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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Розгонюка Дмитра Ігоровича*

академічної групи *125м-22-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Обґрунтування плану розслідування інцидентів інформаційної безпеки в ІКС комерційного підприємства*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Ковальова Ю.В.			
розділів:				
спеціальний	к.т.н., доц. Ковальова Ю.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту *Розгонюку Дмитру Ігоровичу* **академічної групи** *125м-22-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Обґрунтування плану розслідування інцидентів інформаційної безпеки в ІКС комерційного підприємства*

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Нормативні аспекти управління інцидентами інформаційної безпеки	02.11.2023
Розділ 2	Виникнення та розслідування інцидентів інформаційної безпеки	16.11.2023
Розділ 3	Економічна частина	30.11.2023

Завдання видано _____ Ковальова Ю.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Розгонюк Д.І.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка складається з 90 сторінок, 2 рис., 1 табл., 4 додатків, 40 джерел.

Об'єкт дослідження: процес розслідування інцидентів інформаційної безпеки в ІКС.

Мета роботи: підвищення ефективності розслідування інцидентів інформаційної безпеки.

Методи дослідження: системний аналіз, методи порівняння, структурний аналіз та спостереження.

У спеціальній частині дана характеристика процесу розслідування інцидентів інформаційної безпеки в ІКС. У роботі досліджено етапи розслідування інцидентів інформаційної безпеки в інформаційно–комунікаційних системах. Проведено аналіз основних джерел на наявність етапів розслідування інцидентів ІБ, розглянуто та проаналізовано особливості процесу розслідування та управління інцидентами.

Для забезпечення планового та точного розслідування інцидентів інформаційної безпеки в ІКС слід впровадити на комерційних підприємствах запропоновану інструкцію.

В економічному розділі визначено ефективність від впроваджуваних рекомендацій.

Практичне значення роботи полягає в розробці рекомендацій з розслідування інцидентів інформаційної безпеки.

Результати здійснених у роботі досліджень можуть бути використані при розслідуванні інцидентів інформаційної безпеки в ІКС комерційних підприємств.

Наукова новизна дослідження полягає в впровадженні запропонованої інструкції для комерційних підприємств

Ключові слова: ІНЦИДЕНТ, УПРАВЛІННЯ ІНЦИДЕНТАМИ, РОЗСЛІДУВАННЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, ІКС.

THE ABSTRACT

Explanatory notes consist of 90 pages, 2 pictures, 1 table, 4 appendices, 40 sources.

The object of study: the process of investigating incidents of information security in ITS.

Objective: to improve the efficiency of investigation of incidents of information security.

Methods, systems analysis, comparison methods, structural analysis and observation.

The special part describes the process of investigating of incidents of information security in ITS. In this work the investigation stage of information security incidents in information and communication systems. The analysis of the main sources for the stages of investigation of information security incidents was made. It was reviewed and analyzed the features of the investigation process and incident management.

It was offered to provide planned and precise investigation of information security incidents in ITS that should be implemented in commercial enterprises according to instructions.

The economic section includes the calculation of the efficacy of implemented recommendations.

The practical significance of the work is to develop recommendations for investigation of information security incidents/

The results that were made in the research, can be used in the investigation of information security incidents in ITS of commercial enterprises.

The scientific novelty of the research is to implement the proposed guidelines for business.

Keywords: INCIDENT, INCIDENT MANAGEMENT, INVESTIGATION, INFORMATION SECURITY, ITS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДКР – дослідно–конструкторська робота;

ДСТУ – державний стандарт України;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ІТ – інформаційні технології;

ІКС – інформаційно–комунікаційна система;

КЗЗ – комплекс засобів захисту від несанкціонованого доступу;

КСЗІ – комплексна система захисту інформації;

МКС – комп'ютерна система;

НД – нормативний документ;

НД ТЗІ – нормативний документ системи технічного захисту інформації;

НСД – несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ОС – обчислювальна система;

ПБ – політика безпеки;

ПЗ – програмне забезпечення;

ПРД – правила розмежування доступу;

СЗІ – служба захисту інформації;

СЗС – спеціаліст з свідоцтв;

СОР – спеціаліст оперативного реагування;

СРІБ – служба реагування на інциденти інформаційної безпеки;

СУІБ – система управління інцидентами інформаційної безпеки;

ТЗ – технічне завдання;

ТОВ – товариство з обмеженою відповідальністю.

УІБ – управління інцидентами інформаційної безпеки

ЗМІСТ

ВСТУП

Актуальність. Розвиток технологій захисту інформації невпинно йде в гору. З'являються нові методи захисту інформації але також з'являються і нові загрози та нові види порушників. Ніяка найновіша методологія не зможе гарантувати 100% захисту від інцидентів інформаційної безпеки. Правда така, що захист з'являється тільки тоді, коли трапляється інцидент. Виникнення інциденту інформаційної безпеки в організації несе певні наслідки. Ці наслідки можуть проявитися у втратах клієнтів, появі проблем на ринку збуту, втратах грошових коштів й інших загрозах ІБ, що впливають на нормальну роботу системи організації. Складання певного плану, діючи за найкращими міжнародними методиками, можна запобігти інциденту й убезпечити своє підприємство від небажаних подій. Планування грає дуже важливу роль для організацій, які швидко розвиваються. Це допоможе організації повернутися до роботи вмить після інциденту. А також уникнути переривання в роботі інформаційно–комунікаційних систем організації. Аналіз існуючих методів показав, що в державних документах невизначено процес управління інцидентами чи розслідування, а іноземних документах ці процеси охоплюють загальну систему інцидентів на підприємствах та є занадто складними для людей, незнайомих з інформаційною безпекою.

Таким чином, актуальним науковим завданням є створення та удосконалення існуючих рекомендацій з розслідування інцидентів ІБ в ІКС.

Метою роботи є встановлення етапів і підвищення ефективності процесу розслідування інцидентів ІБ в ІКС.

Завдання дослідження. Розробити інструкцію з розслідування інцидентів інформаційної безпеки для ІКС комерційних підприємств. Розроблені рішення представити в цій кваліфікаційній роботі. Розроблений документ повинен бути:

– простим для розуміння як керівництву так і персоналу організації;

– повинен бути гнучким для підлаштування до інших ІКС інших комерційних підприємств;

– мати чіткі вимоги та дії до розслідування інцидентів ІБ;

– відповідати та не порушувати державні закони та нормативні документи.

Для будь–якої організації важливо серйозно ставитися до інформаційної безпеки і мати структурований і спланований підхід до:

– реагування на інциденти інформаційної безпеки, включаючи активізацію відповідних засобів управління для запобігання, мінімізації і відновлення після негативного впливу;

– звітності про уразливість інформаційної безпеки, які раніше не були використані і не стали причиною подій або можливих інцидентів інформаційної безпеки, а також оцінці і боротьби з ними відповідним чином;

– вивчення інцидентів і вразливостей інформаційної безпеки, впровадження превентивних засобів управління і вдосконалення загального підходу до управління інцидентами інформаційної безпеки.

РОЗДІЛ 1. НОРМАТИВНІ АСПЕКТИ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1Терміни та визначення

Відповідно до Закону України «Про інформацію» наведені нижче терміни в цій кваліфікаційній роботі вживаються в такому розумінні:

Документ – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі.

Захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Інформація – будь–які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Суб'єкт владних повноважень – орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

Відповідно до Закону України «Про захист інформації в інформаційно–телекомунікаційних системах» терміни в цій кваліфікаційній роботі вживаються в такому розумінні:

Блокування інформації в системі – дії, внаслідок яких унеможливлюється доступ до інформації в системі.

Виток інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї.

Володілець інформації – фізична або юридична особа, якій належать права на інформацію.

Власник системи – фізична або юридична особа, якій належить право власності на систему.

Доступ до інформації в системі – отримання користувачем можливості обробляти інформацію в системі.

Захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

Знищення інформації в системі – дії, внаслідок яких інформація в системі зникає.

Інформаційна (автоматизована) система – організаційно–технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Інформаційно–комунікаційна система – сукупність інформаційних та комунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно–технічних заходів, засобів і методів захисту інформації.

Користувач інформації в системі (далі – користувач) – фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі.

Несанкціоновані дії щодо інформації в системі – дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства.

Обробка інформації в системі – виконання однієї або кількох операцій, зокрема збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

Порушення цілісності інформації в системі – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст.

Порядок доступу до інформації в системі – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації.

Комунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

В наведених вище законах терміни інцидентів не визначені. Тому застосовуються міжнародні стандарти.

Терміни та визначення за стандартом ISO/IEC TR 18044:2004 «Information technology. Security techniques. Information security incident management» (Інформаційні технології. Методи і засоби забезпечення безпеки. Менеджмент інцидентів ІБ):

Інцидент інформаційної безпеки – подія, що є наслідком одного або кількох небажаних або несподіваних подій ІБ, що мають значну ймовірність компрометації бізнес–операції і створення загрози ІБ.

Подією інформаційної безпеки – є ідентифікована поява певного стану системи, сервісу або мережі, що вказує на можливе порушення політики ІБ або відмова захисних заходів, або виникнення невідомої раніше ситуації, яка може мати відношення до безпеки.

Планування безперервності бізнесу – є процесом забезпечення гарантії відновлення операції в разі виникнення будь–якого несподіваного або небажаного інциденту, здатного негативно впливати на безперервність важливих функцій бізнесу і підтримують його елементів.

Група реагування на інциденти інформаційної безпеки (ГРІБ) – є групою (командою) відповідно навчених і довірених членів організації, яка обробляє інциденти ІБ під час їх життєвого циклу. Іноді ця група може доповнюватися зовнішніми експертами, наприклад, з офіційно визнаною групи реагування на комп'ютерні інциденти або комп'ютерної групи швидкого реагування.

Експертиза інформаційної безпеки – застосування методів дослідження і аналізу для виявлення, реєстрації та перевірки інцидентів інформаційної безпеки.

1.2 Аналіз нормативних документів в сфері УІІБ

В аналізі задіяні найбільш розповсюджені нормативні документи. Аналіз ведеться на наявність методів чи рекомендацій з розслідування інцидентів ІБ, для комерційних підприємств. Не для державних, тому що у них вже існують свої методи. Кожна державна установа вже забезпечена надійним захистом, а існуючі правила або методики не можна використовувати за основу так як відповідно кожна з державних установ має свою специфіку роботи. Тому аналізуючи всі можливі документи державні закони чи стандарти на наявність методів чи правил розслідування інцидентів ІБ буде виключно для комерційних підприємств.

Аналіз Державних нормативних документів України.

Закон України «Про інформацію» встановлює загальні положення, в яких визначаються терміни, державна інформаційна політика, основні принципи інформаційних відносин та інше. Далі регулюються види інформації, а також діяльність журналістів, засобів масової інформації їх працівників. Аналізуючи далі, визначено відповідальність за порушення закону. Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно–правову, адміністративну або кримінальну відповідальність згідно із законами України. В кінці закону зазначенні прикінцеві положення.

Згідно закону України «Про захист інформації в інформаційно–телекомунікаційних системах» об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є:

– володільці інформації;

– власники системи;

– користувачі.

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації.

Власник системи забезпечує захист інформації в системі, в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом.

Власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу.

Власник системи, яка використовується для обробки інформації з іншої системи, забезпечує захист такої інформації в порядку та на умовах, що визначаються договором, який укладається між власниками систем, якщо інше не встановлено законодавством. Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі.

Умови обробки інформації в системі. Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством. Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом.

Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, комунікаційних та інформаційно–телекомунікаційних системах» складається з двадцяти п’яти правил та декількох розділів:

– загальна частина;

– організаційні засади забезпечення захисту інформації.

В «Загальній частині» визначаються пошагові правила з першого по п’ятнадцятий пункт. Встановлюються цілі цих правил, призначення, що полягає під захист в системі та інше. В розділі «Організаційні засади забезпечення захисту інформації» з пункту шістнадцять до пункту двадцять п’ять описується що потрібно для захисту інформації в системі. Наприклад:

Для забезпечення захисту інформації в системі створюється комплексна система захисту інформації.

Відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту покладається на керівника (заступника керівника) організації, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи.

Порядок проведення державної експертизи системи захисту, державної експертизи та сертифікації засобів технічного і криптографічного захисту інформації встановлюється Адміністрацією. Далі в правилах зазначають відповідальність за організацію та проведення робіт із захисту інформації в системі та інше.

Державні Стандарти України. В стандартах таких як:

– ДСТУ 3396.0–96 Захист інформації. Технічний захист інформації. Основні положення;

– ДСТУ 3396.1–96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;

– ДСТУ 3396.2–97 Захист інформації. Технічний захист інформації. Терміни та визначення;

характеризується лише захист інформації, описується технічний захист, основні терміни та порядок ведення робіт. Але не визначається порядок дій після походження інциденту та дії реагування на нього.

Наприклад в інших стандартах України типу ДСТУ ISO/IEC 15288:2005 «Інформаційні технології. Процеси життєвого циклу системи» або ДСТУ ISO/IEC 13335–1:2004 «Інформаційні технології. Методи захисту. Керування інформацією й безпекою технології комунікацій» лише описують процеси системи або методи захисту та керування, тобто вимоги до всіх цих процесів та побудування їх за ДСТУ. На жаль, в державних стандартах не визначають правила дій щодо розслідування інцидентів ІБ. Тому наступним кроком є аналіз нормативних документів системи технічного захисту інформації.

В НД ТЗІ 1.1–002–99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» сформовано основні положення, визначення, основні принципи забезпечення захисту інформації та інше, але про інциденти та їх розслідування нічого не зазначено. Згідно з НД ТЗІ 1.4–001–2000 «Типове положення про службу захисту інформації в автоматизованій системі» сформовано «Завдання служби захисту інформації»:

– організація та координація робіт, пов'язаних з захистом інформації в АС, необхідність захисту якої визначається її власником або чинним законодавством, підтримка необхідного рівня захищеності інформації, ресурсів і технологій;

– розроблення проєктів нормативних і розпорядчих документів, чинних у межах організації, згідно з якими повинен забезпечуватися захист інформації в АС;

– організація робіт зі створення і використання КСЗІ на всіх етапах життєвого циклу АС.

Сформоване завдання СЗІ визначає відповідальність за забезпечення захисту інформації, але плани та рекомендації розслідування інцидентів ІБ не встановлені. За результатами аналізу всіх нормативних документів, планів та рекомендацій з розслідування, не визначено. Потрібно проаналізувати міжнародні документи та стандарти з інцидентів інформаційної безпеки, так як в Україні не приведено спеціального закону, документу чи стандарту.

Іноземні нормативні документи

– Британський стандарт серії BS 25999 «Business Continuity Management Standard» містить загальні рекомендації з управління неперервністю бізнесу, встановлює і деталізує конкретні вимоги до систем управління неперервністю бізнесу (СУНБ), причому тільки ті, дотримання яких може бути об'єктивно перевірено. Вимоги цих стандартів спрямовані на мінімізацію ризиків виникнення інцидентів і зниження втрат від збоїв в роботі. На базі цих вимог можна побудувати процес управління неперервністю бізнесу для цілей

забезпечення безперервності ключових бізнес–процесів в рамках області дії СУІБ.

– CMU/SEI–2004–TR–015 «Defining incident management processes for CISRT». Цей документ описує методологію планування, впровадження, оцінки та поліпшення процесів управління інцидентами. Основна увага робиться на організацію роботи CISRT (Critical Incident Stress Response Team) – групи або підрозділу, що забезпечує сервіс і підтримку запобігання, обробку та реагування на інциденти інформаційної безпеки. Вводиться ряд критеріїв, на підставі яких можна оцінювати ефективність даних сервісів, наводяться докладні процесні карти.

– Міжнародний стандарт ISO/IEC 18044: 2004 описує інфраструктуру управління інцидентами ІБ, в рамках циклічної моделі PDCA. Дає докладні специфікації для стадій планування, експлуатації, аналізу та поліпшення процесу і розглядає питання забезпечення нормативно–розпорядчою документацією і ресурсами і рекомендації щодо необхідних процедур;

– Міжнародний стандарт ISO/IEC 17799. Стандарт надає кращі практичні поради з менеджменту інформаційної безпеки для тих, хто відповідає за створення, реалізацію або обслуговування систем менеджменту інформаційної безпеки. Інформаційна безпека визначається стандартом як «збереження конфіденційності (впевненості в тому, що інформація доступна тільки тим, хто уповноважений мати такий доступ), цілісності (гарантії точності і повноти інформації та методів її обробки) і доступності».

Стандарти серії ISO/IEC 27000 – це міжнародні стандарти, що включають стандарти з інформаційної безпеки.

1 Стандарти ISO/IEC 27001 та ISO/IEC 27002 – стандарти інформаційної безпеки. ISO/IEC 27001 має назву «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги». А ISO/IEC 27002 називається «Інформаційні технології. Технології безпеки. Практичні правила менеджменту інформаційної безпеки». Перший стандарт встановлює вимоги до СУІБ в цілому, а також окремо до процесу управління інцидентами. Він

звертає особливу увагу на необхідність створення процесу управління інцидентами ІБ і підтримки його роботи з документацією, необхідної для регулювання і управління роботою в рамках розробленого процесу, а також визначення обов'язків і необхідних дій співробітників. Другий стандарт надає кращі практичні поради з менеджменту інформаційної безпеки для тих, хто відповідає за створення, реалізацію або обслуговування систем менеджменту інформаційної безпеки.

2 Міжнародний стандарт ISO/IEC 27031:2011 містить концепції і принципи, покладені на інформаційні і комунікаційні технології як на необ'ємну частину критичної інфраструктури будь–якої організації щодо забезпечення безперервності її бізнесу.

3 Міжнародний стандарт ISO/IEC 27035: 2011 «Information technology. Security techniques. Information security incident management» (Інформаційні технології. Методи і засоби забезпечення безпеки. Менеджмент інцидентів ІБ), [4]. Який містить структурований і планомірний підхід до виявлення, складання звітів і оцінці інцидентів ІБ, а також до здійснення відповідної реакції і управління інцидентами ІБ. Після прийняття в кінці 2011р. цей стандарт замінює ISO/IEC 18044: 2004 «Information technology. Security techniques. Information security incident management» (Інформаційні технології. Методи і засоби забезпечення безпеки. Менеджмент інцидентів ІБ). ISO/IEC 27035: 2011 є досить ємним і всебічно розглядає управління як уразливостями, так і інцидентами ІБ. Наводяться шаблони для підготовки звітів щодо подій, інцидентів ІБ і вразливостей.

Перші пункти стандарту з «Постановки управління інцидентами ІБ» розглянемо стисло та деякі не будемо приводити в роботі. А інші, тобто пункти стандарту, де розглядається «Реагування, постановка розслідування, звітність про інциденти ІБ», проаналізуємо більш відкрито. У стандарті після освітлення основ управління інцидентами ІБ, його переваг і ключових питань, деяких прикладів інцидентів ІБ, причин їх виникнення, процес управління інцидентами ІБ розглядається кілька підпроцесів:

– планування та підготовка до обробки інцидентів ІБ, та складання документів;

– виявлення, ідентифікація і підготовка звіту по інциденту ІБ;

– оцінка інциденту і прийняття рішень по інциденту ІБ;

– відповідна реакція на інцидент ІБ;

– витяг уроків з інциденту ІБ.

В перших пунктах стандарту визначається:

– галузь застосування;

– визначення (термінологія).

Далі приводяться Цілі, тобто описуються стратегія інформаційної безпеки, яку повинна виконувати організація, щоб забезпечити планомірний підхід до управління інцидентами ІБ.

В наступних пунктах описуються «Переваги структурованого підходу», «Застосування» та «Етапи». Наступним йде пункт, який описує приклади інцидентів ІБ. Приділяється увага тому, що інциденти інформаційної безпеки можуть бути навмисними або випадковими (наприклад, спровоковані помилкою або стихійним лихом), і можуть виникати в силу технічних чи фізичних факторів. Їх наслідки можуть включати в себе несанкціоноване розголошення, модифікацію, знищення або недоступність інформації, пошкодження або розкрадання активів організації. Якщо події інформаційної безпеки, про які не було повідомлено, визначаються як інциденти – це ускладнює розслідування інцидентів та контроль з метою запобігання рецидиву.

Після цього приділяється увага етапу «Планування та підготовки». Який складається з підпунктів:

– огляд ключових заходів (приведення списку заходів які повинна виконати організація);

– політика управління інцидентами інформаційної безпеки (про документування політики управління подіями);

– зацікавлені сторони (гарантування організацією того, що політика подій затверджена керівництвом і доступна кожному співробітнику);

– зміст (організація повинна забезпечити щоб зміст її політики управління інцидентами інформаційної безпеки охоплював питання зазначені в підпункті).

Інтеграція управління інцидентами інформаційної безпеки з іншими політиками є наступним пунктом.

Розділ стандарту про «Створення служби реагування на інциденти інформаційної безпеки» проаналізуємо детальніше. Тому що служба реагування на інциденти ІБ та її створення має важливу роль для розслідування інцидентів ІБ. Приводимо зміст:

1 Мета

Метою створення СРІІБ є забезпечення організації відповідної можливістю оцінки, реагування на інциденти інформаційної безпеки і винесення висновків з них, а також необхідної координації, управління, зворотного зв'язку і процесу передачі інформації. Члени СРІІБ можуть брати участь в зниженні фізичного і фінансового збитку, а також шкоди репутації організації, пов'язаного іноді з інцидентами інформаційної безпеки.

2 Члени групи і структура

Склад і кількість персоналу, а також структура СРІІБ повинні відповідати масштабу та структурі організації. Хоча СРІІБ може являти собою ізольовану службу або відділ, члени цієї служби можуть виконувати й інші обов'язки, а також залучати співробітників з різних підрозділів організації. Організація повинна оцінити чи потрібна спеціальна служба, віртуальна група, або ж поєднання їх обох. Організації, при виборі одного з цих варіантів, слід керуватися кількістю інцидентів і видами діяльності, здійснюваними СРІІБ.

3 Взаємодія з іншими підрозділами організації

СРІІБ повинна нести відповідальність за забезпечення усунення інцидентів, і в цьому контексті рівень повноважень керівника СРІІБ і членів цієї служби повинен дозволяти вживати необхідних дій, адекватних інциденту

інформаційної безпеки. Однак дії, які можуть мати несприятливий вплив на всю організацію щодо фінансів або репутації, повинні узгоджуватися з вищим керівництвом.

4 Відносини з зовнішніми зацікавленими сторонами

Необхідно встановити відносини між СРІБ з зовнішніми зацікавленими сторонами. Зовнішні зацікавлені сторони можуть бути представлені такими особами та організаціями:

– сторонній допоміжний персонал, який працює за контрактом;

– СРІБ Сторонніх організацій;

– постачальники керованих послуг, в тому числі провайдери послуг телекомунікацій, інтернет–провайдери та інше;

– правоохоронні органи;

– аварійні служби;

– відповідні державні організації;

– юридичний персонал;

– офіційні особи зі зв'язків з громадськістю та/або представники ЗМІ;

– бізнес партнери;

– клієнти;

– громадськість.

Етап «Звітності про події». Незалежно від джерела виявлення події ІБ, особа, яка безпосередньо звернули увагу на щось незвичайне або оповіщення автоматичними засобами, несе відповідальність за ініціювання процесу виявлення і звітності. Цією особою може виявитися будь–який представник персоналу організації, що працює постійно або за договором підряду. Цей представник повинен слідувати процедурам і використовувати форму звіту про події інформаційної безпеки, визначену схемою управління інцидентами ІБ, з метою залучення уваги, перш за все, керівництва. Отже, важливо, щоб весь персонал був ознайомлений з рекомендаціями, що відносяться до питання повідомлення про можливі події інформаційної безпеки, включаючи форми звіту, мав доступ до них і знав співробітників, яких необхідно сповіщати про

кожний випадок появи події інформаційної безпеки. Це включає в себе форму звіту про події інформаційної безпеки і відомості про співробітників, які повинні бути сповіщені відносного кожного випадку (всі співробітники повинні бути, принаймні, обізнані про форму звіту, що сприяло б розумінню ними схеми управління інцидентами інформаційної безпеки). Необхідно відзначити, що стаціонарний, бездротової і мобільний телефон, без захисних заходів від прослуховування, вважається небезпечним. При роботі з конфіденційною і таємною інформацією повинні бути зроблені додаткові захисні заходи.

Наступна інформація може бути використана як основа для форми реєстрації в системі відстеження інцидентів:

– час, дата виявлення;

– спостереження;

– контактна інформація (необов'язково).

Завершена форма (представлена на папері, або по електронній пошті, або по веб–формі) повинна використовуватися співробітниками СРІБ тільки при реєстрації інцидентів інформаційної безпеки в системі відстеження інцидентів. Важливо отримати знання і звіти про передбачувані, виявлених події інформаційної безпеки.

Відстеження події ІБ (можливо інциденту) має підтримуватися, коли це можливо, автоматизованим додатком. Використання інформаційної системи важливо для примусу персоналу слідувати встановленим процедурам і контрольним списками. Також вкрай корисно відстежувати «хто що зробив і коли», подробиці, які можуть бути пропущені помилково під час події ІБ (можливо інциденту).

Обробка конкретної події інформаційної безпеки залежить від того, що вона собою являє, а також від наслідків і впливів, до яких ця подія може призвести. Для багатьох людей прийняття рішення про спосіб обробки події виходить за межі їх компетентності. Тому співробітник, який інформує про

подію інформаційної безпеки, повинен заповнити форму звіту так, щоб в ній було якомога більше інформації, доступної йому на той момент.

При необхідності він зв'язується зі своїм керівником. Цю форму потрібно передати безпечним способом в належну контактну позицію (КП) (працює 24 години на добу, 7 днів на тиждень), а копію повідомлення – передати СРІБ.

СРІБ повинна призначити одного члена служби або представника, відповідального за всі звіти, спрямовані по електронній пошті, телефону, факсу і усній формі. Ця відповідальність може передаватися між членами служби щотижня. Призначений член служби оцінює ситуацію і вживає відповідних заходів для інформування відповідальних і зацікавлених сторін, а також для усунення інциденту інформаційної безпеки.

Також слід підкреслити, що при заповненні форми звіту важлива не тільки точність змісту, але і своєчасність заповнення. Також не слід затримувати подання звіту про подію інформаційної безпеки через уточнення її змісту. Якщо співробітник невпевнений в даних будь–якого поля в формі звіту, то це поле повинно бути позначено, а уточнення – надіслано пізніше. Також слід визнати, що деякі механізми електронної звітності (наприклад, електронна пошта) самі є очевидними цілями атаки. При наявності проблем або підозрі про їхню наявність відносно встановлених за замовчуванням механізмів електронної звітності (наприклад, електронна пошта), а також у випадках атаки на систему і читання звітів неуповноваженими особами, повинні використовуватися альтернативні засоби зв'язку. Альтернативні засоби зв'язку можуть включати службовців, телефони і текстові повідомлення. Такі альтернативні засоби повинні використовуватися на ранніх стадіях розслідування, коли стає очевидним, що подія інформаційної безпеки буде переведена в категорію інциденту, особливо якщо такий інцидент інформаційної безпеки може вважатися значним.

Подія інформаційної безпеки може бути швидко визначено, як помилкова тривога або приведено до задовільного висновку. У цих випадках

форму звітів необхідно заповнити та надіслати місцевому керівництву контактної позиції і СРІІБ з метою реєстрації її, тобто внесення в базу даних подій, інцидентів, вразливостей інформаційної безпеки. У цьому випадку особа, що повідомляє про закриття події інформаційної безпеки, може надати інформацію, необхідну для заповнення форми звіту про інциденти інформаційної безпеки – тоді така форма звіту про інцидент інформаційної безпеки повинна бути заповнена та надана в інстанцію. Використання автоматичних інструментальних засобів може виявитися корисним при заповненні деяких областей, наприклад, із зазначенням часу, а також при обміні, передачі необхідної інформації.

На етапі «Оцінки та прийняття рішень» описуються основні заходи, які організація повинна забезпечити, оцінка і прийняття рішень контрольною групою, а також оцінка і підтвердження інциденту СРІІБ.

Для досліджень про розслідування інцидентів ІБ в ІКС потрібно більш детально розглянути етап «Реагування». Основні заходи.

Це третій етап використання схеми управління інцидентами ІБ, що містить прийняття заходів у відповідь на інциденти інформаційної безпеки відповідно до узгоджених дій на етапі оцінки і прийняття рішень. Залежно від прийнятих рішень реагування може бути негайним, в режимі реального часу або близькому до реального часу, також реагування може включати експертний аналіз інформаційної безпеки. Для етапу реагування на інциденти інформаційної безпеки і прийняття рішень організація повинна забезпечити такі основні заходи:

1 Аналіз СРІІБ з метою визначення чи знаходиться інцидент ІБ під контролем, і діяльність, представлена нижче:

– діяльність, яка ініціює необхідну реакцію на інцидент інформаційної безпеки, якщо він знаходиться під контролем. Таким може бути негайне реагування, що включає активацію процедур по відновленню і або відправлення повідомлень відповідного персоналу, або більш пізній і повільне

реагування (наприклад, сприяння повного відновлення після лиха), що гарантує готовність всієї інформації для аналізу наслідків інциденту;

– діяльність, яка ініціює антикризові дії функції від ескалації до врегулювання кризових ситуацій, якщо вона не знаходиться під контролем або може мати серйозний вплив на основні сервіси організації. Потім функція обробки кризової ситуації відповідає за інцидент інформаційної безпеки, з повною підтримкою СРІБ (включаючи активацію плану антикризового управління ситуацією) і участь відповідного персоналу, наприклад, керівника і служби з антикризового управління організації;

2 Призначення внутрішніх джерел і ідентифікація зовнішніх джерел з метою реагування на інцидент;

3 Проведення експертного аналізу інформаційної безпеки при необхідності і клас згідно класифікаційної шкалою інцидентів інформаційної безпеки та зміна цієї шкали (при необхідності);

4 Активізація діяльності (при необхідності) для подальшого розгляду, перегляду та/або прийняття рішень;

5 Забезпечення належної реєстрації всієї залученої діяльності, зокрема СРІБ, для подальшого аналізу;

6 Забезпечення збору та безпечного зберігання даних в електронному вигляді та постійного контролю безпечного зберігання цих даних на випадок необхідності їх використання для судового переслідування або внутрішнього дисциплінарного розгляду;

7 Підтримка режиму зміни засобів управління, включаючи відстеження подій і вразливостей в області інформаційної безпеки і поновлення звітів по них з метою відповідності дійсності бази даних подій, інцидентів, вразливостей ІБ;

8 Обмін інформацією про існуючі інциденти інформаційної безпеки або будь–яких відповідних подробицях про них з іншими внутрішніми або зовнішніми особами, або організаціями, зокрема власниками активів, інформації, сервісів (визначених під час проведення аналізу негативного

впливу) і внутрішніми, зовнішніми організаціями, які повинні брати участь в управлінні та вирішенні інциденту.

Вся зібрана інформація про події, інциденти або вразливості інформаційної безпеки повинна зберігатися в базі даних подій, інцидентів, вразливостей інформаційної безпеки під керівництвом СРІБ. Вся інформація, що повідомляється в процесі кожного виду діяльності повинна бути максимально повною на даний момент для підтримки бази, доступної для оцінки та прийняття рішень і вибору правильних дій.

Після визначення інцидентів інформаційної безпеки та узгодження заходів у відповідь, слідує наступне:

– розподіл обов'язків по управлінню інцидентами інформаційної безпеки через відповідну ієрархію співробітників за допомогою оцінки, прийняття рішень і дій персоналу, як служби безпеки, так і інших співробітників;

– забезпечення обов'язкових формальних процедур для кожного вказаної в повідомленні особи, включно з переглядом і виправленням складеного звіту, оцінку завданих збитків та звітність відповідного персоналу;

– використання керівних принципів для складання повної документації про події інформаційної безпеки;

– використання керівних принципів для складання повної документації подальших дій;

– оновлення бази даних подій, інцидентів, вразливостей інформаційної безпеки.

Після успішного вирішення інциденту ІБ він повинен бути формально закритий, і це повинно бути зареєстровано в базі даних управління інцидентами ІБ. Організація повинна гарантувати застосування на цьому етапі у відповідь заходів відносно зареєстрованих вразливостей ІБ відповідно до узгоджених дій на етапі оцінки і прийняття рішень. Після усунення вразливості, необхідно зареєструвати даний факт в базі даних управління інцидентами інформаційної безпеки.

Етап «Зразкові дії з реагування». Цей етап є прикладом для досліджень та надає змогу зрозуміти якими повинні бути дії з реагування. Прикладом дій щодо негайного реагування у разі навмисної атаки на інформаційну систему, сервіс і, або мережу може бути те, що вони залишаються підключеними до мережі Інтернет або інших мереж. Це дозволить критично важливим бізнес–додаткам правильно функціонувати і зібрати якомога більше інформації про зловмисника, за умови, що зловмисник не знає, що він перебуває під наглядом. Необхідно дотримуватися запланованих процесів і реєструвати вжиті заходи. Остерігатися потрібно троянських програм, руткітів і модулів ядра, які можуть призвести до серйозного пошкодження системи. Свідоцтва повинні бути захищені за допомогою шифрування і спеціалізованих протоколів передачі даних:

– при прийнятті такого рішення слід враховувати, що зловмисник може зрозуміти, що за ним спостерігають, і вжити заходів, які можуть стати причиною подальшого пошкодження інформаційної системи, сервісу і чи мережі та відповідних даних, так зловмисник може видалити інформацію, яка може бути корисною для спостереження за ним;

– важливо, щоб при прийнятті відповідного рішення зберігалася технічна можливість швидко та надійно відключити і чи вимкнути атакувати інформаційну систему, сервіс і або мережу. Це послужить стримуючим фактором інциденту.

Запобігання повторного прояви інциденту зазвичай є більш пріоритетним завданням. У деяких випадках необхідно враховувати те, що порушник виявив уразливість, яка повинна бути усунуто, а вигоди від виявлення порушника не виправдовують витрачених на це зусиль. Це особливо справедливо, якщо порушник насправді не є зловмисником і не завдав великої, або взагалі не заподіяв ніякої, збитку.

Що стосується інших інцидентів інформаційної безпеки, крім навмисної атаки, то їх джерело повинно бути ідентифікованим. Може знадобитися відключення інформаційної системи, сервісу і чи мережі або ізоляція

відповідних їх частин на час впровадження захисних заходів. Для цього може знадобитися більше часу, якщо уразливість інформаційної системи, сервісу і чи мережі виявиться істотною, або якщо це буде критична уразливість.

Іншим дією з реагування може бути активізація методів спостереження (наприклад, використання пастки). Ця дія має здійснюватися на основі процедур, задокументованих в схемі управління інцидентами інформаційної безпеки.

Інформація, яка могла бути пошкоджена в результаті інциденту ІБ, повинна бути перевірена членом СРІБ на предмет зміни записів резервного копіювання, видалення або модифікації інформації. Може виникнути необхідність перевірки цілісності журналів реєстрації, оскільки зловмисник може підробити їх з метою приховування слідів проникнення.

Етап з «Оновлення інформації про інциденти» полягає в тому, що незалежно від подальших дій, співробітник СРІБ повинен оновити звіт про інцидент ІБ з максимальною деталізацією, додати його в базу даних подій, інцидентів, вразливостей інформаційної безпеки, сповістивши про це керівника СРІБ та інших осіб (при необхідності). Оновлюють наступну інформацію:

– про те, що являє собою інцидент інформаційної безпеки;

– про те, що стало причиною, чому або ким він був викликаний;

– на що впливає або міг впливати інцидент;

– про фактичне або потенційний вплив інциденту інформаційної безпеки на бізнес організації;

– про зміни у вказівці на ймовірну значимість або незначущість інциденту інформаційної безпеки (за шкалою, прийнятою в організації);

– про те, як він оброблявся до цього часу.

Якщо інцидент інформаційної безпеки усунутий, то звіт повинен містити подробиці зроблених захисних заходів і засвоєних уроків. Оновлений звіт слід додавати в базу даних подій, інцидентів, вразливостей інформаційної безпеки і повідомляти керівника СРІБ та інших осіб на їх вимогу.

Слід підкреслити, що СРІІБ відповідає за забезпечення безпечного зберігання інформації, що відноситься до даного інциденту інформаційної безпеки, з метою можливого проведення подальшої експертизи та можливого використання судом як доказ. Наприклад, для інциденту інформаційної безпеки, орієнтованого на інформаційні технології, повинні бути зроблені наступні дії.

Після першого виявлення інциденту ІБ всі тимчасові дані повинні бути зібрані до відключення ураженої системи інформаційних технологій, сервісу і чи мережі до проведення судового розслідування. Призначена для збору інформація містить відомості про будь–яких функціонують процесах і зберігає в пам'яті, кеші і регістрах, подробиці про будь–що робиться і планованої діяльності:

1 В залежності від характеру інциденту інформаційної безпеки провести повне дублювання ураженої системи або резервне копіювання журналів і важливих файлів;

2 Зібрати і проаналізувати журнали сусідніх систем, сервісів і чи мереж, наприклад, маршрутизаторів і міжмережевих екранів;

3 Всю зібрану інформацію зберігати на носіях тільки для читання; при виконанні дублювання на випадок судового розгляду забезпечити присутність не менше двох осіб для затвердження і підтвердження того, що всі дії були виконані згідно з діючими законодавством і нормативними документами;

4 Документувати і зберігати разом з вихідними носіями технічні характеристики і описи інструментальних засобів і сервісних команд, які використовувалися для дублювання аналізу інформаційної безпеки;

5 Представник СРІІБ також є відповідальним, якщо це можливо на даному етапі, за повернення в безпечне робочий стан уражених пристроїв (що мають або не мають відношення до інформаційних технологій) в інтересах виключення атак на ці пристрої.

Додаткові дії – це етап, на якому пропонуються дії якщо членом СРІБ визначено реальність інциденту інформаційної безпеки. Додатковими діями повинні бути:

– проведення експертного аналізу інформаційної безпеки;

– інформування осіб, відповідальних за передачу інформації всередині організації та за її межами, про факти та пропозиції щодо інформації, яку треба передати, в якій формі і кому.

Після можливо найбільш докладного заповнення звіту про інцидент інформаційної безпеки звіт вводиться в базу даних подій, інцидентів, вразливостей ІБ і передається керівнику СРІБ.

Якщо час розслідування перевищує час, раніше узгоджений,всередині організації, то складається проміжний звіт.

Член СРІБ, що оцінює інцидент інформаційної безпеки, на підставі керівництва, що міститься в документації схеми управління інцидентами інформаційної безпеки, повинен знати:

– коли і кому необхідно направляти матеріали;

– що при здійсненні будь–якої діяльності СРІБ необхідно слідувати документованим процедурам контролю за внесенням змін, [19].

При наявності проблем або підозрі про їхню наявність відносно встановлених за замовчуванням механізмів електронної звітності (наприклад, електронна пошта або локально обчислювальна мережа), включаючи випадки, коли система, можливо, піддається атаці, то в першу чергу, слід повідомити про інцидент інформаційної безпеки відповідальним особам особисто, по телефону або текстовим повідомленням.

При необхідності керівник СРІБ спільно з керівником забезпечення безпеки організації і відповідним керівником організації або членом ради директорів правління повинні зв'язатися з усіма відділами, які залучені в інцидент інформаційної безпеки як всередині організації, так і за її межами.

Для швидкої і ефективної організації зв'язку необхідно заздалегідь встановити надійний метод передачі інформації, що не залежить повністю від

системи, сервісу і чи мережі, на які може впливати інцидент ІБ. Такі запобіжні заходи можуть включати в себе призначення запасних консультантів або представників організації на випадок відсутності будь–кого з її основних керівників.

Етап «Експертний аналіз інформаційної безпеки» один з важливих, тому що для нормального забезпечення оцінки інциденту повинна бути зроблена експертна оцінка СРІІБ. Якщо в ході попередньої оцінки було визначено необхідність експертного аналізу з метою доказу значущості інциденту ІБ, то експертний аналіз проводить СРІІБ. З метою проведення більш детального експертного аналізу конкретного інциденту ІБ необхідно застосовувати слідчі методи і засоби, засновані на інформаційних технологіях і підтримувані документально оформленими методиками, які не використовувалися раніше в процесі управління інцидентами інформаційної безпеки. Таку експертизу проводять структурованим методом і визначають, що може використовуватися як доказ при внутрішніх дисциплінарних розглядах або в ході судових процесів. Для проведення експертного аналізу можуть використовуватися технічні (наприклад, засоби і методи аудиту, кошти відновлення даних) і програмні засоби, захищені службові приміщення, а також відповідний персонал.

Кожна дія експертного аналізу інформаційної безпеки має бути повністю документована, включаючи подання відповідних фотографій, складання звітів про аналіз результатів аудиту, перевірку журналів відновлення даних. Кваліфікація особи або осіб, що проводив експертний аналіз, повинна бути документально підтверджена так само, як і результати кваліфікаційного тестування. Необхідно також документувати будь–яку іншу інформацію, здатну продемонструвати об'єктивність і логічний характер експертного аналізу.

Всі записи про самі інциденти інформаційної безпеки, діяльності, пов'язаної з експертним аналізом цих інцидентів, і інше, а також відповідні носії інформації повинні зберігатися в фізично захищеному середовищі і

контролюватися відповідними процедурами для запобігання доступу до них неавторизованих осіб з метою модифікації записів. Засоби експертного аналізу, засновані на застосуванні інформаційних технологій, повинні точно відповідати стандартам з метою виключення можливості оскарження цієї відповідності в судовому порядку і, в той же час, в них повинні враховуватися всі поточні зміни в технологіях. У фізичному середовищі СРІІБ повинні створюватися необхідні умови, що гарантують незаперечність обробки даних. У будь–який час кількість персоналу для забезпечення реагування на інцидент ІБ має бути достатнім.

Згодом, безсумнівно, виникне необхідність розробки вимог до аналізу даних в контексті різноманіття інцидентів ІБ, серед яких шахрайство, крадіжка і акти вандалізму. Отже, для сприяння СРІІБ знадобиться більше коштів, заснованих на інформаційних технологіях, і допоміжних процедур для розкриття інформації, прихованої в інформаційній системі, сервісі та/або мережі, включаючи інформацію, яка, на перший погляд, здається стертою, зашифрованою або пошкодженої. Ці кошти повинні враховувати всі аспекти, пов'язані з відомими типами інцидентів інформаційної безпеки та повинні бути задокументовані в процедурах СРІІБ.

В сучасних умовах в експертний аналіз часто включають складні середовища з мережевою структурою, в яких розслідування поширюється на всю операційну середу, включаючи безліч серверів, а також засоби віддаленого доступу. Існує багато інструментальних засобів, включаючи засоби пошуку текстів, програмне забезпечення формування зображень і пакети програм для експертного аналізу. Головною метою процедур експертного аналізу є збереження недоторканності даних, їх перевірка на предмет протистояння будь–якому оскарженню в суді. Слід підкреслити, що експертний аналіз повинен проводитися на точній копії вихідних даних з тим, щоб уникнути сумнівів в цілісності вихідних носіїв в ході аналітичної роботи. Загальний процес правової експертизи повинен охоплювати наступні види діяльності:

1 Забезпечення захисту цільової системи, сервісу і/або мережі в процесі проведення правової експертизи від можливості їх блокування, зміни чи іншої компрометації, включаючи введення шкідливих кодів (в тому числі вірусів), і забезпечення захисту від впливів або мінімальних впливів на їх нормальну роботу;

2 Призначення пріоритетів збору, доказів, тобто розгляд їх від найбільш до найменш мінливих (що в значній мірі залежить від характеру інциденту інформаційної безпеки);

3 Ідентифікація всіх необхідних файлів в предметної системі, сервісі і/чи мережі, включаючи нормальні файли, захищені паролем або іншим чином, і зашифровані файли;

4 Відновлення якомога більшої кількості стертих файлів і інших даних, розкриття IP–адрес, імен хостів, мережевих маршрутів та інформації інтернет–сайтів;

5 Витягання вмісту прихованих, тимчасових файлів і файлів підкачки, використовуваних як програмне забезпечення операційної системи, так як і прикладне програмне забезпечення;

6 Доступ до вмісту програмного забезпечення захищених або зашифрованих файлів;

7 Аналіз всіх можливо значущих даних, знайдених в спеціальних (зазвичай недоступних) областях пам'яті на дисках;

8 Аналіз часу доступу до файлу, його створення і модифікації;

9 Аналіз журналів реєстрації системи, сервісу, мережі і додатків;

10 Визначення діяльності користувачів і/або додатків в системі, сервісі, мережі;

11 Аналіз електронної пошти на наявність вихідної інформації і її змісту;

12 Проведення перевірок цілісності файлів з метою виявлення файлів, що містять «троянські програми», і файлів, що спочатку були відсутні в системі;

13 По можливості, аналіз фізичних доказів шкоди майну, наприклад, відбитків пальців, результатів відеоспостереження, журналів реєстрації системи сигналізації, журналів реєстрації доступу за перепустками і опитування свідків;

14 Обробка та зберігання здобутих потенційних доказів, і захист їх від пошкодження, приведення в непридатність і перегляду конфіденційного матеріалу неавторизованими особами. Слід підкреслити, що збір доказів повинен проводитися завжди відповідно до правил судочинства або слухання справи, для яких дані докази можуть надаватися;

15 Отримання висновків про причини інциденту інформаційної безпеки, необхідні дії та часу їх виконання з приведенням доказів, включаючи список відповідних файлів, включених в додаток до головного звіту;

16 Забезпечення експертної підтримки для будь–якого дисциплінарного або правової дії (при необхідності).

Метод виконання вищевказаних дій повинен документуватися в виконуваних СРІБ процедурах. СРІБ повинна володіти різноманітними навичками в загальній області технічних знань (включаючи знання засобів і методів, які, можливо, будуть використовуватися зловмисником), досвідом проведення аналізу, розслідування (з урахуванням захисту використовуваних доказів), знанням положень відповідного законодавства і нормативно–правових актів і бути обізнаною про тенденції, пов'язаних з інцидентами ІБ.

Необхідно відзначити наступні положення:

– деякі організації можуть і не мати у своєму розпорядженні всі ці ресурси, в такому випадку їм може знадобитися проведення експертного аналізу інформаційної безпеки із залученням фахівців ззовні;

– збір матеріалу з експертизи інформаційної безпеки може стати єдиною підмогою (тобто виправдати зусилля і витрати), при виявленні серйозних втрат і/чи кримінальному судочинстві;

– непритягнення фахівців до вилучення матеріалів експертизи інформаційної безпеки може призвести до неприйнятного судовим рішенням при розгляді.

Етап «Комунікації». У багатьох випадках, при підтвердженні реальності інциденту інформаційної безпеки СРІБ, виникає необхідність інформування конкретних осіб як всередині організації (поза звичайних ліній комунікації між СРІБ і керівництвом), так і за її межами, включаючи пресу.

Етап «Реєстрація діяльності і зміна засобів управління», на якому важлива документація того, що було зроблено. Слід підкреслити, що всі причетні до оповіщення про виникнення і управління інцидентами інформаційної безпеки особи, повинні належним чином реєструвати всі свої дії для їх подальшого аналізу. Інформацію про ці дії вносять до форми звіту про інциденти інформаційної безпеки і в базу даних подій, інцидентів, вразливостей ІБ, безперервно оновлюють протягом усього циклу дії інциденту ІБ, від першої форми звіту до завершення аналізу інциденту ІБ.

Ця інформація повинна безпечно зберігатися, а також повинна бути забезпечена відповідним режимом резервного копіювання. Крім того, зміни, що вносяться в процесі відстеження інциденту ІБ, поновлення форм звіту і баз даних подій, інцидентів, вразливостей ІБ, повинні вноситися відповідно до формально прийнятої схеми контролю за внесенням змін.

Після всіх етапів йде завершальний – це «Етап засвоєних уроків». Важливий етап, тому що засвоєні уроки дають змогу удосконалити можливі заходи. Поділяється він на такі підпункти:

– огляд основних заходів;

– подальший експертний аналіз інформаційної безпеки;

– ідентифікація засвоєних уроків;

– визначення та удосконалення процесу впровадження засобів управління ІБ;

– визначення та удосконалення результатів перевірки процесу оцінки і управління ризиками ІБ;

– визначення та удосконалення схеми управління інцидентами ІБ;

– інші удосконалення, [4].

Міжнародний стандарт ISO/IEC 27035: 2011 «Information technology. Security techniques. Information security incident management» (Інформаційні технології. Методи і засоби забезпечення безпеки. Менеджмент інцидентів ІБ) наповнений рекомендаціями, які ефективні та охоплюють загальну частину управління інцидентами ІБ. Розслідування інцидентів ІБ в даному стандарті представлене як рекомендаційні дії після проходження інциденту або в час його дії. В стандарті сформована постанова управління інцидентами ІБ, а дії з розслідування інцидентів охоплюють загальні критерії. Без особливих знань, без додаткового залучення інших фахівців, керівництво навряд чи зможе зрозуміти процес розслідування інцидентів ІБ, навіть адміністратору або спеціалісту ІКС, ознайомленим з забезпеченням безпеки інформації, важко буде зрозуміти процес.

Міжнародний стандарт ISO/IEC 27037: 2012 «Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence» містить детальні посібники з ідентифікації, збору та отримання, зберігання, транспортування та зберігання інформації в електронній формі, зокрема з точки зору забезпечення їх цілісності. Стандарти охоплюють галузь знань, присвячених збору доказів для подальшого розслідування комп'ютерного злочину, у міжнародних публікаціях на цю тему використовується термін «техніко–криміналістична експертиза» (ТКЕ).

Найбільш критичними аспектами проведення ТКЕ є збір і збереження доказів, які повинні проводитися таким чином, щоб забезпечити їх цілісність. Як і при зборі звичайних фізичних доказів, для визначення перших і всіх проміжних ланок скоєння злочину вирішальне значення має турбота про послідовне збереження всіх доказів, поданих в електронній формі (англ. Digital evidence). Це гарантує, що вони збиралися і захищалися за допомогою строго структурованих процесів, визнаних судами. Не просто забезпечувати цілісність, такі процеси повинні ще гарантувати, що з доказами нічого

поганого не може статися і в майбутньому. Для цього потрібне дотримання або навіть перевищення базового рівня захисту доказів. Стандарт є дуже ємким, охоплює сферу розслідування інцидентів досить добре. Проблема полягає в тому, що в приведеному стандарті планові дії досить великі та важкі, охоплюють навіть технічні особливості розслідування. Без належних знань зрозуміти правила та етапи важко.

Наступним джерелом для аналізу буде стандарт американського національного інституту стандартизації (NIST – National Institute of Standards and Technology), NIST SP 800–61 «Computer Security Incident Handling Guide». Нормативний документ США NIST SP 800–61 являє собою збірник «кращих практик» з побудови процесів управління інцидентами ІБ і реагування на них. Детально розбираються питання реагування на різні типи інцидентів, такі як атаки «відмова в обслуговуванні» (DoS), поширення шкідливого програмного забезпечення (ПО), несанкціонований доступ (НСД), нерегламентоване використання і розподілені (багатокомпонентні) атаки. Зміст стандартів ISO/IEC 27037: 2012 та NIST SP 800–61 буде застосований для модернізації, скорегований на напрямок досліджень цієї кваліфікаційної роботи.

1.3 Висновки до розділу

В першому розділі представлені нормативні документи. Аналіз державних стандартів, законів, нормативних документів не виявив інструкцій чи рекомендацій з розслідування інцидентів ІБ для комерційних ІКС. Але закони та стандарти дають чіткі визначення з захисту інформації в системах, приводять правила з захисту та визначать відповідальність як за володіння інформацією, так і за порушення законів з захисту. Звернувшись до можливих міжнародних документів, було визначено багато корисної інформації, яку буде використано для проєктування рішень.

РОЗДІЛ 2. ВИНИКНЕННЯ ТА РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Виникнення інцидентів інформаційної безпеки

2.1.1 Основні причини інцидентів ІБ

Інциденти, пов'язані з порушенням інформаційної безпеки у організаціях, можуть привести до прямих фінансових втрат. Тому співробітники відділу ІБ організації повинні мати можливість виявляти і розслідувати будь–які спроби звершення незаконних дій. Приклади «типових» інцидентів ІБ.

Інциденти першої категорії. Протиправні дії співробітника, погано знайомого з основами функціонування ІТ–системи. Як правило, такий співробітник проявляє грамотність тільки в своїй вузькій предметній області (наприклад, в розрахункових операціях). Проте він добре розуміє, як можна модифікувати інформацію, до якої має доступ. Такі випадки, на жаль, відбуваються досить регулярно. З точки зору виявлення та розслідування інциденти першої категорії є для співробітників відділів інформаційної безпеки найбільш простими. Для їх запобігання або збору доказів існує безліч інструментів: вбудовані засоби безпеки, системи моніторингу та аудиту, не зайвими виявляються і системи відеоспостереження.

Інциденти другої категорії. Характеризуються тим, що зловмисники виявляються грамотними не тільки в предметній області організації, а й добре обізнаними про функціонування ІТ–систем. Це можуть бути співробітники ІТ–департаменту, що відповідають за експлуатацію тих чи інших корпоративних ІС (бухгалтерських систем і баз даних або автоматизованих систем). У таких випадках розслідувати здійснені інциденти стає набагато складніше. Протиправні дії можуть здійснюватися зловмисниками віддалено, з попередніми відключенням засобів моніторингу та аудиту. Іноді служба інформаційної безпеки може і зовсім не знайти зловмисника або, знайшовши його, не довести факт вчинення ним кіберзлочину. Найчастіше, щоб отримати необхідні докази, потрібне залучення зовнішніх висококласних експертів, а

також використання спеціальних дорогих засобів для зняття і аналізу інформації з жорстких дисків серверів і робочих станцій.

Інциденти третьої категорії. Як правило найважчі, про них дуже складно отримати повну і достовірну інформацію. У цьому випадку доводиться мати справу з висококласними кіберзлочинцями (хакерами). Ідентифікація мережевих ресурсів є важливим підготовчим етапом перед здійсненням злому. Якщо хакер знає, що система працює під управлінням наприклад Windows Server 2019, то йому необхідно знайти уразливості, до яких схильні дані програмні продукти. Для цього найпростіше пошукати в базах вразливостей. У разі якщо знайти нічого не вдалося, то особливо розумний хакер може спробувати самостійно знайти вразливість, зібравши у себе точну копію зламуваної системи і спробувавши самостійно проаналізувати код. Для цього є спеціальні інструменти. Провівши аналіз вразливостей «офлайн», потім хакер зможе швидко провести атаку і впровадити в систему, що атакується, шкідливий код. Як приклад можна привести зараження внутрішньої системи банку спеціальним зловмисним програмним забезпеченням, яке імітувало дії легальних користувачів по перерахуванню коштів на зовнішні рахунки. Збитки від атак такого рівня, як правило, обчислюються десятками мільйонів.

У розглянутих інцидентах зловмисники мали б мало шансів на успіх, якщо б інші співробітники організації не допускали порушення правил і заходів інформаційної безпеки. Частою причиною порушення ІБ є людська помилка. Людська помилка є найбільшою причиною всіх інцидентів порушення безпеки. В дослідженні журналу з кібербезпеки «Cyberthreat Defense Report» визначено, що людська помилка була відповідальна за цілих 95% всіх порушень безпеки. Але не всі людські помилки є навмисними. Близько 60% всіх людських помилок, які привели до інцидентів, були фактично ненавмисними.

Історично склалося, що підхід до безпеки підприємства полягає в тому, щоб зробити захист міцніше, більше і сильніше – встановити більше

програмного забезпечення, і написати величезну політику безпеки. Навіть при зростанні рівня безпеки, уникнути інцидентів не можливо. Проблема полягає в тому, що атаки не завжди приходять звідти, звідки чекаєш. Справа в тому, що найбільша загроза для організації лежить в межах її кордонів. Типовими порушеннями ІБ є:

Перше типове порушення ІБ. Складається в слабкому захисті паролів для доступу до інформаційних систем. Це найпростіша і поширена ситуація. Горезвісні листівки, приклеєні на монітор, або ті, які лежать під клавіатурою, є типовим порушенням політики ІБ в будь–якій організації. Якщо зловмисник вирішить скористатися чужим обліковим записом для несанкціонованого доступу до інформаційної системи, то він без зусиль зможе це зробити.

Друге типове порушення. Безпосередня передача співробітниками логінів і паролів своїм колегам. Дуже часто здійснюється така процедура між працівниками, а саме уточнення клієнтським менеджером у свого колеги, який запінюється, його пароля по мобільному телефону. Логіни і паролі колеги можуть бути використані для крадіжки грошей. Таким чином, якщо говорити про забезпечення безпеки всередині організації, а також створення умов для успішного розслідування інцидентів ІБ, то виникає кілька завдань, без вирішення яких неможливо домогтися необхідного результату.

Завдання:

1 Забезпечення суворої автентифікації співробітників при доступі до інформаційної системи організації. Як мінімум, на робочих місцях, де здійснюються критично важливі фінансові операції, повинна бути впроваджена система суворої автентифікації;

2 Побудова системи розмежування доступу – впровадження так званого «принципу двох рук» для найважливіших бізнес–процесів організації;

3 Побудова системи моніторингу та аудиту дій користувачів на декількох рівнях: рівні операційної системи робочої станції, рівні входу в корпоративні інформаційні системи, а також на рівні спеціалізованих засобів захисту;

4 Передбачити порядок дій і регламент розслідування в разі виникнення інцидентів ІБ. Для проведення розслідувань у складі департаменту інформаційної безпеки необхідний експерт відповідного рівня. Якщо служба безпеки не має в своєму складі таких співробітників, то в складних випадках краще звертатися до зовнішніх експертів – залучати спеціалізовані компанії, які професійно займаються розслідуваннями інцидентів.

Припущення про те, що в організації стався інцидент інформаційної безпеки, має базуватися на трьох основних факторах:

– повідомлення про інцидент інформаційної безпеки надходять одночасно з декількох джерел (користувачі, IDS, журнальні файли);

– IDS сигналізують про повторення подій;

– аналіз журнальних файлів АС дає підставу для висновку системним адміністраторам про можливість настання події інциденту.

У загальному випадку, ознаки інциденту діляться на дві основні категорії, повідомлення про те, що інцидент відбувається зараз, і повідомлення про те, що інцидент, можливо, відбудеться в недалекому майбутньому. Нижче перераховані деякі ознаки виниклих події:

– IDS фіксує переповнення буфера;

– повідомлення антивірусної програми;

– крах WEB інтерфейсу;

– користувачі повідомляють про вкрай низьку швидкість при спробі виходу до Інтернету;

– системний адміністратор фіксує наявність файлів з назвами, які не можливо прочитати;

– користувачі повідомляють про наявність у своїх поштових скриньках безлічі повторюваних повідомлень;

– ПЗ фіксує в журнальному файлі множинні невдалі спроби авторизації;

– адміністратор мережі фіксує різке збільшення мережевого трафіку.

Статистику частоти походження інцидентів ІБ та модель загроз порушника представлено в наступних підрозділах.

2.1.2 Статистика виникнення інцидентів ІБ

Для аналізу застосовано статистику, яку представив американський статистичний журнал з кібербезпеки «Cyberthreat Defense Report». Статистика повідомляє, що навіть у професіоналів з інформаційної безпеки, їхні інформаційні системи піддаються атакам.

– в 2020 році 71% комерційних організацій були піддані кібератакам, але у 2021 році 52% організацій очікують, що стануть жертвою знову;

– інциденти інформаційної безпеки збільшилися на 66%;

– Європа зазначила на 41% більше виявлених випадків інцидентів, по порівнянні з 2020 роком;

– автомобільні фірми повідомляють про збільшення виявлених випадків інцидентів ІБ на 32%;

– технологічні компанії повідомили що на 17% менше інцидентів в 2020 році;

– на 21% більше професіоналів повідомляють про те, що піддавались DDos атакам;

– навіть 66% професіоналів вважають, що знову будуть піддані кібер–атаці.

Згідно зі статистикою, на першому місці інциденти трапляються в банках, на другому місці телекомунікаційні компанії, а потім державіні підприємства.

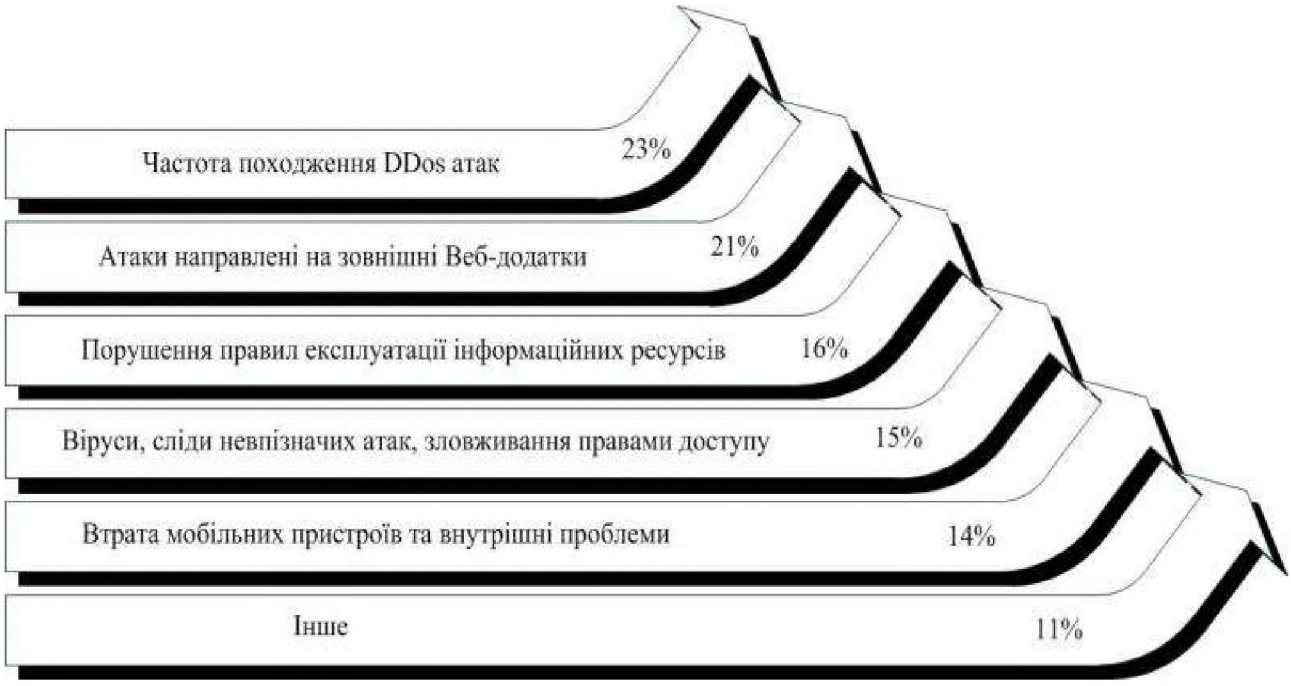

Рисунок 2.1 – Найчастіші інциденти ІБ

Статистика, згідно якої найчастіші порушники – це кіберзлочинці і системні адміністратори, які зловживають своїм положенням, наведено нижче рисунок 2.2. Статистика виводить такі проценти походження:

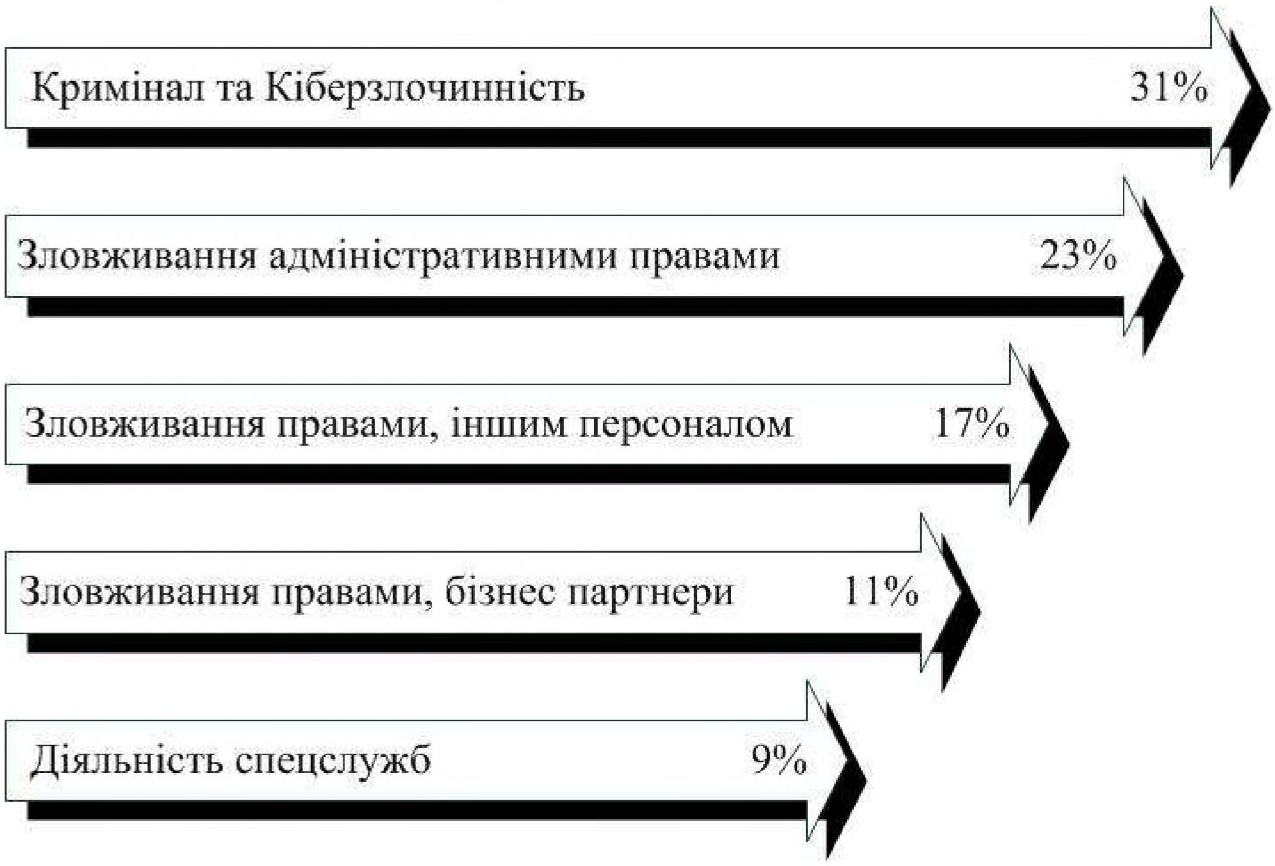

Рисунок 2.2 – Джерела основних інцидентів

Згідно з цими відсотками, виходить, що навіть довірені люди можуть помилятися або навмисне порушувати інформаційну безпеку. Також є статистика вирішення інцидентів згідно якої, інциденти можна в 60% вирішити за декілька днів. На другому місці йдуть вже тижні в 20% випадків, а на третьому в 15% випадків йдуть вже місяці. Але це ще не все, в 5% випадків інциденти не мають дати вирішення. Це той випадок, коли зовсім не знають як вирішувати інцидент або було виявлено дуже масштабні проблеми.

Опитування про реальні інциденти у великих компаніях підтвердили основні тенденції, які спостерігаються за результатами тестів на проникнення і інших технічних досліджень, потенційних загроз в корпоративних інформаційних системах.

Основні тенденції:

– великі компанії все частіше зазнають фінансових і репутаційних втрат через інциденти ІБ;

– активне використання інтернету збільшує число інцидентів, пов'язаних з уразливістю веб–додатків;

– внутрішні загрози, такі як порушення правил безпеки і зловмисні дії співробітників, частіше виявляються та більш небезпечні, ніж віруси і зовнішні атаки;

– виконання державних або галузевих стандартів інформаційної безпеки не вважається в компаніях важливим до тих пір, поки не перетворюється в закон або наказ.

З іншого боку, результати опитування частково розходяться з результатами інших досліджень. Особливо це стосується швидкості усунення критичних вразливостей. Ймовірно, різниця пов'язана з недостатнім розумінням терміна «критична уразливість». Відповідаючи на це питання, керівники компаній, швидше за все, мали на увазі критичні інциденти, тобто ті випадки, коли деструктивні події вже відбулися. У цих випадках компанія дійсно буде «латати дірки» в найближчі дні. Однак критична уразливість це ще не інцидент. Уразливість може ніким не експлуатуватися тривалий час,

тому багато компаній не поспішають усувати навіть відомі уразливості, місяцями і роками. Крім того, опитування підтвердило таку важливу проблему, як брак експертів з безпеки. Можливо, в цьому одна з причин недостатнього розуміння самої ідеї, управління вразливостями.

На закінчення варто відзначити, що дане дослідження проводилося в великих корпораціях, які приділяють підвищену увагу питанням безпеки. Очевидно, що в компаніях менших, всі перераховані проблеми можуть проявлятися ще гостріше.

2.1.3 Критерії створення моделі порушника та моделі загроз

Для забезпечення визначень ким може бути порушник інформаційної безпеки та якими можуть бути загрози згідно НД ТЗІ 1.4–001–2000 «Типове положення про службу захисту інформації в автоматизованій системі» нижче сформульовано типові положення.

Модель порушника – абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії. По відношенню до АС порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь–які особи, що знаходяться за межами контрольованої зони).

Метою порушника можуть бути:

– отримання необхідної інформації у потрібному обсязі та асортименті;

– мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);

– нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Класифікація порушників за рівнем можливостей

Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

– перший рівень визначає найнижчий рівень можливостей ведення діалогу з АС; це можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

– другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

– третій рівень визначається можливістю управління функціонуванням АС, тобто впливом на базове програмне забезпечення системи і на склад та конфігурацію її устаткування;

– четвертий рівень визначається повним обсягом можливостей осіб, що здійснюють проєктування, реалізацію, впровадження, супроводження програмно–апаратного забезпечення АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

За рівнем знань про АС усіх порушників класифікують як таких, що:

– володіють інформацією про функціональні особливості АС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;

– володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

– володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проєктування та експлуатації АС;

– володіють інформацією про функції та механізм дії засобів захисту.

За використовуваними методами і способами порушників можна класифікувати як таких, що:

– використовують виключно агентурні методи одержання відомостей;

– використовують пасивні технічні засоби перехоплення інформаційних сигналів;

– використовують виключно штатні засоби АС або недоліки проєктування КСЗІ для реалізації спроб НСД;

– використовують способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

За місцем здійснення дії можуть класифікуватись:

– без одержання доступу на контрольовану територію організації (АС);

– з одержанням доступу на контрольовану територію, але без доступу до технічних засобів АС;

– з одержанням доступу до робочих місць кінцевих (у тому числі віддалених) користувачів АС;

– з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів, АРМ відповідних адміністраторів тощо);

– з одержанням доступу до засобів адміністрування АС і засобів керування КСЗІ.

Важливість визначення як загроз, так і порушника грає важливу роль в розслідування інцидентів ІБ. Знаючи чого можна чекати та від кого, в розслідуванні можна скорегувати напрямок пошуків та виявлення доказів.

Способи здійснення загроз в АС:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо та радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів.

Загрози для інформації, що обробляється в АС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та

інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні.

Основні види загроз, які можуть бути реалізовані стосовно АС:

– зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

– збої і відмови у роботі обладнання та технічних засобів АС;

– наслідки помилок під час проєктування та розробки компонентів АС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

– помилки персоналу (користувачів) АС під час експлуатації;

– навмисні дії (спроби) потенційних порушників.

Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

– дії, що призводять до відмови АС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм та ін.);

– ненавмисне пошкодження носіїв інформації;

– неумисне зараження ПЗ комп'ютерними вірусами;

– невиконання вимог до організаційних заходів захисту чинних в АС розпорядчих документів;

– помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

– будь–які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

– неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та інше.);

– наслідки некомпетентного застосування засобів захисту.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи АС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

– порушення фізичної цілісності АС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

– порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, заземлення, охоронної сигналізації, вентиляції та інше);

– порушення режимів функціонування АС (обладнання і ПЗ);

– впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

– використання засобів перехоплення побічних електромагнітних випромінювань і наводів, акустоелектричних перетворень інформаційних сигналів;

– використання (шантаж, підкуп тощо) з корисливою метою персоналу АС;

– крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);

– несанкціоноване копіювання носіїв інформації;

– читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;

– неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;

– впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж).

2.2 Розслідування інцидентів інформаційної безпеки

2.2.1 Проєктні рішення з розслідування інцидентів інформаційної безпеки в ІКС

Розслідування інцидентів ІБ – складний і комплексний процес, що вимагає участі співробітників багатьох підрозділів компанії: співробітників відділу кадрів, юристів, технічних експертів ІТ–системи, зовнішніх консультантів з ІБ, бізнес–менеджерів, кінцевих користувачів інформаційної системи, співробітників служб технічної підтримки, співробітників служби безпеки та інших.

Фаза розслідування покликана визначити: хто, що, коли, де, як і чому були залучені в інцидент. Розслідування включає перевірку і збір доказів з серверів, мережевих пристроїв, а також традиційні заходи нетехнічного характеру. Воно може бути розділене на два етапи: збір даних і їх криміналістичний аналіз. Інформація, зібрана в ході виконання першого етапу розслідування, служить надалі для вироблення стратегії реагування на інцидент. На етапі аналізу, власне, і визначається, хто, що, як, коли, де і чому були залучені в інцидент.

Аналіз зібраних даних включає аналіз файлів протоколів роботи, конфігураційних файлів, історії Інтернет–провідників (включаючи cookies), повідомлень електронної пошти та прикріплених файлів, інстальованих додатків, графічних файлів і іншого. Необхідно провести аналіз ПЗ, пошук за ключовими словами, перевірити дату і час інциденту. Криміналістичний аналіз може також включати аналіз на "низькому" рівні – пошук видалених файлів і областей, втрачених кластерів, вільного місця, а також аналіз відновлених даних з зруйнованих носіїв (наприклад, по залишкової намагніченості).

При розслідуванні інциденту збір даних може бути виконаний за допомогою програмного забезпечення "Disk Duplicate". Воно дозволяє зробити точні копії жорстких дисків ("сектор в сектор") автоматизованих робочих місць користувачів (співробітників компанії) і серверів. Для аналізу

отриманих даних можуть використовуватися спеціальні засоби емуляції робочих машин користувачів, наприклад, "VMware Virtual Machine". Аналіз просторів жорстких дисків може проводитися з використанням спеціалізованого програмного продукту "Encase Enterprise Edition" або експертних засобів компанії Vogon International. Ці два продукти – провідні в світі при проведенні розслідування інцидентів ІБ. У ряді випадків для виявлення слідів комп'ютерних інцидентів можуть бути використані різноманітні програмно–апаратні комплекси для "прослуховування" локальної мережі компанії (часто використовується продукт Ettercap – мережевий сниффер), різноманітні програми–пастки (HoneyPot).

Спланована послідовність дій з використанням наведеного ПЗ є досить важкою без додаткових знань. Тому у приватних організаціях, а конкретніше керівництву чи власникам цих організацій, зовсім нема бажання зв’язуватись з міжнародними стандартами для повноцінного будування процесу управління інцидентами ІБ. Керівництво, власники часто вважають це або зайвим, додатковими витратами, або занадто складним для їх маленького підприємства. Це потрібно всім. Так як організаціям здається процес управління складним, потрібно модернізувати його. Якщо організації не хочуть проваджувати рекомендації з управління інцидентами ІБ, то хоча б розслідували ці інциденти правильно. Нижче сформовано наслідки неправильних розслідувань інцидентів в ІКС:

– втрата можливості відновити документи що було втрачено;

– нанесення додаткових збитків через не обізнаність або невизначеність в діях;

– випадкова втрата, знищення доказів злочину, через не знання плану дій;

– зупинка бізнес процесів та важливих систем;

– простої системи через довге розслідування;

– неможливість визначити винних у злочинах;

– несвоєчасне інформування правоохоронних органів про злочин.

Проєктним вирішенням цих проблем є створення документу, що має регламентувати або приводити покрокові дії з розслідування інцидентів інформаційної безпеки в інформаційно–комунікаційних системах.

Цей документ повинен бути:

– простим, що забезпечить розуміння для людей незнайомих з розслідуванням інцидентів ІБ;

– гнучким для використання різними комерційними організаціями, з різною специфікою дій;

– не порушувати законодавства чи нормативних документів;

– відповідати міжнародним стандартам та постійно, своєчасно оновлюватись разом із ними.

При створенні документу потрібно забезпечити чітку структуру, що дасть змогу в випадку помилок при розслідуванні інцидентів ІБ повернутися до минулих кроків. На основі ISO/IEC 27037: 2012 «Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence», нормативного документу США NIST SP 800–61 «Computer Security Incident Handling Guide» та ISO/IEC 27035: 2011 «Information technology. Security techniques. Information security incident management» модернізуємо рекомендації. Створення документу, на основі цих стандартів буде доступним для розуміння, як керівництва, так і людей, які залучаються до розслідування інцидентів та не буде перечити цим стандартам та законодавству. Керівництво забезпечить себе корисною інформацією та методами, що дасть змогу розуміти як правила розслідування, так і правила зберігання доказів. Також з’являється можливість зрозуміти чи правильно виконується розслідування, якщо залучаються зовнішні спеціалісти.

2.2.2 Інструкція з розслідування інцидентів інформаційної безпеки в інформаційно–комунікаційних системах

Ця інструкція призначена для розслідування інцидентів інформаційної безпеки в інформаційно–комунікаційних системах комерційних підприємств. Використовується тільки для комерційних організацій. Потрібно зауважити, що в цій інструкції термін «спеціаліст оперативного реагування» (СОР) вживається в загальному розумінні. Тобто спеціалістом СОР можуть бути особи, яким надані керівництвом організації права на розслідування інцидентів ІБ. Це можуть бути як працівники компанії, так і зовнішні особи, яких було залучено. Порядок дій та рекомендації наведені нижче.

1 Загальні відомості

Використання свідчень, представлених в цифровій формі, може вимагатися в цілому ряді різних сценаріїв, кожен з яких характеризується співвідношенням між досягненням якості доказів, своєчасністю аналізу, відновленням послуг і витратами на збір свідчень, представлених в цифровій формі. Тому організаціям необхідний процес встановлення пріоритетів, що ідентифікує потреби і співвідношення якості доказів, своєчасність аналізу і відновлення послуг, перш ніж перед спеціалістом оперативного реагування (надалі – СОР) буде поставлена відповідна задача. Процес встановлення пріоритетів включає оцінювання доступного матеріалу для визначення можливої доказової цінності і порядку, відповідно до якого повинен здійснюватися збір, отримання, збереження потенційних свідчень, представлених в цифровій формі. Для забезпечення правильного плану розслідування інцидентів ІБ повинні виконуватися такі критерії:

– критерії контрольованості. Незалежний фахівець з оцінки або інші уповноважені зацікавлені сторони повинні мати можливість оцінювання дій, виконуваних СОР і спеціалістом з свідоцтв (надалі – СЗС);

– критерії повторюваності. Факт повторюваності визнається, якщо ті ж результати тесту отримують при умовах використання такої ж процедури і методу вимірів, використання таких же інструментальних засобів і при таких

же умовах, а також можливе повторення в будь–який час після первинного тестування;

– критерії відтворюваності. Факт відтворюваності визнається, якщо ті ж результати тесту отримують при умовах використання такого ж методу вимірювання, використання різних інструментальних засобів і при різних умовах, а також можливе повторення в будь–який час після первинного тестування;

– критерії обґрунтованості. СОР повинен бути здатний обґрунтувати всі дії і методи, використані для звернення зі свідченнями, представленими в цифровій формі.

1.1 Процеси обробки свідчень, представлених в цифровій формі

Хоча повний процес обробки свідчень, представлених в цифровій формі, включає і інші дії (наприклад, передача, знищення і так далі). За своїм характером свідоцтва, представлені в цифровій формі, можуть бути вразливими. Вони можуть бути змінені, фальсифіковані або зруйновані в результаті неналежного поводження або вивчення. Обробники свідоцтв, представлених в цифровій формі, повинні бути компетентними в питанні ідентифікації та менеджменту ризиків, а також наслідків можливих варіантів дій при зверненні зі свідченнями, представленими в цифровій формі.

1.1.1 Ідентифікація

Свідоцтва, представлені в цифровій формі, можуть бути в фізичному або логічному вигляді. Фізичний вигляд означає представлення даних в матеріальному пристрої. Логічний вид потенційних свідчень, представлених в цифровій формі, відноситься до віртуального представлення даних в пристрої.

Процес ідентифікації включає пошук, розпізнавання і документування потенційних свідчень, представлених в цифровій формі. У процесі ідентифікації повинні визначатися цифрові носії інформації і пристрої обробки, які можуть містити потенційні свідоцтва, представлені в цифровій формі, що мають відношення до інциденту. Даний процес включає також дію щодо встановлення пріоритетів для збору свідчень, на основі їх мінливості.

Для забезпечення впевненості в належному порядку процесів збору та отримання свідоцтв слід ідентифікувати мінливість даних, щоб звести до мінімуму шкоду для потенційних свідчень, представлених в цифровій формі, і отримати найкращі свідоцтва. Крім того, під час цього процесу слід ідентифікувати приховані потенційні свідоцтва, представлені в цифровій формі. СОР і СЗС повинні усвідомлювати, що не всі види цифрових носіїв інформації можуть бути легко ідентифіковані і локалізовані. СОР і СЗС повинні систематично проводити ретельний пошук елементів, які можуть містити потенційні свідоцтва, представлені в цифровій формі. Різні види цифрових пристроїв, які можуть містити потенційні свідоцтва, представлені в цифровій формі, легко можуть бути не помічені (наприклад, через малий розмір), приховані або перемішані з іншим, що не відносяться до справи матеріалом.

1.1.2 Збір

Після ідентифікації цифрових пристроїв, які можуть містити потенційні свідоцтва, представлені в цифровій формі, СОР і СЗС повинні вирішити, чи буде здійснюватися збір або отримання свідчень протягом наступного процесу. Існує ряд чинників, що впливають на таке рішення. Рішення повинно бути засноване на обставинах.

Збір є одним з процесів обробки свідчень, представлених в цифровій формі, якщо пристрої, які можуть містити потенційні свідоцтва, представлені в цифровій формі, переміщаються з їх робочого середовища в лабораторію або іншу контрольоване середовище для подальшого отримання і аналізу свідоцтв. Пристрої, що містять потенційні свідоцтва, представлені в цифровій формі, можуть бути в одному з двох станів: коли живлення системи включено або коли живлення системи вимкнено. Залежно від стану пристрою потрібні різні методи та інструментальні засоби. До методів і інструментальних засобів, що використовуються для збору даних, можуть застосовуватися спеціальні процедури.

Цей процес включає документування всіх дій, а також упаковку пристроїв перед їх транспортуванням. Для СОР і СЗС важливо зібрати будь-який матеріал, який може мати відношення до потенційної цифрової інформації (наприклад, листи паперу з записаними паролями, підставки і силові роз'єми для вбудованих пристроїв). При відсутності розумної обережності потенційні свідоцтва, представлені в цифровій формі, можуть бути втрачені або пошкоджені. СОР і СЗС повинні вибрати найкращий можливий метод збору на основі ситуації, витрат і часу, і документально оформити рішення про використання конкретного методу.

1.1.3 Отримання свідчень

Процес отримання свідчень включає створення цифрової копії свідоцтв, представлених в цифровій формі (наприклад, повного жорсткого диска, розділу диска, вибраних файлів), і документування використаних методів і виконуваних дій. СОР повинен вибрати належний метод отримання свідоцтв, виходячи з ситуації, витрат і часу, і документально оформити рішення про використання конкретного методу або інструментального кошти, відповідно.

Методи, які використовуються для отримання потенційних свідчень, представлених в цифровій формі, повинні бути чітко і детально задокументовані, і, наскільки це практично можливо, відтворюватися або піддаватися перевірці компетентним СОР. СОР або СЗС повинні отримувати потенційні свідоцтва, представлені в цифровій формі, невідкладним способом, щоб уникнути, де це можливо, внесення змін. Якщо в результаті процесу неминучі зміни в цифрових даних, виконувана діяльність повинна бути задокументована для обліку змін в даних.

В процесі отримання свідчень слід створювати копію потенційного свідоцтва, представленого в цифровій формі, або цифрових пристроїв, які можуть містити потенційні свідоцтва, представлені в цифровій формі. Якщо створення образу, копії свідоцтва не може бути перевірено, то це повинно бути задокументовано і обґрунтовано. Можуть бути випадки, коли неможливо або неприпустимо створення копії свідоцтва, представленого в цифровій

формі, наприклад, коли джерело занадто великий. У таких випадках СОР повинен здійснити логічне отримання свідоцтва, яке орієнтоване тільки на певні типи даних, директорії або адреси. Це зазвичай відбувається на рівні файлів і розділів диска.

1.1.4 Збереження

Потенційні свідоцтва, представлені в цифровій формі, повинні зберігатися для забезпечення впевненості в їх корисності при розслідуванні Важливо забезпечити захист цілісності свідоцтв. Процес збереження включає захист потенційних свідчень, представлених в цифровій формі, і цифрових пристроїв, які можуть містити потенційні свідоцтва, представлені в цифровій формі, від фальсифікації або пошкодження. Процес збереження повинен ініціюватися і підтримуватися протягом усіх етапів звернення зі свідченнями, представленими в цифровій формі, починаючи з ідентифікації цифрових пристроїв, які можуть містити потенційні свідоцтва, представлені в цифровій формі.

При найкращому сценарії розвитку не повинно бути ніякого ушкодження самих даних або будь–яких пов'язаних з ними метаданих (наприклад, мітки дати і часу). СОР повинен бути здатний продемонструвати, що свідчення не модифікувалися після їх збору або отримання, або, якщо було внесено неминучі зміни, надати логічне обґрунтування і документально підтвердити ці дії.

2 Ключові компоненти ідентифікації, збір, одержання і збереження свідчень, представлених в цифровій формі

2.1 Історія зберігання

При будь–якому розслідуванні СОР повинен нести відповідальність за всі отримані дані і пристрої на час перебування їх в його розпорядженні. Запис історії зберігання – це документ, що засвідчує хронологію переміщення і обробки потенційних свідчень, представлених в цифровій формі. Вона повинна бути почата від процесу збору або отримання свідчень. Зазвичай це досягається шляхом реєстрації історії елемента від моменту його

ідентифікації, збору або отримання групою розслідування до його поточного стану і місцезнаходження.

Запис історії зберігання – це документ або кілька взаємопов'язаних документів, що детально описують історію зберігання і фіксують осіб, що відповідають за поводження з потенційними свідченнями, представленими в цифровій формі, або у вигляді цифрових даних, або в інших форматах (наприклад, замітки на папері). Мета підтримки запису історії зберігання складається в створенні можливості ідентифікації переміщення потенційних свідчень, представлених в цифровій формі, і доступу до них в будь–який даний момент часу. Сам запис історії зберігання може містити більше одного документа, наприклад, для потенційних свідчень, представлених в цифровій формі, повинен бути актуальний документ, що фіксує отримання цифрових даних з конкретного пристрою і переміщення цього пристрою, і документація, яка фіксує подальше вилучення або копіювання потенційних свідчень, представлених в цифровій формі.

2.2 Запобіжні заходи на місці інциденту

Як тільки СОР з'являється на місці інциденту, він повинен виконати дії щодо забезпечення безпеки та захисту місцезнаходження потенційних свідчень, представлених в цифровій формі.

Заходи для забезпечення безпеки свідоцтв:

– убезпечити і взяти під контроль майданчик, що містить пристрої;

– визначити, хто несе відповідальність за майданчик;

– забезпечити впевненість у тому, що люди віддалені від пристроїв і джерел живлення;

– документально відзначити всіх, хто має доступ на майданчик, або всіх, у кого може бути причина виявитися пов'язаним з місцем інциденту;

– якщо пристрій включено, не вимикати його, а після вимкнення пристрою, не включати його;

– якщо це можливо, документально зафіксувати місце події (наприклад, ескіз, фотографія чи відео) з усіма компонентами і кабелями в початковому положенні;

– якщо це дозволено, провести на майданчику пошук таких предметів, як самоклеючі записки, щоденники, документи, ноутбуки або керівництва по апаратним і програмних засобів з найважливішими подробицями про пристрої, такими як паролі та PIN–коди.

В першу чергу СОР повинен уявити собі всі ризики, пов'язані із здійсненням всіх процесів з розслідування. На місці інциденту необхідно розглянути питання захисту персоналу і потенційних свідчень, представлених в цифровій формі.

2.2.1 Персонал

До початку процесу важливо провести оцінку ризику щодо безпеки персоналу, оскільки безпека персоналу, який бере участь в процесі, є життєво важливою. Питання, які повинні бути розглянуті в процесі оцінки ризиків для персоналу, включають наступне:

– чи існує підозрювана особа? Якщо так, чи є у нього (їх) схильність до протиправних дій?

– протягом якого часу буде проводитися робота?

– чи може місце інциденту бути ізольовано від сторонніх?

– чи може місце інциденту вважатися ненадійним?

2.2.2 Потенційні свідоцтва, представлені в цифровій формі

СОР повинен бути обережний при використанні конкретного інструментального забезпечення для збору або отримання потенційних свідчень, представлених в цифровій формі. Неприйняття до уваги ризиків перед збором може призводити до втрати деяких або всіх потенційних свідчень, представлених в цифровій формі, за рахунок технології, застосовуваної для збору або отримання свідчень. Повинна бути проведена оцінка ризиків для зниження можливості появи позовів про відшкодування шкоди.

Оцінка ризику включає систематичне оцінювання ризиків і потенційного впливу, який вони можуть надавати на вивчення свідчень, представлених в цифровій формі. Аспекти, які підлягають розгляду при оцінці ризику для свідчень, представлених в цифровій формі, включають наступне:

– який вид методів збору, отримання свідоцтв повинен застосовуватися?

– яке обладнання може знадобитися на місці?

– який рівень мінливості даних та інформації, пов'язаних з потенційними свідченнями, представленими в цифровій формі?

– чи можливий віддалений доступ до будь–якого цифрового пристрою і чи представляє це загрозу для цілісності доказів?

– що станеться в разі пошкодження даних, обладнання?

– чи могла статися компрометація даних?

– чи міг цифровий пристрій бути налаштований так, щоб викликати руйнування (наприклад, використовуючи логічну бомбу), зіпсувати або заплутати дані в разі виключення або неконтрольованого доступу?

2.3 Ролі та обов'язки

Роль СОР включає ідентифікацію, збір, отримання та збереження потенційних свідчень, представлених в цифровій формі, на місці інциденту. Вона охоплює створення звіту по збору та отриманню свідоцтв, але не обов'язково створення звіту з аналізу. У роль СОР також входить забезпечення впевненості в цілісності та автентичності потенційних свідчень, представлених в цифровій формі. СОР може також знадобитися допомога персоналу, який здійснює технічну підтримку у відповідних сферах. Роль СЗС полягає в забезпеченні технічної підтримки СОР при ідентифікації, зборі, отриманні і збереженні потенційних свідчень, представлених в цифровій формі, на місці інциденту. СЗС забезпечує експертний аналіз для СОР.

2.4 Застосування розумної обережності

Слід уникати будь–яких дій, які можуть призводити до пошкодження потенційних свідчень, представлених в цифровій формі, що зберігаються в цифрових пристроях в результаті навмисних або ненавмисних дій. Наприклад,

магнітні поля можуть призводити до пошкодження потенційних свідчень, представлених в цифровій формі, які містяться на магнітних носіях. СОР не повинні мати доступ до цифрових пристроїв, якщо вони не володіють необхідною компетентністю і не використовують достовірні і валідні процеси.

Причини, при яких СОР не може зібрати докази:

– якщо немає юридичного документа або повноважень, що дають право на збір цифрових пристроїв;

– якщо є зобов'язання використовувати інші методи (наприклад, щоб уникнути переривання бізнесу);

– якщо СОР хоче зафіксувати спосіб роботи підозрюваного під час зловживання системою;

– якщо це виявиться критичним для цифрового пристрою, що не допускає ніякого простою.

2.5 Документування

Документування має вирішальне значення при обробці цифрових пристроїв, які можуть містити свідоцтва, представлені в цифровій формі, Під час документування СОР повинен дотримуватися наступних моментів:

– кожна розпочата дія має документуватися. Це робиться для забезпечення впевненості в тому, що під час ідентифікації, збирання, одержання і збереження свідчень ніякі деталі не були упущені;

– якщо цифрові пристрої включені, СОР повинен бути уважним до встановлених часу і даті. Потрібно порівняти настроєний час з надійним джерелом. Час потрібно синхронізувати з надійним і контрольованим джерелом часу;

– СОР повинен документувати все видиме на екрані цифрового пристрою. Активні програми і процеси, а також імена відкритих документів. Ця документація повинна включати опис того, що є видимим, оскільки деякі шкідливі програми можуть імітувати відомі програмні засоби;

– будь–яке переміщення цифрових пристроїв повинно бути документовано відповідно до внутрішніх вимог;

– слід документувати всі унікальні ідентифікатори цифрових пристроїв і взаємопов'язаних частин, такі як серійні номери та унікальну маркування.

2.6 Інструктаж

Дуже важливо, щоб СОР і СЗС були адекватно проінструктовані відповідним органом до виконання ними завдань з дотриманням будь–яких законів і обмежень щодо конфіденційності. Важливо провести офіційний інструктаж, щоб забезпечити розуміння інциденту, а також чого слід і чого не слід очікувати в ході розслідування і нагадати про фальсифікації або пошкодженні свідоцтва. Інструктаж повинен бути достатнім, щоб члени групи були добре підготовлені для виконання своїх ролей і обов'язків; забезпечуючи, таким чином, впевненість в отриманні всіх необхідних потенційних свідчень, представлених в цифровій формі.

2.6.1 Спеціальний інструктаж за свідченнями, представленим в цифровій формі

Щоб проінформувати СОР про пов'язані з розслідуванням деталі, потрібно провести детальний інструктаж, чітко зосередити увагу на конкретних рекомендаціях щодо свідчень, представлених в цифровій формі. Під час інструктажу СОР і СЗС надається відповідна інформація про:

– вид інциденту (якщо відомо);

– дату і час інциденту (якщо відомо);

– розгляд того, де і яким чином буде здійснюватися зберігання, транспортування потенційних свідчень, представлених в цифровій формі, після їх збору або отримання;

– конкретні інструментальні засоби, необхідні для отримання потенційних свідчень, представлених в цифровій формі;

– потенційні свідоцтва, представлені в цифровій формі, які мають відношення до конкретних видів розслідування;

– обладнання і керівництво, що мають відношення до цифрових пристроїв;

– застосовується правові чи інші фактори, які можуть забороняти збір якихось пристроїв і містяться в них потенційних свідчень, представлених в цифровій формі.

2.6.2 Спеціальний інструктаж щодо персоналу

Щоб проінформувати СОР про аспекти, пов'язані з залученими в розслідування сторонами, потрібен інструктаж, чітко зосереджений на спеціальних рекомендаціях щодо персоналу. Під час інструктажу групі, що проводить розслідування будуть надані інструкції, які стосуються персоналу і включають:

– завдання, ролі та обов'язки членів групи що проводить розслідування на місці інциденту;

– нагадування членам групи про те, що не слід приймати технічну допомогу від будь–яких неуповноважених осіб;

– нагадування членам групи про необхідність суворо дотримуватися процедури мінімізації можливого пошкодження свідоцтв, представлених в цифровій формі.

2.6.3 Інциденти в реальному часі

Дуже бажано, щоб розслідування інциденту планувалося заздалегідь, але існують обставини, при яких повне планування не може бути виконано. У таких ситуаціях група повинна бути проінструктована про початкову стратегію і тактику розслідування, і повинна існувати можливість розробки нових стратегій і тактик у відповідь на сформовані умови. Інформація про розвиток інциденту, повинна бути поширена між членами групи якомога швидше, щоб забезпечити впевненість у прийнятті ефективних рішень щодо дій, які вживаються, при відповідному підході до необхідності їх обґрунтування.

2.7 Встановлення пріоритетів для збору і отримання свідоцтв

При встановленні пріоритетів для збору або отримання потенційних свідчень, представлених в цифровій формі, необхідно, щоб СОР розумів причину збору або отримання потенційних свідчень, представлених в

цифровій формі. Як правило, СОР повинен намагатися максимально збільшити кількість даних, які зберігаються шляхом збору та отримання свідоцтв. Може виникнути необхідність у встановленні пріоритетів для елементів по мінливості.

Встановлення пріоритетів може бути застосовано тільки в тому випадку, якщо цього вимагають конкретні обставини розслідуваної справи. Потенційні свідоцтва, представлені в цифровій формі, можна розбити на дві категорії: енергозалежні і енергонезалежні. Мінливі дані легко можуть бути зруйновані або назавжди втрачені, якщо не застосовуються заходи щодо забезпечення захисту даних. Наприклад, відключення електроживлення цифрового пристрою може призвести до втрати мінливих даних. Незмінність дані залишаються на носії навіть при відключенні електроживлення. Оскільки деякі види свідоцтв, представлених в цифровій формі, можуть мати короткий термін життя, потенційні свідоцтва, представлені в цифровій формі, легко можуть бути зіпсовані або пошкоджені. Якщо неясно, чи містять цифрові пристрої потенційні свідоцтва, представлені в цифровій формі, або які елементи більш значимі по відношенню до інших, то необхідно вивчити їх до початку збору, використовуючи процес встановлення пріоритетів. Цифрові пристрої, які підлягають розгляду на предмет збору, включають ІТ–обладнання та цифрові носії даних, автомобільні системи, системи управління і нестандартні електронні пристрої. Спочатку треба отримати найбільш мінливі потенційні свідоцтва, представлені в цифровій формі, наприклад з ОЗУ, простору підкачки, активних процесів і інші.

При ідентифікації СОР повинен:

– встановити пріоритети для потенційних свідчень, представлених в цифровій формі, які будуть назавжди втрачені при відключенні електроживлення; і

– вжити негайних заходів для збору і отримання таких даних затвердженими методами.

При деяких умовах обмежуючим фактором в розслідуванні може бути час. У таких випадках слід віддавати перевагу потенційним свідченнями, представленим в цифровій формі, які ідентифіковані як значущі для конкретного інциденту.

2.8 Збереження потенційних свідчень, представлених в цифровій формі

Для збереження отриманих потенційних свідчень, представлених в цифровій формі, і зібраних цифрових пристроїв важливо під час упаковки убезпечити їх таким чином, щоб виключити пошкодження або фальсифікацію. Пошкодження може бути результатом погіршення якості через вплив магнітного або електричного поля, впливу тепла, високої або низької вологості, а також струсу і вібрації. Фальсифікація може бути результатом навмисного здійснення або допущення здійснення змін потенційних свідчень, представлених в цифровій формі. Тому важливо якомога краще захищати потенційні свідоцтва, представлені в цифровій формі, і як можна менше використовувати вихідні дані.

Всі зібрані цифрові пристрої і отримані потенційні свідоцтва, представлені в цифровій формі, повинні бути захищені, наскільки це можливо, від втрати, фальсифікації або пошкодження. Найбільш важливим дією в процесі збереження є підтримка цілісності та автентичності потенційних свідчень, представлених в цифровій формі, і їх історії зберігання.

Зібрані цифрові пристрої і отримані потенційні свідоцтва, представлені в цифровій формі, повинні зберігатися в приміщенні для зберігання свідоцтв з використанням заходів і засобів контролю та управління фізичної безпеки, таких як системи управління доступом, системи спостереження або системи виявлення вторгнень, або в інший контрольованому середовищі для зберігання свідоцтв, представлених в цифровій формі.

Зібрані цифрові пристрої, повинні бути поміщені в належну упаковку, відповідну характеру пристрою, для запобігання забруднення цифрового пристрою (пристроїв) до транспортування в інше місце(-я). Щоб уникнути

фізичного пошкодження будь–яких компонентів пристрою (пристроїв), може бути використана ударостійка упаковка.

Інструкція користувача

Типовий сценарій при порушеннях ІБ може бути заснований на наведених нижче базових діях.

У разі виникнення інциденту ІБ необхідно:

1 Ідентифікувати інцидент і переконатися, що він дійсно має місце бути;

2 Локалізувати область ІТ–інфраструктури, задіяної в інциденті;

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

4 Оформити службову записку організації про факт виникнення інциденту;

5 Залучити компетентних фахівців для консультації;

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

7 Забезпечити збереження і належне оформлення доказів;

7.1 Зняти енергозалежну інформацію з працюючої системи;

7.2 Зібрати інформацію про перебіг в реальному часі інцидент;

7.3 Відключити від мережі 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, що витягають дані, а також місць їх збереження;

8.3 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 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 і зовнішніми організаціями (компанії, що надають послуги в області розслідування інцидентів ІБ і забезпечення ІБ). А в зверненні до правоохоронних органів представити їм докладний опис інциденту, опис зібраних доказів і результати їх аналізу;

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

Оскільки не тільки важливо розслідувати, але і документувати процес, наведено як повинні оформлюватись документи. Відповідно, для сприяння обміну потенційними свідченнями, представленими в цифровій формі, між сторонами потрібно визначити мінімальний набір вимог до документації. Маючи чіткі визначення між сторонами, які обмінюються доказами та інформацією про інцидент, не виникне плутанини і все буде іти за планом.

Вимоги до документів. Мінімальною документованою інформацією, що підлягає передачі, є:

– найменування та адресу компетентного органу;

– виклад повноважень, рівня навчання та кваліфікації СОР;

– мета вивчення доказів;

– які дії були виконані;

– хто і коли здійснював їх;

– історія зберігання, що відноситься до конкретного розслідування;

– описовий перелік зібраних і отриманих потенційних свідчень, представлених в цифровій формі, і цифрових носіїв інформації;

– інформація, що стосується будь–якого розгляду, тестування або дослідження, використана у відношенні створеної копії свідоцтва.

Якщо керівництво забезпечить працівників та своїх або зовнішніх спеціалістів інструкцією, це вплине на покращення процесу розслідування

інцидентів ІБ. Покращення полягає в тому що правильність та визначеність в діях економить час на розслідування інцидентів ІБ. До того ж спеціалісти, які залучаються зовні, мають змогу оцінити встановлені правила та діяти за наведеним алгоритмом.

2.3 Висновки до розділу

Визначена інформація в другому розділі є корисною. Оскільки для забезпечення як захисту інформації, так і процесу розслідування інцидентів ІБ потрібно розуміти що захищати та від кого. Представлена статистика є прикладом того, що незабезпечення керівництвом організації певних мір з інформаційної безпеки і розслідування, можна отримати такі ж матеріальні втрати. Керівництво або власник підприємства повинні розуміти, що представлені можливі загрози та можливості порушника також можуть проявитися і в їх організації. Кожен інцидент, який потрібно розслідувати повинен бути правильно ідентифікований. Неправильна ідентифікація тягне за собою певні наслідки, за рахунок чого можна втратити докази. Визначені причини інцидентів, статистика їх появи та описи створення моделей загроз і порушника формують чітку проблематику та важливість впровадження практичних рішень. А саме забезпечення комерційних організацій чітко визначеними правилами чи інструкцією з розслідування інцидентів інформаційної безпеки в ІКС.

Також представлено інструкцію з розслідування інцидентів ІБ в ІКС, яка допоможе комерційним підприємствам визначити чіткі вимоги та правила в процесі розслідування. Наведена інструкція складається з опису та постановки розслідування інцидентів ІБ в ІКС, забезпечуються основні етапи «Ідентифікація», «Збір», «Отримання свідчень» та «Збереження». Також наведена інструкція користувача, яка покроково визначає певні дії та вимоги до оформлення документації, яка підлягає передачі.

В межах загальної системи управління інцидентами ІБ організації наведена інструкція відповідає завданню А16 стандарту ISO/IEC 27001 «Гарантування послідовності і результативності підходу до управління

інцидентами інформаційної безпеки, включаючи інформування про події, пов'язані з безпекою, і вразливістю». А також не суперечить та доповнює міжнародні стандарти ISO/IEC 27037: 2012 «Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence», ISO/IEC 27035: 2011 «Information technology. Security techniques. Information security incident management».

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Кваліфікаційна робота передбачає створення інструкції з розслідування інцидентів інформаційної безпеки в інформаційно-комунікаційних системах комерційних підприємств. Тому метою даного розділу є визначення витрат на впровадження розробленої інструкції.

3.1 Обґрунтування необхідності розробки

Розроблена інструкція забезпечує планомірний підхід до розслідування інцидентів ІБ персоналом комерційних організацій. Визначені дії забезпечують покроковий процес, що вбереже організації від додаткових, раптових витрат при пошкодженні майна чи втраті доказів, що мають матеріальну цінність, витрат на послуги юристів.

Оскільки інструкція розроблялась для комерційних підприємств, незалежно від виду її діяльності, для ведення розрахунків цього розділу застосовано середньостатистична комерційне підприємство України.

Загальні відомості про підприємство

Товариство з обмеженою відповідальністю «ТехноКом». Займається онлайн-консультаціями, приймає замовлення на ремонт електронної та побутової техніки, діагностування електронних елементів. Підприємство розташоване за адресою: м. Дніпро, вул. Лаврова, 8.

3.2 Розрахунок капітальних витрат

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

Фіксовані витрати на впровадження системи розраховуватимуться за формулою (3.1):

$$К = К_{пр} + К_{навч} + К_{н} + К_{зпз}, \text{ грн.} \quad (3.1)$$

де $К_{пр}$ – вартість впровадження, грн;

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

$К_{н}$ – витрати на встановлення та налагодження прийняття мір протидії витокам інформації, грн;

$К_{зпз}$ –вартість закупівель, грн.

Розрахунок капітальних витрат буде проводитися на прикладі впровадження засобів захисту інформації: резервне копіювання, блок безперервного живлення, кодовий замок, журнал обліку носіїв інформації, контроль стану обладнання, інструктаж з ІБ, Firewall Analyzer Standard Edition, ESET Internet Security.

3.2.1 Розрахунок заробітної плати системного адміністратора

Обліком носіїв інформації, резервним копіюванням, встановленням кодового замка, встановленням фаєрволу, антивірусу та обліком носіїв інформації займається системний адміністратор.

Заробітна плата при простій часовій системі оплати праці визначається за формулою:

$$З = ТС* Ф , \quad (3.2)$$

де ТС – тарифна ставка привласненого робітникові кваліфікаційного розряду в одиницю часу (година, день, місяць), грн;

Ф – фактично відпрацьований час;

Почасова тарифна ставка системного адміністратора складає ТС = 220 грн/год.

Час на налагодження резервного копіювання займе 2 год.:

$$З = ТС* Ф = 220*2 = 440 \text{ грн.}$$

Час на встановлення блоку безперервного живлення займе 1 год., затрати:

$$З = ТС* Ф = 220*1 = 220 \text{ грн.}$$

Час на встановлення кодового замку займе 1 год., затрати:

$$З = ТС* Ф = 220*1 = 220 \text{ грн.}$$

Час на встановлення фаєрволу займе 1 год., затрати:

З = ТС* Ф = 220*1 = 220 грн.

Час на встановлення антивірусу займе 1 год, затрати:

З = ТС* Ф = 220*1 = 220 грн.

Час на створення журналу обліку носіїв займе 4 год, затрати:

З = ТС* Ф = 220*4 = 880 грн.

3.2.2 Розрахунок капітальних витрат

В таблиці 3.1 наведена кількісно-вартісна характеристика заходів, що впроваджується в підприємстві великого бізнесу.

Таблиця 3.1 – Кількісно-вартісна характеристика заходів

Міри	Характеристика	Вартість
Резервне копіювання	SSD Samsung T7 2TB Shield Blue (MU-PE2T0R) 2022, up to 1050MB/s, www.rozetka.com.ua	11500
Блок безперервного живлення	Powercom BNT-800AP USB, www.rozetka.com.ua	4900
Кодовий замок на серверну	RZ M-1603BK-30, встановлюється своїми силами, www.rozetka.com.ua	800
Облік носіїв інформації	Створення журналу (4 год., переоблік раз на тиждень)	880
Фаєрвол	Firewall Analyzer Standard Edition, hhttps://www.fortsoft.com.ua/	18500
Антивірус	ESET Internet Security www.rozetka.com.ua	1300

Фіксовані витрати на проектування та впровадження заходів захисту інформації складатимуть:

Резервне копіювання:

К = 440 + 11500 = 11940 грн.

Блок безперервного живлення:

К = 220 + 4900 = 5120 грн.

Кодовий замок на серверну:

$$К = 220 + 800 = 1020 \text{ грн.}$$

Облік носіїв інформації:

$$К = 880 \text{ грн.}$$

Фаєрвол:

$$К = 220 + 18500 = 18720 \text{ грн.}$$

Антивірус:

$$К = 220 + 1300 = 1520 \text{ грн.}$$

Загальні затрати складуть 39200 грн.

3.3 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проєктування за визначений період (наприклад, рік), що виражені у грошовій формі.

Під «витратами на керування системою» маються на увазі витрати, пов'язані з керуванням й адмініструванням компонентів системи інформаційної безпеки. До цієї статті витрат можна віднести наступні витрати:

- навчання адміністративного персоналу й кінцевих користувачів;
- амортизаційні відрахування від вартості обладнання та ПЗ;
- заробітна плата персоналу;
- навчальні курси й сертифікація обслуговуючого персоналу;
- технічне й організаційне адміністрування й сервіс.

До експлуатаційних витрат віднесено:

- заробітну плату співробітника системного адміністратора;
- витрати на ліцензію антивірусу;
- витрати на резервне копіювання;
- витрати на замок на серверну;

- витрати на ліцензію фаєрволу;
- витрати на блок безперебійного живлення;
- витрати на облік носіїв інформації;

Річні поточні витрати на функціонування системи заходів протидії загрозам інформації визначаються за формулою (3.3):

$$C = C_1 + C_2 + \ldots + C_n, \text{ грн}, \quad (3.3)$$

де С – вартість підтримки заходу протидії загрозам інформації;

n – порядковий номер заходів протидії загрозам інформації.

Обліком носіїв інформації, резервним копіюванням, підтримкою фаєрволу, антивірусу та обліком носіїв інформації займається системний адміністратор.

Заробітна плата системного адміністратора складає $З_{СА}$ = 220 грн/год.

Час на резервного копіювання займе 0,5 год/день.

$$С = ТС^* Ф = 220*0,5*250 = 27500 \text{ грн.}$$

Час на підтримку фаєрволу займе 1 год/тиждень, затрати:

$$С = ТС^* Ф = 220*1*50 = 11000 \text{ грн.}$$

Час на підтримку антивірусу займе 1 год/тиждень, затрати:

$$С = ТС^* Ф = 220*1*50 = 11000 \text{ грн.}$$

Час на створення журналу обліку носіїв займе 1 год/тиждень, затрати:

$$С = ТС^* Ф = 220*1*50 = 11000 \text{ грн.}$$

Затрати на продовження ліцензії антивірусу складають 800 грн.

Затрати на продовження ліцензії фаєрволу складають 6500 грн.

Значення загальних річних поточних витрат складає:

$$С = 27500 + 11000 + 11000 + 11000 + 800 + 6500 = 67800 \text{ грн.}$$

3.4 Оцінка можливого збитку від порушення інформаційної безпеки

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (КСІБ):

- порушення конфіденційності ресурсів КСІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);
- порушення доступності ресурсів КСІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);
- порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);
- порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

3.5 Визначення збитку від поломок обладнання

Запобігти поломкам обладнання практично неможливо. Природньо, первинна передумова наступна: витрати на ремонт або заміну деяких деталей обладнання не повинні перевищувати вартість самого обладнання.

Вихідні дані для підрахунку збитку:

–час простою внаслідок поломки, $t_п$ (в годинах), $t_п$ = 4 год;

–час відновлення після поломки, $t_в$ (в годинах), $t_в$ = 2 год;

–час повторного введення втраченої інформації, $t_{ви}$ (в годинах), $t_{ви}$ = 1 год;

–заробітна плата обслуговуючого персоналу, Z_0 (грн. в місяць з податками), Z_0 = 20000 грн.;

–заробітна плата співробітників, Z_c (грн. в місяць з податками), Z_c = 18000 грн.;

–кількість обслуговуючого персоналу, N_0, N_0 = 2;

–число співробітників, N_c, N_c = 30;

–прибуток , O (грн. на рік), O = 14800000 грн.;

–вартість заміни обладнання та запасних частин, виправлення помилок в роботі системи, $П_{зч}$ (грн.), $П_{зч}$ = 5000 грн.;

–число зламаного обладнання, I, I = 1;

–число поломок на рік, n, n = 6.

Вартість втрат від зниження продуктивності співробітників несправного обладнання розраховується за формулою 3.10:

$$П_п = \frac{\sum Z_c}{\frac{N_c}{160}} \cdot t_п, \text{ грн.}, \quad (3.4)$$

де місячний фонд робочого часу складає 160 годин.

Підставивши вихідні дані отримаємо:

$$П_п = (30*18000/160)*4 = 13500 \text{ грн.}$$

Вартість відновлення зламаного обладнання розраховується за формулою 3.11:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн.} \quad (3.5)$$

де $П_{ви}$ – вартість повторного введення інформації (формула 3.12),

$П_{пв}$ – вартість відновлення обладнання (формула 3.13).

$$П_{ви} = \frac{\sum Z_c}{\frac{N_c}{160}} \cdot t_{ви}, \text{ грн.} \quad (3.6)$$

$$П_{пв} = \frac{\sum Z_o}{\frac{N_o}{160}} \cdot t_в, \text{ грн.} \quad (3.7)$$

Отримаємо:

$$П_{ви} = (30*18000/160)*2 = 6750 \text{ грн.}$$

$$П_{пв} = (2*20000/160)*3 = 750 \text{ грн.}$$

Вартість заміни обладнання та запасних частин, виправлення помилок в системі, $П_{зч}$ (грн.)

$$П_{зч} = 5000 \text{ грн.}$$

Підставивши отримані результати в загальну формулу отримаємо:

$$П_в = 6750 + 750 + 5000 = 12500 \text{ грн.}$$

Втрачена вигода від простою зламаного обладнання становить та розраховується за формулою 3.14 й 3.15 відповідно:

$$U = П_п + П_в + V, \text{ грн.} \quad (3.8)$$

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви}), \text{ грн,} \quad (3.9)$$

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

$$V = (14800000/2080)*(4+3+2) = 64038,5 \text{ грн.}$$

$$U = 13500 + 12500 + 64038,5 = 90038,5 \text{ грн.}$$

Таким чином, загальний збиток від поломки обладнання, повторного введення інформації в системі, виявлення та усунення помилок в системі складає (формула 3.16):

$$ОУ = \sum_n \sum_I U, \text{ грн.} \quad (3.10)$$

$$ОУ = 6 * 1 * 90038,5 = 540231 \text{ грн.}$$

3.6 Загальний ефект від впровадження моделі

Загальний ефект від впровадження моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компанії визначається за формулою 3.17 з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = ОУ \cdot R - C, \text{ грн,} \quad (3.11)$$

де $ОУ$– загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн.;

R – очікувана ймовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компанії, грн.

Таким чином, загальний ефект від впровадження становить:

$$E = 540231 * 0,5 – 67800 = 202315,5 \text{ грн.}$$

3.7 Визначення та аналіз показників економічної ефективності моделі

Оцінка економічної ефективності моделі, розглянутої у спеціальній частині кваліфікаційної роботи, здійснюється на основі визначення та аналізу коефіцієнта повернення інвестицій *ROSI* (Return on Investment for Security) за формулою 3.18 та терміну окупності капітальних інвестицій T_o за формулою 3.19.

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \quad (3.12)$$

де E – загальний ефект від впровадження системи захисту, грн.;

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

Підставивши відповідні значення, маємо:

$$ROSI = 202315,5 / 39200 = 5,16$$

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів (частини прибутку та амортизаційних відрахувань).

Проєкт визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта формула 3.20:

$$ROSI > (N_{деп} – N_{інф})/100) \quad (3.13)$$

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

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

Підставивши відповідні значення, маємо:

$$ROSI > (17 – 21,8)/100),$$

$$5{,}16 > -0{,}048$$

Отже, проєкт є економічно доцільним.

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років.} \quad (3.14)$$

Підставимо значення:

$$T_o = 1 / 5{,}16 = 0{,}19 \text{ року (2,3 місяці).}$$

3.8 Висновки до розділу

Проведені розрахунки визначають річні витрати на експлуатацію та ефект від впровадження інструкції з розслідування інцидентів інформаційної безпеки в інформаційно-комунікаційних системах комерційних організацій. Результати є позитивними з точки зору економіки.

ВИСНОВКИ

В ході виконання цієї кваліфікаційної роботи були проаналізовані нормативні документи як державного зразка, так й іноземного. На основі отриманої інформації були представлені рішення з розслідування інцидентів інформаційної безпеки в ІКС.

В першому розділі цієї кваліфікаційної роботи проведений аналіз нормативних документів, визначено порядок управління інцидентами за міжнародними стандартами. Визначено процес створення служби реагування на інциденти інформаційної безпеки. А саме – що є метою служби з реагування на інциденти, що склад і кількість персоналу, а також структура СРІБ, повинні відповідати масштабу та структурі організації. Проведений аналіз також визначив процес побудови самого управління інцидентами.

В другому розділі було проаналізовано причини появи інцидентів, а також приведено статистику з різних джерел щодо частоти їх походження. Приведена статистика застосувалась для наочного прикладу чому потрібно визначати чіткі правила та дії в процесі розслідування інцидентів інформаційної безпеки. Статистика дає зрозуміти, що навіть у найзахищеніших системах та у професіоналів з інформаційної безпеки трапляються інциденти. Також в розділі сформовано основні критерії, за якими визначають порушника та загрози згідно з державним нормативним документом.

Також було наведено засоби, за допомогою яких може бути проведений процес розслідування інцидентів ІБ. В розділі сформовано за міжнародними стандартами інструкцію з розслідування інцидентів ІБ. В інструкції визначені покрокові дії з поясненнями, також приведено інструкцію для користувачів системи.

В економічному розділі розраховано витрати на впровадження інструкції та позитивний ефект для організації від її використання.

Запропонована інструкція є ефективною та не суперечить законодавству України та іноземним нормативним документам, на основі яких вона була розроблена.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Закону України «Про інформацію»/ Спосіб доступу URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.– Заголовок з екрану.

2 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

3 ISO/IEC TR 18044:2004 «Information technology. Security techniques. Information security incident management ». Інформаційні технології. Методи і засоби забезпечення безпеки. Менеджмент інцидентів ІБ.

4 ISO / IEC 27035: 2011 «Information technology. Security techniques. Information security incident management».

5 Постанова «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»/ 2006 рік.

6 ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення».

7 ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт».

8 ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення».

9 ДСТУ ISO/IEC 15288:2005 «Інформаційні технології. Процеси життєвого циклу системи».

10 ДСТУ ISO/IEC 13335-1:2004 «Інформаційні технології. Методи захисту. Керування інформацією й безпекою технології комунікацій».

11 НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».

12 НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

13 BS 25999 «Business Continuity Management Standard».

14 CMU / SEI-2004-TR-015 «Defining incident management processes for CISRT».

15 ISO/IEC 17799: 2005 Міжнародний стандарт «Information Security Management as part of management in the field of information security management».

16 ISO/IEC 27001 - Information security management/ 2013 рік.

17 ISO/IEC 27002 - Information technology. Security techniques. Code of practice for information security controls/ 2013 рік.

18 ISO/IEC 27031: 2011 «Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity»

19 ISO/IEC 27037: 2012 «Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence»

20 В. Безмалий. Реагування на інциденти інформаційної безпеки / (Електронний ресурс) спосіб доступу URL: https://www.it-community.in.ua/2014/07/reagirovanie-na-intsidenty-informatsionnoj-bezopasnosti.html/

21 NIST SP 800-61r2 «Computer Security Incident Handling Guide»

22 Cyberthreaa Defense Report North America and Europe / Журнал/ 2015 рік/ Видавництво США/ сторінка 41.

23 Питання управління інформаційною безпекою / Книга 3, 2е видання, 2014 рік. / Автори: Милославська Н.Г. Сенаторів М.Ю. Толстой А. І.

24 ДСТУ 3918-99 (ISO/IEC 12207:1995) Інформаційні технології. Процеси життєвого циклу програмного забезпечення;

25 ДСТУ 4302:2004 Інформаційні технології. Настанови щодо документування комп`ютерних програм (ISO/IEC 6592:2000, MOD) ;

26 ДСТУ ISO 9735-1:2006 Електронний обмін даними для адміністрування, у торгівлі і на транспорті (EDIFACT). Правила синтаксису прикладного рівня (номер версії синтаксису: 4, номер редакції синтаксису: 1), у 10 частинах.

27 ДСТУ ISO/TS 20625:2007 Обмін електронними даними для управління, торгівлі і транспорту (EDIFACT). Правила генерації файлів XML-схем (XSD) на основі настанови з реалізації EDI(FACT);

28 ДСТУ ISO/IEC TR 13335-1:2001 Інформаційні технології. Настанова для керування IT безпекою. Частина 5. Настанова керування безпекою мережі.

29 ДСТУ 4358-2004 Інформаційні технології. Процедури реєстрації культурних елементів (ISO/IEC 15897:1999).

30 ДСТУ ISO/IEC TR 11017:2004 Інформаційні технології. Середовище інтернаціоналізації (ISO/IEC TR 11017:1998).

31 ДСТУ 3986:2000 (ISO 8879:1986) Інформаційні технології. Електронний документообіг. Стандартна мова узагальненої розмітки (SGML).

32 ДСТУ 3719:1998 (ISO/IEC 8613:1989) Інформаційні технології. Електронний документообіг. Архітектура службових документів (ODA) та обмінний формат. Частини 1-4.

33 НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу».

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

35 НД ТЗІ 2.5-005 -99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

36 НД ТЗІ 3.1-001-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроєктні роботи».

37 Інформаційні технології та послуги / (Електронний ресурс) спосіб доступу URL: http://www.ucop.edu/information-technology-services/ initiatives/ resources-and-tools/security-incident-handling.html

38 ISO/IEC 15408: 1999-1-3. «Методи та засоби забезпечення безпеки»/ Стандарт.

39 С. Білоус. Поліпшення процесу управління інцидентами. Публікація «S&T Soft-Tronik», 2007.

40 IT сервіс-менеджмент. Вступ до ITSMF. – М.: IT Expert, 2003. – 228 с., с. 33 – 46.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Розділ 1	28	
6	А4	Розділ 2	32	
7	А4	Розділ 3	10	
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	2	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація_Розгонюк.ppt

2 Кваліфікаційна робота_Розгонюк.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125м-22-2 Розгонюка Д.І. на тему: «Обґрунтування плану розслідування інцидентів інформаційної безпеки в ІКС комерційного підприємства»

Кваліфікаційна робота представлена пояснювальною запискою на 90 с., містить 2 рис., 1 табл., 4 додатків, 40 джерел.

Робота є актуальною оскільки розглядає питання управління інцидентами ІБ та їх розслідування.

Метою роботи є підвищення ефективності розслідування інцидентів інформаційної безпеки.

У спеціальній частині дана характеристика процесу розслідування інцидентів інформаційної безпеки в ІКС. У роботі досліджено етапи розслідування інцидентів інформаційної безпеки в інформаційно–комунікаційних системах. Проведено аналіз основних нормативно-правових документів в сфері інформаційної безпеки, управління інцидентами ІБ та їх розслідування. Розглянуто та проаналізовано особливості процесу розслідування інцидентів ІБ.

В роботі запропоновано для забезпечення планового та точного розслідування інцидентів інформаційної безпеки в ІКС впровадити на комерційних підприємствах розроблені рекомендації.

В економічному розділі визначено ефективність від впроваджуваних рекомендацій.

Практичне значення роботи полягає в розробці рекомендацій з розслідування інцидентів інформаційної безпеки в ІКС.

Результати здійснених у роботі досліджень можуть бути використані при розслідуванні інцидентів інформаційної безпеки в ІКС комерційних підприємств.

До недоліків слід віднести недостатню обґрунтованість отриманих результатів та неточність окремих положень. Також до недоліків слід віднести окремі неточності при оформленні пояснювальної записки.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Розгонюк Д.І. заслуговує на оцінку « » та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доц. **Ковальова Ю.В.**