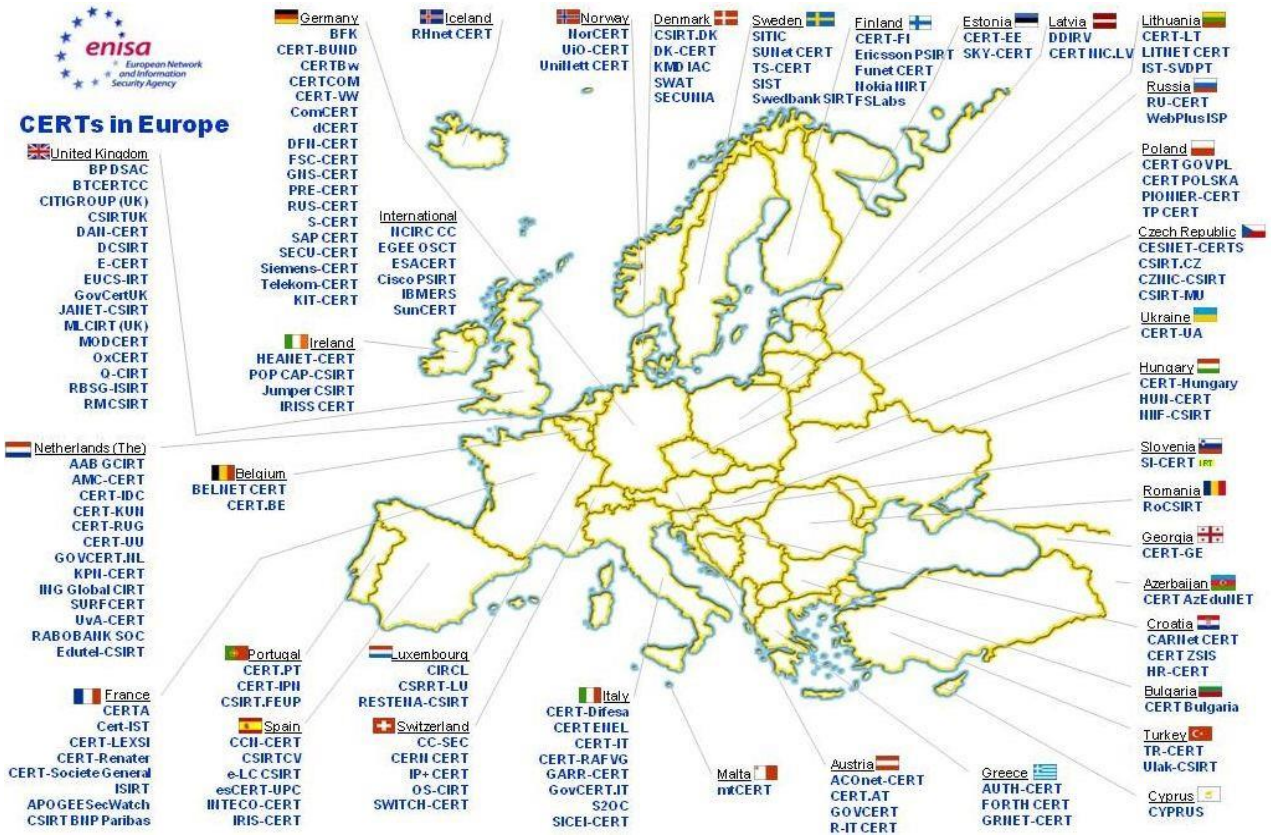

Рис.3.22. Мережа європейських команд CERT/CSIRT

Як правило, такі документи повинні описувати:

1) Визначення інциденту ІБ – перелік подій, що є інцидентами (тобто, що саме в цій організації є інцидентом ІБ);

2) Порядок сповіщення відповідальної особи про виникнення інциденту (необхідно визначити формат звіту, а також відобразити контактну інформацію осіб, яких слід оповіщати про інцидент);

3) Порядок усунення наслідків і причин інциденту;

4) Порядок розслідування інциденту (визначення причин інциденту, винних у виникненні інциденту, порядок збору і збереження доказів);

5) Внесення дисциплінарних стягнень;

6) Реалізація корегуючих і превентивних заходів.

У межах СУІБ необхідно збирати і обробляти велику кількість подій ІБ, які надходять з різних джерел. Ці події мають бути приведені до єдиного вигляду, що дозволяє застосовувати єдині алгоритми обробки та безпомилкового виділення з них саме інцидентів ІБ. Необхідно зберігати події ІБ протягом часу, достатнього для забезпечення розслідування інцидентів. Потрібно розробити архітектуру СУІБ, спроектувати комплекс рішень, що реалізують дану архітектуру, вибрати комплекс технічних засобів, здійснити впровадження системи.

При розробці технічних рішень необхідно враховувати особливості функціонування інфраструктури інформаційних технологій (ІТ-інфраструктури) організації, наявні засоби автоматизації тощо. Для ефективного функціонування СУІБ необхідно, на стадії впровадження, забезпечити ряд ключових чинників. У першу чергу, система управління має бути забезпечена вхідним потоком подій ІБ, що адекватно відображає стан в рамках обраної області дії.

При виявленні і реагуванні на інцидент, необхідно мати дані щодо задіяних ресурсів (активів), їх власників і ступінь критичності, а також мати доступ до даних про події, що вплинули на інцидент ІБ, таких як дані аудиту дій користувачів і адміністраторів. При наданні звітності про інциденти керівництву, необхідно мати можливість зіставлення ресурсів, що підпали під вплив в результаті інциденту і ризиків для основних бізнес-процесів організації.

Відповідно до [23] роботи з впровадження СУІБ пропонується проводити у декілька етапів: обстеження об'єкту; розробка процедур та процесів системи управління, написання відповідних документів; впровадження СУІБ; впровадження АС моніторингу й управління інцидентами ІБ.

Для візуалізації результатів аналізу подій, що відбуваються в інформаційній системі, використовується складання діагностичних матриць. Матриця формується з рядків потенційних ознак інциденту та стовпців – типів інцидентів. Дається оцінка події за шкалою пріоритетів – «високий», «середній», «низький». Діагностична матриця покликана документувати хід логічних

висновків експертів в процесі прийняття рішення і, поряд з іншими документами, служить свідченням розслідування інциденту.

При аналізі інцидентів ІБ організація повинна виконати такі дії: своєчасно ідентифікувати невдалі та успішні порушення і інциденти ІБ; допомогти у виявленні подій безпеки, таким чином запобігти інцидентам безпеки шляхом використання індикаторів.

Управління інцидентами ІБ повинно включати такі дії:

– повідомлення про уразливі місця ІКС та події ІБ;
– відповідальність і процедури;
– навчання на інцидентах ІБ;
– збір доказів.

Документування подій інциденту ІБ необхідне, перш за все, для збору і консолідації технологічних та операційних свідчень розслідування. Документуванню підлягають усі факти та докази зловмисного впливу, типовою практикою є ведення журналу розслідування інциденту, який не має стандартної форми і розробляється командою CERT/CSIRT.

Архітектура типової СУІБ має включати такі основні компоненти [13, 18, 19]:

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

Інтеграційна платформа є ядром системи, вона покликана забезпечувати чітку і оперативну координацію та взаємодію осіб, що відповідають за реакцію на події, пов'язані з інцидентами ІБ.

Апаратно-програмні засоби моніторингу і аудиту – засоби, що реалізують функції з протоколювання, збору, накопичення та обробки інформації

функціонування ІКС організації. Вони складають підсистему збору інформації про інциденти ІБ. Результатом їх роботи є дані, на основі яких системою приймається рішення щодо настання інциденту.

Апаратнопрограмні засоби захисту в контексті СУІБ – засоби, які забезпечують локалізацію інцидентів або зниження збитку. Ці засоби мають механізми, що дозволяють проводити швидку і дистанційну зміну своєї конфігурації або мати в своєму складі наперед розроблені автоматизовані сценарії дій з мінімізації можливого збитку від інцидентів ІБ. Також, в організації повинна бути розроблена та впроваджена система сповіщення про інциденти.

Узагальненою метою забезпечення ІБ організації є зниження ризиків, діючих відносно інформаційних ресурсів, і як наслідок запобігання або мінімізація збитку від можливих інцидентів ІБ.

Основною задачею процесу УІБ є усунення інцидентів в гранично стислі терміни. У ході процесу управління інцидентами ІБ проводиться виявлення, реєстрація, класифікація і початкова підтримка запитів, а також пошук рішення, його застосування, контроль, інформування і підготовка звітності. Оскільки, як ми вже визначили, інцидентом, в першу чергу, є певна недозволена подія, то вона має бути кимось заборонена. Отже, існує необхідність розробки та затвердження документів, що чітко описують всі дії, які можна виконувати в ІКС і які виконувати заборонено.

Однією з кращих СУІБ серед присутніх на вітчизняному ринку є програмний продукт для обробки подій – netForensics nFX Open Security Platform [33], зображений на рис. 3.5:

Система netForensics призначена для роботи з гетерогенним середовищем продуктів забезпечення ІБ і реалізує безперервний збір, обробку та відображення подій безпеки. Система може працювати на платформах Windows, Linux або Solaris, використовуючи в якості сховища даних повнофункціональну СУБД Oracle. Ця СУІБ має широкі можливості щодо роботи в розподіленому режимі, підтримку різних відмовостійких конфігурацій тощо. СУІБ netForensics

реалізована на базі технології Java за модульним принципом. Основними модулями системи є сервер додатків (реалізує основну логіку обробки подій, представлення даних, взаємодії з користувачами); база даних (забезпечує зберігання інформації, що надходить до системи); модуль кореляції (здійснює кореляцію зібраних даних); модуль автоматизації УІІБ (здійснює автоматизацію процесів УІІБ); агенти (збирають інформацію безпосередньо з пристроїв). До складу системи також входять засоби щодо написання агентів збору даних з нестандартних систем захисту, засоби формалізації користувацьких правил кореляції і створення звітів.

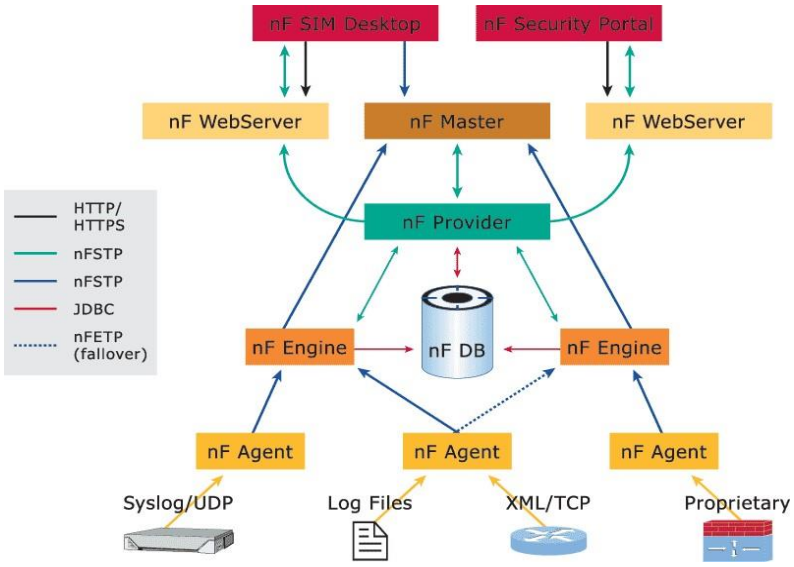

Рис.3.23. СУІІБ netForensics

Для опису процедури УІІБ відповідно до [13, 19, 30] можна використати класичну модель безперервного поліпшення процесів, що отримала назву від циклу Шухарта-Демінга – модель PDCA (плануй – «Plan», виконуй – «Do», перевіряй – «Check», дій – «Act»). Стандарт [31] описує модель PDCA як основу функціонування всіх процесів системи управління інформаційною безпекою. Ця модель об'єднує 4 взаємозв'язані процеси: розробка, впровадження, моніторинг і розвиток.

Життєвий цикл системи управління буде визначатись такими стадіями:

1) Планування і підготовка. Здійснюється розробка схеми УІІБ, розробка і затвердження ряду організаційно-регламентуючих документів, виділення людських і матеріальних ресурсів, проведення необхідного навчання та апробація обраної схеми управління.

2) Експлуатація. Здійснюється виявлення та ідентифікація інциденту ІБ, реагування, розслідування й аналіз.

3) Аналіз. Здійснюється аналіз системи управління інцидентами інформаційної безпеки, виявляються ділянки щодо поліпшення та міри з поліпшення.

4) Поліпшення. Реалізуються рекомендації, розроблені на етапі аналізу. Загалом, ця процедура регулюється стандартом [19], що прийшов на зміну BS 15000:2002, який, у свою чергу, взяв за основу бібліотеку ITIL.

Слід зазначити, що всі стандарти ISO/IEC серій 9000, 14000, 20000, 27000 та ін., що описують правила створення систем управління різними процесами, гармонійно поєднуються один з одним, і в якості основи управління підконтрольними процесами використовують процесний підхід, який розглядає управління як процес, тобто як набір взаємозв'язаних безперервних дій. Процесний підхід акцентує увагу на досягненні поставлених цілей, а також на ресурсах, витрачених для цього.

Процес УІІБ, як правило, покладається на службу ІТ-підтримки, яка обробляє інциденти ІБ (у випадку, якщо така служба існує в організації). Це ще раз доводить факт доцільності розробки єдиної системи управління всіма процесами в компанії, так як управління подібними процесами в різних галузях її діяльності часто виконується за однією схемою. Варто також розуміти, що УІІБ не попереджує нанесення збитку компанії, проте розслідування інциденту ІБ та своєчасне впровадження превентивних і корегуючих заходів знижує ймовірність його рецидиву. Робота організації без СУІІБ може обернутися рядом неприємностей. У результаті впровадження процесу управління проблемами організація отримує такі важливі і корисні властивості як якість сервісів, скорочення числа інцидентів та безперервне функціонування. В умовах

зростання впливу ІТ на діяльність сучасних організацій, значна увага приділяється організації підтримки та супроводу ІТ-систем. Світовий досвід щодо управління ІТ-організаціями та їх взаємодією із замовниками описаний у, згаданій раніше, бібліотеці ITIL. Вона містить комплекс необхідних для побудови СУІБ рекомендацій.

По-перше, в ITIL з певним ступенем деталізації описаний процес управління безпекою (Security Management). По-друге, надання ІТ-послуг, включаючи сервіси ІБ, відноситься до відповідальності служб ІТ та ІБ організацій. Для ефективного розслідування інцидентів ІБ необхідні не просто диференційований інструментарій, а спеціалізований уніфікований комплекс таких інструментів, так званий toolkit. Необхідність дотримання вимог стандартів, а також законів щодо проведення розслідувань, накладає певні складності у роботі слідчих, приводить до нагромадження неструктурованих даних, а також збільшує витрати на проведення розслідування.

Все це стало підґрунтям розробки інтегрованих спеціалізованих наборів інструментів для проведення розслідувань, що включають в себе такі можливості як аналіз смартфонів, мобільних телефонів, розподілені обчислення, планування задач тощо. Тобто, основними вимогами, для ефективного проведення розслідувань інцидентів, мають бути інтегрованість всіх інструментів, розподілення обчислень, оперування великими об’ємами даних без збоїв, оперативне виявлення спроб вторгнення та вразливих місць ІКС, можливість розширення функціоналу, створення деталізованих звітів, швидкий доступ до пов’язаних даних, а також можливість взаємодії з іншими групами CERT/CSIRT. Також, для підвищення ймовірності ідентифікації зловмисника, відстеження активності та виявлення його істинних намірів слід проводити аналіз мережевої активності та здійснювати візуалізацію інформаційних потоків.

Таким чином, аналіз науково-методичних та нормативно-правових джерел показав необхідність та дозволив систематизувати теоретичні засади розробки СУІБ. У роботі також визначено фази життєвого циклу інциденту ІБ та наведено компоненти типової СУІБ. Ефективне функціонування останньої дозволить

акумулювати інформацію щодо інцидентів ІБ, категоризувати їх та визначити найбільш актуальні загрози і, як результат, максимально ефективно впроваджувати превентивні заходи, що дасть можливість підвищити рівень захищеності ІКС організації в цілому.

ВИСНОВКИ

Проблема формування системи управління інформаційною безпекою має велике значення для стабільного та максимально ефективного функціонування підприємств та створення високого потенціалу розвитку в майбутньому.

Узагальнення отриманих результатів дослідження дозволило сформулювати та обґрунтувати такі висновки і рекомендації.

1. Аналіз науково-методичних та нормативно-правових джерел показав необхідність та дозволив систематизувати теоретичні засади розроблення СУІБ. У роботі також визначено фази життєвого циклу інциденту ІБ та наведено компоненти типової СУІБ. Ефективне функціонування останньої дозволить акумулювати інформацію щодо інцидентів ІБ, категоризувати їх та визначити найбільш актуальні загрози і, як результат, максимально ефективно впроваджувати превентивні заходи, що дасть можливість підвищити рівень захищеності ІКС організації в цілому.

2. Розкрито сутність поняття «інцидент інформаційної безпеки». Продемонстровано процес розслідування інцидентів інформаційної безпеки на етапах ініціювання, перевірки політики безпеки, формування групи, збирання фахівців, аналізу та складання звітів.

3. Проаналізовано вимоги і методичні матеріали щодо розробки СУІБ підприємства. Були розглянуті проблеми побудови СУІБ та досліджені процеси УІБ підприємства, які показали, що стандарти побудови СУІБ постійно розвиваються з року в рік і проблема побудови більше не в застарілості нормативної бази, не в актуальності стандартів, а в халатному відношенні керівництва підприємства до організації забезпечення ІБ або надмірною економією на її складових.

4. Розроблено рекомендації щодо покращення побудови системи управління інформаційною безпекою. Особливу увагу треба виділити знаходженню та оцінки ризиків, загроз та можливих матеріальних та репутаційних втрат організації, щоб правильно оцінити економічну доцільність побудови СУІБ. Для управління будь-якої складної системою необхідно створити жорсткий, але простий регламент обслуговування цієї системи і забезпечити контроль за тим, щоб настройки системи змінювалися відповідно до цього регламенту.

5. На основі узагальнення запропоновано структурну модель інформаційної безпеки систем, що базується на положеннях комплексного підходу. Пропонована структурна модель передбачає, що рішення проблеми безпеки в інформаційних системах полягає в аналізі її основних компонентів: визначенні головних завдань захисту інформації, визначенні суб'єктів інформаційних процесів, класифікації основних можливих загроз безпеки, визначенні рівнів вразливості інформаційних систем, визначенні джерел інформації, ознайомленні з особливостями джерел загроз, дослідженні способів та напрямів захисту та цілей захисту.

6. На основі інтеграції зазначених підходів запропоновано формалізовану модель інформаційної безпеки, яка є функцією з множини області значень складових системи інформаційної безпеки і передбачає, що постійне зростання потреби в інформації обумовлює необхідність нарощування та ефективного використання інформаційних ресурсів, формування інформаційного потенціалу організаційних утворень, що виступає основною передумовою зміни стану системи інформаційної безпеки, перебудови або вдосконаленні її моделі.

7. Побудовано систему управління інцидентами інформаційної безпеки, що дозволить фахівцям перейняти досвід та краще забезпечити своє підприємство від небажаних атак

8. На основі аналізу наукових джерел, міжнародних та вітчизняних стандартів і рекомендацій, зроблено спробу систематизації принципів та

формалізації процедур розробки систем управління інцидентами інформаційної безпеки. Також, на базі часткових узагальнень, визначено фази життєвого циклу інцидентів та наведено компоненти типової системи управління інцидентами інформаційної безпеки. Крім того, показано номенклатуру європейських груп реагування на інциденти інформаційної безпеки CERT/CSIRT.

Таким чином, отримані результати та рекомендації є науково-методичною та практичною базою для вдосконалення процесу управління інцидентами інформаційної безпеки підприємств та спрямовані на підвищення ефективності їх господарської діяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Critical infrastructure companies and the global cybersecurity threat // McKinsey Global Institute. 2019. Жовтень. - [Електронний ресурс]. - Режим доступу: https://www.mckinsey.com/business-functions/risk/our-insights/critical-nfrastructurecompanies-and-the-global-cybersecurity-threat# (дата звернення 20.12.2019).

2. European Network and Information Security Agency [Electronic resource] : ENISA. — Electronic data. — Heraklion, Greece: ENISA, [04.02.2018]. — Mode of access: World Wide Web. — URL: http:// www.enisa.europa.eu. — Description based on screen.

3. European Network and Information Security Agency [Electronic resource] : ENISA. — Electronic data. — Heraklion, Greece: ENISA, [04.02.2012]. — Mode of access: World Wide Web. — URL: http:// www.enisa.europa.eu. — Description based on screen.

4. GFI Security survey in the United States. [Електронний ресурс] – 2017. – Режим доступу: www.gfi.com

5. Harrison M. Protection in operating systems / M. Harrison, W. Ruzzo, J. Ullman // Communication of ACM. – 1976. – № 19(8). – P. 461-471.

6. Information technology - Security techniques - Information security incident management (IDT) : ISO/IEC TR 18044:2014. – 76 с.

7. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response – Recommendations of the National Institute of Standards and Technology (NIST). – Publ. 800-86. – 2016.

8. Moira J.W.-B. Handbook for Computer Security Incident Response Teams (CSIRTs) / Moira J.W.-B., Stikvoort D., Kossakowski K.-P. et al. — Pittsburgh, 2013. — 223 p.

9. Moira J.W.-B. Handbook for Computer Security Incident Response Teams (CSIRTs) / Moira J.W.-B., Stikvoort D., Kossakowski K.-P. et al. — Pittsburgh, 2013. — 223 p.

10. Гладиш С.В. Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах / Гладиш С.В. // Реєстрація, зберігання і обробка даних. — 2018 — Т. 10, № 1. — С. 116–124.

11. Голубів В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Навч. посібник / За заг. ред. доктора юридичних наук, професора Р. А. Калюжного. - Запоріжжя: ГУ "ЗІДМУ", 2012. - 292 с.

12. Данільян О. Г. Національна безпека України: сутність, структура та напрямки реалізації / О. Г. Данільян, О. П. Дзьобань, М. І. Панов. – Х.: «ФОЛІО», 2012. – 296 с.

13. Драб Ю. Основні підходи до побудови системи управління інформаційною безпекою / Ю.Драб, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.29-32).

14. Звіт «Розробка та впровадження типових рішень щодо комплексної системи захисту інформації в АІС НАНУ» (КСЗІ АІС НАНУ): Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. 05540149.90000.043.И3-06. — К.: НАН України 209. — 149 с.

15. Звіт «Розробка та впровадження типових рішень щодо комплексної системи захисту інформації в АІС НАНУ» (КСЗІ АІС НАНУ): Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. 05540149.90000.043.И3-06. — К.: НАН України 2019. — 149 с.

16. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. — [Чинний від 2010-07-01]. — К.: Національний банк України 2020. — 163 с. — (Галузевий стандарт України).

17. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою : ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – [проект]. - К.: Національний банк України 2020. – 163 с. : табл. – (Галузевий стандарт України).

18. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. — [Чинний від 2010-07-01]. — К.: Національний банк України 2010. — 163 с. — (Галузевий стандарт України).

19. Калюжний Р. Питання концепції реформування інформаційного законодавства України / Калюжний Р., Говловський В., Цимбалюк В., Гузалюк М. // Збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». К.: НТУУ «КПІ», Міністерсово освіти і науки України, СБУ. – К. – 2017. – С. 17-21.

20. Ковтун С. В. Інформаційна безпека: підручник / С.В. Ковтун. – Харків. Вид. ХНЕУ, 2019. – 368 с.

21. Кожунова О.О. Забезпечення інформаційної безпеки на сучасному підприємстві // Школа науки. - 2018. - №2. - С. 19-21.

22. Кононович В.Г. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Ч. 4. Інформаційна безпека комунікаційних мереж та послуг. Реагування на атаки. Навчальний посібник / В.Г. Кононович, С.В. Гладиш. — Одеса : ОНАЗ ім. О.С. Попова, 2019. — 208 с.

23. Концепція створення та забезпечення функціонування інфраструктури захисту державних інформаційних ресурсів в інформаційно - телекомунікаційних системах. [Електронний ресурс] – Режим доступу:http://www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=16D68 FCE54A40938081139F546DD E47B?art_id=38814&cat_id=38712

24. Малькевич Р. Проблеми забезпечення безпеки інформації підприємства в умовах пандемії / Р. Малькевич, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.69-72).

25. Мамаєва Л.М., Кондратьєва О.А. Основні напрями забезпечення інформаційної безпеки підприємства // Інформаційна безпека регіонів. - 2016. - №2. - С. 5-9.

26. Модель підсистеми моніторингу інцидентів безпеки інформації в інформаційних системах організацій / І.А. Пількевич, В.І. Котков, Н.М. Лобанчикова, І.І. Сугоняк // Восточноевропейский журнал передовых технологий. — 2012. — № 2 (56). — С. 18–21.

27. НД ТЗІ 1.3-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – 30 с.

28. НД ТЗІ 1.4-001-00 Типове положення про службу захисту інформації в автоматизованій системі. – 32 с.

29. Організація щодо реагування на інциденти та обробка інцидентів безпеки: Керівництво для організації електрозв'язку. Рекомендація МСЭ-Т E.409 (ITU-T E.409. — [Чинне від 2004-28-05]. — Женева. — 22 с. — (Рекомендація Міжнародної організації телекомунікацій (ITU)).

30. Організація щодо реагування на інциденти та обробка інцидентів безпеки: Керівництво для організації електрозв'язку. Рекомендація МСЭ-Т E.409 (ITU-T E.409. — [Чинне від 2004-28-05]. — Женева. — 22 с. — (Рекомендація Міжнародної організації телекомунікацій (ITU)).

31. Потий А. В. Формальная модель процесса защиты информации / А. В. Потий // Радіоелектрон. і комп'ют. системи. – 2016. – №5. – С. 128-133.

32. Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. [Електронний ресурс] – 2009. – 143 с. – Режим доступу: www.isofts.kiev.ua

33. ДСТУ ISO/IEC 27035-2:2018 Информационные технологии. Методы защиты. Управление инцидентами информационной безопасности. Часть 2. Руководство по планированию и подготовке к реагированию на инциденты (ISO/IEC 27035-2:2016, IDT) від 10.12.2018.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ)