**Міністерство освіти і науки України**
**Національний технічний університет**
**«Дніпровська політехніка»**

**Інститут електроенергетики**
**Факультет інформаційних технологій**
**Кафедра безпеки інформації та телекомунікацій**

# ПОЯСНЮВАЛЬНА ЗАПИСКА
## кваліфікаційної роботи ступеню магістра

**студента** *Дем'янюка Максима Юрійовича*

**академічної групи** *125м-17-1*

**спеціальності** *125 Кібербезпека*

**спеціалізації**[1]

**за освітньо-професійною програмою** *Кібербезпека*

**на тему** *Обґрунтування моделі розслідування інцидентів кібербезпеки із врахування критеріїв захищеності інформації*

| Керівники | Прізвище, ініціали | Оцінка за шкалою | | Підпис |
|---|---|---|---|---|
| | | рейтинговою | інституційною | |
| кваліфікаційної роботи | д.т.н., проф. Корнієнко В.І. | | | |
| розділів: | | | | |
| спеціальний | ст. викл. Мєшков В.І. | | | |
| економічний | к.е.н., доц. Пілова Д.П. | | | |

| | | | | |
|---|---|---|---|---|
| **Рецензент** | | | | |

| | | | | |
|---|---|---|---|---|
| **Нормоконтролер** | ст. викл. Мєшков В.І. | | | |

**Дніпро**
**2018**

**ЗАТВЕРДЖЕНО:**
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

# ЗАВДАННЯ
## на кваліфікаційну роботу ступеня магістра

**студенту** *Дем'янюку М.Ю.* **академічної групи** *125м-17-1*
(прізвище та ініціали) (шифр)

**спеціальності** *125 Кібербезпека*

**спеціалізації**[1]

**за освітньо-професійною програмою** *Кібербезпека*

**на тему** *Обґрунтування моделі розслідування інцидентів кібербезпеки із врахуванням критеріїв захищеності інформації*

**1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ**

Наказ ректора НТУ «Дніпровська політехніка» від 29.11.2018 № 2025-л_____

**2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ**

**Об'єкт досліджень** *процес розслідування інцидентів кібердезпеки*

**Предмет досліджень** *методи розслідування інцидентів кібербезпеки*

**Мета** *аналіз моделей розслідування інцидентів кібербезпеки та підвищення ефективності розслідування відповідних інцидентів*

**Вихідні дані для проведення роботи** *законодавство України та міжнародні стандарти у сфері кібербезпеки, існуючі алгоритми оцінки загроз інформаційної безпеки підприємства, підходи до розслідування інцидентів кібербезпеки*

**3 ОЧІКУВАНІ РЕЗУЛЬТАТИ**

**Наукова новизна** *сформовані рекомендації розслідування інцидентів кібербезпеки за методикою міжнародного стандарту ISO 27037 з врахуванням критеріїв захищеності інформації*

**Практична цінність** ***розробка рекомендацій щодо розслідування інцидентів кібербезпеки***

## 4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

***Дати рекомендації щодо застосування запропонованого алгоритму розслідування інцидентів кібербезпеки***

## 5 ЕТАПИ ВИКОНАННЯ РОБІТ

| **Найменування етапів робіт** | **Строки виконання робіт** (початок-кінець) |
|---|---|
| Огляд джерел за темою та напрям досліджень | 03.09.18-06.10.18 |
| Методи досліджень | 07.10.18-31.10.18 |
| Результати досліджень | 01.11.18-24.11.18 |
| Виконання економічного розділу | 25.11.18-04.12.18 |
| Оформлення пояснювальної записки | 05.12.18-10.12.18 |

## 6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

**Економічний ефект** ***від реалізації запропонованого процесу розслідування інцидентів, очікується позитивна динаміка розвитку підприємства, за рахунок зниження вартості системи захисту інформації***

**Соціальний ефект** ***полягає у швидкому розслідувані інцидентів кібербезпеки, що зменшить час відновлення системи після атаки***

## 7 ДОДАТКОВІ ВИМОГИ

**Завдання видано** _____ Корнієнко В.І.
(підпис керівника) (прізвище, ініціали)

**Дата видачі: 03.09.18р.**

**Дата подання до екзаменаційної комісії: 14.12.18р.**

**Прийнято до виконання** _____ Дем'янюк М.Ю.
(підпис студента) (прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка: ___ с., __ рис., __ табл., 4 додатки, 37 джерел.

Об’єкт дослідження: процес розслідування інцидентів кібербезпеки.

Метою дипломної роботи є аналіз моделей розслідування інцидентів кібербезпеки та підвищення ефективності розслідування відповідних інцидентів.

Методи дослідження: порівняння, узагальнення, вивчення і аналіз літератури, аналіз отриманих даних, накопичення і відбір фактів, встановлення зв’язків, опис, послідовна підстановка.

Найважливішим результатом дипломної роботи є аналіз статистичних даних, сучасних моделей і процесів розслідування інцидентів кібербезпеки в інформаційно-телекомунікаційній системі підприємства. Формалізація рекомендацій процесу розслідування інцидентів з врахуванням критеріїв захищеності інформації.

В дипломній роботі проведено аналіз актуальних проблем забезпечення кібербезпеки в Україні, аналіз міжнародних стандарті у сфері кібербезпеки, аналіз моделей розслідування інцидентів кібербезпеки, надана класифікація загроз і інцидентів, проаналізовано процеси управління кібербезпекою, проведено аналіз критеріїв захищеності інформації, досліджено процеси розслідування інцидентів кібербезпеки, сформовано рекомендації для розслідування інцидентів на підприємстві.

КІБЕРБЕЗПЕКА, АВТОМАТИЗОВАНА СИСТЕМА, ІНФОРМАЦІЙНА СИСТЕМА, МОДЕЛІ РОЗСЛІДУВАННЯ, АНАЛІЗ ЗАГРОЗ, ІНЦИДЕНТИ.

# РЕФЕРАТ

Пояснительная записка: ___ с., __ рис., __ табл., 4 приложений, 37 источников.

Объект исследования: процесс расследования инцидентов кибербезопасности.

Целью дипломной работы является анализ моделей расследования инцидентов кибербезопасности и повышения эффективности расследования соответствующих инцидентов.

Методы исследования: сравнение, обобщение, изучение и анализ литературы, анализ полученных данных, накопления и отбор фактов, установления связей, описание, последовательная подстановка.

Важнейшим результатом работы является анализ статистических данных, современных моделей и процессов расследования инцидентов кибербезопасности в информационно-телекоммуникационной системе предприятия. Формализация рекомендаций процесса расследования инцидентов с учетом критериев защищенности информации.

В дипломной работе проведен анализ актуальных проблем обеспечения кибербезопасности в Украине, анализ международных стандартов в области кибербезопасности, анализ моделей расследования инцидентов кибербезопасности, предоставленная классификация угроз и инцидентов, проанализированы процессы управления кибербезопасностью, проведен анализ критериев защищенности информации, исследованы процессы расследования инцидентов кибербезопасности, сформированы рекомендации для расследования инцидентов на предприятии.

КИБЕРБЕЗОПАСНОСТЬ, АВТОМАТИЗИРОВАННАЯ СИСТЕМА, ИНФОРМАЦИОННАЯ СИСТЕМА, МОДЕЛИ РАССЛЕДОВАНИЯ, АНАЛИЗ УГРОЗ, ИНЦИДЕНТОВ.

# ABSTRACT

Explanatory note: ___ p., __ fig., __ tab., 4 application, 37 sources.

Object of study: the process of investigating cybersecurity incidents.

The aim of the thesis is to analyze the models for investigating cybersecurity incidents and to increase the effectiveness of investigating relevant incidents.

Research methods: comparison, synthesis, study and analysis of the literature, analysis of the data obtained, the accumulation and selection of facts, establishing links, description, consistent substitution.

The most important result of the work is the analysis of statistical data, modern models and processes for the investigation of cybersecurity incidents in the information and telecommunication system of the enterprise. Formalizing the recommendations of the incident investigation process, taking into account information security criteria.

The thesis analyzes the current problems of ensuring cybersecurity in Ukraine, analyzes international standards in the field of cybersecurity, analyzes models for investigating cybersecurity incidents, provides a classification of threats and incidents, analyzes cybersecurity management processes, analyzes the cybersecurity incidents, and draws up recommendations to investigate incidents in the enterprise.

CYBERBE SECURITY, AUTOMATED SYSTEM, INFORMATION SYSTEM, INVESTIGATION MODELS, THREAT ANALYSIS, INCIDENTS.

# СПИСОК УМОВНИХ СКОРОЧЕНЬ

SIEM – Security Information and Event Management;

TCO – Total Cost of Ownership;

АС – автоматизована система;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ІС – інформаційна система;

КС – комп’ютерна система;

КЗЗ – комплекс засобів захисту;

НД – нормативний документ;

НД ТЗІ – нормативний документ системи технічного захисту інформації;

НСД – несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ОПР – особа, що приймає рішення;

ПЗ – програмне забезпечення;

СППР – системи підтримки прийняття рішень;

СТЗ – спеціальні технічні засоби.

ЗМІСТ

с.

# ВСТУП

В сучасних умовах, що характеризуються значними обсягами інформаційного контенту і ресурсів, якими володіють існуючі організації і установи все більшої актуальності набувають проблеми забезпечення захисту інформацією. Для адекватного захисту від різних спроб небажаного вторгнення зловмисників з метою попередження можливих загроз необхідна розробка і впровадження комплексу ініціатив, що включає науково-дослідні розробки в області захисту інформації.

Основне завдання забезпечення кібербезпеки все частіше вирішується внаслідок поліпшення процесу управління інформацією на базі реалізації різних підходів і методів, дотримання нормативних вимог і застосування організаційних заходів.

Інциденти інформаційної безпеки є окремим підкласом кризових і надзвичайних ситуацій, що можуть відбутися в інформаційній, соціальній, технічній інфраструктурі держави, організації, як окремий випадок, – в організаційно-технічних системах та інформаційно-комунікаційних мережах, впливаючи на стан державних інформаційних ресурсів і національної безпеки.

Дослідженню процесів реагування, обробки, розслідування, керування інцидентами кібербезпеки присвячено багато публікацій, зокрема науково-теоретичного, науково-прикладного та виробничо-практичного змісту. Існує стандартизована міжнародна нормативно-методологічна база.

Але на сьогодні все ще існує цілий ряд наукових, технічних, організаційних і нормативно-правових завдань, які є недостатньо вирішеними.

Як в Україні, так і в світовій практиці завдання підтримки прийняття рішень й автоматизації керування інцидентами кібербезпеки потребує подальшого дослідження. В жодному міжнародному чи вітчизняному нормативно-технічному документі, які частково торкаються або повністю

присвячені керуванню інцидентами кібербезпеки, не визначено, що саме можна/треба розуміти під розслідуванням інцидентів, з яких функцій, елементів, процесів та методів складається розслідування, та як його проводити.

Тому тематика розслідування інцидентів кібербезпеки, є не достатньо вивченою серед науковців і найближчому майбутньому досліджуватиметься, розроблятимуться нові моделі розслідування, вдосконалюватиметься процес розслідування інцидентів кібербезпеки.

Актуальність. З провадження інформаційних технологій майже у всіх сферах життя людини, виникає проблема із захистом і стабільною роботою цих систем. Як технічний прогрес так і зловмисники котрі хочуть заволодіти інформацією і використовувати її в зловмисних цілях, не стоять на одному місці і з кожним днем зловмисники вигадують нові способи заволодіння такими даними. З міжнародної статистики по інцидентам кібербезпеки, ми можемо прослідкувати таку тенденцію, що з кожним роком збільшується кількість інцидентів, їх різноманітність і найголовніше прибуток зловмисників.

Те що вважалося неможливим раніше, сьогодні стає реальністю. Це різного характеру програмні і технічні закладки, це персонал, який з однієї сторони із-за своєї неуважності, з іншої з корисливих мотивів, передає інформацію зловмиснику. Купуючи нову техніку чи програмне забезпечення, не можна бути впевненим, що в ньому не вбудована закладка.

Звісно виникає питання навіщо розслідувати інцинденти, якщо їх можна не допускати. Але це дуже складно зробити, так як запобігти реалізації інциденту – це мабуть не можливо, тому що у найдосконалішої системи є слабкі місця, потрібен тільки час, щоб їх знайти.

Отже потрібно прийняти такі заходи після інциденту, котрі дадуть можливість мінімізувати збитки і в подальшому знизять ризики реалізації такого виду інциденту.

Вирішити це питання може модель розслідування інцидентів інформаційної безпеки, котра у найкоротші терміни дасть можливість відновити систему, виявити слабке місце, яким скористався зловмисник і знайти докази котрі вкажуть на особу зловмисника.

# РОЗДІЛ 1. АНАЛІЗ МОДЕЛЕЙ ТА ПРОЦЕСІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

На сьогодні актуальність проблеми кібербезпеки не викликає жодних сумнівів: щодня кожен громадянин України стикається з необхідністю користування інформаційними технологіям: від соціальних мереж і розміщення інформації, що містить персональні дані в мережі Інтернет, до користування банкоматами, банківськими рахунками тощо. У зв'язку із цим виникає питання, чи врегульовано проблему із безпекою в кіберпросторі у вітчизняному законодавстві і як себе захистити від кіберзлочинців.

Варто відмітити, що питання про забезпечення кібербезпеки повільно, але все ж таки вирішується, Верховна Рада прийняла закон «Про основні засади забезпечення кібербезпеки України», що пропонує запровадити до термінології національного законодавства нові поняття, зокрема, «індикатори кіберзагроз», «інформація про інцидент кібербезпеки», «кіберінцидент», «кібератака», «кібербезпека», «кіберзагроза», «кіберзахист», «кіберзлочин», «кіберзлочинність», «кібероборона», «кіберпростір», «кіберрозвідка», «кібертероризм», «кібершпигунство», «критична інформаційна інфраструктура».

Недосконаліть законодавчої бази, не тільки в Україні, а й на міжнародній арені, призводить до невтішної статистики: у 2007 році дохід кіберзлочинців вперше перевищив дохід від продажу наркотичних засобів. І саме тому хочеться навести деякі статистичні дані, що підтвердять те, що забезпечення кібербезпеки залишається відкритим питанням і в цьому напрямку потрібно виконати багато роботи, для того щоб почуватися у певній безпеці.

Статистичні дані, котрі пропонують міжнародні організації, які займаються їх збором, а саме Infowatch, Kaspersky, U.S. Department of Justice Federal Bureau of Investigation , свідчать проте, що Україна посіла п'яте місце в світі (і перше в Європі) за ризиками зіткнення з веб-загрозами в першому кварталі 2016 року. За даними Kaspersky Security Network у 2017 третина (33%)

українських користувачів мережі зіткнулися з загрозами, що поширюються через мережу Інтернет [1-3].

До основних кіберзагроз можна віднести такі:

– таргетовані атаки;

– зловживання у соціальних мережах (вплив на суспільство);

– атаки на банківські системи (викрадення грошей);

– атаки на системне урядування;

– апаратні закладки у мікросхемах і прошивках комп'ютерного і мережного обладнання.

Україна, крім того, займає четверте місце за кількістю підприємств, що зазнали DDoS-атаки. Так, за перший квартал 2016 року частка України за даною величиною на міжнародній арені стрімко збільшилась. Про це свідчить статистика, яку нам пропонує Kaspersky Security Network: з усіх DDoS-атак 93,6% приходяться на десять країн [4-8].

## 1.1 Методи оцінки інформаційної безпеки

Призначення системи інформаційної безпеки полягає в організації безпечних і надійних: заходів з доступу до інформації, способів передачі та зберігання інформації, методів обробки інформації, правил управління доступом до інформації, способів відновлення інформації, методів резервування інформації тощо.

Завдання системи інформаційної безпеки обумовлюються її призначенням і полягають у: забезпеченні безпечного, надійного зберігання і передачі інформації в електронному вигляді, розташованої на різних носіях; організації надійного доступу до електронної інформації; обмеження і контроль доступу до інформації, з якою працюють співробітники; створенні правил безпечної роботи з інформацією; проведенні заходів щодо резервування інформації; забезпеченні відновлення інформації в аварійних ситуаціях; підтримці інформаційної безпеки на заданому рівні.

Забезпечення інформаційної безпеки в епоху постіндустріальної

економіки стає життєво важливим для успішного існуванні підприємства. З іншого боку, постає питання належного визначення стану інформаційної безпеки підприємства, показників, що його характеризують, а також значень цих показників, які б забезпечували належний рівень інформаційної безпеки підприємства.

Також важливим є питання оцінювання значень цих показників в умовах невизначеності, яка притаманна сфері безпеки.

В нинішній час для забезпечення належного стану інформаційної безпеки потрібна не просто розробка окремих механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів і т.д.).

Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування підприємства, запобігання загроз його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення в рамках виробничої діяльності всіх підрозділів підприємства.

Унаслідок сукупної дії зовнішніх і внутрішніх дестабілізуючих факторів перед службами захисту інформації стоять завдання не тільки створення, а й постійного вдосконалення захисту інформації. Необхідність вдосконалення призводить до постійного проведення моніторингу і аналізу стану інформаційної безпеки.

Удосконалення, поліпшення стану ІБ можливо за умови знання станів характеристик і параметрів використовуваних засобів захисту, процесів менеджменту, усвідомлення ІБ і розуміння ступеня їх відповідності необхідним результатам. Зрозуміти ці аспекти безпеки можна лише за результатами оцінки ІБ організації, отриманої за допомогою моделі оцінки ІБ на підставі свідчень оцінки, критеріїв оцінки та з урахуванням контексту оцінки.

Критерії оцінки – це все те, що дозволяє встановити значення оцінки для

об’єкта оцінки. В якості критеріїв оцінки ІБ можуть використовуватися вимоги ІБ, процедури ІБ, поєднання вимог і процедур ІБ, рівень інвестицій, витрат на ІБ.

До свідчень оцінки ІБ відносяться записи, виклад фактів або будь-яка інформація, яка має відношення до критеріїв оцінки ІБ і може бути перевірена. Такими посвідченнями оцінки ІБ можуть бути докази виконуваної й виконаної діяльності по забезпеченню ІБ у вигляді звітних, нормативних, розпорядчих документів, результатів опитувань, спостережень.

Контекст оцінки ІБ об’єднує цілі і призначення оцінки ІБ, вид оцінки (незалежна оцінка, самооцінка), об’єкт та області оцінки ІБ, обмеження оцінки та ролі.

Модель оцінки ІБ визначає сферу оцінки, що відображає контекст оцінки ІБ в рамках критерію оцінки ІБ, відображення і перетворення оцінки в параметри об’єкта оцінки, а також встановлює показники, що забезпечують оцінку ІБ у сфері оцінки.

У загальному вигляді процес проведення оцінки ІБ (рис. 1.1.) представлений основними компонентами процесу: контекст, свідоцтва, критерії та модель оцінки – необхідними для реалізації процесу оцінки.

Оцінка ІБ полягає у виробленні оціночного судження щодо придатності (зрілості) процесів забезпечення ІБ, адекватності використовуваних захисних заходів або доцільності (достатності) інвестицій (витрат) для забезпечення необхідного рівня ІБ на основі вимірювання та оцінювання критичних елементів (факторів) об’єкта оцінки.

Поряд з найважливішим призначенням оцінки ІБ – створення інформаційної потреби для вдосконалення ІБ, можливі й інші цілі проведення оцінки ІБ, такі як:

– визначення міри відповідності встановленим критеріям окремих областей забезпечення ІБ, процесів забезпечення ІБ, захисних заходів;

– виявлення впливу критичних елементів (факторів) та їх сполучень на ІБ організації;

– порівняння зрілості різних процесів забезпечення ІБ і порівняння ступеня відповідності різних захисних заходів встановленим вимогам.

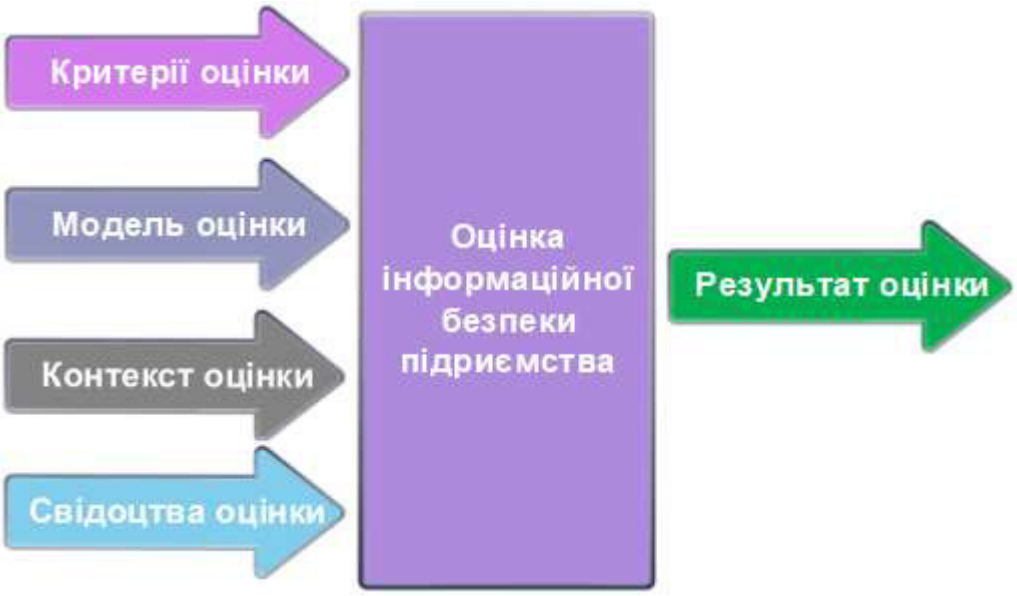


Рисунок 1.1 – Загальний вид процесу оцінки ІБ підприємства

Результати оцінки ІБ підприємства можуть також використовуватися зацікавленою стороною для порівняння рівня ІБ схожих організацій.

В залежності від обраного для оцінки ІБ критерію можна розділити способи оцінки ІБ організації на:

– оцінку за еталоном;
– ризик-орієнтовану оцінку;
– оцінку за економічними показниками.

Спосіб оцінки ІБ за еталоном зводиться до порівняння діяльності та заходів щодо забезпечення ІБ організації з вимогами, закріпленими в еталоні. По суті справи проводиться оцінка відповідності СЗІБ організації встановленому еталону. Під оцінкою відповідності ІБ організації встановленим критеріям розуміється діяльність, пов’язана з прямим або непрямим визначенням виконання або невиконання відповідних вимог ІБ в організації. За допомогою оцінки відповідності ІБ вимірюється правильність реалізації процесів системи забезпечення ІБ організації та ідентифікуються недоліки такої реалізації.

У результаті проведення оцінки ІБ має бути сформована оцінка ступеня відповідності системи захисту інформації еталону, в якості якого можуть бути прийняті (у сукупності і окремо):

– вимоги вітчизняного законодавства в області ІБ;

– галузеві вимоги щодо забезпечення ІБ;

– вимоги нормативних, методичних та організаційно-розпорядчих документів щодо забезпечення ІБ;

– вимоги національних і міжнародних стандартів в області ІБ.

Основні етапи оцінки інформаційної безпеки за еталоном включають вибір еталона і формування на його основі критеріїв оцінки ІБ, збір свідчень оцінки і вимірювання критичних елементів (факторів) об’єкта оцінки, формування оцінки ІБ.

Ризик-орієнтована оцінка ІБ підриємства являє собою спосіб оцінки, при якому розглядаються ризики ІБ, що виникають в інформаційній сфері організації, і зіставляються існуючі ризики ІБ і вжиті заходи по їх обробці. В результаті має бути сформована оцінка здатності організації ефективно управляти ризиками ІБ для досягнення своїх цілей.

Основні етапи ризик-орієнтованої оцінки інформаційної безпеки включають ідентифікацію ризиків ІБ, визначення адекватних процесів менеджменту ризиків і ключових індикаторів ризиків ІБ, формування на їх основі критеріїв оцінки ІБ, збір свідчень оцінки і вимірювання ризик-факторів, формування оцінки ІБ [12-15].

Спосіб оцінки ІБ на основі економічних показників оперує зрозумілими для бізнесу аргументами про необхідність забезпечення та вдосконалення ІБ. Для проведення оцінки в якості критеріїв ефективності засобів інформаційної безпеки використовуються, наприклад, показники сукупної вартості володіння (Total Cost of Ownership – TCO).

Під показником TCO розуміється сума прямих і непрямих витрат на впровадження, експлуатацію та супровід системи захисту інформації. Під прямими витратами розуміються всі матеріальні витрати, такі як купівля

обладнання та програмного забезпечення, трудовитрати відповідних категорій співробітників. Непрямими є всі витрати на обслуговування системи захисту інформації, а також втрати від інцидентів, що відбулися. Збір та аналіз статистики по структурі прямих і непрямих витрат проводиться, як правило, протягом року. Отримані дані оцінюються по ряду критеріїв із показниками ТСО аналогічних організацій галузі.

Оцінка на основі показника ТСО дозволяє оцінити витрати на інформаційну безпеку і порівняти ІБ організації з типовим профілем захисту, а також управляти витратами для досягнення необхідного рівня захищеності.

Основні етапи оцінки ефективності СЗІБ на основі моделі ТСО включають збір даних про поточний рівень ТСО, аналіз областей забезпечення ІБ, вибір порівнянної моделі ТСО в якості критерію оцінки, порівняння показників з критерієм оцінки, формування оцінки ІБ.

Однак цей спосіб оцінки вимагає створення загальної інформаційної бази даних про ефективність СЗІБ організацій схожого бізнесу та постійної підтримки бази даних в актуальному стані. Така інформаційна взаємодія організацій, як правило, не відповідає цілям бізнесу. Тому оцінка ІБ на основі показника ТСО практично не застосовується.

Далі розглянемо докладніше спосіб оцінки ІБ на основі еталона і спосіб ризик-орієнтованої оцінки ІБ.

## 1.2 Процеси забезпечення кібербезпеки

Зростає різноманітність, складність і технологічність загроз та засобів впливу, збільшується кількість вразливостей елементів сучасного кіберпростору внаслідок його надзвичайної гнучкості. При цьому, існуючі засоби та заходи захисту не здатні в повному обсязі протидіяти наявній множині загроз [22-25].

До основних міжнародних стандартів у сфері управління інцидентами належать:

ISO/IEC 27001:2013 «Система управління інформаційною безпекою. Вимоги». В рамках даного стандарту висуваються загальні вимоги до побудови

системи управління інформаційною безпекою, що відносяться у тому числі і до процесів управління інцидентами.

ISO/IEC 27032:2012 «Інформаційні технології – Методи забезпечення безпеки – Керівництво з ІБ».

Він охоплює базові практики безпеки для зацікавлених сторін в кіберпросторі . Цей стандарт встановлює:

– пояснення взаємозв'язку між кібербезпека і іншими видами безпеки;

– визначення зацікавлених сторін і опис їх ролі в кібербезпеці;

– керівництво для вирішення спільних питань кібербезпеки і рамки для того, щоб зацікавлені сторони співпрацювали у вирішенні питань кібербезпеки.

ISO/IEC 27035:2016 «Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки», надає практичні рекомендації з виявлення, реєстрації і оцінки випадків порушення інформаційної безпеки і вразливостей. Інтеграція системи управління інцидентами інформаційної безпеки дає ряд переваг:

– підвищення загального рівня інформаційної безпеки;

– зменшення негативних наслідків для бізнесу;

– посилення акценту на попередження інцидентів інформаційної безпеки,

– призначення пріоритетів і збору даних;

– внесок в обґрунтування рішень щодо виділення бюджету та ресурсів;

– поліпшення якості результатів оцінки та управління ризиками інформаційної безпеки;

– поліпшення інформованості в галузі інформаційної безпеки і допомога у підготовці матеріалів для навчання;

– надання додаткової інформації для розроблення політики інформаційної безпеки та супутньої документації для процесу розслідування інцидентів кібербезпеки.

ISO/IEC 27037:2012 «Методи та засоби забезпечення безпеки».

Керівні принципи для ідентифікації, збору, одержання та збереження цифрових доказів

У цьому стандарті розглянуте наступне:

– вимоги поводження з доказами;

– ідентифікація, збір, отримання та зберігання доказів;

COBIT 5:2012 – цілі контролю за інформаційними та суміжними технологіями. На стандарт покладене вирішення наступних завдань: збереження єдиного підходу до збору, аналізу інформації, підготовки висновків і висновків на всіх етапах управління, контролю і аудиту IT, можливість порівняння існуючих IT-процесів з «кращими» практиками, в тому числі галузевими.

NIST SP 800-61 у цьому стандарті розглянуті наступні аспекти:

– організація у комп'ютерної безпеки з реагування на інциденти;

– звернення до інциденту;

– координація та обмін інформацією з інциденту.

BSI-DSZ-CC-0931-2015 – німецький стандарт, у якому представлено наступне:

– загальний метод управління інформаційною безпекою;

– описи компонентів сучасних інформаційних технологій;

– описи основних компонентів організації режиму інформаційної безпеки;

– характеристики об'єктів інформатизації;

– характеристики основних інформаційних активів компанії;

– характеристики комп'ютерних мереж на основі різних мережевих технологій;

– характеристика активного і пасивного телекомунікаційного обладнання провідних брендів;

– докладні каталоги загроз безпеки і заходів контролю.

Стандарти рекомендують, що має бути впроваджено для того, щоб забезпечити максимальний рівень захисту. Але для того, щоб впроваджувати потрібно визначитись у яких процесах ІБ та кібербезпеки це можливо зробити:

1 Процес управління інформаційними активами;

2 Процес управління ризиками інформаційної безпеки;

3 Процес управління документацією в області інформаційної безпеки;

4 Процес управління записами в області інформаційної безпеки;

5 Процес моніторингу та аналізу системи управління інформаційною

безпекою;

6 Процес аналізу системи управління інформаційною безпекою з боку керівництва;

7 Процес аудиту інформаційної безпеки;

8 Процес управління інцидентами інформаційної безпеки.

Розглянемо кожен з процесів детальніше:

Процес управління інформаційними активами необхідний для того, щоб:

– створити, впровадити, експлуатувати, постійно контролювати, аналізувати, підтримувати активи в робочому стані і покращувати СУІБ;

– гарантувати, що процедури захисту інформації підтримують ділові вимоги;

– виявити і розглядати законодавчі та нормативні вимоги, а також договірні зобов'язання щодо захисту;

– підтримувати в робочому стані адекватний захист шляхом правильного застосування всіх реалізованих засобів управління;

– проводити аналіз, коли це необхідно, і відповідним чином реагувати на результати цього аналізу;

– коли це доцільно, покращувати результативність СУІБ.

Метою процесу управління ризиками ІБ є виявлення, контроль та мінімізація невизначеності впливу ЧД. Виділимо чотири основні етапи управління ризиками ІБ, яке здійснюється з метою забезпечення неперервності функціонування ІТС, зокрема підсистеми СЗІ:

1 Аналіз ризику. Виявлення та оцінка ЧД, які можуть скомпрометувати ІБ важливих інформаційних активів. Дає змогу визначити профілактичні заходи щодо зниження ймовірності виникнення ЧД і визначити контрзаходи з метою успішної нейтралізації цих обмежень ще на етапі проектування.

2 Оцінка ризику. Є процесом визначення рівня ризику. Ризик традиційно обчислюватимемо як функцію важливості активів, ймовірності виникнення загрози і наявності вразливостей, величини завданого збитку.

3 Зниження ризику. Це етап, на якому реалізовуються контролі та заходи щодо запобігання визначеним ризикам, а також впроваджуються засоби відновлення у разі реалізації ризиків, що можуть порушити неперервне

функціонування СЗІ.

4 Оцінка вразливостей та контролів. Аналіз основних властивостей ІТС та виявлення тих, які можна використати з метою реалізації загрози порушення властивості живучості, а також визначення ефективності та адекватності заходів ІБ та виявлення недоліків в її реалізації.

Стандартизація управління документацією дозволяє більш ефективно організувати роботу з документами у галузі управлінської діяльності. Стандартизація політики та процедур управління документацією забезпечує наявність належної уваги процесам ведення документації та збереженості всіх документів, а використання стандартної методики і процедур – більш швидкий і ефективний пошук інформації.

Управління документами всіх видів та на всіх носіях, створених або отриманих організацією (державною і недержавною) в процесі її діяльності, а також фізичними особами (суб'єктами підприємницької діяльності), які зобов'язані створювати та використовувати документи. Він визначає обов'язки організації під час реалізації процесів документування, надає рекомендації щодо розроблення політики управління документацією в організації та пов'язаних з нею процедур, систем і процесів, а також щодо розроблення та впровадження систем документації.

Процес управління документацією в області інформаційної безпеки. Методичний документ має бути створений для визначення дій керівництва, необхідних для наступного:

– затверджувати документи на адекватність перед випуском;

– аналізувати і оновлювати документи, в разі потреби, а також повторно затверджувати документи;

– гарантувати, що вказані зміни і поточний статус редакції документів затверджений;

– гарантувати, що мають відношення до справи версії застосовних документів доступні в місцях використання;

– гарантувати, що документи залишаються розбірливими та легко ідентифікуються в містах їх використання;

– гарантувати, що документи доступні тим, кому вони потрібні, і що

вони переміщаються, зберігаються, і, врешті-решт, ліквідуються відповідно до процедур , які застосовуються до їх класифікації;

– гарантувати, що документи зовнішнього походження ідентифіковані;

– гарантувати контроль за поширення документів;

– запобігати ненавмисне використання застарілих документів;

– застосовувати відповідну ідентифікацію до них, якщо вони зберігаються для будь-якої мети.

Процес управління записами в області інформаційної безпеки визначає наступне:

Записи повинні створюватися і підтримуватися в робочому стані для того, щоб забезпечувати підтвердження відповідності вимогам і результативної роботи СУІБ.

Записи повинні залишатися розбірливими, придатними для легкого ідентифікування та вилучення. Управлінські дії, необхідні для ідентифікації, зберігання, захисту, пошук, а також терміни зберігання і ліквідації записів повинні бути задокументовані та впроваджені.

У записах повинні бути відображені показники процесу, а також всі епізоди значних інцидентів в системі безпеки, пов'язані з СУІБ.

Процес аналізу системи управління інформаційною безпекою з боку керівництва, яке повинно аналізувати СУІБ організації через заплановані інтервали (по що найменш, один раз на рік), щоб гарантувати її постійну придатність, адекватність і результативність. Цей аналіз повинен включати в себе оцінювання можливостей для поліпшення і визначення потреби в змінах СУІБ, включаючи політику захисту інформації і мети захисту інформації. Результати аналізу повинні бути чітко задокументовані, а записи повинні підтримуватися в робочому стані [22-25].

Вихідні дані аналізування з боку керівництва повинні включати в себе рішення і дії направлені на:

– поліпшення результативності СУІБ;

– оновлення оцінки ризику і плану обробки ризику;

– зміни процедур і засобів управління, які впливають на захист інформації, якщо це необхідно, для того щоб зреагувати на внутрішні або

зовнішні події, які могли негативно вплинути на СУІБ, включаючи зміни в наступному:

1 Ділові вимоги;

2 Вимоги захисту;

3 Ділові процеси, що впливають на існуючі ділові вимоги;

4 Нормативні або законодавчі вимоги;

5 Договірні зобов'язання;

6 Рівні ризику і / або критерії прийняття ризику.

– необхідні ресурси;

– покращення в тому, як вимірюється результативність засобів управління.

Організація повинна проводити внутрішні аудити СУІБ через заплановані інтервали, з метою визначити чи цілі управління, заходи управління, процеси і процедури СУІБ відповідають наступним вимогам:

– чи відповідають вимогам цього державного стандарту і відносяться до них законів або норми;

– чи відповідають виявленим вимогам захисту інформації;

– чи ефективно реалізуються і підтримуються в робочому стані;

– чи функціонує належним чином система.

Програма аудити повинна бути спланована з урахуванням статусу та важливості процесів і областей, які потрібно перевіряти, а також результатів попередніх аудитів. Повинні бути визначені критерії, область застосування, частота і методи аудиту. Вибір аудиторів і проведення аудитів повинні гарантувати об'єктивність і неупередженість процесу аудиту. Аудитори не повинні здійснювати аудит своєї роботи.

Керівництво відповідальне за визначену область перевірки, повинно своєчасно і без затримок забезпечити проведення перевірки в цілях усунення виявлених невідповідностей і їх причин.

Міжнародний стандарт ISO 27001:2013 звертає особливу увагу на необхідність створення процедури управління інцидентами інформаційної безпеки – очевидно, що без своєчасної реакції на інциденти інформаційної безпеки і усунення їх наслідків неможливо ефективне функціонування системи

управління інформаційною безпекою. Основними завданнями, які повинні вирішуватися при управлінні інцидентами є:

– виявлення інциденту;

– оповіщення про виникнення інциденту;

– реєстрація інциденту;

– усунення наслідків та причин інциденту;

– розслідування інциденту;

– реалізація дій, покликаних унеможливлювати повторне виникнення інциденту.

До процесів забезпечення кібербезпеки відносяться:

1 Організація безпечної експлуатації засобів обробки, зберігання і передачі інформації;

2 Реєстрація та облік подій кібербезпеки;

3 Захист від шкідливого програмного забезпечення;

4 Резервне копіювання інформаційних ресурсів;

5 Захист мережевих сервісів і забезпечення мережевої безпеки;

6 Забезпечення кібербезпеки при поводженні зі змінами носіями інформації;

7 Захист програмного забезпечення;

8 Криптографічний захист інформації;

9 Контроль доступу;

10 Контроль захищеності і стану кібербезпеки.

Щоб впроваджувати процеси забезпечення кібербезпеки, потрібно розуміти, які є види інцидентів, загроз і атак.

Під загрозою безпеки КС будемо розуміти сукупність умов і факторів, що визначають потенційну або реально існуючу небезпеку порушення конфіденційності, цілісності і доступності інформації або зниження надійності реалізації функцій КС.

## 1.3 Процес оцінки інформаційної безпеки

### 1.3.1 Основні елементи процесу оцінки

Процес оцінки ІБ включає такі елементи проведення оцінки:

– зміст оцінки, який визначає вхідні дані: цілі й призначення оцінки ІБ, вид оцінки (незалежна оцінка, самооцінка), об’єкт та області оцінки ІБ, обмеження оцінки і ролі;

– критерії оцінки;

– модель оцінки;

– заходи процесу оцінки: збір свідчень оцінки та перевірка їх достовірності, вимірювання та оцінювання атрибутів об’єкта оцінки;

– вихідні дані оцінки.

– Основні елементи процесу оцінки ІБ представлені на рис. 1.2 у вигляді процесної моделі.

Перш ніж розглянути особливості способів оцінки ІБ підприємства, необхідно описати загальні для будь-якої оцінки ІБ компоненти: контекст оцінки, збір свідчень оцінки та перевірка їх достовірності, вимірювання та оцінювання атрибутів при проведенні оцінки різного виду (незалежна оцінка, самооцінка) і вихідні дані оцінки. Модель оцінки і критерії оцінки, що визначають особливості способів оцінки, будуть розглянуті в інших розділах.

### 1.3.2 Зміст оцінки інформаційної безпеки організації

Зміст оцінки ІБ включає цілі й призначення оцінки ІБ, вид оцінки, об’єкт та області оцінки ІБ, обмеження оцінки, ролі.

До ролей, які беруть участь у реалізації процесу оцінки, ставляться організатор, аналітик, керівник групи оцінки, оцінювач, власник активів, представник об’єкта оцінки.

Організатор (замовник) оцінки ІБ формує ціль оцінки (вдосконалення об’єкта оцінки, визначення відповідності об’єкта оцінки встановленим критеріям і т.д.) і визначає критерій оцінки, об’єкт та область оцінки. Під організатором оцінки розуміється особа або організація, що є внутрішніми або зовнішніми стосовно до оцінюваного об’єкта оцінки, які організовують проведення оцінки та надають фінансові та інші ресурси, необхідні для її проведення.

Організатор повинен забезпечити доступ групи оцінки (керівник групи

оцінки, оцінювач) до активів об’єкта оцінки для вивчення, до персоналу для проведення опитувань, до інфраструктури, необхідної під час оцінювання. Хоча керівництво об’єкта оцінки безпосередньо не має ніяких конкретних обов’язків з проведення оцінювання, усвідомлення важливості оцінки має дуже велике значення. Це особливо актуально в тому випадку, коли організатор оцінки не є членом керівництва об’єкта оцінки.


Рисунок 1.2 – Основні елементи процесу оцінювання ІБ

По завершенню оцінки організатор передає звітні документи по оцінці зацікавленим сторонам для використання їх у відповідності із заявленою метою оцінки.

Аналітик оцінки ІБ вибирає спосіб оцінки ІБ, модель оцінки і визначає методичне та інформаційне забезпечення оцінки, тобто методики, дані для оцінки. Аналітик оцінки аналізує результати оцінки і формує звіт і рекомендації за результатами оцінки ІБ.

Керівник групи оцінки та оцінювач вимірюють і оцінюють свідоцтва оцінки, надані власниками активів, і формують результати оцінки. Керівник групи повинен розподілити відповідальність між членами групи за оцінювання конкретних процесів, підрозділів, областей або видів діяльності об’єкта оцінки. Такий розподіл повинен враховувати потребу в незалежності, компетентності

фахівців з оцінки та результативному використанні ресурсів. Заходи по вимірюванню та оцінюванню виконуються виключно керівником групи оцінки та оцінювачем, що входять до групи оцінки. Інший персонал (представник об’єкта оцінки, технічний експерт) може брати участь у роботі групи оцінки для забезпечення спеціалізованих знань або консультацій. Вони можуть обговорювати з оцінювачем формулювання суджень, але не нестимуть відповідальність за остаточну оцінку.

На рис. 1.3 показані ролі учасників процесу оцінки ІБ і їх основні функції.

Важливим аспектом при визначенні контексту оцінки є вид оцінки: незалежна або самооцінка. Залежно від виду оцінки розрізняється відношення ролей процесу оцінки та об’єкта оцінки.

Незалежна оцінка досягається шляхом проведення оцінки групою оцінки, члени якої незалежні від об’єкта оцінки. Організатор оцінки може відноситися до тієї ж організації, до якої відноситься об’єкт оцінки, але не обов’язково до оцінюваного об’єкта. Ступінь незалежності може варіюватися відповідно до мети і областю оцінки. У разі зовнішнього організатора оцінки передбачається наявність взаємної угоди між організатором оцінки та організацією, до якої відноситься об’єкт оцінки. Представник об’єкта оцінки бере участь у формуванні свідоцтв оцінки, забезпечує взаємодію групи оцінки з власниками активів. Їх участь у проведенні оцінки дає можливість визначити і врахувати особливості об’єкта оцінки, забезпечити достовірність результатів оцінки.

Самооцінка виконується організацією з метою оцінки власної СЗІБ. Організатор самооцінки зазвичай входить до складу об’єкта оцінки, як і члени групи оцінки.

Область оцінки може включати, наприклад, один або декілька процесів об’єкта оцінки, наприклад, організатор може зосередити увагу на одному або декількох критичних процесах і / або захисних заходах. Вибір об’єкта оцінки повинен відображати намічене використання організатором вихідних даних оцінки. Наприклад, якщо вихідні дані призначені для використання при вдосконаленні діяльності по забезпеченню ІБ, то область оцінки повинна

відповідати області намічених робіт по вдосконаленню.

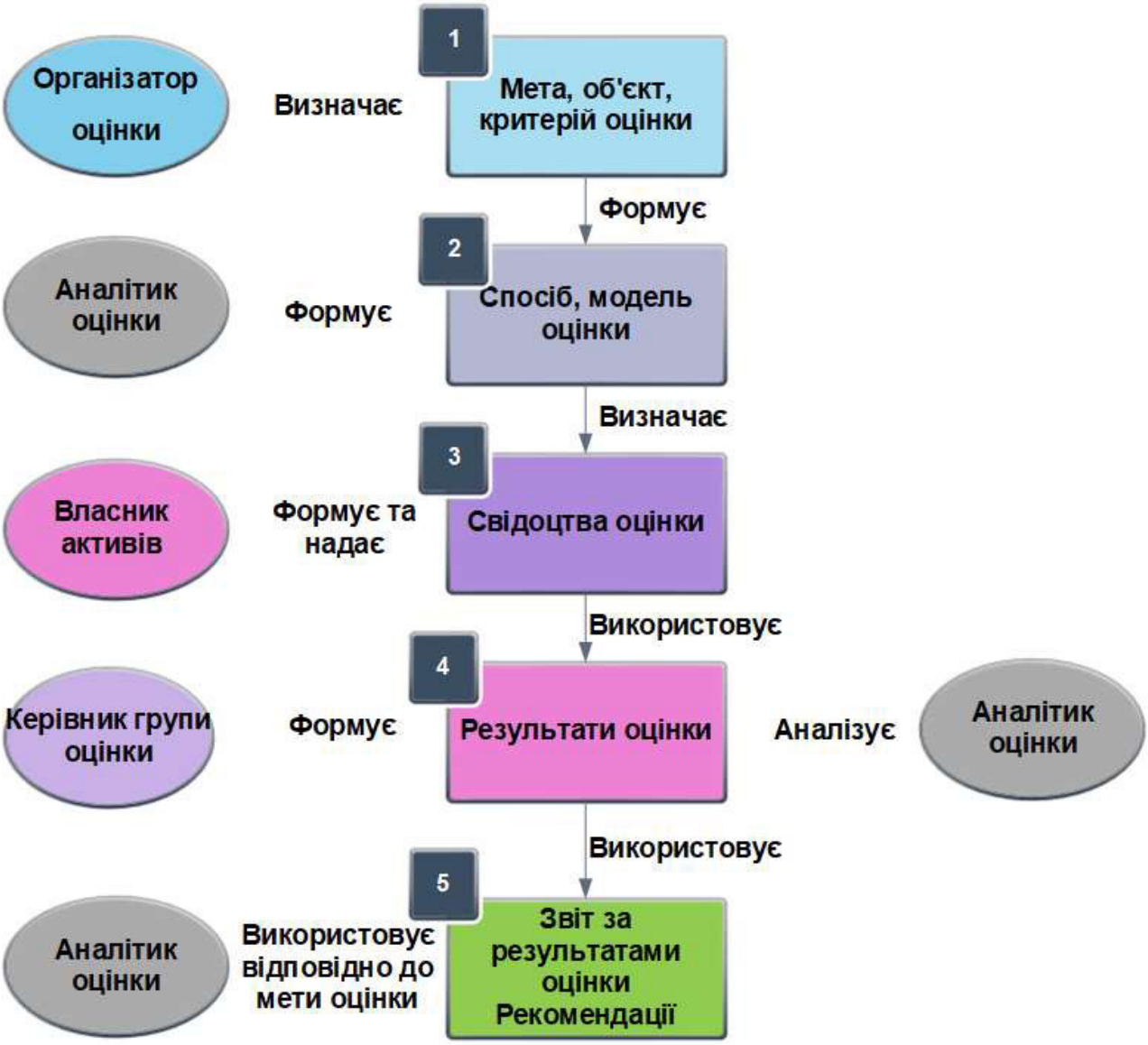


Рисунок 1.3 – Ролі учасників процесу оцінки ІБ і їх функції

Область оцінки може бути будь-якою: від окремого процесу до всієї організації. В контексті оцінки має бути представлено докладний опис об’єкта оцінки, що включає розміри об’єкта оцінки, область застосування продуктів або послуг об’єкта оцінки, основні характеристики (наприклад, обсяг, критичність, складність і якість) продуктів або послуг об’єкта оцінки.

До обмежень оцінки можна віднести можливу недоступність основних активів, використовуваних у звичайної ділової діяльності організації; недостатній часовий інтервал, виділений для проведення оцінювання;

необхідність виключення певних частин об’єкта оцінки через стадії життєвого циклу. Крім того, можуть бути накладені обмеження на кількість і вид даних, які повинні бути зібрані і вивчені.

Зміст контексту оцінки повинне бути погоджене керівником групи оцінки з організатором та уповноваженим представником об’єкта оцінки та задокументовано до початку процесу оцінки. Фіксування контексту оцінки важливо, так як він містить вихідні елементи процесу оцінки [31-35].

Під час виконання оцінки можуть відбуватися зміни в контексті оцінки. Зміни повинні бути схвалені організатором оцінки та уповноваженим представником об’єкта оцінки. Якщо ці зміни впливають на часовий графік і ресурси проведення оцінки, то планування оцінки має бути відповідним чином переглянуто.

## 1.4 Заходи та вихідні дані процесу оцінки

### 1.4.1 Збір свідчень оцінки та перевірка їх достовірності

Призначення заходу: збір свідчень оцінки з дотриманням умов забезпечення достовірної оцінки ІБ.

Незалежна оцінка ІБ може бути здійснена за допомогою внутрішнього і зовнішнього аудиту ІБ. Аудит ІБ визначається як систематичний, незалежний і документований процес отримання доказів діяльності організації по забезпеченню ІБ, визначення ступеня виконання в організації критеріїв ІБ, а також допускає можливість формування професійного аудиторського судження про інформаційну безпеку організації [31-35].

Необхідними умовами забезпечення достовірної оцінки ІБ при проведенні аудиту є:

– використання довіреної процесу аудиту та дотримання основних принципів аудиту;

– менеджмент програми аудиту ІБ;

– використання найбільш достовірних джерел свідоцтв оцінки;

– визначення обсягу вибірки з урахуванням заданої достовірності

свідчень оцінки;

– облік факторів, що впливають на аудиторський ризик, з метою зниження аудиторського ризику.

Довірений процес аудиту ІБ повинен відповідати вимогам прийнятого в організації нормативного документа, що описує процес аудиту ІБ, або вимогам визнаного співтовариством міжнародного (національного) нормативного документа (стандарту, рекомендації).

До основних принципів проведення аудиту ІБ відносяться:

1) незалежність аудиту ІБ.

Аудитори (група оцінки) незалежні у своїй діяльності і невідповідальні за діяльність, яка піддається аудиту ІБ. Незалежність є підставою для неупередженості при проведенні аудиту ІБ і об'єктивності при формуванні висновку за результатами аудиту ІБ.

2) повнота аудиту ІБ.

Аудит ІБ повинен охоплювати всі області аудиту ІБ, відповідні цілі оцінки. Крім того, повнота аудиту ІБ визначається достатністю затребуваних і наданих матеріалів, документів та рівнем їх відповідності поставленим завданням. Повнота аудиту ІБ є необхідною умовою для формування об'єктивних висновків за результатами оцінки ІБ.

3) оцінка на основі доказів аудиту ІБ.

При періодичному проведенні аудиту ІБ оцінка на основі доказів аудиту ІБ є єдиним способом, що дозволяє отримати повторюваний висновок за результатами аудиту ІБ, що підвищує довіру до такого висновку. Для повторюваності укладення свідоцтва аудиту ІБ повинні бути перевіреними.

4) достовірність доказів аудиту ІБ.

Оцінювачі повинні бути впевнені в достовірності свідчень оцінки ІБ. Довіра до документальних свідчень оцінки ІБ підвищується при підтвердженні їх достовірності третьою стороною або керівництвом організації. Довіра до фактів, отриманих при опитуванні співробітників об'єкта оцінки, підвищується при підтвердженні даних фактів з різних джерел. Довіра до фактів, отриманим

при спостереженні за діяльністю в області ІБ об’єкта оцінки, підвищується, якщо вони отримані безпосередньо при функціонуванні процедур або процесів, які перевіряються.

5) компетентність і етичність поведінки.

Довіра до процесу і результатів оцінки ІБ залежить від компетентності тих, хто проводить аудит ІБ, і від етичності їх поведінки. Компетентність базується на здатності аудитора застосовувати знання та навички. Етичність поведінки передбачає відповідальність, непідкупність, уміння зберігати таємницю, неупередженість.

Дотримання принципів проведення аудиту ІБ є передумовою для об’єктивних висновків за результатами оцінки.

Основними методами одержання свідчень оцінки повинні бути:

– перевірка та аналіз документів, що відносяться до об’єкта оцінки;

– спостереження за процесами об’єкта оцінки;

– опитування співробітників об’єкта оцінки і незалежної (третьої) сторони.

Поряд з ручними способами збору інформації формування доказів аудиту може бути автоматичним або напівавтоматичним в результаті застосування якогось інструментального засобу чи застосування декількох інструментальних засобів.

При зборі даних оцінювачі повинні виходити з того, що діяльність по забезпеченню ІБ в області оцінки здійснюється відповідно до критеріїв оцінки ІБ, якщо цьому є докази. Оцінювачі повинні проявляти достатню ступінь професійного скептицизму у відношенні збираних свідоцтв оцінки, беручи до уваги можливість наявності порушень ІБ.

Перевірка та аналіз документів дозволяють оцінювачу отримати свідоцтва оцінки, що володіють найбільшою повнотою і зручністю сприйняття і використання в порівнянні з іншими методами отримання доказів аудиту. Однак ці свідчення аудиту мають різну ступінь достовірності залежно від їх характеру і джерела, а також від ефективності контролю за процесом

підготовки та обробки поданих документів.

Свідоцтвами оцінки ІБ, отриманими в результаті перевірки та аналізу документів, можуть бути, наприклад:

– наявність документа (документів) з релевантним вмістом;

– витяги з документа (документів), що підтверджують реалізацію діяльності по забезпеченню ІБ, покладання відповідальності та обов'язків на співробітника (співробітників) за реалізацію діяльності по забезпеченню ІБ;

– витяги з документа (документів), що містять описи реалізованих захисних методів, процесів забезпечення ІБ.

Спостереження являє собою відстеження оцінювачем процедур або процесів забезпечення ІБ, виконуються іншими особами (в т.ч. персоналом організації). Інформація вважається достовірною тільки в тому випадку, якщо вона отримана безпосередньо в момент функціонування процедур або процесів, які перевіряються.

Свідоцтвами аудиту, отриманими за допомогою спостереження за діяльністю, можуть бути, наприклад, записи, факти або інша інформація, які мають відношення до результатів автоматичного контролю технічними засобами, зафіксовані оцінювачами в ході спостереження.

Усне опитування проводять оцінювачі серед співробітників (власників активів), затверджених представником об'єкта оцінки для надання джерел свідоцтв і свідоцтв оцінки. Результати усних опитувань повинні оформлятися у вигляді протоколу чи короткого конспекту, в якому обов'язково має бути зазначено прізвище, ім'я, по батькові оцінювача, який проводив опитування, прізвище, ім'я, по батькові опитуваної особи, а також їх підписи. Для проведення типових опитувань можуть бути підготовлені бланки з переліками питань, що цікавлять. Результати усного опитування слід перевіряти, так як опитуваний може виражати свою суб'єктивну думку.

Свідоцтвами аудиту, отриманими при проведенні опитування, можуть бути, наприклад, описи та роз'яснення опитуваних осіб по реалізації процесів, процедур по забезпеченню ІБ.

Для впевненості в достовірності оцінки оцінювачі повинні бути впевнені в достовірності виявлених доказів аудиту. Зібрані свідчення оцінки, використовувані для оцінювання показників, повинні бути точним представленням оцінюваного об’єкта оцінки. Для цього слід враховувати достовірність джерел доказів аудиту.

За ступенем достовірності (від найбільшої до найменшої) джерела свідоцтв оцінки діляться на:

– документальні джерела свідоцтв, отримані з різних джерел третьої сторони (відомості про використання ліцензійних заходів і засобів забезпечення ІБ, договору із супроводу заходів і засобів забезпечення ІБ і т.д.);

– документальні джерела свідоцтв, отримані на (від) об’єкті (та) оцінки та підтверджені третьою стороною (план заходів за результатами зовнішнього аудиту ІБ, матеріали відомчих перевірок ІБ і т.д.);

– джерела свідоцтв, отримані в ході проведення аудиторських процедур, які не передбачають періодичну документальну звітність (результати спостереження за діяльністю, аналізу даних системи моніторингу ІБ і т.д.);

– джерела свідоцтв, отримані у вигляді нормативних та розпорядчих документів (політики, регламенти, звіти про діяльність, накази, розпорядження і т.д.), що вказують на належне застосування процесів і заходів забезпечення ІБ на практиці (наявність дозвільних записів уповноважених осіб, даних контролю ризиків і т.д.);

– свідоцтва, отримані в результаті усних і письмових опитувань про об’єкт оцінки, і спостереження за застосуванням заходів і засобів забезпечення ІБ, які не залишають документальних свідчень (виявлення ролей процесів, послідовності застосування захисних методів і т.д.).

Поряд з достовірністю джерел свідоцтв слід враховувати часовий період отримання свідоцтв та поєднання джерел свідоцтв оцінки. Наприклад, довіра до фактів, отриманим при спостереженні за діяльністю, підвищується, якщо вони отримані безпосередньо при функціонуванні процедур або процесів; довіру до фактів, отриманим при опитуванні співробітників, підвищується при підтвердженні даних фактів з різних джерел.

### 1.4.2 Вимірювання та оцінювання атрибутів об’єкта оцінки

Призначення заходу: вимірювання і оцінювання атрибутів об’єкта оцінки на основі свідчень оцінки ІБ з метою визначення ступеня виконання критеріїв оцінки і формування звіту за результатами оцінки.

Атрибут являє собою властивість або характеристику сутності, які можуть бути визначені кількісно або якісно ручними або автоматичними засобами.

Інформаційна потреба визначає, що потрібно виміряти для досягнення цілей оцінки ІБ об’єкта оцінки. Вимірювання, пов’язані із забезпеченням ІБ, можуть застосовуватися до різних об’єктів в рамках контексту оцінки. Для ідентифікації об’єктів вимірювання виділяються критичні атрибути процесів, процедур, захисних заходів, які можуть надати дані, відповідні інформаційній потребі.

Метод вимірювання використовується для кількісного виміру об’єкта вимірювання за допомогою перетворення атрибутів в основну міру. Основна міра – це міра, визначена в термінах атрибуту і методу його кількісного визначення (міра – це змінна, якій присвоюється значення). Основна міра функціонально незалежна від інших заходів. Основна міра збирає інформацію про єдиний атрибут [31-35].

Метод кількісного вимірювання вимірює атрибути за допомогою відповідної шкали.

Методи вимірювання можуть бути суб’єктивними або об’єктивними. Суб’єктивні методи покладаються на кількісний вимір, що включає думку людини, тоді як об’єктивні методи використовують кількісне визначення, засноване на числових правилах, які можуть бути реалізовані за допомогою ручних або автоматичних засобів.

Функція вимірювання визначає, як основні заходи об’єднуються у кінцеву міру. Кінцева міра – це спосіб об’єднання двох або більше основних заходів.

Функції вимірювання можуть включати різноманітні прийоми, такі як

усереднення всіх основних заходів, застосування вагових коефіцієнтів до основних заходів або присвоєння якісних значень основним заходам перед їх об'єднанням в кінцеві заходи.

Для кожної міри повинна бути визначена аналітична модель з метою перетворення однієї або більше кінцевих заходів в показник. Показник – це результат застосування аналітичної моделі до одної або більше мірам по відношенню до критеріїв прийняття рішень або інформаційної потреби.

Показники будуть формуватися шляхом об'єднання кінцевих заходів та інтерпретації їх на основі критеріїв прийняття рішень.

Для кожного показника повинні бути ідентифіковані та задокументовані засновані на цілях інформаційної безпеки критерії прийняття рішень, які встановлюють максимальне значення показника і надають керівництво для інтерпретації поточного значення показника.

Повідомлення результатів оцінки може проходити неформально при внутрішній оцінці або може відбуватися у формі детального звіту за незалежної зовнішньої оцінки. Крім того, для представлення результатів оцінки можуть бути підготовлені і інші висновки і запропоновані плани дій, рекомендації, в залежності від призначення оцінки. Результати можуть бути представлені в абсолютних виразах або у відносних виразах у порівнянні з результатами попередніх оцінок, контрольними даними, в порівнянні з діловими потребами і т.д. Результати оцінки ІБ зазвичай використовуються в якості основи для визначення ризиків ІБ і розробки плану вдосконалення системи забезпечення.

Вихідні дані оцінки включають дату проведення оцінки, вхідні дані оцінки, зібрані свідчення оцінки, опис використовуваного процесу вимірювання та оцінювання. Зареєстровані вихідні дані оцінки можуть зберігатися в різній формі – паперовій або електронній – в залежності від обставин та інструментів, використаних для проведення і підтримки оцінки.

На основі будь-якої угоди про забезпечення конфіденційності або обмежень доступу зареєстровані дані можуть зберігатися організатором оцінки або керівництвом об'єкта оцінки.

Важливими чинниками досягнення мети оцінки ІБ є наступні:

– усвідомлення і мотивація керівництва організації;
– конфіденційність;
– довіра.

Позиція керівництва організації робить істотний вплив на процес оцінки. Тому керівництво організації повинне спонукати учасників оцінки до відкритості і конструктивності. Оцінка об’єкта зосереджується на оцінці процесів, процедур, захисних заходів, а не на функціонуванні персоналу об’єкта оцінки. Сенс оцінки полягає в тому, щоб зробити об’єкт оцінки більш ефективними в досягненні цілей бізнесу, а не в тому, щоб покласти провину на окремих осіб.

Забезпечення зворотного зв’язку та підтримка атмосфери, що заохочує відкрите обговорення попередніх висновків під час оцінювання, сприяють забезпеченню того, щоб вихідні дані оцінки були значущими для об’єкта оцінки. Керівникам організації та персоналу об’єкта оцінки необхідно усвідомлювати, що учасники оцінки є основним джерелом знань і досвіду, пов’язаних з процесом, і що керівники та персонал мають гарну можливість для ідентифікації потенційних слабких місць.

Повага до конфіденційності джерел інформації та документації, зібраної під час оцінювання, необхідно для забезпечення безпеки цієї інформації. У тих випадках, коли використовуються опитування чи обговорення, слід звернути увагу на забезпечення того, щоб їх учасники не відчували загрози або не відчували якогось неспокою щодо конфіденційності. Деяка з наданої інформації може становити власність організації. Тому важливо наявність адекватних засобів контролю для поводження з такою інформацією.

Організатор оцінки, керівництво і персонал об’єкта оцінки повинні вірити в те, що оцінка принесе результат, який є об’єктивним для об’єкта оцінки. Важливо, щоб усі сторони могли бути впевнені в тому, що фахівці з оцінки володіють адекватними знаннями та досвідом для проведення оцінки, неупереджені та володіють адекватним розумінням об’єкта оцінки та його

бізнесу для проведення оцінки.

### 1.4.3 Способи вимірювання атрибутів об’єкта оцінки

Атрибути, виділені для вимірювання як критичні елементи процесу, процедури, захисної заходи або об’єкта оцінки, повинні бути представлені в зручному для аналізу вигляді з метою адекватного перетворення атрибуту в основну міру. Оцінювач отримує більше можливостей для адекватного представлення атрибуту основною мірою, якщо вимірюваний атрибут буде доповнений елементами, що відображають контекст оцінки.

В даний час використовуються дві форми опису вимірюваного атрибуту: форма анкет і форма метрики.

Для підготовки процесу вимірювання атрибутів за допомогою анкет вимагається:

– виділити серед атрибутів критичні, тобто ті атрибути, які дозволять досягти мети оцінки і сформувати питання анкети;

– визначити за допомогою моделі оцінки спосіб вимірювання.

Це дозволить оцінювачу перетворити вимірювані атрибути в основні заходи за наявності необхідних для виміру джерел свідоцтв і свідоцтв оцінки. Відображення контексту оцінки в анкеті мінімально, а саме опис атрибута у вигляді питання.

Елементи контексту оцінки можуть бути присутніми в додаткових методичних та розпорядчих документах, що забезпечують процес оцінки ІБ. У цих документах, як правило, вказуються джерела свідоцтв оцінки, а також персонал, відповідальний за заповнення анкет.

Анкети можуть бути побудовані не лише для отримання основної міри атрибуту, але і для формування кінцевої міри. У цьому випадку в анкеті має бути визначена модель об’єднання основних заходів в кінцеву міру.

Інший підхід до виміру атрибутів спирається на застосування метрик при вимірюванні атрибутів. Для підготовки процесу вимірювання атрибутів за допомогою метрик:

– виділити серед атрибутів критичні, тобто ті атрибути, які дозволять досягти мети оцінки;

– визначити за допомогою моделі оцінки спосіб вимірювання;

– сформувати перелік джерел свідоцтв оцінки та свідоцтв оцінки, необхідних для виміру атрибутів;

– встановити ролі і їх функції при проведенні вимірювання;

– визначити умови функціонування процесу, процедури, захисної заходи або об’єкта оцінки, що включають період збору, аналізу даних, звітності.

При розробці метрик і реалізації метрик ІБ повинні виконуватися наступні умови:

– метрики повинні давати результат в кількісно вимірної формі (у відсотках, у усереднених і абсолютних значеннях). Наприклад: «відсоток систем, для яких є план роботи в надзвичайній ситуації», «відсоток унікальних ідентифікаторів користувачів», «відсоток систем, в яких застосовуються заборонені до використання протоколи», «відсоток систем, для яких існують документовані звіти про оцінку ризиків» та т.п.;

– дані для підтримки метрик повинні бути доступними;

– значення метрик повинні бути досяжні і мати сенс для бізнесу;

– не слід вимірювати атрибути, які не потрібно удосконалювати.

В кожному з розглянутих вище способах вимірювання є свої сильні сторони. Анкети краще застосовувати при роботі в ситуаціях, коли кількісна оцінка всіх атрибутів неможлива і є деякі невизначеності. І навпаки, в ситуаціях, в яких можливо кількісно характеризувати атрибути, краще застосовувати метрики. Перший спосіб дає нам можливість опрацювання будь-яких даних, а другий – дає більш точну оцінку з відповідними даними.

## 1.5 Життєвий цикл атаки

У процесі атаки зловмисники здійснюють структуровану послідовність кроків, звану kill chain. Спочатку kill chain використовувався як військовий термін для опису структури військового вторгнення. [5-7] Знаючи послідовність дій противника, що обороняється сторона може виробити

стратегію захисту та протистояти нападу. Згодом термін kill chain став використовуватися для опису комп'ютерних загроз. Аналогічно, на основі інформації про етапи компрометації ІС, співробітники, відповідальні за ІБ, можуть вибудовувати систему захисту ІС (рис. 1.4).


Рисунок 1.4 – Життєвий цикл атаки

Від того, на якому етапі kill chain була виявлена загроза, залежить ефективність розслідування і розмір матеріального і репутаційного збитку, нанесеного атакується організації. Виявлення на етапі досягнення мети (пізнє виявлення) означає, що система ІБ ІС виявилася нездатна протистояти атаці і зловмисник досяг поставлених цілей. Найменший збиток буде завдано в разі виявлення на етапах Доставки або Закріплення (раннє виявлення).

### 1.5.1 Розвідка і збір даних

На цьому етапі відбувається збір інформації про організацію, яка буде атакована, а також про її інформаційних активах. Зокрема, зловмисник намагається встановити організаційну структуру компанії, стек технологій, який використовується в організації, засоби забезпечення ІБ, можливості використання соціальної інженерії по відношенню до співробітників (наприклад, виявити їх акаунти в соціальних мережах).

Розвідка може бути пасивною (Passive reconnaissance) і активної (Active reconnaissance). Пасивна розвідка полягає в отриманні інформації без

безпосереднього впливу на ІС (наприклад, перегляд DNS і Whois інформації, пов'язаної з ІС організації). Активна розвідка включає в себе взаємодію з ІС: сканування портів, пошук вразливостей ІС та інші дії.

Вся зібрана зловмисником інформація служить джерелом знань для наступного етапу.

### 1.5.2 Вибір способу атаки

Використовуючи інформацію, отриману на етапі розвідки та збору даних, зловмисник визначає спосіб атаки. При цьому зловмисник може створити нове шкідливе ПЗ, що дозволяє експлуатувати виявлені вразливості.

Зловмисник впроваджує ПЗ, яке буде використовуватися при атаці, в файли MS Office (.docx, .xlsx), PDF-документи, електронні листи або на знімні носії.

На цьому ж етапі відбувається вибір способу доставки створеного шкідливого ПЗ в атакується організацію: за допомогою зараження публічного ресурсу компанії, через одного зі співробітників або через компрометацію компаній-субпідрядників, які працюють з атакується організацією.

### 1.5.3 Доставка

Атакуючий повинен забезпечити потрапляння розробленого на попередньому кроці шкідливого ПЗ в ІС організації. Зазвичай для цього використовуються вкладення електронної пошти, шкідливі і фішингові посилання, watering hole-атаки (зараження сайтів, які відвідують співробітники атакується організації) або заражені USB-пристрої.

### 1.5.4 Експлуатація

Після потрапляння в ІС організації шкідливе ПЗ, використовуючи вразливості ІБ, поширюється по мережі і закріплюється на заражених машинах в очікуванні команд, що надходять від зловмисника.

Команди від зловмисника можуть надходити як через Інтернет, так і за

допомогою доставки іншого шкідливого ПЗ (наприклад, якщо на машині відсутній пряме підключення до Інтернету).

1.5.5 Закріплення

Шкідливе ПЗ здійснює зараження комп'ютера для того, щоб не бути виявленим або віддаленим після перезавантаження або установки оновлення, блокуючого можливість використовувати одну з вразливостей ІС. Зазвичай для зараження використовуються утиліти несанкціонованого управління (backdoor).

1.5.6 Виконання команд

За допомогою з'єднання, що встановлюється зсередини ІС організації, шкідливе ПЗ реалізує взаємодію з сервером управління, підконтрольним зловмисникові. Таким чином, атакуючий отримує управління комп'ютером всередині ІС організації.

1.5.7 Досягнення мети

Отримавши управління, зловмисник може працювати з даними на скомпрометувати комп'ютері, не тільки здійснюючи несанкціонований доступ, але і змінюючи або видаляючи їх. Крім того, атакуючий може спробувати заразити інші машини в ІС, для того щоб збільшити обсяг доступної інформації.

1.6 Реагування на інциденту ІБ

1.6.1 Цілі процесу реагування

Основними цілями реагування на інциденти ІБ є мінімізація шкоди, якнайшвидше відновлення вихідного стану ІС і розробка плану щодо недопущення подібних інцидентів у майбутньому. Ці цілі досягаються на двох основних етапах: розслідування інциденту і відновлення системи.

При розслідуванні потрібно визначити:

– початковий вектор атаки;
– шкідливі програми і інструменти, які були використані в процесі атаки;

– які системи були порушені в ході атаки;
– розмір збитку, нанесеного атакою;
– завершена атака чи ні, тобто чи досяг атакуючий своєї мети;
– тимчасові рамки атаки.

Після завершення розслідування необхідно розробити і впровадити план відновлення системи, використовуючи інформацію, отриману під час розслідування.

### 1.6.2 Основні етапи процесу реагування на інциденту ІБ

На основі інформації про життєвий цикл атаки (kill chain), можливе формування системи захисту. Виходячи з аналізу стратегії, використовуваної при атаці на ІС, фахівцями ІБ вироблена стратегія реагування на інциденти (рис. 1.5).


Рисунок 1.5 – Процес реагування на інциденти ІБ

#### 1.6.2.1 Підготовка

У момент, коли відбувається інцидент ІБ, від співробітників, відповідальних за ІБ, потрібні моментальні і точні дії. Тому для ефективного реагування необхідна попередня підготовка. Співробітники, відповідальні за ІБ, повинні забезпечити захист ІС і проінформувати користувачів, а також ІТ-персонал, про важливість заходів щодо забезпечення ІБ. Співробітники, що займаються реагуванням на інциденти ІБ, повинні пройти відповідне навчання і

регулярно відвідувати тренінги з ІБ, для того щоб оперативно і ефективно реагувати на інциденти ІБ.

1.6.2.2 Виявлення

Співробітники, що займаються реагуванням на інциденти, повинні визначити, чи є виявлене ними за допомогою різних систем забезпечення ІБ подія інцидентом чи ні. Для цього можуть використовуватися публічні звіти, потоки даних про загрози, засоби статичного і динамічного аналізу зразків ПЗ і інші джерела інформації. Статичний аналіз виконується без безпосереднього запуску досліджуваного зразка і дозволяє виявити різні індикатори, наприклад, рядки, що містять URL-адреси або адреси електронної пошти. Динамічний аналіз має на увазі виконання досліджуваної програми в захищеному середовищі або на ізольованій машині з метою виявлення поведінки зразка і збору артефактів його роботи (рис 1.6).


Рисунок 1.6 – Цикл виявлення індекаторів компрометації

Збір індикаторів компрометації є ітераційним процесом. На основі

первинної інформації, отриманої від SIEM-системи (Security Information and Event Management), відбувається формування сценаріїв виявлення, застосування яких, як правило, призводить до виявлення нових індикаторів компрометації. Отримані таким чином індикатори допомагають уточнити межі атаки і служать відправною точкою для нового циклу виявлення.

SIEM-систем – система, яка забезпечує аналіз подій ІБ, що виходять від мережевих пристроїв і додатків, в реальному часі. Однією з можливостей SIEM-систем є зіставлення подій з потоками даних про загрози.

Подальші кроки робляться тільки якщо подія вирішено вважати інцидентом ІБ.

1.6.2.3 Стримування

Співробітники, відповідальні за ІБ, повинні ідентифікувати скомпрометовані комп'ютери і налаштувати правила безпеки таким чином, щоб зараження не поширилося далі по мережі. Крім того, на цьому етапі необхідно переналаштувати мережу таким чином, щоб ІС компанії могла продовжувати працювати без заражених машин.

1.6.2.4 Видалення

Мета цього етапу – привести скомпрометовану ІС в стан, в якому вона була до зараження. Співробітники, відповідальні за ІБ, видаляють шкідливе ПЗ, а також всі артефакти, які воно могло залишити на заражених комп'ютерах в ІС.

1.6.2.5 Відновлення

Раніше скомпрометовані комп'ютери вводяться назад в мережу. При цьому співробітники, відповідальні за ІБ, деякий час продовжують спостерігати за станом цих машин і ІС в цілому, щоб переконатися в повному усуненні загрози.

1.6.2.6 Висновки

Співробітники, відповідальні за ІБ, аналізують інцидент, вносять

необхідні зміни в конфігурацію ПЗ і устаткування, що забезпечує ІБ, і формують рекомендації для того, щоб в майбутньому запобігти подібним інцидентам. При неможливості повного запобігання майбутньої атаки складені рекомендації дозволять прискорити реагування на подібні інциденти.

## 1.7 Висновок

В даному розділі було проведено аналіз моделей та процесів забезпечення кібербезпеки. Наведені методи оцінки інформаційної безпеки, визначені процеси заберпечення кібербезпеки на об’єкті. Проаналізовано міжнародне законодавство у сфері інформаційної безпеки. Розглінуто життєвий цикл атаки та визначені основні етапи процесу реагування на інціденти ІБ.

# РОЗДІЛ 2. СИНТЕЗ МОДЕЛІ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ НА ПРИВАТНИХ ПІДПРИЄМСТВАХ

## 2.1 Аналіз методів збору експертної інформації

Для реалізації завдань, поставлених в дипломній роботі треба обрати метод збору експертної інформації для розслідування інцидентів кібербезпеки. Існує велика кількість методів збору експертної інформації. Для того, щоб вирішити цю задачу, потрібну проаналізувати основні методи експертизи [31-37]. Всі методи експертизи поділяються на дві групи:

– індивідуальні методи експертизи;

– групові методи експертизи.

### 2.1.1 Індивідуальні методи експертизи

Експертні методи, що відносяться до першої групи, припускають індивідуальну роботу дослідників з кожним із залучених експертів. При цьому може бути задіяний і один експерт, якщо його кваліфікації достатньо для зняття інформаційної невизначеності з проблеми, проте зазвичай задіють кілька експертів для підвищення надійності експертизи.

Індивідуальність полягає в тому, що експерти не збираються разом, не знайомляться з оцінками інших експертів, різних експертів можуть опитувати щодо різних аспектів однієї проблеми, також можуть бути різні і процедури опитування різних експертів. Найчастіше при індивідуальному експертному опитуванні використовуються такі методи:

#### 2.1.1.1 Стандартизоване експертне опитування

Даний метод вимагає від дослідницької команди попереднього чіткого структурування проблеми і визначення переліку всіх питань, на які повинні бути отримані однозначні відповіді. Для реалізації опитування, збору даних розробляється стандартизована анкета з питаннями закритого типу (з пропозицією варіантів відповіді). Анкетування може проводитися як при особистій бесіді інтерв’юера з експертом, так і шляхом самостійного заповнення. У цьому випадку присутність інтерв’юера необов’язково, анкета

може бути відправлена за звичайною або електронною поштою, проте потрібно висновок попередньої домовленості з експертом про опитування.

Метод передбачає високу кваліфікацію фахівців-дослідників на етапі постановки завдання і планування дослідження, проте вельми простий в частині організації та проведення опитування, а також у частині обробки отриманої інформації. Вимоги до анкет (структура, формулювання питань і варіантів відповідей) досить стандартні і аналогічні вимогам, що пред'являються до опитувань не експертного рівня. Одна з основних вимог – використання загальноприйнятого професійної мови, однозначність трактування використовуваних термінів.

2.1.1.2 Не стандартизоване експертне опитування

Метод являє собою особисте інтерв'ю з експертом з певної проблеми. Ступінь формалізації інтерв'ю може бути різною. Низький рівень формалізації опитування - неформальна бесіда, для якої визначається тільки тема, а далі експерт сам вирішує, як її висвітлювати (інтерв'юер при цьому задає уточнюючі або навідні запитання). Високий рівень формалізації передбачає розробку чітко структурованого опитувальника з питаннями відкритого типу. Даний метод порівняно з попереднім більш складний як на етапі проведення опитування (вимагає високої кваліфікації інтерв'юера), так і на етапі інтерпретації отриманої інформації і вимагає високої кваліфікації дослідника.

2.1.1.3 Метод "індивідуального блокнота"

Метод являє собою заочну роботу експерта без безпосереднього спілкування з дослідниками. Експерт отримує блокнот, на першій сторінці якого описана проблема, і потім протягом обумовленого періоду часу (визначеного складністю проблеми і терміновістю її рішення) заносить в цей блокнот всі свої думки, ідеї, зауваження, що стосуються поставленого завдання, після чого здає блокнот дослідникам. Істотну складність представляє наступна обробка інформації та її інтерпретація. Метод вимагає значного залучення експерта і, отже, передбачає високий рівень оплати його праці.

### 2.1.2 Групові методи експертизи

На відміну від індивідуальних групові методи передбачають колективну роботу експертів (очну або заочну), вони вимагають узгодження думок всіх експертів і розробку загального експертного висновку на основі консенсусу. Групові методи краще з точки зору підвищення надійності експертизи, проте вони вельми складні з підготовки та проведення. Потрібні висококваліфіковані фахівці для розробки процедури групової взаємодії. Далеко не завжди вдається зібрати в один час і в одному місці необхідну кількість експертів, що відповідають потрібним вимогам.

Групові методи формування експертизи в залежності від характеру та спрямованості обговорення підрозділяють на аналітичні та креативні. Аналітичні методи націлені переважно на дослідження характеристик досліджуваного об’єкта. Креативні мають своєю метою колективну генерацію ідей або вироблення рішення проблеми.

Групові методи формування експертизи досить різноманітні, опишемо основні з них:

#### 2.1.2.1 Метод номінальних груп

Метод являє собою якусь перехідну різновид від індивідуального опитування до групового. При реалізації цього методу спочатку здійснюється індивідуальне опитування одних експертів, а потім результати даних інтерв’ю так само автономно і незалежно один від одного обговорюються іншими експертами. Експерти можуть висловити згоду чи незгоду з раніше прозвучали думками, необхідно, щоб критика або вираз солідарності були чітко аргументовані.

#### 2.1.2.2 Мозковий штурм

Метод являє собою спільне очне обговорення проблеми групою експертів. Метод реалізується у два етапи. Перший етап носить назву "конференції ідей", його тривалість становить приблизно 1-1,5 години. У ході цього етапу експерти висувають різні ідеї, що стосуються трактування

аналізованої ситуації і чи прогнозу розвитку явища. Ідеї протоколюються, але не обговорюються і не критикуються. При цьому ідеї можуть бути самими різними, в тому числі і "маячними". Головує принцип: чим більше ідей, тим краще. Після перерви, на другому етапі, ідеї обговорюються, оцінюються, і вибираються ті з них, які визнаються найбільш вірними. Остаточний вердикт з проблеми може бути прийнятий шляхом явного або неявного голосування. Процедури генерації та обговорення ідей можуть бути більшою ними меншій мірі формалізовані.

2.1.2.3 Метод "635"

Метод являє собою досить формалізовану варіацію методу мозкового штурму. Цей метод має на увазі наступну регламентацію роботи експертної команди: до групи входять 6 осіб, кожен з яких протягом 5 хвилин повинен висунути три пропозиції або висловити три гіпотези з приводу деякого аспекту розв’язуваної задачі або аналізованої ситуації. Ідеї кожного експерта заносяться в спеціальні формуляри, які передаються по колу. Після того як були розглянуті всі аспекти поставленого завдання і всі експерти отримали можливість висловитися, відбувається обговорення та оцінка рішень і вибір найбільш вірного.

2.1.2.4 Критична атака

Метод також є варіацією методу мозкового штурму, принципова відмінність – у критичній спрямованості обговорення. Реалізація методу включає кілька етапів. На першому етапі кожен учасник експертної групи пропонує своє вирішення поставленого завдання (свою інтерпретацію при аналізі ситуації) або свою версію розвитку подій (при прогнозі). Рішення має пропонуватися з докладною аргументацією. Далі кожен експерт повинен ознайомитися з думками своїх колег і знайти і аргументувати в пропоновані рішення максимально можливе число слабкостей. На наступному етапі експерти збираються разом і по черзі обговорюють усі висунуті рішення. Завдання кожного учасника – відстояти свою версію рішення, завдання опонентів – "рознести її в пух і прах". За підсумками дискусії експерти

вибирають те рішення, яке викликало найменше нарікань і було найбільш обґрунтованим.

2.1.2.5 Експертне фокусування

Метод являє собою одну з форм спільного очного обговорення проблеми. Експерти всебічно розглядають досліджувану ситуацію, "фокусуються" на ній. Основна мета – виявити структуру даної проблеми, визначити по можливості всі фактори, що визначають дану ситуацію, встановити взаємозв’язки між ними. Обговорення носить більш діловий характер, ніж при класичній версії мозкового штурму, тобто проходить без зайвого "марення".

2.1.2.6 Метод комісій

Метод також полягає у спільному обговоренні проблеми. Основна відмінність від фокусування – прагнення з’ясувати, в чому полягає суперечність між різними варіантами пропонованих рішень, знайти максимальне число "точок згоди" і прийти до консенсусу.

2.1.2.7 Метод інтеграції рішень

Метод у своїй основі аналогічний методу комісій, проте більшою мірою формалізований. Метод полягає у виробленні спільного вирішення проблеми на основі виявлення сильних сторін окремих рішень та їх об’єднання. Метод реалізується в кілька етапів. На першому етапі експертам пропонується завдання, і вони розглядають і вирішують її незалежно один від одного. Потім у заздалегідь підготовлений формуляр експерти заносять свої індивідуальні рішення, тобто трактування аналізованої ситуації або прогноз розвитку подій. На наступному етапі експерти спільно обговорюють завдання і всі запропоновані рішення з метою виявити сильні сторони кожного окремого рішення, які також фіксуються в формулярі. При поданні індивідуальних рішень можливі варіації – або кожне рішення презентується автором і детально аргументується, або дотримується анонімність рішень, щоб уникнути тиску авторитетів. Після того як обговорені всі рішення та визначено сильні сторони

кожного з них, виробляється синтезоване рішення на основі комбінування переваг окремих рішень.

2.1.2.8 Ділова гра

Метод може бути реалізований в різних формах. Найбільш поширена форма – моделювання аналізованих процесів і / або майбутнього розвитку прогнозованого явища в різних варіантах і розгляд отриманих даних. Розробка процедури проведення ділової гри – досить складне завдання, і їй має бути приділено серйозну увагу. Мають бути чітко визначені і формально описані наступні елементи гри: цілі та завдання, ролі учасників, сюжет і регламент. Важливим етапом будь-якої ділової гри є рефлексія – розбір ходу гри і підведення підсумків. У даному випадку рефлексія полягає в аналізі самого ігрового процесу та аналізі результатів моделювання досліджуваного явища.

2.1.2.9 Метод "суду"

Метод являє собою одну з різновидів ділових ігор. Обговорення поставленого завдання реалізується у вигляді судового процесу: моделюється "процес над проблемою". Вибираються "адвокат", "прокурор", "суд", "присяжні" та інші учасники "процесу". Кожен відстоює свою точку зору, що стосується аналізованого або прогнозованого явища, аргументуючи свої висловлювання. Остаточний вердикт про досліджуваної проблеми визначається в два етапи: голосування "присяжних" і конкретизація рішення "суддями".

2.1.2.10 "Консиліум"

Експерти досліджують проблему подібно до того, як лікарі обстежують пацієнта: визначаються "симптоми" прояви проблеми, розкриваються причини виникнення проблеми, проводиться аналіз, ставиться "діагноз", і дається прогноз розвитку ситуації.

2.1.2.11 "Колективний блокнот"

Метод в основі своїй аналогічний "індивідуальним блокноту", проте в даному випадку блокноти отримують кілька експертів, кожен з яких знає, що він є учасником експертної групи. Можливий варіант, коли на початку роботи

всі експерти збираються разом і їм розповідають про сутність виниклої проблеми і формулюють завдання. Далі кожен експерт працює зі своїм блокнотом протягом певного часу (при цьому також можливо, що різні експерти зосереджуються на різних сторонах проблеми). Другий етап реалізації експертизи полягає в тому, що блокноти збираються, інформація систематизується (дослідницької командою або керівником експертної групи) і далі в очному спільному обговоренні накопиченого і систематизованого матеріалу експерти приходять до вирішення проблеми.

2.1.2.12 Метод Дельфі

Метод являє собою заочний і анонімне опитування експертної групи в кілька турів з узгодженням думок експертів. Експертам пропонуються опитувальні листи з досліджуваної проблеми. Ступінь стандартизованість питань може бути різна (вони можуть бути як закритими, так і відкритими, мати на увазі як кількісну, так і якісну відповідь). Можливі варіації і в плані аргументації і обґрунтування експертних оцінок (що може бути обов’язковим чи ні). Як правило, метод Дельфі реалізується в 2-3 туру, причому при повторних опитуваннях експертам пропонується ознайомитися або з думками і аргументами кожного експерта, або з середньою оцінкою. На повторних турах експерти можуть поміняти свою оцінку, взявши до уваги аргументи колег, а можуть залишитися при колишньому думці і висловити обґрунтовану критику інших оцінок. Існують різні методики узгодження експертних оцінок (з урахуванням (або без) кваліфікації експертів (як вагових коефіцієнтів), з відкиданням (або без) крайніх оцінок і інші). По-перше, заочність і анонімність дозволяють уникнути конформізму або орієнтації на авторитети, що могло б виникнути, якби експертів зібрали разом і вони повинні були б оприлюднити свою думку. По-друге, експерти мають можливість змінити свою думку без ризику "втратити обличчя".

2.2 Аналіз загроз

Для подальшої роботи з розслідування інцидентів кібербезпеки на підприємстві необхідно визначити можливі сценарії реалізації загроз.

Таблиця 2.1 – Можливі сценарії реалізації загроз

| **Джерело загрози** | | | **Вразливості** | | **Загроза** |
|---|---|---|---|---|---|
| Антропогенні | Зовнішні | Кримінальні структури | Об’єктивні | Апаратні закладки | Розкрадання |
| | | | | Обумовлені місцем розташування об’єкта | Розкрадання, знищення, блокування |
| | | | Суб’єктивні | Порушення режиму захисту і охорони | Розкрадання, знищення, блокування |
| | | | Випадкові | Збої електропостачання | Розкрадання, знищення, блокування |
| | | | | Пошкодження життєзабезпечуючих комунікації | Розкрадання, знищення, блокування |
| | | | | Пошкодження огороджувальних конструкцій | Розкрадання, знищення, блокування |
| | | Потенційні злочинці і хакери | Об’єктивні | Електромагнітні випромінювання | Розкрадання |
| | | | | Електричні випромінювання | Розкрадання |
| | | | | Звукові випромінювання | Розкрадання |
| | | | | Апаратні закладки | Розкрадання |
| | | | | Програмні закладки | Розкрадання, знищення, модифікація, блокування |
| | | | | Елементи що володіють електроакустичними перетвореннями | Розкрадання |
| | | | | Елементи схильні до дії електромагнітного поля | Розкрадання |
| | | | | Обумовлені організацією каналів обміну інформації | Розкрадання, знищення, модифікація, блокування, нав’язування неправдивої інформації |
| | | | Суб’єктивні | Помилки при підготовці та використанні ПЗ | Розкрадання, модифікація |
| | | | | Порушення режиму конфіденційності | Розкрадання |
| | | | Випадкові | Відмови і несправності технічних засобів | Розкрадання, знищення, модифікація, блокування, нав’язування |
| | | | | Збої ПЗ | Розкрадання, модифікація |
| | | Несумлінні партнери | Об’єктивні | Апаратні закладки | Розкрадання |
| | | | | Програмні закладки | Розкрадання, модифікація |
| | | | | Обумовлені місцем розташування об’єкта | Розкрадання, знищення, блокування |
| | | | | Обумовлені організацією каналів обміну інформації | Розкрадання, блокування |

Продовження таблиці 2.1

| Джерело загрози | | | Вразливості | | Загроза |
|---|---|---|---|---|---|
| Антропогенні | Зовнішні | | Суб'єктивні | Порушення режиму використання інформації | Розкрадання, модифікація |
| | | | | Порушення режиму конфіденційності | Розкрадання |
| | | | Випадкові | Збої ПЗ | Розкрадання, модифікація |
| | | Технічний персонал постачальників послуг | Об'єктивні | Апаратні закладки | Розкрадання |
| | | | | Програмні закладки | Розкрадання, модифікація |
| | | | | Елементи що володіють електроакустичними перетвореннями | Розкрадання |
| | | | | Обумовлені організацією каналів обміну інформації | Розкрадання, блокування, відмова |
| | | | Суб'єктивні | При підготовці та використанні ПЗ | Розкрадання, знищення |
| | | | | Порушення режиму охорони та захисту | Розкрадання, знищення, модифікація, нав'язування неправд. інформації |
| | | | Випадкові | Відмови і несправності технічних засобів | Розкрадання, нав'язування неправд. інформації |
| | | | | Пошкодження огороджуючих конструкцій | Розкрадання |
| | | Представники наглядових організацій та аварійних служб | Об'єктивні | Апаратні закладки | Розкрадання |
| | | | Суб'єктивні | Порушення режиму охорони та захисту | Розкрадання, знищення, модифікація, нав'язування неправд. інформації |
| | | | Випадкові | Пошкодження огороджуючих конструкцій | Розкрадання |
| | | Представники силових структур | Об'єктивні | Електромагнітні випромінювання | Розкрадання |
| | | | | Електричні випромінювання | Розкрадання |
| | | | | Звукові випромінювання | Розкрадання |
| | | | | Апаратні закладки | Розкрадання |
| | | | | Елементи схильні до дії електромагнітного поля | Розкрадання |
| | | | | Обумовлені місцем розташування об'єкта | Розкрадання, знищення, блокування |
| | | | | Обумовлені організацією каналів обміну інформації | Розкрадання, блокування |

Продовження таблиці 2.1

| Джерело загрози | | | Вразливості | | Загроза |
|---|---|---|---|---|---|
| Антропогенні | Зовнішні | | Суб'єктивні | Порушення режиму охорони та захисту | Розкрадання, знищення, модифікація, нав'язування неправд. інформації |
| | | | Випадкові | Пошкодження огороджуючих конструкцій | Розкрадання |
| | | Конкуренти | Об'єктивні | Електромагнітні випромінювання | Розкрадання |
| | | | | Електричні випромінювання | Розкрадання |
| | | | | Звукові випромінювання | Розкрадання |
| | | | | Апаратні закладки | Розкрадання |
| | | | | Обумовлені місцем розташування об'єкта | Розкрадання, знищення, блокування |
| | | | | Обумовлені організацією каналів обміну інформації | Розкрадання, блокування |
| | | | Суб'єктивні | Порушення режиму охорони та захисту | Розкрадання, знищення, модифікація, нав'язування неправд. інформації |
| | | | Випадкові | Пошкодження огороджуючих конструкцій | Розкрадання |
| Антропогенні | Внутрішні | Основний персонал | Об'єктивні | Апаратні закладки | Розкрадання |
| | | | | Програмні закладки | Розкрадання, модифікації, блокування |
| | | | Суб'єктивні | Помилки при підготовці та використанні ПЗ | Розкрадання, модифікації, блокування |
| | | | | Помилки при управлінні складними системами | Блокування, нав'язування неправдивої інформації |
| | | | | Помилки при експлуатації технічних засобів | Розкрадання, блокування |
| | | | | Порушення режиму охорони та захисту | Розкрадання, знищення |
| | | | | Порушення режиму експлуатації технічних заходів | Блокування |
| | | | | Порушення режиму використання інформації | Розкрадання, модифікація |
| | | | | Порушення режиму конфіденційності | Розкрадання |
| | | | Випадкові | Збої ПЗ | Розкрадання, модифікація, блокування |

Продовження таблиці 2.1

| Джерело загрози | | | Вразливості | | Загроза |
|---|---|---|---|---|---|
| Антропогенні | Внутрішні | | Випадкові | Пошкодження огороджувальних конструкцій | Розкрадання |
| | | Представники служби захисту інформації | Об’єктивні | Апаратні закладки | Розкрадання |
| | | | | Програмні закладки | Розкрадання, модифікації, блокування |
| | | | Суб’єктивні | Помилки при підготовці та використанні ПЗ | Розкрадання, модифікації, блокування |
| | | | | Помилки при управлінні складними системами | Блокування, нав’язування неправд. інформації |
| | | | | Помилки при експлуатації технічних засобів | Розкрадання, блокування |
| | | | | Порушення режиму охорони та захисту | Розкрадання, знищення |
| | | | | Порушення режиму експлуатації технічних заходів | Блокування |
| | | | | Порушення режиму використання інформації | Розкрадання, модифікація |
| | | | | Порушення режиму конфіденційності | Розкрадання |
| | | Допоміжний персонал | Об’єктивні | Апаратні закладки | Розкрадання |
| | | | Суб’єктивні | Порушення режиму охорони та захисту | Розкрадання |
| | | | | Порушення режиму експлуатації технічних заходів | Розкрадання |
| | | | | Порушення режиму використання інформації | Розкрадання |
| | | | | Порушення режиму конфіденційності | Розкрадання |
| | | Технічний персонал | Об’єктивні | Апаратні закладки | Розкрадання |
| | | | Суб’єктивні | Помилки при експлуатації технічних засобів | Розкрадання, блокування |
| | | | | Порушення режиму використання інформації | Розкрадання |
| | | | | Порушення режиму конфіденційності | Розкрадання |
| | | | Випадкові | Пошкодження огороджувальних конструкцій | Розкрадання |

Продовження таблиці 2.1

| **Джерело загрози** | | | **Вразливості** | | **Загроза** |
|---|---|---|---|---|---|
| Техногенні | Зовнішні | Засоби зв'язку | Об'єктивні | Електромагнітні випромінювання | Розкрадання |
| | | | | Електричні випромінювання | Розкрадання |
| | | | | Звукові випромінювання | Розкрадання |
| | | | | Апаратні закладки | Розкрадання |
| | | | Випадкові | Збої електропостачання | Блокування |
| | | Мережі інженерних комунікацій | Об'єктивні | Електромагнітні випромінювання | Розкрадання |
| | | | | Електричні випромінювання | Розкрадання |
| | | | | Звукові випромінювання | Розкрадання |
| | | | | Обумовлені місцем розташування об'єкта | Розкрадання |
| | | Транспорт | Об'єктивні | Обумовлені місцем розташування об'єкта | Блокування |
| Техногенні | Внутрішні | Неякісні технічні засоби обробки інформації | Об'єктивні | Електромагнітні випромінювання | Розкрадання, модифікація |
| | | | | Електричні випромінювання | Розкрадання, модифікація |
| | | | | Елементи схильні до дії електромагнітного поля | Розкрадання, знищення |
| | | | Суб'єктивні | Помилки при підготовці та використанні ПЗ | Модифікація, блокування |
| | | | | Помилки при управлінні складними системами | Модифікація, блокування |
| | | | | Помилки при експлуатації технічних засобів | Модифікація, блокування |
| | | | | Порушення режиму експлуатації технічних засобів | Блокування |
| | | | Випадкові | Відмови і несправності технічних засобів | Блокування |
| | | | | Старіння та розмагнічування носіїв інформації | Знищення |
| | | | | Збої електропостачання | Знищення, блокування |
| | | | | Пошкодження життєзабезпечуючих комунікацій | Знищення, блокування |

Продовження таблиці 2.1

| Джерело загрози | | | Вразливості | | Загроза |
|---|---|---|---|---|---|
| Техногенні | Внутрішні | Неякісні програмні засоби обробки інформації | Суб'єктивні | Помилки при підготовці та використанні ПЗ | Розкрадання, модифікація, блокування |
| | | | | Помилки при управлінні складними системами | Модифікація, блокування |
| | | | | Помилки при експлуатації технічних засобів | Модифікація, блокування |
| | | | | Порушення режиму використання інформації | Модифікація, блокування |
| | | | | Порушення режиму конфіденційності | Розкрадання |
| | | | | Збої ПЗ | Блокування |
| | | Допоміжні засоби | Об'єктивні | Звукові випромінювання | Розкрадання |
| | | | | Елементи що володіють електроакустичними перетвореннями | Розкрадання |
| | | | | Елементи схильні до дії електромагнітного поля | Розкрадання |
| | | | Суб'єктивні | Порушення режиму експлуатації технічних засобів | Розкрадання, блокування |
| | | Інші технічні засоби, що застосовуються в установі | Об'єктивні | Електромагнітні випромінювання | Розкрадання |
| | | | | Електричні випромінювання | Розкрадання |
| | | | | Звукові випромінювання | Розкрадання |
| | | | | Елементи що володіють електроакустичними перетвореннями | Розкрадання |
| | | | | Елементи схильні до дії електромагнітного поля | Розкрадання |
| | | | Суб'єктивні | Помилки при експлуатації технічних засобів | Блокування |
| | | | | Порушення режиму експлуатації технічних засобів | Блокування |
| | | | Випадкові | Відмови і несправності технічних засобів | Блокування |

Продовження таблиці 2.1

| Джерело загрози | | Вразливості | | Загроза |
|---|---|---|---|---|
| Стихійні | Пожежі | Випадкові | Порушення режиму охорони і захисту | Розкрадання, знищення |
| | | | Порушення режиму експлуатації технічних засобів | Знищення, блокування |
| | | | Обумовлені місцем розташування об’єкта | Знищення, блокування |
| | Землетрус, повінь, ураган | Об’єктивні | Обумовлені місцем розташування об’єкта | Знищення, блокування |
| | Різні непередбачувані обставини | Об’єктивні | Обумовлені місцем розташування об’єкта | Знищення, блокування |
| | Нез’ясовані явища | Об’єктивні | Обумовлені місцем розташування об’єкта | Знищення, блокування |
| | Інші форс-мажорні обставини | Об’єктивні | Обумовлені місцем розташування об’єкта | Знищення, блокування |

## 2.3 Аналіз критеріїв захисту інформації

До критеріїв захисту інформації відносяться наступні: конфіденційність, цілісність, доступність, спостережність.

Виділимо критерій захисту – спостереження. При розслідувані інцидентів він є основним, так як при використані цього критерію відстежити реалізацію інцидентів легше, за рахунок постійного моніторингу кібербезпеки на підприємстві. При розслідувані інцидентів необхідно враховувати критерій спостережності, так як КС повинна бути оцінена на предмет відповідності критерію, КЗЗ оцінюваної КС повинен надавати послуги з забезпечення відповідальності користувача за свої дії і з підтримки спроможності КЗЗ виконувати свої функції [16, 29, 27].

Спостереженість забезпечується в КС такими послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача.

Першою послугою є реєстрація (НР), яка дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і

спроможності вияву потенційних порушень, дана послуга має 5 рівнів:

1 Зовнішній аналіз НР-1;

2 Захищений журнал НР-2;

3 Сигналізація про небезпеку НР-3;

4 Детальна реєстрація НР-4;

5 Аналіз в реальному часі НР-5.

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації. Ця послуга складається з наступних рівнів:

1 Зовнішня ідентифікація і автентифікація НИ-1;

2 Одиночна ідентифікація і автентифікація НИ-2;

3 Множинна ідентифікація і автентифікація НИ-3.

Послуга достовірний канал гарантуватиме користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін. Ця послуга складається з наступних рівнів:

1 Однонаправлений достовірний канал НК-1;

2 Двонаправлений достовірний канал НК-2.

Послуга розподілу обов'язків дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів. Ця послуга складається з наступних рівнів:

1 Виділення адміністратора НО-1;

2 Розподіл обов'язків адміністраторів НО-2;

3 Розподіл обов'язків на підставі привілеїв НО-3.

Цілісність комплексу засобів захисту визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами. Ця послуга складається з наступних рівнів:

1 КЗЗ з контролем цілісності НЦ-1;

2 КЗЗ з гарантованою цілісністю НЦ-2;

3 КЗЗ з функціями диспетчера доступу НЦ-3.

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжируються на підставі можливості виконання тестів у процесі запуску або штатної роботи. Ця послуга складається з наступних рівнів:

1 Самотестування за запитом НТ-1;

2 Самотестування при старті НТ-2;

3 Самотестування в реальному часі НТ-3.

Ідентифікація і автентифікація при обміні дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації. Ця послуга складається з наступних рівнів:

1 Автентифікація вузла НВ-1;

2 Автентифікація джерела даних НВ-2;

3 Автентифікація з підтвердженням НВ-3.

Автентифікація відправника дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною. Ця послуга складається з наступних рівнів:

1 Базова автентифікація відправника НА-1;

2 Автентифікація відправника з підтвердженням НА-2.

Автентифікація отримувача дозволяє забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою

стороною. Ця послуга складається з наступних рівнів:

1 Базова автентифікація отримувача НП-1;

2 Автентифікація отримувача з підтвердженням НП-2.

Впровадження критерію – «спостереження» на підприємстві, дозволить зменшити реалізацію інцидентів кібербезпеки і спростить процес розслідування інцидентів за рахунок вже зібраної інформації про можливі загрози. Враховуючи критерії захисту інформації і правильність визначення збору доказів, необхідно розуміти в якому фізичному стані знаходиться пристрій, так як він може бути ввімкнений до мережі, може і ні. Тому і збір доказової бази буде проводитись за різним алгоритмом [16, 29, 27].

2.4 Розробка опитувального листа для експерта з розслідування інцидентів кібербезпеки

Таблиця 2.2 – Питання опитувального листа

| **Питання** | **Менеджер** | **Економіст** | **Програміст** | **Системний адміністратор** | **Інші** |
|---|---|---|---|---|---|
| Охарактеризуйте сумлінність партнерів Вашого підприємства? | + | + | + | + | + |
| Чи є КЗ на підприємстві? | + | + | + | + | + |
| Як Ви оцінюєте привабливість для хакерів і потенційних злочинців Вашого підприємстві? | + | + | + | + | + |
| Який рівень конкуренції в сфері діяльності Вашого підприємства? | + | + | + | + | + |
| Як часто відвідують Ваше підприємство представники постачальників послуг | + | + | + | + | + |
| Як часто відвідують Ваше підприємство представники наглядових організацій та аварійних служб? | + | + | + | + | + |
| Як Ви оцінюєте якість технічних засобів на Вашому підприємстві? | + | + | + | + | + |
| Як Ви оцінюєте якість програмних засобів На Вашому підприємстві? | + | + | + | + | + |
| Як Ви оцінюєте якість допоміжних засобів на Вашому підприємстві? | + | + | + | + | + |
| Як Ви оцінюєте можливість виявлення пошкодження огороджувальних конструкцій? | + | + | + | + | + |

Продовження таблиці 2.2

| Питання | Менеджер | Економіст | Програміст | Системний адміністратор | Інші |
|---|---|---|---|---|---|
| Визначте потенційну небезпеку від пошкодження огороджувальних конструкцій? | + | + | + | + | + |
| Оцініть будь-ласка можливість виявлення закладних пристроїв на Вашому підприємстві? | + | | + | + | |
| Як часто на Вашому підприємстві проводиться пошук закладних пристроїв? | + | | + | + | |
| Як Ви оцінюєте потенційну небезпеку від витоку інформації через закладки? | + | | + | + | |
| Дайте оцінку можливості виявлення підглядання за об'єктами, де циркулює ІзОД? | + | + | + | + | + |
| Як Ви оцінюєте можливість нейтралізувати підглядання за об'єктами, де циркулює ІзОД?? | + | + | + | + | + |
| Оцініть будь-ласка потенційну небезпеку від прямої видимості об'єктів, де циркулює ІзОД? | + | + | + | + | + |
| Як би Ви оцінили можливість виявлення порушення режиму охорони об'єкта? | + | + | + | + | + |
| Охарактеризуйте можливість нейтралізувати порушення режиму охорони об'єкта? | + | + | + | + | + |
| Оцініть будь-ласка можливість виявлення відмов і несправностей в технічних засобах, що забезпечують охорону і контроль доступу? | | | + | + | |
| Як би Ви охарактеризували можливість нейтралізації відмов і несправностей в технічних засобах, що забезпечують охорону і контроль доступу? | | | + | + | |
| Визначте будь-ласка частоту відмов і несправностей в технічних засобах, що забезпечують охорону і контроль доступу? | | | + | + | |
| Який на Вашу думку рівень потенційної небезпеку від відмов і несправностей в технічних засобах, що забезпечують охорону і контроль доступу? | | | + | + | |

Продовження таблиці 2.2

| Питання | Менеджер | Економіст | Програміст | Системний адміністратор | Інші |
|---|---|---|---|---|---|
| Як би Ви охарактеризували можливість виявлення підслуховування? | + | + | + | + | + |
| Визначте можливість нейтралізувати підслуховування. | + | + | + | + | + |
| Оцініть частоту підслуховувань на Вашому підприємстві? | + | + | + | + | + |
| Охарактеризуйте можливість виявлення програмних закладок. | | | + | + | |
| Визначте можливість нейтралізувати програмні закладки. | | | + | + | |
| Дайте оцінку частоти появи на Вашому підприємстві програмних закладок. | | | + | + | |
| Оцініть потенційну небезпеку від програмних закладок. | | | + | + | |
| Як би Ви охарактеризували можливість виявлення нелегальних дій при використанні радіоканалів/глобальних інформаційних мереж? | + | + | + | + | + |
| Як Ви оцінюєте можливість нейтралізації нелегальних дій при використанні радіоканалів/глобальних інформаційних мереж? | + | + | + | + | + |
| Визначте частоту нелегальних дій при використанні радіоканалів/глобальних інформаційних мереж? | + | + | + | + | + |
| Дайте оцінку рівня потенційної небезпеки від нелегальних дій при використанні радіоканалів/глобальних інформаційних мереж? | + | + | + | + | + |
| Охарактеризуйте можливість виявлення помилок в ПЗ? | + | + | + | + | + |
| Оцініть можливість нейтралізації помилок в ПЗ? | + | + | + | + | + |
| Як Ви оцінюєте частоту виникнення помилок в ПЗ? | + | + | + | + | + |
| Як би Ви охарактеризували потенційну небезпеку від помилок в ПЗ? | + | + | + | + | + |
| Яка на Вашу думку можливість виявлення порушення режиму використання інформації? | + | + | + | + | + |

Продовження таблиці 2.2

| Питання | Менеджер | Економіст | Програміст | Системний адміністратор | Інші |
|---|---|---|---|---|---|
| Дайте оцінку можливості нейтралізації порушення режиму використання інформації? | + | + | + | + | + |
| Визначте частоту виникнення порушень режиму використання інформації? | + | + | + | + | + |
| Як би Ви оцінили потенційну небезпеку від порушення режиму використання інформації? | + | + | + | + | + |
| Охарактеризуйте можливість виявлення відмов і несправностей технічних засобів? | + | + | + | + | + |
| Оцініть можливість нейтралізації відмов і несправностей технічних засобів? | + | + | + | + | + |
| Як Ви оцінюєте частоту відмов і несправностей технічних засобів? | + | + | + | + | + |
| Який на Вашу думку рівень потенційної небезпеки від відмов і несправностей технічних засобів? | + | + | + | + | + |
| Дайте оцінку можливості виявлення збоїв ПЗ? | + | + | + | + | + |
| Визначте можливість нейтралізації збоїв ПЗ? | + | + | + | + | + |
| Яка на Вашу думку частота збоїв ПЗ? | + | + | + | + | + |
| Оцініть рівень потенційної небезпеки від збоїв ПЗ? | + | + | + | + | + |
| Оцініть можливість виявлення порушення режиму конфіденційності. | + | + | + | + | + |
| Охарактеризуйте можливість нейтралізації порушення режиму конфіденційності. | + | + | + | + | + |
| Визначте частоту порушень режиму конфіденційності. | + | + | + | + | + |
| Як би Ви охарактеризували потенційну небезпеку від порушення режиму конфіденційності? | + | + | + | + | + |
| Як би Ви оцінили можливість виявлення помилок при управлінні складними системами. | + | + | + | + | |
| Охарактеризуйте можливість нейтралізації помилок при управлінні складними системами. | + | + | + | + | |

Продовження таблиці 2.2

| Питання | Менеджер | Економіст | Програміст | Системний адміністратор | Інші |
|---|---|---|---|---|---|
| Оцініть частоту виникнення помилок при управлінні складними системами. | + | + | + | + | |
| Який на Вашу думку рівень потенційної небезпеки від помилок при управлінні складними системами? | + | + | + | + | |
| Дайте оцінку можливості виявлення помилок при експлуатації технічних засобів. | | | + | + | |
| Як би Ви охарактеризували можливість нейтралізації помилок при експлуатації технічних засобів? | | | + | + | |
| Визначте частоту помилок при експлуатації технічних засобів? | | | + | + | |
| Як би Ви оцінили потенційну небезпеку від помилок при експлуатації технічних засобів? | | | + | + | |
| Оцініть можливість виявлення порушення режиму експлуатації технічних засобів. | | | + | + | |
| Дайте оцінку можливості нейтралізації порушення режиму експлуатації технічних засобів. | | | + | + | |
| Визначте частоту порушення експлуатації технічних засобів. | | | + | + | |
| Охарактеризуйте потенційну небезпеку від порушення режиму експлуатації технічних засобів. | | | + | + | |
| Оцініть можливість виявлення збоїв електропостачання. | + | + | + | + | + |
| Охарактеризуйте можливість нейтралізації збоїв електропостачання. | + | + | + | + | + |
| Як би Ви оцінили частоту збоїв електропостачання? | + | + | + | + | + |
| Визначте потенційну небезпеку від збоїв електропостачання? | + | + | + | + | + |
| Як Ви оцінюєте можливість виявлення пошкодження життєзабезпечуючих комунікацій? | + | + | + | + | + |
| Визначте можливість нейтралізації пошкодження життєзабезпечуючих комунікацій. | + | + | + | + | + |

Продовження таблиці 2.2

| Питання | Менеджер | Економіст | Програміст | Системний адміністратор | Інші |
|---|---|---|---|---|---|
| Дайте оцінку частоти пошкоджень життєзабезпечуючих комунікацій. | + | + | + | + | + |
| Оцініть рівень потенційної небезпеки від пошкоджень життєзабезпечуючих комунікацій. | + | + | + | + | + |
| Як Ви оцінюєте можливість виявлення виникнення пожежі? | + | + | + | + | + |
| Охарактеризуйте можливість нейтралізації виникнення пожежі. | + | + | + | + | + |
| Як часто виникають пожежі на Вашому підприємстві? | + | + | + | + | + |
| Як Ви оцінюєте потенційну небезпеку від пожежі на Вашому підприємстві? | + | + | + | + | + |
| Визначте можливість виявлення пожежі в районі, де знаходиться підприємство? | + | + | + | + | + |
| Як Ви оцінюєте можливість нейтралізації пожежі в районі, де знаходиться підприємство? | + | + | + | + | + |
| Охарактеризуйте потенційну небезпеку для Вашого підприємства від пожежі в районі, де воно знаходиться? | + | + | + | + | + |
| Як Ви оцінюєте можливість стихійного лиха в районі де знаходиться Ваше підприємство? | + | + | + | + | + |
| Як Ви оцінюєте можливість відновлення працездатності підприємства після стихійного лиха? | + | + | + | + | + |
| Охарактеризуйте частоту можливих стихійних лих в районі де знаходиться Ваше підприємство. | + | + | + | + | + |
| Визначте потенційну небезпеку для Вашого підприємства від стихійних лих в районі де знаходиться Ваше підприємство. | + | + | + | + | + |
| Дайте оцінку можливості виявити непередбачувані обставини? | + | + | + | + | + |
| Охарактеризуйте можливість нейтралізації непередбачуваних обставин? | + | + | + | + | + |
| Визначте частоту непередбачуваних обставин? | + | + | + | + | + |

Продовження таблиці 2.2

| Питання | Менеджер | Економіст | Програміст | Системний адміністратор | Інші |
|---|---|---|---|---|---|
| Як Ви оцінюєте потенційну небезпеку від непередбачуваних явищ? | + | + | + | + | + |
| Дайте оцінку можливості виявити нез'ясовані явища? | + | + | + | + | + |
| Охарактеризуйте можливість нейтралізації нез'ясованих явищ? | + | + | + | + | + |
| Визначте частоту нез'ясованих явищ? | + | + | + | + | + |
| Як Ви оцінюєте потенційну небезпеку від нез'ясованих явищ? | + | + | + | + | + |
| Дайте оцінку можливості виявити форс-мажорних обставин? | + | + | + | + | + |
| Охарактеризуйте можливість нейтралізації форс-мажорних обставин? | + | + | + | + | + |
| Визначте частоту форс-мажорних обставин? | + | + | + | + | + |
| Як Ви оцінюєте потенційну небезпеку від форс-мажорних обставин? | + | + | + | + | + |

## 2.5 Збір доказів та їх підготовка до прийняття рішення з розслідування інцидентів кібербезпеки

Зазвичай місце інциденту вміщує різні види цифрових носіїв інформації. Вони використовуються для збереження даних цифрових пристроїв і відрізняються обсягом пам'яті.

Прикладами цифрових носіїв є зовнішні переносні жорсткі диски, флеш-пам'ять, DVD-диски, Blu-Ray-диски.

І для того, щоб розпочати процес розслідування необхідно прийняти рішення про збір доказової бази, який приймає спеціаліст з розслідування інцидентів кібербезпеки.

При прийнятті рішення про збір цифрових пристроїв або отриманні потенційних доказів, потрібно враховувати кілька факторів, які включають наступне:

– мінливість потенційних доказів, представлених в цифровій формі;

– наявність повного шифрування диска або зашифрованих томів, паролів або ключів яких можуть знаходитися у вигляді мінливих даних в ОЗП, смарт-картах , інших пристроях або носіях;

– критичність системи, яка обговорюється;

– правові вимоги;

– ресурси, такі як розмір необхідної пам'яті, наявність персоналу, і тимчасові обмеження.

Якщо живлення цифрового пристрою ввімкнено (жорсткий диск, флеш-пам’ять):

1 За допомогою програмної утілити перевірити вміст носія на наявність конференційної інформації.

2 Зробити резервне копіювання вмісту носія на окремий носій для збереження доказу.

3 Зробити опис метаданих.

4 Відімкнути носій.

5 Промаркувати носій.

6 Звіт.

Якщо живлення цифрового пристрою вимкнено (DVD-диски, Blu-Ray-диски):

1 Промаркувати носій.

2 Підключити носій до автономного ПК.

3 За допомогою програмної утілити перевірити вміст носія на наявність конференційної інформації.

4 Зробити резервне копіювання вмісту носія на окремий носій для збереження доказу.

5 Зробити опис метаданих.

6 Вилучити носій.

7 Звіт.

За результатами отриманих доказів, виникає необхідність в їх застосуванні. А саме надати їх керівництву чи передати в правоохоронні

органи. Тому у спеціаліста з розслідування інцидентів кібербезпеки в ІТС повинна бути сформована чітка інструкція, що за чим робити і в яких випадках звертатися в правоохоронні органи, а в яких вирішувати реалізований інцидент внутрішніми силами.

2.6 Дії спеціаліста з розслідування інциденту кібербезпеки

При розслідувані інциденту кібербезпеки, спеціаліст такої сфери повинен розуміти, якими моделями розслідування користуватися, які першочергові заходи необхідно здійснити при виявлені інциденту, як формувати доказову базу, тобто за яким алгоритмом необхідно збирати докази, що робити із зібраними доказами, в яких випадках їх передавати керівництву, а в яких відразу звертатися до правоохоронних органів.

Тому проводячи розслідування інцидентів кібербезпеки необхідно виконати наступні дії спеціалістом у такій галузі:

1 Ідентифікувати інцидент;

2 Локалізувати сферу ІТ-інфраструктури, задіяної в інциденті;

3 Обмежити доступ до об'єктів, задіяних в інциденті;

4 Написати службову записку на ім'я відповідальної особи про факт виникнення інциденту;

5 Залучити за необхідністю, компетентних фахівців для консультації, такими можуть бути і співробітники правоохоронних органів;

6 Створити робочу групу з розслідування інциденту, за необхідністю, і скласти план робіт зі збору доказів і відновленню систем. Протоколювати всі дії, які здійснюються в ході реагування і розслідування інциденту.

7 Забезпечити збереження і належне оформлення доказів;

7.1 Зняти енергозалежну інформацію з працюючої системи, якщо це можливо;

7.2 Відтворити послідовність здійснення, реалізованого інциденту, в реальному часі;

7.3 Відключити пристрої від мереж живлення;

8 У присутності третьої незалежної сторони провести вилучення і опечатування носіїв інформації з доказовою базою, а також зняття образів та іншої інформації для подальшого аналізу і збереження;

8.1 Оформити протоколом всі операції з носіями інформації;

8.2 Провести детальний опис об'єктів з інформацією, на які була здійснена атака;

8.4 Зберегти опечатані об'єкти разом з протоколом в надійному місці до передачі носіїв на дослідження або в правоохоронні органи;

9 Після збереження і оформлення речових доказів відновити працездатність атакованої інформаційних систем;

10 При проведенні дослідження джерел інформації забезпечити незмінність доказів. Працювати тільки з копією;

11 При проведенні розслідування забезпечити коректну взаємодію з зацікавленими підрозділами;

12 По завершенні розслідування оформити відповідний звіт і скласти рекомендації щодо зниження ризиків виникнення подібних інцидентів в майбутньому;

13 При зверненні до правоохоронних органів представити їм докладний опис інциденту, опис зібраних доказів і результати їх аналізу.

Спеціаліст з розслідування інцидентів кібербезпеки повинен звертатися до правоохоронних органів, якщо реалізований інцидент, який не можливо розслідувати внутрішніми силами, тобто притягнути до відповідальності зловмисника або не входить до компетенції спеціаліста з розслідування інцидентів кібербезпеки, який трапився на підприємстві.

Тому його дії з розслідування на ОІД зводяться до:

– проводить збір доказів;

– проводить аналіз доказової бази (жорстких дисків, журналів, шкідливого програмного забезпечення);

– визначає причини;

– виявляє атаковані сфери підприємства на які була здійснена атака;

– формує список потенційних шахраїв.

Якщо підприємству нанесені значні збитки і реалізований інцидент підпадає під кримінальну відповідальність, залучаються правоохоронні органи, які в свою чергу виконують наступні дії:

1 Проводять оперативно-розшукові дії;

2 Перевіряють матеріали зібрані спеціалістом, який проводив розслідування інциденту;

3 Залучають експертів, проводять експертизи і за необхідністю вилучає техніку, яка задіяна в інциденті;

4 Проводять слідчі дії;

5 Передає матеріали до суду.

## 2.7 Висновок

В розділі виконаний аналіз методів збору експертної інформації для розслідування інцидентів кібербезпеки, наведений аналіз загроз, висунуті вимоги до критерії захисту інформації, запропоновано ввести підвищені вимоги до критерію «спостереженість».

Для експерта з розслідування інцидентів розроблено лист для опитування працівників підприємства (менеджер, економіст, програміст, системний адміністратор та інші) для виявлення загроз ІБ та каналів витоку інформації.

Запропоновано покроковий алгоритм збору доказів та їх підготовки до прийняття рішення з розслідування інцидентів кібербезпеки. та визначені основні етапи процесу реагування на інціденти ІБ.

# РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

З метою обґрунтування моделі розслідування інцидентів кібербезпеки із врахування критеріїв захищеності інформації в роботі запропоновано ввести підвищені вимоги до критерію «спостереженість».

Для експерта з розслідування інцидентів розроблено лист для опитування працівників підприємства (менеджер, економіст, програміст, системний адміністратор та інші) для виявлення загроз ІБ та каналів витоку інформації. Запропоновано покроковий алгоритм збору доказів та їх підготовки до прийняття рішення з розслідування інцидентів кібербезпеки та визначені основні етапи процесу реагування на інциденти ІБ.

Для економічного обґрунтування запропонованих рішень необхідно здійснити наступні розрахунки:

– капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення;

– річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;

– річний економічний ефект;

– показники економічної ефективності застосування моделі розслідування інцидентів кібербезпеки із врахування критеріїв захищеності інформації.

## 3.1 Розрахунок (фіксованих) капітальних витрат

*Капітальні інвестиції* – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

### 3.1.1. Визначення витрат на розробку моделі розслідування інцидентів кібербезпеки із врахування критеріїв захищеності інформації

3.1.1.1 Визначення трудомісткості розробку моделі розслідування інцидентів кібербезпеки із врахування критеріїв захищеності інформації

Трудомісткість розробки моделі розслідування визначається тривалістю кожної робочої операції:

$$t = tmз + tв + ta + tз + tобр + tзз + tр + tд, \text{ годин,}$$

де $tmз$ – тривалість складання технічного завдання, $tmз = 6$;

$tв$ – тривалість вивчення ТЗ, літературних джерел за темою тощо, $tв = 20$;

$ta$ – тривалість аналізу методів збору експертної інформації для розслідування інцидентів кібербезпеки, $ta = 27$;

$tз$ – тривалість розробки вимог до критерію захисту інформації та критерію «спостереженість», $tз = 32$;

$tобр$ – тривалість розробки листів для опитування працівників підприємства (менеджер, економіст, програміст, системний адміністратор та інші) для виявлення загроз ІБ та каналів витоку інформації, $tобр = 22$;

$tзз$ – тривалість розробки покрокового алгоритму збору доказів та їх підготовки до прийняття рішення з розслідування інцидентів кібербезпеки, $tзз = 44$;

$tр$ – тривалість визначення основних етапів процесу реагування на інціденти ІБ, $tр = 38$;

$tд$ – тривалість підготовки технічної документації, $tд = 8$.

Таким чином,

$$t = 6 + 20 + 27 + 32 + 22 + 44 + 38 + 8 = 197 \text{ годин,}$$

3.1.1.2 Розрахунок витрат на розробку моделі розслідування інцидентів кібербезпеки із врахування критеріїв захищеності інформації

Витрати на створення програмного продукту Кпз складаються з витрат на заробітну плату виконавця програмного забезпечення *Ззп* і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК *Змч*:

$$К_{пз} = З_{зп} + З_{мч} = 23837 + 68{,}32 = 23905{,}32 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 197*121 = 23837 \text{ грн.}$$

де $t$ – загальна тривалість створення ПЗ, годин;

*Зпр* – средньогодинна заробітна плата програміста з нарахуваннями, грн/годину.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_{д} \cdot С_{мч} = 8 \cdot 8{,}54 = 68{,}32 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = 0{,}9 \cdot 5 \cdot 1{,}64 + \frac{3600 \cdot 0{,}5}{1920} + \frac{2100 \cdot 0{,}2}{1920} = 8{,}54 \text{ грн.}$$

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = 23905{,}32 + 3000 = 26905{,}32 \text{ грн.}$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, $К_{навч}$=3000 грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \quad грн.$$

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн.).

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{ел} + С_{о} + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_{н}$ = 8000 грн.).

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_{з}$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 18000 грн. Для виконання розслідування інцидентів кібербезпеки із врахування критеріїв захищеності інформації працюватиме один спеціаліст. Додаткова заробітна плата – 10% від основної заробітної плати. Отже,

$$С_з = 18000*12 + 18000*12*0,1= 237600 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2016 р. складає 22%.

$$С_{єв} = 237600*0,22 = 52272 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1,8 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,64 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 1,8*1920*1,64 = 5702,4 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 2% (Стос = 26905,32*0,02=538,11 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 8000 + 237600 + 52272 + 5702,4 + 538,11 = 304112,51 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 304112,51 грн.

## 3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

### 3.2.1 Оцінка величини збитку

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 3 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 3 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 4500 грн на місяць;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 5500 грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 10 осіб.;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 500 осіб.;

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 10.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_П = \frac{4500 \cdot 500}{176} \cdot 4 = 51136{,}36 \quad \text{грн.}$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, 3000 грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ВИ} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{4500 \cdot 500}{176} \cdot 3 = 38352{,}27 \text{ грн.}$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{ПВ} = \frac{\sum Зо}{F} \cdot t_в = \frac{5500 \cdot 10}{176} \cdot 3 = 937{,}5 \text{ грн.}$$

$$П_в = 38352{,}27+937{,}5+3000=42289{,}77 \text{ грн.}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із средньогодинного обсягу продажів і сумарного часу простою атакованого взла або сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ})$$

$$V = \frac{50000000}{2080} \cdot (4+3+3) = 240384 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 ч.

$$U = 51136{,}36+42289{,}77+240384=333810{,}13 \text{ грн.}$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U = \sum_1 \sum_{10} 333810{,}13 = 3338101{,}3 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C \text{ грн.},$$

де $B$ – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (20%);

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 3338101{,}3*0{,}2 - 304112{,}51 = 363507{,}75 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де $E$ – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{363507,75}{26905,32} = 13,51, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$\text{ROSI} > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (18 %);

$N_{інф}$ – річний рівень інфляції, (11%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$13,51 > (18 - 11)/100 = 13,51 > 0,07.$$

Термін окупності капітальних інвестицій $T_o$ показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{13,51} = 0,07, \quad \text{років.}$$

## 3.4 Висновок

Відповідно до проведених розрахунків економічної ефективності застосування моделі розслідування інцидентів кібербезпеки із врахування критеріїв захищеності інформації можна зробити висновок щодо її економічної доцільності, оскільки значення коефіцієнта повернення інвестицій (ROSI = 13,51) перевищує величину річної депозитної ставки з урахуванням інфляції (13,51 > 0,07). Термін окупності складає 0,07 років (26 днів). Загальний ефект від впровадження моделі розслідування інцидентів кібербезпеки із врахування критеріїв захищеності інформації складатиме 363507,75 грн.

# ВИСНОВКИ

Розкриття сутності поняття інцидент інформаційної безпеки дозволяє відтворити образ потенційного порушника, зрозуміти причини та процес настання інциденту.

Як показали результати аналізу статистики, значна частина інцидентів кібербезпеки, що приводили до витоку конфіденційних даних, відбувалася з вини співробітників компанії, випадково або навмисно провокували втрату цінної інформації.

Дана робота дозволить сформувати загальні представлення про процес розслідування інцидентів кібербезпеки, хоча кожен із етапів процесу може стати в подальшому темою окремого дослідження.

Запровадження організаціями процесу розслідування інцидентів кібербезпеки дозволить:

– підвищити рівень кібербезпеки;

– посилити увагу до попередження інцидентів шляхом віднаходження винних у його виникненні та його причин;

– знизити негативні наслідки на бізнес-процеси організації;

– дозволить скоректувати політику інформаційної безпеки організації.

За результатами дипломної роботи були досягнуті наступні завдання:

– проведено аналіз законодавчої бази та міжнародних стандартів з розслідування інцидентів кібербезпеки;

– проведено аналіз методів збору експертної інформації для розслідування інцидентів кібербезпеки;

– наведений аналіз загроз;

– висунуті вимоги до критерії захисту інформації, запропоновано ввести підвищені вимоги до критерію «спостереженість»;

– розроблено лист для опитування працівників підприємства (менеджер, економіст, програміст, системний адміністратор та інші) для виявлення загроз ІБ та каналів витоку інформації;

- визначено основні моделі розслідування інцидентів кібербезпеки;
- проаналізовано процес розслідування інцидентів кібербезпеки;
- сформовано рекомендації з розслідування інцидентів кібербезпеки.

# ПЕРЛІК ПОСИЛАНЬ

1 Конвенція про кіберзлочинність (набула чинність 01.07.2006) // Верховна Рада України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_575.

2 Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : закон України від 9.01.2007 р. № 537-V [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/ laws/show/537–16.

3 Про Стратегію національної безпеки України : указ Президента України від 12.02.2007 р. № 105/2007 (із змінами від 8.06.2012 р. № 389/2012) [Електронний ресурс]. – Режим доступу: http:// zakon4.rada.gov.ua/laws/show/105/2007.

4 Офіційний сайт Міжнародного фонду збору інформації про комп'ютерні інциденти в світі DataLossDB [Електронний ресурс]. – Режим доступу: http://Datalossdb.org/statistics.

5 Статистичні данні про ризики зіткнення з веб-програмами[Електронний ресурс]. – Режим доступу: https://securelist.ru/analysis/ksb/27543/kaspersky-security-bulletin-2015-osnovnaya-statistika-za-2015-god/.

6 Статистичні дані щодо DDoS-атак у країнах світу [Електронний ресурс]. – Режим доступу: https://www.infowatch.ru/report2015-2016.

7 Статистичні дані країн, які є постачальниками спаму [Електронний ресурс]. – Режим доступу: https://securelist.ru/analysis/ksb/24580/kaspersky-security-bulletin-2014-osnovnaya-statistika-za-2015-god/.

8 Статистичні дані, щодо витоку конфіденційної інформації [Електронний ресурс]. – Режим доступу: https://www.antimalware.ru/.

9 U.S. Department of Justice, Federal Bureau of Investigation Internet Crime Report 2015.

10 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=
6D68FCE54A40938081139F546DD E47B?art_id=38814&cat_id=38712.

11 Canada's Cyber Security Strategy: For a stronger and more prosperous Canada. – Her Majesty the Queen in Right of Canada, 2010. – 14 с. – [Електронний ресурс]. – Режим доступу: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

12 Национальная стратегия кибербезопасности (NCSS). От понимания к возможности.– Holland, Den Haag: National Coordinator for Security and Counterterrorism, 2013. – [Електронний ресурс]. – Режим доступу: //www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.

13 Соколов М.С. Кибернетическая безопасность – понятие, значение и эволюция от военных основ к самостоятельному виду безопасности // Военное право. – 2012. – № 1. – [Електронний ресурс]. – Режим доступу: http://db.inforeg.ru/eni/artList.asp?j=4&id=0220913464&idfull=0421200099.

14 Мельник С.В., Тихомиров О.О., Лєнков О.С. До проблеми формування понятійно-термінологічного апарату кібербезпеки: зб. матер. наук.-практ. конф. [Актуальні проблеми управління інформаційною безпекою держави], (Київ, 22 березня 2011 р.). – К. : Вид-во НА СБ України, 2011. – Ч. 2. – С. 43-48.

15 Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право. – 2012. – № 2. – С. 162-169.

16 НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс]. – Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407.

17 Про Доктрину інформаційної безпеки України : указ Президента України [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/514/2009.

18 СБУ: Головні проблеми для України – тероризм і кіберзлочинність // Українська Правда [Електронний ресурс]. – Режим доступу: http://www.pravda.com.ua/news/2012/03/23/6961285.

19 Управління боротьби з кіберзлочинністю // Міністерство внутрішніх справ України [Електронний ресурс]. – Режим доступу: http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754.

20 Securing Cyberspace for the 44th Presidency / James A. Lewis // Center for Strategic and International Studies [Електронний ресурс]. – Режим доступу: http://csis.org/files/media/csis/pubs/081208_ securingcyberspace_44.pdf.

21 Дубов Д. В. Кібербезпека : світові тенденції та виклики для України / Д. В. Дубов, М. А. Ожеван. – К. : НІСД, 2011. – 30 с.

22 ISO/IEC 27001:2013 «Система управління інформаційною безпекою. Вимоги».

23 ISO/IEC 27032:2012 «Інформаційні технології – Методи забезпечення безпеки - Керівництво з кібербезпеки».

24 ISO/IEC 27035:2011 «Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки».

25 COBIT – Цілі контролю за інформаційними та суміжними технологіями, 2012 р.

26 Гладиш С.В., Кононович В.Г., Тардаскін М.Ф. Порівняльний аналіз стандартів ISO/IEC та української нормативної бази в частині керування інцидентами інформаційної безпеки // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2013. – № 15. – с. 31–39.

27 Гладиш С.В. Реагування та обробка інцидентів інформаційної безпеки в мережі GSM // Вісник Державного університету інформаційно-комунікаційних технологій. – 2008. – № 1. – с. 58-72.

28 Порядок захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах. – Затв. наказом ДСТСЗІ СБУ № 76 від 24.12.2001 р.

29 Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 2594-IV від 31.05.2006.

30 Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою КМУ від 29.03.2006 р. № 373.

31 Малюк А. Информационная безопасность: концептуальные и методологические основы защиты информации. – М.: Горячая линия – Телеком, 2009. – 280 с.

32 Интеллектуальные системы управления организационно-техническими системами / Под ред. проф. А.А. Большакова. – М.: Горячая Линия – Телеком, 2010. –160 с.

33 Коробко В.В., Скоропаденко А.П., Задоя Г.М., Вовк В.М. Интегрированная система сбора информации об экстремальных состояниях телекоммуникационных сетей и их защиты // Зв'язок. – 2011. – № 1. – С. 39-45.

34 Сакович Л.М., Політов В.І. Використання системи підтримки прийняття рішення під час експлуатації та ремонту засобів і комплексів зв'язку // Зв'язок. – 2012. – № 5. – С. 37-39.

35 Єрохін А.Л. Модель візуалізації нештатних подій у складних інформаційних системах // Зв'язок. – 2009. – № 6. – С. 52-56.

36 Кримінальний кодекс України: Закон України // Відомості Верховної Ради України – 2001. – № 25-26. – Ст. 131.

37 НД ТЗІ 1.3-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

ДОДАТОК А. Відомість матеріалів дипломного проекту

| № | Формат | Найменування | Кількість листів | Примітка |
|---|---|---|---|---|
| 1 | А4 | Реферат | 3 | |
| 2 | А4 | Список умовних скорочень | 1 | |
| 3 | А4 | Зміст | 2 | |
| 4 | А4 | Вступ | 3 | |
| 5 | А4 | 1 Розділ | 35 | |
| 6 | А4 | 2 Розділ | 27 | |
| 7 | А4 | 3 Розділ | 11 | |
| 8 | А4 | Висновки | 2 | |
| 9 | А4 | Перелік посилань | 4 | |
| 10 | А4 | Додаток А | 1 | |
| 11 | А4 | Додаток Б | 1 | |
| 12 | А4 | Додаток В | 1 | |
| 13 | А4 | Додаток Г | 1 | |

# ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

# ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на дипломну роботу магістра на тему:

Обґрунтування моделі розслідування інцидентів кібербезпеки із врахуванням критеріїв захищеності інформації

студента групи 125м-17-1

Дем’янюка Максима Юрійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, 37 джерел та 4 додатка.

Актуальність теми полягає в необхідності розробки моделі, алгоритмів, підходів до проведення розслідування інцидентів кібербезпеки на приватних підприємствах.

Зміст та структура дипломної роботи дозволяють розкрити поставлену тему повністю.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію) на основі аналізу нормативно-правової бази в сфері захисту інформації.

Практична значущість полягає в можливості використання даного проекту при проведенні розслідування інцидентів кібербезпеки на приватних підприємствах.

Робота виконана самостійно. У дослідженні виконано аналіз моделей та процесів забезпечення кібербезпеки, проаналізовано життєвий цикл атаки, визначено основні етапи процесу реагування на інциденту ІБ, розроблені рекомендації для експерта з проведення розслідування інцидентів кібербезпеки. Це підтверджує самостійність обробки даних, практичні рекомендації та висновки.

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому дипломна робота задовольняє усім вимогам і може бути допущена до захисту, а його автор Дем’янюк Максим Юрійович заслуговує на оцінку «_____».

Керівник дипломної роботи,
д.т.н., проф. В.І. Корнієнко

Керівник спец. част.

ст. викл. кафедри БІТ В.І. Мєшков