Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи

магістра
(ступінь підготовки)

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

напрям підготовки (спеціальність) *125 Кібербезпека*
(код і назва напряму підготовки)

спеціалізація (освітня програма) *Кібербезпека*
(код і назва спеціальності)

ступінь підготовки *магістр*
(назва освітнього рівня)

кваліфікація *професіонал із організації інформаційної безпеки*
(код і назва кваліфікації)

на тему: ***Синтез системи підтримки прийняття рішень для оцінки загроз інформаційної безпеки підприємства***

Виконавець: студент ***6*** **курсу, групи** ***125м-16-1***

_____ ***Затуливітер Володимир Анатолійович***
(підпис) (прізвище ім'я по-батькові)

Керівники	Прізвище, ініціали	Оцінка	Підпис
роботи	д.т.н., проф. Корнієнко В.І.		
розділів:			
спеціальний	ст.викл. Начовний І.І.		
економічний	к.е.н., доц. Волотковська Ю.О.		

Рецензент			

Нормоконтроль	к.ф.-м.н., доц. Гусєв О. Ю.		

Дніпро
2018

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

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

«_____»_____20___року

ЗАВДАННЯ
на виконання кваліфікаційної роботи магістра

напряму підготовки (спеціальності) *125 Кібербезпека*
(код і назва спеціальності)

студенту ***125м-16-1*** (група) ***Затуливітеру Володимиру Анатолійовичу*** (прізвище ім'я по-батькові)

Тема дипломної роботи ***Синтез системи підтримки прийняття рішень для оцінки загроз інформаційної безпеки підприємства***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора Державного ВНЗ «НГУ» від _____ № _____

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***система підтримки прийняття рішень для оцінки загроз інформації***

Предмет досліджень ***алгоритми проведення оцінки загроз інформаційної безпеки підприємства з використанням СППР та без***

Мета НДР ***забезпечення потрібного рівню точності аналізу загроз при зменшенні витрат на спеціалістів та зниження витрат часових ресурсів при оцінці загроз інформації***

Вихідні дані для проведення роботи ***існуючі алгоритми оцінки загроз інформаційної безпеки підприємства***

3 ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна ***полягає у розробці СППР для оцінки загроз інформації, з метою підвищення рівня інформаційної безпеки підприємства та зменшення фінансових затрат на проведення експертної оцінки***

Практична цінність ***полягає у зниженні часову проведення оцінки загроз інформації за допомогою запропонованої СППР***

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Дати рекомендації щодо застосування запропонованої системи підтримки прийняття рішень для оцінки загроз інформаційної безпеки підприємства

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Огляд джерел за темою та напрям досліджень	18.09.17-06.10.17
Методи досліджень	07.10.17-24.11.17
Результати досліджень	25.11.17-15.12.17
Виконання економічного розділу	16.12.17-29.12.17
Оформлення пояснювальної записки	30.12.17-10.01.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***економія досягається завдяки одноразовим витратам на розробку СППР та його застосуванню***

Соціальний ефект ***застосування системи підтримки прийняття рішень покращити якість оцінки загроз інформаційної безпеки підприємства***

7 ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Начовний І.І.
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ Затуливітеру В.А.
(підпис) (прізвище, ініціали)

Дата видачі завдання: 01.09.17р.
Термін подання дипломної роботи до ДЕК 16.01.18р.

РЕФЕРАТ

Пояснювальна записка: 107 с., 5 рис., 9 табл., 3 додатки, 20 джерел.

Об’єкт дослідження: система підтримки прийняття рішень для оцінки загроз інформації.

Мета дипломної роботи: забезпечення потрібного рівню точності аналізу загроз при зменшенні витрат на спеціалістів та зниження витрат часових ресурсів при оцінці загроз інформації.

У спеціальній частині проаналізовані основні класи та види систем підтримки прийняття рішень. Розроблена система підтримки прийняття рішень щодо оцінки актуальних загроз інформації на підприємстві на підставі даних опитування співробітників підприємства.

У роботі наведені:

- методика оцінки інформаційної безпеки;
- класифікація компонентів моделі загроз;
- алгоритм системи підтримки прийняття рішень;
- вихідні дані роботи системи підтримки прийняття рішень.

В економічному розділі проведено розрахунок вартості розробки системи підтримки прийняття рішень і обґрунтована її економічна доцільність.

Наукова новизна полягає у розробці системи підтримки прийняття рішень для оцінки загроз інформації, з метою підвищення рівня інформаційної безпеки підприємства та зменшення фінансових затрат на проведення експертної оцінки.

МОДЕЛЬ ЗАГРОЗ, СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ, ЗАГРОЗА, ІНФОРМАЦІЙНА БЕЗПЕКА, ОЦІНКА ЗАХИЩЕНОСТІ.

РЕФЕРАТ

Пояснительная записка: 107 с., 5 рис., 9 табл., 3 приложений, 20 источников.

Объект исследования: система поддержки принятия решений для оценки угроз информации.

Цель дипломной работы: обеспечение требуемого уровня анализа угроз при уменьшении затрат на специалистов и снижения затрат временных ресурсов при оценке угроз информации.

В специальной части проанализированы основные классы и виды систем поддержки принятия решений. Разработана система поддержки принятия решений для оценки актуальных угроз информации на предприятии на основании данных опроса сотрудников предприятия.

В работе приведены:

- методика оценки информационной безопасности;
- классификация компонентов модели угроз;
- алгоритм системы поддержки принятия решений;
- выходные данные работы системы поддержки принятия решений.

В экономическом разделе проведен расчет стоимости разработки системы поддержки принятия решений и обоснована ее экономическая целесообразность.

Научная новизна заключается в разработке системы поддержки принятия решений для оценки угроз информации, с целью повышения уровня информационной безопасности предприятия и уменьшения финансовых затрат на проведение экспертной оценки.

МОДЕЛЬ УГРОЗ, СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ, УГРОЗА, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ОЦЕНКА ЗАЩИЩЕННОСТИ

ABSTRACT

Explanatory note: 107 p., 5 fig., 9 tab., 3 application, 20 sources.

Object of study: the decision support system for assessment of threats to information.

The aim of research paper: support of threats analysis accuracy to reduce costs for employment of professionals and decrease time expenses when assessing the threat information.

In the special part, we analyzed basic classes and types of decision support systems. Using developed the decision support systems for the assessment of current threats to the enterprise information based on employees questioning results.

The paper contains:

- method of assessing informational security;
- threats model components classification;
- the decision support systems algorithm;
- Input data of the decision support systems.

In the economic section, the value of decision support systems development was calculated and proved its economic feasibility.

Scientific novelty lies in development of the decision support systems for assessment of threats to the information to improve the enterprise informational security level and reduce financial costs for peer review.

THREATS MODEL, DECISION SUPPORT SYSTEM, THREAT, INFORMATIONAL SECURITY, ASSESSMENT OF VULNERABILITY

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ІС – інформаційна система;

КС – комп’ютерна система;

НД – нормативний документ;

НД ТЗІ – нормативний документ системи технічного захисту інформації;

НСД – несанкціонований доступ;

ОПР – особа, що приймає рішення;

ПЗ – програмне забезпечення;

СППР – системи підтримки прийняття рішень;

СТЗ – спеціальні технічні засоби.

ЗМІСТ

с.

ВСТУП

Розвиток суспільства неможливе без постійного застосування інформаційних технологій. Комп’ютери обслуговують банківські системи, контролюють роботу атомних реакторів, розподіляють енергію, стежать за розкладом потягів і літаків, керують космічними кораблями. Комп’ютерні системи і телекомунікації визначають надійність і потужність систем оборони і безпеки країни. Комп’ютери забезпечують збереження інформації, її обробку і надання її споживачам, реалізуючи в такий спосіб інформаційні технології. Однак саме найвищий ступінь автоматизації, до якого прагне сучасне суспільство, ставить його в залежність від ступеня безпеки використовуваних ним інформаційних технологій, з якими пов’язані благополуччя і навіть життя безлічі людей.

Технічний прогрес має одну неприємну особливість – у кожному його досягненні завжди криється щось, що обмежує його розвиток і на якомусь етапі обертає його досягнення не на користь, а на шкоду людству. Стосовно інформаційних технологій це означає, що широке впровадження популярних дешевих комп’ютерних систем масового попиту і застосування робить їх надзвичайно вразливими щодо деструктивних впливів. При цьому проблема ускладнюється тим, що загальноприйнятого і автоматизованого методу аналізу загроз і подальшої побудови моделі загроз як невід'ємної умови для побудови ефективної системи захисту інформації до цих пір не було запропоновано. Ще однією проблемою даної області є необізнаність і нерозуміння важливості інформаційної безпеки. Тому прийняття рішень стосовно інформаційної безпеки стає дедалі складнішим і вимагає більше інформації.

Розв’язанням проблеми оцінки загроз є використання системи підтримки прийняття рішень (СППР) і залучення до даного процесу персоналу, який

приймаючи участь в оцінці загроз інформації, буде підвищувати свою обізнаність.

В умовах сьогодення проведення комплексного аналізу загроз інформації займає одне з передових місць в функціонуванні будь-якого підприємства. У зв’язку з цим якісно побудована модель загроз є однією з складових успішного функціонування підприємства.

РОЗДІЛ 1. ОЦІНКА ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Методи оцінки інформаційної безпеки

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

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

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

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

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

підприємства, запобігання загроз його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення в рамках виробничої діяльності всіх підрозділів підприємства.

Унаслідок сукупної дії зовнішніх і внутрішніх дестабілізуючих факторів перед службами захисту інформації стоять завдання не тільки створення, а й постійного вдосконалення захисту інформації. Необхідність вдосконалення призводить до постійного проведення моніторингу і аналізу стану інформаційної безпеки. Розглянемо один з методів оцінки захищеності інформації наведений у [1].

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

Критерії оцінки – це все те, що дозволяє встановити значення оцінки для об’єкта оцінки. В якості критеріїв оцінки ІБ можуть використовуватися вимоги ІБ, процедури ІБ, поєднання вимог і процедур ІБ, рівень інвестицій, витрат на ІБ.

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

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

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

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

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

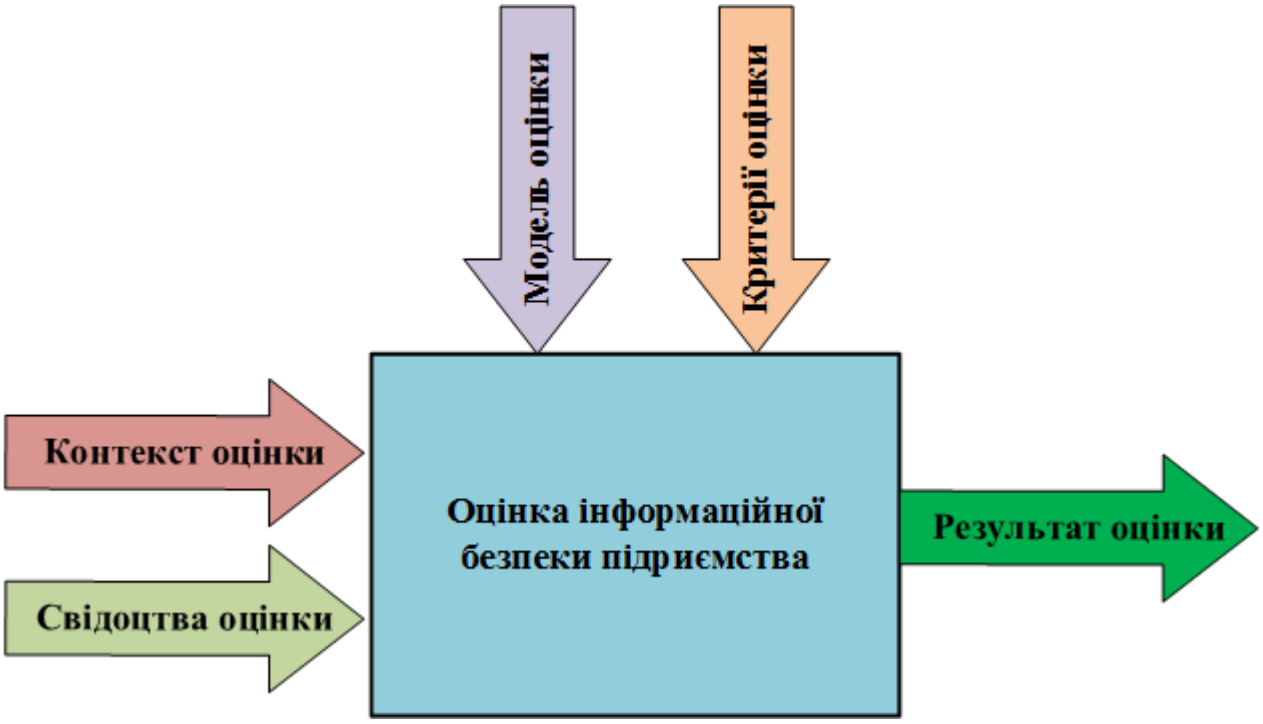

Рисунок 1.1 – Загальний вид процесу оцінки ІБ підприємства

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

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

- виявлення впливу критичних елементів (факторів) та їх сполучень на ІБ організації;
- порівняння зрілості різних процесів забезпечення ІБ і порівняння ступеня відповідності різних захисних заходів встановленим вимогам.

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

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

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

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

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

- вимоги вітчизняного законодавства в області ІБ;
- галузеві вимоги щодо забезпечення ІБ;
- вимоги нормативних, методичних та організаційно-розпорядчих документів щодо забезпечення ІБ;
- вимоги національних і міжнародних стандартів в області ІБ.

Основні етапи оцінки інформаційної безпеки за еталоном включають вибір еталона і формування на його основі критеріїв оцінки ІБ, збір свідчень

оцінки і вимірювання критичних елементів (факторів) об’єкта оцінки, формування оцінки ІБ.

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

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

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

Під показником TCO розуміється сума прямих і непрямих витрат на впровадження, експлуатацію та супровід системи захисту інформації. Під прямими витратами розуміються всі матеріальні витрати, такі як купівля обладнання та програмного забезпечення, трудовитрати відповідних категорій співробітників. Непрямими є всі витрати на обслуговування системи захисту інформації, а також втрати від інцидентів, що відбулися. Збір та аналіз статистики по структурі прямих і непрямих витрат проводиться, як правило, протягом року. Отримані дані оцінюються по ряду критеріїв із показниками TCO аналогічних організацій галузі.

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

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

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

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

1.2 Процес оцінки інформаційної безпеки

1.2.1 Основні елементи процесу оцінки

Процес оцінки ІБ включає такі елементи проведення оцінки:

- контекст оцінки, який визначає вхідні дані: цілі й призначення оцінки ІБ, вид оцінки (незалежна оцінка, самооцінка), об’єкт та області оцінки ІБ, обмеження оцінки і ролі;
- критерії оцінки;
- модель оцінки;
- заходи процесу оцінки: збір свідчень оцінки та перевірка їх достовірності, вимірювання та оцінювання атрибутів об’єкта оцінки;
- вихідні дані оцінки.

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

Перш ніж розглянути особливості способів оцінки ІБ підприємства, необхідно описати загальні для будь-якої оцінки ІБ компоненти: контекст оцінки, збір свідчень оцінки та перевірка їх достовірності, вимірювання та оцінювання атрибутів при проведенні оцінки різного виду (незалежна оцінка,

самооцінка) і вихідні дані оцінки. Модель оцінки і критерії оцінки, що визначають особливості способів оцінки, будуть розглянуті в інших розділах.

Рисунок 1.2 – Основні елементи процесу оцінювання ІБ

1.2.2 Контекст оцінки інформаційної безпеки організації

Контекст оцінки ІБ включає цілі й призначення оцінки ІБ, вид оцінки, об'єкт та області оцінки ІБ, обмеження оцінки, ролі.

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

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

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

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

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

Керівник групи оцінки та оцінювач вимірюють і оцінюють свідоцтва оцінки, надані власниками активів, і формують результати оцінки. Керівник групи повинен розподілити відповідальність між членами групи за оцінювання конкретних процесів, підрозділів, областей або видів діяльності об’єкта оцінки. Такий розподіл повинен враховувати потребу в незалежності, компетентності фахівців з оцінки та результативному використанні ресурсів. Заходи по вимірюванню та оцінюванню виконуються виключно керівником групи оцінки та оцінювачем, що входять до групи оцінки. Інший персонал (представник об’єкта оцінки, технічний експерт) може брати участь у роботі групи оцінки для забезпечення спеціалізованих знань або консультацій. Вони можуть обговорювати з оцінювачем формулювання суджень, але не нестимуть відповідальність за остаточну оцінку.

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

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

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

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

Область оцінки може включати, наприклад, один або декілька процесів об’єкта оцінки, наприклад, організатор може зосередити увагу на одному або декількох критичних процесах і / або захисних заходах. Вибір об’єкта оцінки повинен відображати намічене використання організатором вихідних даних оцінки. Наприклад, якщо вихідні дані призначені для використання при вдосконаленні діяльності по забезпеченню ІБ, то область оцінки повинна відповідати області намічених робіт по вдосконаленню. Область оцінки може бути будь-якою: від окремого процесу до всієї організації. В контексті оцінки має бути представлено докладний опис об’єкта оцінки, що включає розміри об’єкта оцінки, область застосування продуктів або послуг об’єкта оцінки, основні характеристики (наприклад, обсяг, критичність, складність і якість) продуктів або послуг об’єкта оцінки.

До обмежень оцінки можна віднести можливу недоступність основних активів, використовуваних у звичайної ділової діяльності організації;

недостатній часовий інтервал, виділений для проведення оцінювання; необхідність виключення певних частин об’єкта оцінки через стадії життєвого циклу. Крім того, можуть бути накладені обмеження на кількість і вид даних, які повинні бути зібрані і вивчені.

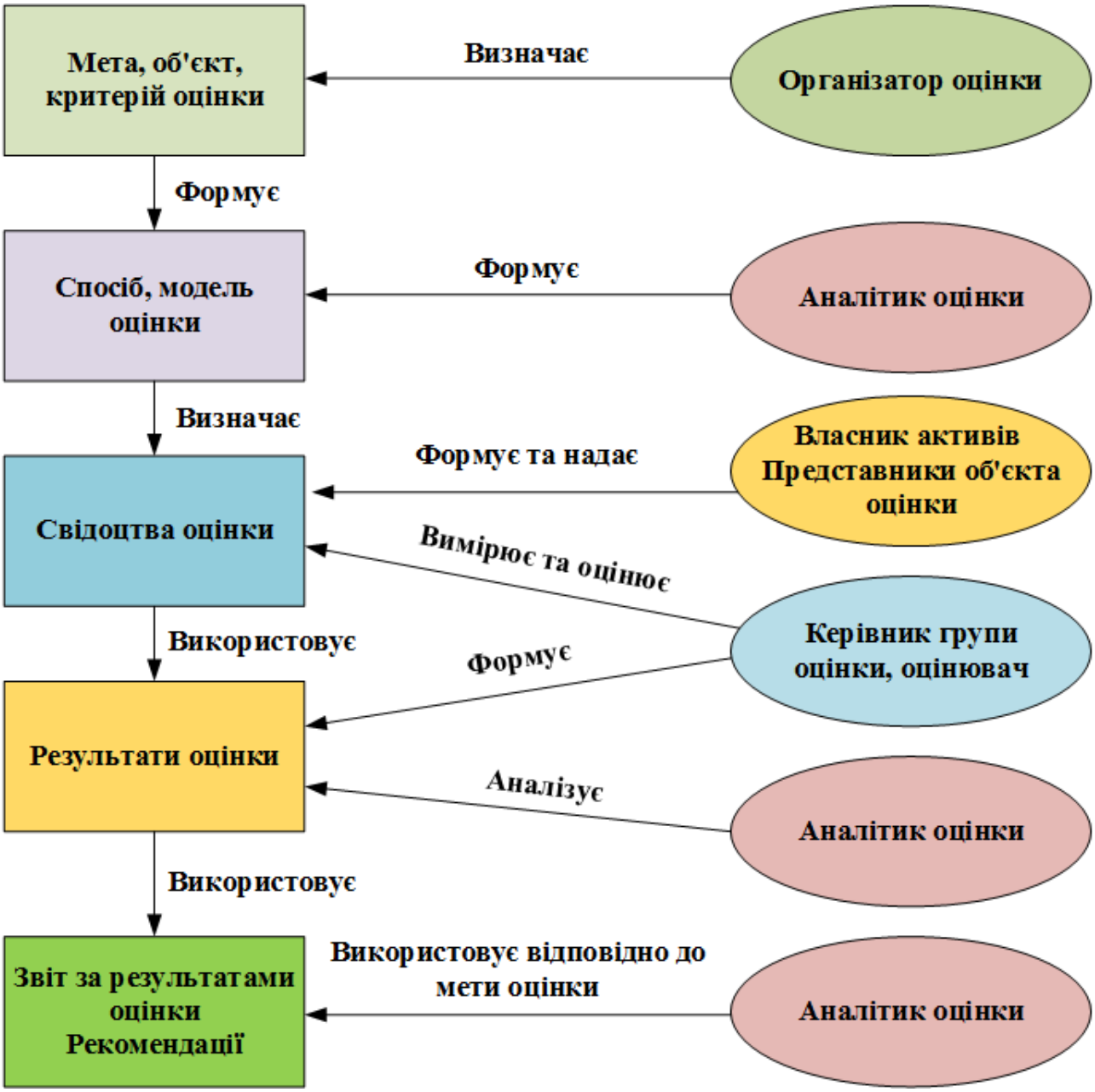

Рисунок 1.3 – Ролі учасників процесу оцінки ІБ і їх функції

Зміст контексту оцінки повинне бути погоджене керівником групи оцінки з організатором та уповноваженим представником об’єкта оцінки та

задокументовано до початку процесу оцінки. Фіксування контексту оцінки важливо, так як він містить вихідні елементи процесу оцінки.

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

1.3 Заходи та вихідні дані процесу оцінки

1.3.1 Збір свідчень оцінки та перевірка їх достовірності

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

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

Необхідними умовами забезпечення достовірної оцінки ІБ при проведенні аудиту є:

- використання довіреної процесу аудиту та дотримання основних принципів аудиту;
- менеджмент програми аудиту ІБ;
- використання найбільш достовірних джерел свідоцтв оцінки;
- визначення обсягу вибірки з урахуванням заданої достовірності свідчень оцінки;
- облік факторів, що впливають на аудиторський ризик, з метою зниження аудиторського ризику.

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

До основних принципів проведення аудиту ІБ відносяться:

1) незалежність аудиту ІБ.

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

2) повнота аудиту ІБ.

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

3) оцінка на основі доказів аудиту ІБ.

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

4) достовірність доказів аудиту ІБ.

Оцінювачі повинні бути впевнені в достовірності свідчень оцінки ІБ. Довіра до документальних свідчень оцінки ІБ підвищується при підтвердженні їх достовірності третьою стороною або керівництвом організації. Довіра до фактів, отриманих при опитуванні співробітників об’єкта оцінки, підвищується при підтвердженні даних фактів з різних джерел. Довіра до фактів, отриманим при спостереженні за діяльністю в області ІБ об’єкта оцінки, підвищується, якщо вони отримані безпосередньо при функціонуванні процедур або процесів, які перевіряються.

5) компетентність і етичність поведінки.

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

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

Основними методами одержання свідчень оцінки повинні бути:

- перевірка та аналіз документів, що відносяться до об'єкта оцінки;
- спостереження за процесами об'єкта оцінки;
- опитування співробітників об'єкта оцінки і незалежної (третьої) сторони.

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

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

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

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

- наявність документа (документів) з релевантним вмістом;
- витяги з документа (документів), що підтверджують реалізацію діяльності по забезпеченню ІБ, покладання відповідальності та обов’язків на співробітника (співробітників) за реалізацію діяльності по забезпеченню ІБ;
- витяги з документа (документів), що містять описи реалізованих захисних методів, процесів забезпечення ІБ.

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

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

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

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

Для впевненості в достовірності оцінки оцінювачі повинні бути впевнені в достовірності виявлених доказів аудиту. Зібрані свідчення оцінки, використовувані для оцінювання показників, повинні бути точним

представленням оцінюваного об’єкта оцінки. Для цього слід враховувати достовірність джерел доказів аудиту.

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

- документальні джерела свідоцтв, отримані з різних джерел третьої сторони (відомості про використання ліцензійних заходів і засобів забезпечення ІБ, договору із супроводу заходів і засобів забезпечення ІБ і т.д.);
- документальні джерела свідоцтв, отримані на (від) об’єкті (та) оцінки та підтверджені третьою стороною (план заходів за результатами зовнішнього аудиту ІБ, матеріали відомчих перевірок ІБ і т.д.);
- джерела свідоцтв, отримані в ході проведення аудиторських процедур, які не передбачають періодичну документальну звітність (результати спостереження за діяльністю, аналізу даних системи моніторингу ІБ і т.д.);
- джерела свідоцтв, отримані у вигляді нормативних та розпорядчих документів (політики, регламенти, звіти про діяльність, накази, розпорядження і т.д.), що вказують на належне застосування процесів і заходів забезпечення ІБ на практиці (наявність дозвільних записів уповноважених осіб, даних контролю ризиків і т.д.);
- свідоцтва, отримані в результаті усних і письмових опитувань про об’єкт оцінки, і спостереження за застосуванням заходів і засобів забезпечення ІБ, які не залишають документальних свідчень (виявлення ролей процесів, послідовності застосування захисних методів і т.д.).

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

1.3.2 Вимірювання та оцінювання атрибутів об’єкта оцінки

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

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

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

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

Метод кількісного вимірювання вимірює атрибути за допомогою відповідної шкали.

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

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

Функції вимірювання можуть включати різноманітні прийоми, такі як усереднення всіх основних заходів, застосування вагових коефіцієнтів до основних заходів або присвоєння якісних значень основним заходам перед їх об'єднанням в кінцеві заходи.

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

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

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

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

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

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

Важливими чинниками досягнення мети оцінки ІБ є наступні:

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

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

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

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

Організатор оцінки, керівництво і персонал об’єкта оцінки повинні вірити в те, що оцінка принесе результат, який є об’єктивним для об’єкта оцінки.

Важливо, щоб усі сторони могли бути впевнені в тому, що фахівці з оцінки володіють адекватними знаннями та досвідом для проведення оцінки, неупереджені та володіють адекватним розумінням об’єкта оцінки та його бізнесу для проведення оцінки.

1.3.3 Способи вимірювання атрибутів об’єкта оцінки

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

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

Для підготовки процесу вимірювання атрибутів за допомогою анкет вимагається:

- виділити серед атрибутів критичні, тобто ті атрибути, які дозволять досягти мети оцінки і сформувати питання анкети;
- визначити за допомогою моделі оцінки спосіб вимірювання.

Це дозволить оцінювачу перетворити вимірювані атрибути в основні заходи за наявності необхідних для виміру джерел свідоцтв і свідоцтв оцінки. Відображення контексту оцінки в анкеті мінімально, а саме опис атрибута у вигляді питання. Елементи контексту оцінки можуть бути присутніми в додаткових методичних та розпорядчих документах, що забезпечують процес оцінки ІБ. У цих документах, як правило, вказуються джерела свідоцтв оцінки, а також персонал, відповідальний за заповнення анкет. Анкети можуть бути побудовані не лише для отримання основної міри атрибуту, але і для формування кінцевої міри. У цьому випадку в анкеті має бути визначена модель об’єднання основних заходів в кінцеву міру.

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

- виділити серед атрибутів критичні, тобто ті атрибути, які дозволять досягти мети оцінки;
- визначити за допомогою моделі оцінки спосіб вимірювання;
- сформувати перелік джерел свідоцтв оцінки та свідоцтв оцінки, необхідних для виміру атрибутів;
- встановити ролі і їх функції при проведенні вимірювання;
- визначити умови функціонування процесу, процедури, захисної заходи або об’єкта оцінки, що включають період збору, аналізу даних, звітності.

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

- метрики повинні давати результат в кількісно вимірної формі (у відсотках, у усереднених і абсолютних значеннях). Наприклад: «відсоток систем, для яких є план роботи в надзвичайній ситуації», «відсоток унікальних ідентифікаторів користувачів», «відсоток систем, в яких застосовуються заборонені до використання протоколи», «відсоток систем, для яких існують документовані звіти про оцінку ризиків» та т.п.;
- дані для підтримки метрик повинні бути доступними;
- значення метрик повинні бути досяжні і мати сенс для бізнесу;
- не слід вимірювати атрибути, які не потрібно удосконалювати.

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

1.4 Побудова моделі загроз

Однією з головних процедур оцінки захищеності інформації є проведення оцінки загроз інформації. Вихідними даними оцінки загроз є модель загроз. Модель загроз безпеки необхідна для визначення вимог до системи захисту. Без моделі загроз неможливо побудувати адекватну (з точки зору грошових витрат) систему захисту інформації, що забезпечує безпеку інформації. У систему захисту включаються тільки ті засоби захисту інформації, які нейтралізують актуальні загрози.

Модель загроз повинна стати відправною точкою для проектування майбутніх систем захисту чи прийняття рішення про захищеність системи. Тому грамотно складена модель загроз дозволяє адекватно захистити інформацію і зробить мету прийнятих нормативних актів не примарною, а реальної. З іншого боку, погано або поверхнево складена модель загроз зробить всю подальшу роботу марною, не дозволить вірно скласти технічне завдання на розробку системи захисту персональних даних, призведе до необґрунтованих витрат на засоби захисту.

Відповідно до вітчизняних нормативних документів формування моделі загроз є необхідною умовою розробки системи захисту інформації.

Відповідно до НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу», модель загроз – це абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.

Роботи зі створення моделі загроз безпеки інформації повинна проводитися в відповідності з наступними основними документами:

- ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт.»;
- НД ТЗІ 1.6-003-2004 «Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації»;

- НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»;
- НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»;
- Постанова КМУ від 16.02.98 №180 «Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах».

Модель загроз формується і затверджується відповідно до даних методичних документів, і може бути переглянута на основі:

- періодично аналізу та оцінки загроз безпеки інформації з урахуванням особливостей і (або) змін конкретної інформаційної системи;
- заходів з контролю за виконанням вимог до забезпечення безпеки інформації при їх обробці в інформаційній системі.

Розробка моделі загроз повинна базуватися на наступних принципах:

1) Безпека інформації при її циркуляції в ІС забезпечується системою захисту інформації.

2) Засоби захисту не можуть забезпечити захист інформації від дій, які виконуються в рамках наданих суб'єкту дій повноважень (наприклад, система захисту не може забезпечити захист інформації від розкриття особами, яким надано право на доступ до цієї інформації). Тому потрібно використовувати організаційні заходи разом з технічними засобами.

3) При формуванні моделі загроз необхідно враховувати як загрози, здійснення яких порушує безпеку інформації (далі - пряма загроза), так і загрози, що створюють умови для появи прямих загроз (далі - непрямі загрози) або непрямих погроз.

4) Інформація обробляються і зберігаються в ІС з використанням певних інформаційних технологій і технічних засобів, що є об'єктами захисту різного рівня, атаки на які створюють прямі або непрямі загрози інформації.

Для розробки моделі загроз необхідно послідовно здійснити наступні кроки:

1) провести категорювання об’єкту інформаційної діяльності;

2) розглянути логічну послідовність процесу порушення інформаційної безпеки;

3) ідентифікувати всі складові моделі загроз та зіставити їх;

4) дослідити зіставлені складові та зробити висновки про їх актуальність;

5) оформити результати висновків відповідно підготовленого шаблону;

Розробка моделі загроз проводиться на основі детального аналізу атрибутів. У випадку побудови моделі загроз, атрибутами є загрози, їх джерела та вразливості.

Після проходження всіх кроків буде сформована модель загроз.

1.4.1 Процес реалізації загроз ІБ

Моделювання процесів порушення інформаційної безпеки доцільно здійснювати на основі розгляду логічного ланцюжка: «загроза – джерело загрози – вразливість – наслідки » (рис. 1.4).

З даної послідовності видно, що порушення ІБ являється послідовним процесом і залежить від певних складових. Тому бажання мати адекватні методи захисту призводять до детального аналізу вище згаданих складових. Удосконалення та поліпшення системи захисту інформації та поліпшення можливо за умови комплексного підходу до побудови моделі загроз і розуміння ступеня її відповідності необхідним результатам.

Для комплексного підходу необхідні детальні класифікації складових. На сучасному етапі розвитку науки в даній області існує велика кількість класифікацій по різним ознаками. Із всього різноманіття класифікацій було обрано класифікацію представлену в [3], яка найбільш повна та легка до

сприйняття. Згідно обраної класифікації детально розберемо кожну складову моделі загроз.

1.4.2 Джерела загроз ІБ

Поняття загрози інформації є основним в теорії і практиці захисту інформації. Аналіз загроз є початковим і одним з основних етапів при розробці моделі загроз. Він має виявити можливі загрози інформації, а також показати, з якого боку і в якій точці системи слід чекати атаки.

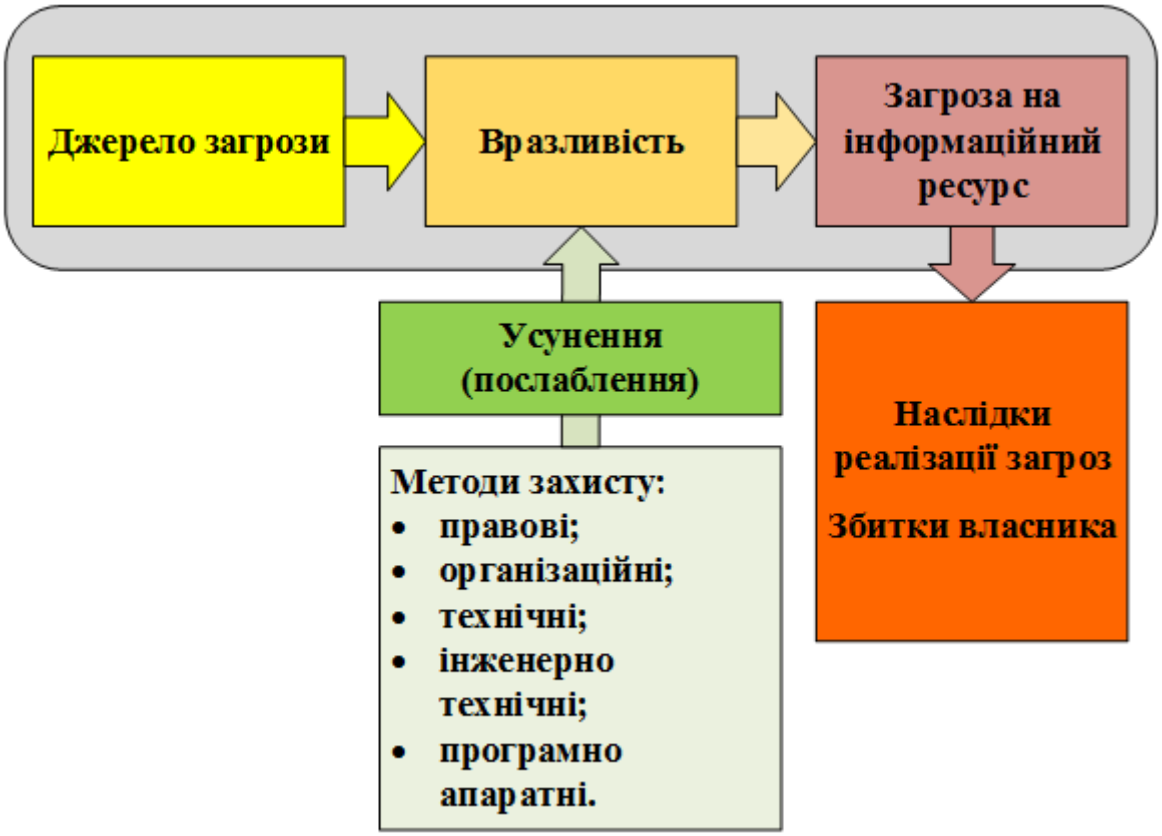

Рисунок 1.4 – Модель реалізації загроз ІБ

Носіями загроз безпеки інформації є джерела загроз. В якості джерел загроз можуть виступати як суб'єкти (особистість) так і об'єктивні прояви. Причому, джерела загроз можуть знаходитися як всередині підприємства – внутрішні джерела, так і поза нею – зовнішні джерела. Поділ на внутрішні і зовнішні джерела виправдано тому, що для однієї і тієї ж загрози методи парирування для зовнішніх і внутрішніх джерел можу бути різними.

Всі джерела загроз безпеки інформації можна розділити на три основні групи:

- обумовлені діями суб’єкта (антропогенні джерела загроз);
- обумовлені технічними засобами (техногенні джерела загрози);
- обумовлені стихійними джерелами.

1.4.2.1 Антропогенні джерела загроз ІБ

Антропогенними джерелами загроз безпеці інформації виступають суб’єкти, дії яких можуть бути кваліфіковані як навмисні чи випадкові. Ця група найбільша й представляє зацікавлення з погляду організації захисту, оскільки дії суб’єкта можна оцінити, спрогнозувати і прийняти адекватні заходи.

Антропогенним джерелом загроз може бути суб’єкт, який має доступ (санкціонований чи несанкціонований) до роботи із штатними засобами об’єкта, який захищається. Суб’єкти (джерела), дії яких можуть призвести до порушення безпеки інформації можуть бути зовнішніми і внутрішніми.

В Україні, в зв’язку зі своєрідною комерційною діяльністю, зовнішні джерела загроз займають вагоме місто. Причинами цього є:

- відсутність ефективних норм господарського права;
- залежність ряду керівників від кримінального світу;
- широке поширення прийомів недобросовісної конкуренції;
- поширеність використання методів промислового шпигунства;
- низький освітній рівень керівної ланки щодо проблем ринку підприємництва, безпеки;
- наявність тіньових економічних процесів;
- встановлення контролю кримінальних структур над рядом секторів економіки і суб’єктами господарської діяльності;
- збереження значного тиску на суб’єкти господарської діяльності з боку корумпованих працівників державних органів;

- зростання криміналізації національного бізнесу взагалі і частіше використання кримінальними структурами угод з метою відмивання брудних» грошей, вивезення їх за кордон тощо;
- наявність ряду соціальних проблем (низький рівень доходів населення, безробіття, плинність кадрів, правовий нігілізм тощо), які збільшують ймовірність кримінальної поведінки громадян;
- відсутність єдності дій і взаємної узгодженості різних правоохоронних органів, у тому числі із службами безпеки суб'єктів господарювання;
- неготовність вітчизняного бізнесу правовими методами забезпечувати захист власної безпеки, відсутність досвідчених фахівців і, як наслідок цього, постійне прагнення до використання не правових методів вирішення господарських конфліктів.

Зовнішні джерела можуть бути випадковими або навмисними і мати різний рівень кваліфікації. До них належать:

- кримінальні структури;
- потенційні злочинці і хакери;
- несумлінні партнери;
- технічний персонал постачальників телематических послуг;
- представники наглядових громадських організацій і аварійних служб;
- представники силових структури.

Зовнішні загрози реалізуються методами промислового шпигунства або соціальної інженерії.

Промислове шпигунство. Вперше термін «промислове шпигунство» було сформульовано на початку 60-х років минулого століття під час семінару з методів збирання інформації для менеджерів вищої ланки, що проводився американською консалтинговою компанією Management Investigation Services. Західні теоретики розуміють під «промисловим шпигунством» добування законним і незаконним шляхом у конкуруючих фірм (монополій, політичних партій, фізичних та юридичних осіб, правоохоронних органів тощо) відомостей

або інформації у сфері наукових досліджень, виробництва продукції за найбільш перспективними технологіями тощо, а також персональних даних з метою їх використання у конкурентній боротьбі або у корисливих цілях.

Метою промислового шпигунства частіш всього буває: або перевірка ділового партнера на благонадійність, або ж знищення конкурента чи нанесення йому серйозних збитків. І, якщо в першому варіанті немає загроз підприємству, то в другому, якщо конфіденційна інформація потрапить до рук таких агентів, це може призвести до дуже серйозних наслідків для підприємства, закінчуючи його банкрутством та ліквідацією.

І хоча існує багато технічних засобів для здобуття інформації, промисловим шпигунам інколи просто достатньо поговорити з працівниками і які, самі того не підозрюючи, можуть надати досить суттєву інформацію, якою конкуренти не втратять нагоди скористуватися. За оцінками фахівців, на частку людського фактору, тобто на балакучість співробітників, припадає до 60% всього витоку інформації. Інші 40% - це те, що вдається перехопити технічними засобами. Але й використовуючи технічні засоби, промислові шпигуни дуже часто «звертаються» за допомогою до співробітників компанії, про яку хочуть роздобути інформацію. Навіть співробітникам найнижчої ланки під силу встановити відповідну апаратуру для зняття інформації.

Тож промислове шпигунство є тією загрозою, від якої потрібно захищатися. Як би інформація підприємства нікого не цікавила, не було б сенсу її оберігати. Але, промислові шпигуни не досягали б поставленої мети, якби не загрози внутрішні: необережні чи навмисні дії співробітників.

Соціальна інженерія – це метод несанкціонованого доступу до інформації або систем зберігання інформації без використання технічних засобів. Метод заснований на використанні слабкості людського чинника і вважається дуже руйнівним. Зловмисник отримує інформацію, наприклад, шляхом збору персональних даних про службовців об’єкту атаки, за допомогою звичайного телефонного дзвінка або шляхом проникнення в організацію під виглядом її службовця. Зловмисник може подзвонити працівникові компанії (під виглядом

технічної служби) і вивідати пароль, пославшись на необхідність вирішення невеликої проблеми в комп'ютерній системі. Дуже часто це спрацьовує. Найсильніша зброя в цьому випадку — приємний голос і акторські здібності.

Методи соціальної інженерії:

1) Претекстінг – дії, що в ході атаки, здійснюваної зазвичай по телефону, відпрацьовуються порушником за заздалегідь сформованим сценарієм і мають на меті забезпечити його входження у довіру до жертви.

2) Фішинг – дії, що в ході атаки, здійснюваної порушником через e-mail, вимагають від потенціальної жертви розголосити певну конфіденційну інформацію про себе – логіни, паролі тощо шляхом її так званої перевірки.

3) Несанкціоноване надання додаткових прав і можливостей зареєстрованим користувачам системи.

4) Запуск злоякісного ПЗ, наприклад, троянських програм (бекдорів, руткітів, кейлогерів, клікерів та проксі-троянів) як відповіді на e-mail запит порушника або через інфікований CD (флеш-накопичувач) тощо.

Внутрішніми суб'єктами (джерелами), зазвичай, є висококваліфіковані спеціалісти у галузі розробки та експлуатації програмного забезпечення і технічних засобів, знайомі зі специфікою розв'язуваних завдань, структурою, функціями і принципами роботи програмно-апаратних засобів захисту інформації, які мають зокрема можливість використання штатного устаткування і технічних засобів мережі.

До них належать:

1) основний персонал (користувачі, програмісти, розробники);

2) представники служби захисту;

3) допоміжний персонал (прибиральники, охорона);

4) технічний персонал (життєзабезпечення, експлуатація).

Інциденти через дані загрози трапляються через необережність або через умисні дії персоналу.

Необережність персоналу.

Дуже часто співробітники, хоч і не мають на меті розголосити конфіденційні відомості, роблять це, інколи навіть не розуміючи цього. Тож необережність можна поділити на дві категорії:

- дії чи бездіяльність співробітників, спричинені необізнаністю у сфері захисту інформації;
- дії чи бездіяльність співробітників у випадку, в яких співробітники знали або не знали, але повинні були знати про можливі негативні наслідки.

У першому випадку не можна казати про вину співробітника, скоріше це прорахунки вищого керівництва, яке не потурбувалося роз'яснити персоналу про важливість інформації і про її захист. Якщо мова йде про державну таємницю, то такі ситуації не можуть виникнути, бо є чітко визначений законодавством порядок допуску до державної таємниці. Одним з пунктів є підписання зобов'язання про нерозголошення довірених даних. Багато комерційних фірм використовують законодавство про державну таємницю як приклад для аналогічного захисту своєї, комерційної таємниці. Але цього прикладу додержуються не всі компанії. Інколи керівники, як метод захисту інформації, практикують не казати працівникам про важливість даних. Як приклад можна привести ситуацію: прибиральниця, яка прийшла прибрати кабінет керівника фірми, побачила в нього на столі дуже красиву модель якогось пристрою. Вина керівника полягає вже в тому, що він дозволив прибирати в кабінеті тоді, коли працює там сам, коли документи не сховані в сейфі та працює комп'ютер, де також можуть бути відкриті секретні файли. Але він також не попередив прибиральницю про те, що не потрібно розповідати про будь що, що вона бачила. Прибиральниця, якій сподобалася модель з чисто мистецьких поглядів, може поділитися своїми враженнями з людиною, яка зацікавиться цією інформацією. Тож керівникам потрібно попереджати всіх співробітників, які хоч якось взаємодіють з конфіденційною інформацією і можуть ознайомитися з нею в розмірі, достатньому для відтворення хоча б частини такої інформації.

В іншому випадку співробітника повідомили про те, що він не повинен розголошувати конфіденційні відомості підприємства, але він вважаючи, що його дії не призведуть ні до яких наслідків, призводить до втрати інформації чи ознайомлення з нею третіх осіб. У кримінальному кодексі необережність поділяють саме на злочинну самовпевненість та злочинну недбалість.

Під злочинною самовпевненістю розуміють дії чи бездіяльність особи, коли вона знала про можливі негативні наслідки, передбачала їх настання, але зухвало розраховувала на їх відвернення.

Злочинною недбалістю є дії чи бездіяльність особи, коли вона не знала, але повинна була знати про можливі негативні наслідки свого діяння.

В усіх цих випадках метою співробітника не було розголошення конфіденційних відомостей, та саме до цього призвели його дії.

Умисні дії працівників по розголошенню інформації та мотиви цих дій

На відміну від необережності, умисел передбачає, що метою дій співробітників було саме розголошення інформації, що є конфіденційною. Причому співробітників могли завербувати агенти промислового шпигунства або ж вони самі ініціативно вирішили зрадити організацію, на яку працювали (в цих випадках вони вже самі можуть шукати контактів з представниками конкуруючих фірм чи інших осіб, зацікавлених в отриманні певної інформації).

Для того, щоб виявити або попередити такі дії, потрібно визначитися, чому ж саме працівники пішли на них. Кожна людина є індивідуальною, в кожного своє життя та свої проблеми, через які він приймає ті чи інші рішення. Тож кожна ситуація має свої нюанси, але є декілька розповсюджених причин для розголошення інформації співробітниками. До них відносяться:

- помста;
- матеріальна або інша вигода;
- самореалізація.

Саме з цих причин персонал фірми найчастіше зраджує її інтереси. Багато в чому тут також є прорахунки керівництва. Саме це найчастіше є тим, через що вербують співробітників. Невдоволені працівники краще йдуть на контакт з

промисловими шпигунами, бо не відчувають патріотизму до цієї фірми, мріють поквитатися з кимось із колег чи з керівництвом, або прагнуть покращити своє матеріальне становище. Таким особам пропонують те, чого в них немає і не буде на даній фірмі: або значні матеріальні виплати, або ж пропонування роботи, де їх працю оцінять, де їх будуть поважати, або ж інші речі, що відповідають потребам цих співробітників.

Тож загроза цілісності інформації йде від людини. Можна встановити найсучасніші системи технічного захисту, видати мільйони нормативних актів, які регулюють захист інформації, але поки буде ігноруватися людський фактор (тобто фактор людського впливу на інформацію, загрози, які йдуть від людей та причини цих загроз), доти юридичні, організаційні та технічні засоби будуть мало ефективними.

Проаналізувавши загрози конфіденційності даних, які пов’язані з персоналом, можна побачити, що ігнорування цих загроз призводить до серйозних збитків на підприємствах. Мова йде не тільки про фінансові втрати компанії, але й про різке падіння її іміджу у зв’язку з тим, що вона не може захистити власну конфіденційну інформацію.

Необхідно враховувати також, що особливу групу внутрішніх антропогенних джерел становлять особи з порушеною психікою і спеціально впроваджені і завербовані агенти, які можуть бути присутні у складі основного, допоміжного і технічного персоналу, і навіть представниками служби захисту. Ця група може бути у складі перелічених вище джерел загроз, але методи парирування загрозам з цією групи може мати свої відмінності.

1.4.2.2 Техногенні джерела загроз ІБ

Техногенні джерела загроз залежать від технократичної діяльності людини і розвитку цивілізації. Ці джерела загроз менш прогнозовані, безпосередньо залежать від властивостей техніки і тому вимагають особливої уваги. З одного боку вони викликані фізичним і моральним старінням технічного парку використовуваного обладнання, а з іншого значним технічним

прогресом людства. Мережі зв’язку, інженерних комунікацій та транспортні мережі у більшості випадків не відповідають сучасним потребам безпеки. Деякі з них потребують ремонту та переобладнання, але це не завжди фінансується. Через це дані комунікації стають джерелами загроз для інформації.

З іншого боку, масова комп’ютеризація усіх можливих сфер життя людини, яка спричинила виникнення нових засобів негласного знімання інформації: віруси вільного поширення, спеціалізовані комп’ютерні закладки, що у потрібний час зчитують і надають зацікавленим особам певну інформацію. Але все ж основну масу займають пристрої знімання відео та акустичної інформації. В Україні законне використання СТЗ можливе лише правоохоронними органами, під час здійснення оперативно-розвідувальної діяльності, згідно з законом України «Про оперативно-розшукову діяльність», Кримінально-процесуальним кодексом України та окремими підзаконними актами. Спеціальними технічними засобами є технічні засоби, устаткування, апаратура, прилади, пристрої, препарати та інші вироби, спеціально створені, розроблені, запрограмовані або модернізовані для виконання завдань з негласного отримання інформації під час здійснення оперативно-розшукової діяльності.

До таких засобів належать:

- спеціальні технічні засоби для негласного отримання та реєстрації аудіоінформації;
- спеціальні технічні засоби для негласного візуального спостереження та документування;
- спеціальні технічні засоби для негласного прослуховування телефонних переговорів;
- спеціальні технічні засоби для негласного перехоплення та реєстрації інформації з технічних каналів зв’язку;
- спеціальні технічні засоби для негласного контролю поштових повідомлень і відправлень;

- спеціальні технічні засоби для негласного обстеження предметів і документів;
- спеціальні технічні засоби для негласного проникнення у приміщення, транспортні засоби, інші об’єкти та їх обстеження;
- спеціальні технічні засоби для негласного контролю за переміщенням транспортних засобів та інших об’єктів;
- спеціальні технічні засоби для негласного отримання (зміни, знищення) інформації з технічних засобів її зберігання, обробки та передачі.

Та в сучасному інформаційному просторі СТЗ зазнали широкого незаконного використання. Їх можливості визначаються загальним технічним розвитком людства та технологічними можливостями суб’єктів, що їх виробляють. За допомогою СТЗ перехоплюються телефонні розмови, електронна пошта, інформація відправлена через глобальну мережу, зміст важливих документів та інше.

Даний клас джерел загроз, як і попередній, поділяється на внутрішні та зовнішні. До зовнішніх джерел відносяться засоби зв’язку, інженерні комунікації та транспорт. Ця група повністю залежить від зовнішніх факторів.

До внутрішніх техногенних джерел відносяться:

- неякісні технічні засоби обробки інформації;
- неякісні програмні засоби обробки інформації;
- допоміжні засоби (охорони, сигналізації, телефонії);
- інші технічні засоби, що застосовуються в установі.

Ці засоби напряму чи побічно пов’язані з обробкою інформації, або функціонують поруч з ними. Програмні засоби можуть бути джерелом загрози через:

- наявність на підприємстві піратського ПЗ;
- неякісне налаштування мережевого екрану;
- наявність в ПЗ неліцинзованих можливостей.

Що стосується технічних засобів, то ці загрози пов’язані з їх побічними та не документованим технічними можливостями. До побічних можливостей відносяться:

- небажані електромагнітні випромінювання;
- наявність наведень електромагнітних випромінювань на різні струмоведучі ланцюга та конструкції;
- наявність випадкових електроакустичних перетворювачів в окремих елементах технічних засобів;
- вплив акустичних і віброакустичних коливань на елементи технічних засобів;
- помилки при проектуванні та налаштуванні технічних засобів;
- помилки при проектуванні систем живлення;
- наявність нелінійних процесів в елементах технічних засобів.

До недокументованих відносяться можливості спеціально чи випадково закладені виробниками.

1.4.2.3 Стихійні загрози інформаційної безпеки

Природна надзвичайна ситуація – це обстановка на певній території чи акваторії, що склалася в результаті виникнення джерела природної надзвичайної ситуації, яка може спричинити або спричинила людські жертви, шкоду здоров’ю людей і (або) навколишнього природного середовищі, значні матеріальні збитки та порушення умов життєдіяльності людей. Природні надзвичайні ситуації розрізняють за характером джерела і за масштабами.

Джерело природної надзвичайної ситуації - небезпечне природне явище або процес, в результаті якого на певній території або акваторії сталася або може відбутися надзвичайна ситуація.

Кожне стихійне лихо має свою фізичну сутність, свої, тільки йому притаманні, причини виникнення, рушійні сили, характер і стадії розвитку, свої особливості впливу на навколишнє середовище.

Незважаючи на різкі відмінності стихійних лих один від одного, їм притаманні і загальні риси – великий просторовий розмах, значний вплив на навколишнє середовище, сильний психологічний вплив на людину.

В законодавстві та договірній практиці використовують поняття «непереборної сили». До непереборної сили відносять стихійні лиха чи інші обставини, які неможливо передбачити або запобігти або можливо передбачити, але неможливо запобігти при сучасному рівні людського знання і можливостей. Такі джерела загроз абсолютно не піддаються прогнозуванню і тому заходи захисту від них повинні застосовуватися завжди.

Стихійні джерела потенційних загроз інформаційної безпеки як правило є зовнішніми стосовно до захищається і під ними розуміються насамперед природні катаклізми:

- пожежі;
- землетрусу;
- повені;
- урагани;
- різні непередбачені обставини;
- нез’ясовні явища;
- інші форс-мажорні обставини.

1.4.3 Вразливості інформаційних систем

Загрози, як можливі небезпеки вчинення будь-якої дії, спрямованої проти об’єкта захисту, проявляються не самі по собі, а через вразливості (фактори), що призводять до порушення безпеки інформації на конкретному об’єкті інформатизації.

Вразливості притаманні об’єкту інформатизації, невіддільні від нього і обумовлюються недоліками процесу функціонування, властивостями архітектури автоматизованих систем, протоколами обміну і інтерфейсами, застосовуваними програмним забезпеченням і апаратною платформою, умовами експлуатації та розташування.

Джерела загроз можуть використовувати вразливості для порушення безпеки інформації, отримання незаконної вигоди (нанесення шкоди власнику, користувачеві інформації). Крім того, можливі не зловмисні дії джерел загроз щодо активізації тих чи інших вразливостей, що завдають шкоди.

Кожна загроза може використовувати різні вразливості. Усунення або істотне ослаблення вразливостей впливає на можливість реалізації загроз безпеці інформації.

Для зручності аналізу, вразливості розділені на класи, групи і підгрупи. Вразливості безпеки інформації можуть бути:

- об’єктивними;
- суб’єктивними;
- випадковими.

Об’єктивні вразливості:

- супутні технічним засобам випромінювання:

1) електромагнітні (побічні випромінювання елементів технічних засобів, кабельних ліній технічних засобів, випромінювання на частотах роботи генераторів, на частотах самозбудження підсилювачів);

2) електричні (наведення електромагнітних випромінювань на лінії і провідники , просочування сигналів у колі електроживлення, в колі заземлення, нерівномірність споживання струму електроживлення);

3) звукові (акустичні, віброакустичні);

- керуючі:

1) апаратні закладки (встановлювані в телефонні лінії, в мережі електроживлення, в приміщеннях, в технічних засобах);

2) програмні закладки (шкідливі програми, технологічні виходи з програм, нелегальні копії ПЗ);

- обумовлені особливостями елементів:

1) елементи, що володіють електроакустичними перетвореннями (телефонні апарати, гучномовці та мікрофони, котушки індуктивності, дроселі, трансформатори та ін.);

2) елементи, схильні до дії електромагнітного поля (магнітні носії, мікросхеми, нелінійні елементи, повалені ВЧ нав’язування);

- обумовлені особливостями об’єкта, що захищається:

1) місцем розташування об’єкта (відсутність контрольованої зони, наявність прямої видимості об’єктів, віддалених і мобільних елементів об’єкта, вібруючих поверхонь, що відбивають);

2) організацією каналів обміну інформацією (використання радіоканалів, глобальних інформаційних мереж, орендованих каналів).

Суб’єктивні вразливості:

- помилки:

1) при підготовці та використанні програмного забезпечення (при розробці алгоритмів та програмного забезпечення, інсталяції та завантаження програмного забезпечення, експлуатації програмного забезпечення, введенні даних);

2) при управлінні складними системами (при використанні можливостей самонавчання систем, налаштуванні сервісів універсальних систем, організації управління потоками обміну інформацією);

3) при експлуатації технічних засобів (при включенні / виключенні технічних засобів, використанні технічних засобів охорони, використанні засобів обміну інформацією);

- порушення:

1) режиму охорони і захисту (доступу на об’єкт, доступу до технічних засобів);

2) режиму експлуатації технічних засобів (енергозабезпечення, життєзабезпечення);

3) режиму використання інформації (обробки і обміну інформацією, зберігання і знищення носіїв інформації, знищення виробничих відходів і браку);

4) режиму конфіденційності (співробітниками в неробочий час, звільненими співробітниками).

Випадкові вразливості:

- збої і відмови:

1) відмови і несправності технічних засобів (опрацьовують інформацію, що забезпечують працездатність засобів обробки інформації, що забезпечують охорону і контроль доступу);

2) старіння і розмагнічування носіїв інформації (дискет і знімних носіїв, жорстких дисків, елементів мікросхем, кабелів та з'єднувальних ліній);

3) збої програмного забезпечення (операційних систем і СУБД, прикладних програм, сервісних програм, антивірусних програм);

4) збої електропостачання (обладнання, обробного інформацію, що забезпечує та допоміжного обладнання);

- пошкодження:

1) життєзабезпечуючих комунікацій (електро-, водо-, газо-, теплопостачання, каналізації, кондиціювання та вентиляції);

2) огороджувальних конструкцій (зовнішніх огорож територій, стін і перекриттів будинків, корпусів технологічного обладнання).

1.4.4 Загрози інформаційній безпеці

Сучасна література поняття "інформаційна загроза" розглядає як потенційну можливість певним чином порушити інформаційну безпеку або як ступінь імовірності виникнення такого явища (події), наслідком якого можуть бути небажані впливи на інформацію. Наприклад, загроза зйому інформації і перехоплення випромінювання з дисплею може привести до втрати таємності або конфіденційності, загроза пожежі може привести до порушення цілісності та доступності інформації, загроза розриву каналу передачі інформації може реалізувати втрату доступності. Існує багато підходів щодо класифікації загроз. Проте в літературі та законодавстві найчастіше зустрічаються такі підходи:

- заснований на основних (фундаментальних) властивостях;
- виходячи зі складу протиправної діяльності.

В першому випадку, розрізняються наступні класи загроз інформації:

- порушення конфіденційності;
- порушення цілісності;
- порушення доступності або відмова в обслуговуванні;
- порушення спостереженості або керованості.

В другому випадку, розрізняють:

- розкрадання (копіювання) інформації;
- знищення інформації;
- модифікація (спотворення) інформації;
- порушення доступності (блокування) інформації;
- заперечення автентичності інформації;
- нав’язування неправдивої інформації.

Більш придатним для аналізу являється другий випадок.

В першій класифікації залишається певна абстракція і питання про певну конкретику і практичність. При роботі з даною класифікацією треба будувати ієрархічну систему, яка б розкривала зміст кожного пункту. Така класифікація являється громіздкою и не лаконічною. З іншого боку, ми маємо другу класифікацію, яка має потрібну конкретику і практичність, і до того ж являється лаконічною і зрозумілою. Тому більш придатною для аналізу є класифікація загроз за складом протиправної діяльності. Розглянемо її детальніше.

Розкрадання – це вчинене з корисливою метою протиправне безплатне вилучення і (або) звернення чужого майна на користь винного або інших осіб, яке завдало збитки власнику чи іншому власникові цього майна.

Знищення – дії, унаслідок яких інформація в системі зникає. Тобто порушуються цілісність і доступність інформації, і її неможливо відновити.

Спотворення – зміна змісту повідомлення, що передається лінією зв’язку.

Спотворення інформації – випадкова несанкціонована модифікація інформації при її обробці технічними засобами в результаті зовнішніх впливів (перешкод), збоїв в роботі апаратури або невмілих дій обслуговуючого персоналу.

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

Поняття «автентичний» означає цілком вірогідний, заснований на першоджерелах.

Заперечення автентичності інформації – відмова суб’єкта в авторстві на відправлене повідомлення чи інформацію.

Нав’язування неправдивої інформації – надання некоректної інформації під видом коректної.

1.4.5 Аналіз взаємозв’язків між компонентами моделі загроз

Розібравши всі компоненти переходимо до аналізу взаємозв’язків між ними. Спираючись на думку авторів [1-2], були проаналізовані та побудовані взаємозв’язки між загрозами, джерелами та їх вразливостями. Дані взаємозв’язки представлені в формі таблиці у 2 розділі.

1.5 Аналіз існуючих способів виявлення загроз інформації

Як зазначалося раніше, оцінку ІБ можна проводити різними способами. Та найбільш ефективними є два наступних:

- на основі еталона;
- ризик-орієнтована оцінка.

В першому випадку аналіз проводиться шляхом порівняння ситуації на підприємстві з еталонним чи стандартизованими значеннями чи даними. В кінці даної процедури отримуємо список атрибутів і їх коефіцієнт відповідності. Цей спосіб застосовується в тих випадках, коли організація і діяльність самої організації відповідають стандартизованим даним. В іншому випадку дані, отримані після оцінювання не будуть відповідати дійсності.

Позитивною стороною даного способу є наявність розробленої та структурованої бази знань.

Негативною стороною аналізу на основі еталону є можливі складності при інтерпретації еталонних даних і неможливість використання способу при нестандартно структурованих підприємствах.

В іншому випадку аналізуються можливості порушення захищеного стану підприємства. В кінці даної процедури ми отримуємо список атрибутів і їх коефіцієнт небезпеки. Цей спосіб можна застосовувати в будь якому випадку. Але зі збільшенням розмірів підприємства, збільшується об’єм інформації, яку потрібно опрацювати.

Позитивною стороною даного способу є можливість використання даного підходу на будь якому підприємстві.

Негативною стороною ризик-орієнтованої оцінки є необхідність аналізу існуючих загроз і складності при збільшенні розмірів підприємства.

В різних джерелах можна знайти різні реалізації обох способів. Та незважаючи на це, не існує єдиних стандартизованих підходів використання вищезгаданих способів. Кожен спеціаліст реалізує ці способи на свій розсуд, а великі компанії намагаються створити програмні комплекси, які реалізують змішані підходи. Все це свідчить про наявність труднощів та проблем області оцінки стану ІБ.

1.6 Висновок. Постановка задачі

В даному розділі були проаналізовані методи оцінки ІБ та основні складові цього процесу. В якості основи для оцінки рівня захищеності інформації на об’єкті було обрано модель загроз ІБ. Аналіз взаємозв’язків складових моделі загроз дозволив побудувати можливі сценарії реалізації загроз ІБ. Рівень небезпеки цих загроз і визначає рівень ІБ на об’єкті. На базі отриманих даних приймаються рішення щодо удосконалення існуючої системи захисту та рівня фінансування цих заходів, і при цьому необхідно враховувати різні чинники та обробляти великий обсяг інформації. Тому розроблювана система допоможе зменшити затрати на спеціалістів та часових ресурсів при

оцінці загроз інформації. Для забезпечення цих умов, в дипломній роботі необхідно вирішити наступні задачі:

- проаналізувати системи підтримки прийняття рішень;
- розробити алгоритм СППР;
- розробити модель оцінки даних в СППР;
- розробити опитувальник;
- по отриманим даним реалізувати СППР.

РОЗДІЛ 2. СИНТЕЗ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ОЦІНКИ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

2.1 Поняття та аналіз основних систем підтримки прийняття рішень

Забезпечення інформацією і підтримка на всіх рівнях прийняття управлінських рішень є нетривіальним завданням. Розрізняють такі основні типи інформаційних систем: інформаційно-управлінські системи; системи підтримки прийняття рішень; виконавчі інформаційні системи.

Діяльність людей пов’язана з необхідністю щодня приймати рішення різноманітної складності, наприклад: вибір напрямку розвитку фірми, вибір варіанту автоматизації діяльності компанії, визначення стану інформаційної безпеки, вибір приміщення для переговорів, типу обладнання, призначення на вакантну посаду одного з багатьох кандидатів і т.д.

Необхідність врахування при прийнятті рішень щодо забезпечення безпеки інформації на підприємстві великої кількості економічних, соціальних, юридичних і моральних факторів значно ускладнює задачу вибору правильного варіанту рішення. А для прийняття рішення необхідно врахувати взаємозв’язок усіх факторів, що відносяться до компетенції різних експертів. У той самий час керівник, який приймає рішення, – звичайна людина з притаманними усім людям психофізіологічними обмеженнями. Одним з шляхів вирішення наявного протиріччя є використання математичних методів, що втілені у сучасних інформаційних СППР.

Система підтримки прийняття рішень – комп’ютерна автоматизована система, метою якої є допомога людям, що приймають рішення у складних умовах для повного й об’єктивного аналізу предметної діяльності [4].

Як справедливо зауважено в [4], чіткого визначення СППР з моменту появи їх перших розробок так і не було сформульовано. Але слід зауважити, що усі ранні визначення СППР відображали наступні моменти:

1) можливість оперувати неструктурованими чи слабко структурованими задачами;

2) дослідження операцій;

3) інтерактивні автоматизовані системи;

4) розподіл даних і моделей.

Сучасні СППР – це системи, що максимально пристосовані до вирішення завдань повсякденної управлінської діяльності; інструмент, пристосований для надання допомоги особам, що приймають рішення (ОПР). СППР використовують матеріали баз даних не тільки у вигляді вихідних («сирих») даних, а й попередньо оброблених. Мета такої обробки полягає у тому, щоб зробити дані придатними і зручними для аналітичного використання різними групами користувачів та зберегти при цьому їх вихідну інформативність.

Можна навести деякі елементи і характеристики, загальновизнані як частини СППР. Turban [5] запропонував список характеристик ідеальної СППР:

1) оперує зі слабо структурованими рішеннями;

2) призначена для ОПР різного рівня;

3) може бути адаптована для групового та індивідуального використання;

4) підтримує як взаємозалежні, так і послідовні рішення;

5) підтримує три фази процесу рішення: інтелектуальну частину, проектування і вибір;

6) підтримує різноманітні стилі й методи рішення, що може виявитись корисним при вирішенні завдання групою ОПР;

7) є гнучкою і адаптується до змін як підприємства, так і його оточення;

8) проста у використанні і модифікації;

9) покращує ефективність процесу прийняття рішень;

10) дозволяє людині управляти процесом прийняття рішень за допомогою комп’ютера, а не навпаки;

11) може бути легко побудована, якщо може бути сформульована логіка конструкції СППР;

12) підтримує моделювання;

13) дозволяє використовувати знання.

Виходячи з принципів підтримки прийняття рішень, представляється доцільним визначити три класи СППР залежно від складності розв’язуваних завдань і областей застосування.

СППР першого класу, що володіють найбільшими функціональними можливостями, призначені для застосування в органах державного управління вищого рівня та органах управління великих компаній при плануванні великих комплексних програм для обґрунтування рішень щодо включення в програму різних заходів і розподілу між ними ресурсів на основі оцінки їх впливу на досягнення основної цілі програми. СППР цього класу є системами колективного користування, бази знань яких формуються багатьма експертами – фахівцями в різних галузях знань.

СППР другого класу є системами індивідуального користування, бази знань яких формуються безпосереднім користувачем. Вони призначені для використання державними службовцями середнього рангу, а також керівниками малих і середніх фірм для вирішення оперативних завдань управління.

СППР третього класу є системами індивідуального користування, що адаптуються до досвіду користувача. Вони призначені для рішення прикладних завдань системного аналізу та управління, що часто зустрічаються (наприклад, вибір суб’єкта кредитування, призначення на посаду та ін.)

Крім того, виділяють чотири види СППР залежно від їх архітектури та способу зберігання даних.

Функціональні СППР є найбільш простими з точки зору архітектури. Вони поширені в організаціях, що не ставлять перед собою глобальних завдань і мають невисокий рівень розвитку інформаційних технологій. Відмінною особливістю функціональних СППР є те, що аналізу піддаються дані, що містяться в операційних системах. Перевагами подібних СППР є компактність і оперативність у зв’язку з відсутністю необхідності перевантажування даних у спеціалізовану систему. З недоліків можна відзначити наступні: звуження кола питань,

що вирішуються за допомогою системи, збільшення навантаження на операційну систему.

СППР, що використовують незалежні вітрини даних застосовуються у великих організаціях, що мають декілька підрозділів, у тому числі відділи інформаційних технологій. Кожна конкретна вітрина даних створюється для вирішення певних завдань і орієнтована на окреме коло користувачів. Це значно підвищує продуктивність системи. З негативних моментів можна відзначити те, що дані багаторазово вводяться в різні вітрини, тому можуть дублюватися. Наповнення вітрин даних досить ускладнене у зв'язку з тим, що доводиться використовувати численні джерела. Відсутня єдина картина бізнесу організації, внаслідок того що немає остаточної консолідації даних.

СППР на основі дворівневого сховища даних використовуються у великих компаніях, дані яких консолідовані в єдину систему. Визначення і способи обробки інформації в цьому випадку уніфіковані. На забезпечення нормальної роботи подібної СППР потрібно виділити спеціалізовану команду, яка буде її обслуговувати. Така архітектура СППР позбавлена можливості структурування даних для окремих груп користувачів, а також обмеження доступу до інформації. Можливе виникнення труднощів з продуктивністю системи.

СППР на основі трьохрівневого сховища даних застосовують сховище даних, з якого формуються вітрини даних, що використовуються групами користувачів для вирішення подібних завдань. Таким чином, забезпечується доступ, як до конкретних структурованих даних, так і до єдиної консолідованої інформації. Такі СППР відрізняються гарантованою продуктивністю, але в них існує надмірність даних, яка веде до зростання вимог на їх зберігання. Крім того, необхідно узгодити подібну архітектуру з безліччю областей, що мають потенційно різні запити.

Для СППР відсутня єдина загальноприйнята класифікація. Проте різні автори [6-8] пропонують різні види та класифікації СППР. Зведемо їх до однієї.

1 На рівні користувача СППР поділяються на:

- пасивні – системи, які допомагають процесу прийняття рішення, але не можуть винести пропозицію, яке рішення прийняти;
- активні – системи, які можуть зробити пропозицію, яке рішення слід обрати;
- кооперативні СППР дозволяють ОПР змінювати, доповнювати або поліпшувати рішення, запропоновані системою, посилаючи потім ці зміни в систему для перевірки. Система змінює, доповнює або поліпшує ці рішення й посилає їх знову користувачеві. Процес продовжується до отримання узгодженого рішення.

2 На концептуальному рівні відрізняють:

- СППР, керовані повідомленнями (Communication-Driven DSS);
- СППР, керовані даними (Data-Driven DSS);
- СППР, керовані документами (Document-Driven DSS);
- СППР, керовані знаннями (Knowledge-Driven DSS);
- СППР, керовані моделями (Model-Driven DSS).

3 На технічному рівні розрізняють

- СППР усього підприємства – підключена до великих сховищ інформації й обслуговує багатьох менеджерів підприємства.
- настільна СППР – це мала система, що обслуговує лише один комп’ютер користувача.

4 Залежно від даних, з якими ці системи працюють, СППР умовно можна розділити на:

- Оперативні – призначені для негайного реагування на зміни поточної ситуації в управлінні фінансово – господарськими процесами компанії. Такі СППР отримали назву Інформаційні Системи Керівництва. По суті, вони являють собою кінцеві набори звітів, побудовані на підставі даних з транзакційної інформаційної системи підприємства.
- Стратегічні – орієнтовані на аналіз значних обсягів різнорідної інформації, яка збирається з різних джерел. Вони припускають досить глибоке опра-

цювання даних, спеціально перетворених так, щоб їх було зручно використовувати в ході процесу прийняття рішень. Невід'ємним компонентом СППР цього рівня є правила прийняття рішень, які на основі агрегованих даних дають можливість керівництву компанії обґрунтовувати свої рішення, використовувати фактори стійкого зростання бізнесу компанії і знижувати ризики, у тому числі ІБ. СППР другого типу останнім часом активно розвиваються.

2.2 Аналіз методів збору експертної інформації

Для реалізації завдань, поставлених в дипломній роботі треба обрати метод збору експертної інформації. Існує велика кількість методів збору експертної інформації. Для того, щоб вирішити цю задачу, потрібну проаналізувати основні методи експертизи. Всі методи експертизи поділяються на дві групи:

- індивідуальні методи експертизи;
- групові методи експертизи.

2.2.1 Індивідуальні методи експертизи

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

Індивідуальність полягає в тому, що експерти не збираються разом, не знайомляться з оцінками інших експертів, різних експертів можуть опитувати щодо різних аспектів однієї проблеми, також можуть бути різні і процедури опитування різних експертів. Найчастіше при індивідуальному експертному опитуванні використовуються такі методи [10]:

1) Стандартизоване експертне опитування. Даний метод вимагає від дослідницької команди попереднього чіткого структурування проблеми і визначення переліку всіх питань, на які повинні бути отримані однозначні відповіді. Для реалізації опитування розробляється стандартизована анкета з питаннями

закритого типу (з пропозицією варіантів відповіді). Анкетування може проводитися як при особистій бесіді інтерв'юера з експертом, так і шляхом "самозаполнения". У цьому випадку присутність інтерв'юера необов'язково, анкета може бути відправлена за звичайною або електронною поштою, проте потрібно висновок попередньої домовленості з експертом про опитування. Метод передбачає високу кваліфікацію фахівців-дослідників на етапі постановки завдання і планування дослідження, проте вельми простий в частині організації та проведення опитування, а також у частині обробки отриманої інформації. Вимоги до анкет (структура, формулювання питань і варіантів відповідей) досить стандартні і аналогічні вимогам, що пред'являються до опитувань не експертного рівня. Одна з основних вимог - використання загальноприйнятого професійної мови, однозначність трактування використовуваних термінів.

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

3) Метод "індивідуального блокнота". Метод являє собою заочну роботу експерта без безпосереднього спілкування з дослідниками. Експерт отримує блокнот, на першій сторінці якого описана проблема, і потім протягом обумовленого періоду часу (визначеного складністю проблеми і терміновістю її рішення) заносить в цей блокнот всі свої думки, ідеї, зауваження, що стосуються поставленого завдання, після чого здає блокнот дослідникам. Істотну складність представляє наступна обробка інформації та її інтерпретація. Метод вима-

гає значного залучення експерта і, отже, передбачає високий рівень оплати його праці.

2.2.2 Групові методи експертизи

На відміну від індивідуальних групові методи передбачають колективну роботу експертів (очну або заочну), вони вимагають узгодження думок всіх експертів і розробку загального експертного висновку на основі консенсусу. Групові методи краще з точки зору підвищення надійності експертизи, проте вони вельми складні з підготовки та проведення. Потрібні висококваліфіковані фахівці для розробки процедури групової взаємодії. Далеко не завжди вдається зібрати в один час і в одному місці необхідну кількість експертів, що відповідають потрібним вимогам [10-11].

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

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

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

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

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

3) Метод "635". Метод являє собою досить формалізовану варіацію методу мозкового штурму. Цей метод має на увазі наступну регламентацію роботи експертної команди: до групи входять 6 осіб, кожен з яких протягом 5 хвилин повинен висунути три пропозиції або висловити три гіпотези з приводу деякого аспекту розв’язуваної задачі або аналізованої ситуації. Ідеї кожного експерта заносяться в спеціальні формуляри, які передаються по колу. Після того як були розглянуті всі аспекти поставленого завдання і всі експерти отримали можливість висловитися, відбувається обговорення та оцінка рішень і вибір найбільш вірного.

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

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

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

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

8) Ділова гра. Метод може бути реалізований в різних формах. Найбільш поширена форма - моделювання аналізованих процесів і / або майбутнього розвитку прогнозованого явища в різних варіантах і розгляд отриманих даних. Розробка процедури проведення ділової гри - досить складне завдання, і їй має

бути приділено серйозну увагу. Мають бути чітко визначені і формально описані наступні елементи гри: цілі та завдання, ролі учасників, сюжет і регламент. Важливим етапом будь-якої ділової гри є рефлексія - розбір ходу гри і підведення підсумків. У даному випадку рефлексія полягає не тільки в аналізі самого ігрового процесу, а й в аналізі результатів моделювання досліджуваного явища.

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

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

11) "Колективний блокнот". Метод в основі своїй аналогічний "індивідуальним блокноту", проте в даному випадку блокноти отримують кілька експертів, кожен з яких знає, що він є учасником експертної групи. Можливий варіант, коли на початку роботи всі експерти збираються разом і їм розповідають про сутність виниклої проблеми і формулюють завдання. Далі кожен експерт працює зі своїм блокнотом протягом певного часу (при цьому також можливо, що різні експерти зосереджуються на різних сторонах проблеми). Другий етап реалізації експертизи полягає в тому, що блокноти збираються, інформація систематизується (дослідницької командою або керівником експертної групи) і далі в очному спільному обговоренні накопиченого і систематизованого матеріалу експерти приходять до вирішення проблеми.

12) Метод Дельфі. Метод являє собою заочний і анонімне опитування експертної групи в кілька турів з узгодженням думок експертів. Експертам про-

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

Проаналізувавши основні методи збору експертних оцінок, було обрано метод Дельфі. Він був обраний тому, що дає можливість проведення анонімного опитування з урахуванням кваліфікації експертів.

2.3 Розробка СППР

2.3.1 Підготовка даних для розробки СППР

Першим етапом розробки СППР було проаналізовано компоненти моделі загроз. На основі аналізу було побудовано можливі сценарії реалізації загроз.

Таблиця 2.1 – Можливі сценарії реалізації загроз

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

Продовження таблиці 2.1

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

Продовження таблиці 2.1

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

Продовження таблиці 2.1

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

Продовження таблиці 2.1

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

Продовження таблиці 2.1

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

Продовження таблиці 2.1

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

На другому етапі розробки СППР були розроблені питання щодо оцінки рівня небезпеки загроз інформаційних систем, спираючись на попередні результати. Перелік питань, що подається учаснику опитування, залежить від його посади. Дані розмежування представлені в таблиці 2.2.

Таблиця 2.2 – Питання до анкет

Питання	**Менеджер**	**Адміністратор безпеки**	**Системний адміністратор**	**Економіст/ аналітик**	**Програміст**	**Інші**
Охарактеризуйте рівень розвитку кримінальних структур району, де розташоване Ваше підприємство?	+	+	+	+	+	+
Чи є КЗ на підприємстві?	+	+	+	+	+	+
Як Ви оцінюєте привабливість для хакерів і потенційних злочинців Вашого підприємстві?	+	+	+	+	+	+
Охарактеризуйте сумлінність партнерів Вашого підприємства?	+	+	+	+	+	+
Як часто відвідують Ваше підприємство представники постачальників послуг	+	+	+	+	+	+
Як часто відвідують Ваше підприємство представники наглядових організацій та аварійних служб?	+	+	+	+	+	+
Який рівень конкуренції в сфері діяльності Вашого підприємства?	+	+	+	+	+	+

Продовження таблиці 2.2

Питання	Менеджер	Адміністратор безпеки	Системний адміністратор	Економіст/ аналітик	Програміст	Інші
Як Ви оцінюєте якість технічних засобів На Вашому підприємстві?	+	+	+	+	+	+
Як Ви оцінюєте якість програмних засобів На Вашому підприємстві?	+	+	+	+	+	+
Як Ви оцінюєте якість допоміжних засобів на Вашому підприємстві?	+	+	+	+	+	+
Як Ви оцінюєте можливість виявлення пошкодження огороджувальних конструкцій?	+	+	+	+	+	+
Дайте оцінку можливості нейтралізації пошкодження огороджувальних конструкцій?	+	+	+	+	+	+
Визначте потенційну небезпеку від пошкодження огороджувальних конструкцій?	+	+	+	+	+	+
Оцініть будь-ласка можливість виявлення закладних пристроїв на Вашому підприємстві?	+	+	+		+	
Як часто на Вашому підприємстві проводиться пошук закладних пристроїв?	+	+	+		+	
Яка на Вашу думку частота появи на Вашому підприємстві апаратних закладок?	+	+	+		+	
Як Ви оцінюєте потенційну небезпеку від витоку інформації через закладки?	+	+	+		+	
Дайте оцінку можливості виявлення підглядання за об’єктами, де циркулює ІзОД?	+	+	+	+	+	+
Як Ви оцінюєте можливість нейтралізувати підглядання за об’єктами, де циркулює ІзОД??	+	+	+	+	+	+
Як би Ви оцінили частоту підглядання за об’єктами, де циркулює ІзОД?	+	+	+	+	+	+
Оцініть будь-ласка потенційну небезпеку від прямої видимості об’єктів, де циркулює ІзОД?	+	+	+	+	+	+
Як би Ви оцінили можливість виявлення порушення режиму охорони об’єкта?	+	+	+	+	+	+
Охарактеризуйте можливість нейтралізувати порушення режиму охорони об’єкта?	+	+	+	+	+	+
Дайте оцінку частоти порушення режиму охорони об’єкта?	+	+	+	+	+	+

Продовження таблиці 2.2

Питання	Менеджер	Адміністратор безпеки	Системний адміністратор	Економіст/ аналітик	Програміст	Інші
Як Ви оцінюєте потенційну небезпеку від порушення режиму охорони об'єкта?	+	+	+	+	+	+
Оцініть будь-ласка можливість виявлення відмов і несправностей в технічних засобах, що забезпечують охорону і контроль доступу?		+	+		+	
Як би Ви охарактеризували можливість нейтралізації відмов і несправностей в технічних засобах, що забезпечують охорону і контроль доступу?		+	+		+	
Визначте будь-ласка частоту відмов і несправностей в технічних засобах, що забезпечують охорону і контроль доступу?		+	+		+	
Який на Вашу думку рівень потенційної небезпеку від відмов і несправностей в технічних засобах, що забезпечують охорону і контроль доступу?		+	+		+	
Охарактеризуйте частоту пошкодження огороджувальних конструкцій?	+	+	+	+	+	+
Як би Ви охарактеризували можливість виявлення перехоплення електромагнітних випромінювань на Вашому підприємстві?	+	+	+	+	+	+
Як Ви оцінюєте можливість нейтралізувати перехоплення електромагнітних випромінювань на Вашому підприємстві?	+	+	+	+	+	+
Оцініть частоту спроб перехопити електромагнітні випромінювання на Вашому підприємстві?	+	+	+	+	+	+
Який на Вашу думку рівень потенційної небезпеки від перехоплення електромагнітних випромінювань на Вашому підприємстві?		+	+		+	
Визначте можливість виявлення перехоплення електричних випромінювань на Вашому підприємстві?		+	+		+	
Охарактеризуйте можливість нейтралізувати перехоплення електричних випромінювань на Вашому підприємстві?		+	+		+	

Продовження таблиці 2.2

Питання	Менеджер	Адміністратор безпеки	Системний адміністратор	Економіст/ аналітик	Програміст	Інші
Як би Ви оцінили частоту спроб перехопити електричні випромінювання на Вашому підприємстві?		+	+		+	
Як Ви оцінюєте рівень потенційної небезпеки від перехоплення електричних випромінювань на Вашому підприємстві?		+	+		+	
Як би Ви охарактеризували можливість виявлення підслуховування?		+	+		+	
Визначте можливість нейтралізувати підслуховування.		+	+		+	
Оцініть частоту підслуховувань на Вашому підприємстві?		+	+		+	
Охарактеризуйте рівень потенційної небезпеки від підслуховувань.		+	+		+	
Охарактеризуйте можливість виявлення програмних закладок.		+	+		+	
Визначте можливість нейтралізувати програмні закладки.		+	+		+	
Дайте оцінку частоти появи на Вашому підприємстві програмних закладок.		+	+		+	
Оцініть потенційну небезпеку від програмних закладок.		+	+		+	
Як Ви оцінюєте можливість виявлення витоку інформації через елементи, що володіють електроакустичними перетвореннями?		+	+		+	
Визначте можливість нейтралізації витоку інформації через елементи, що володіють електроакустичними перетвореннями.		+	+		+	
Як часто, на Вашу думку, можливий витік інформації через елементи, що володіють електроакустичними перетвореннями?		+	+		+	
Охарактеризуйте потенційну небезпеку від витоку інформації через елементи, що володіють електроакустичними перетвореннями.		+	+		+	
Як би Ви оцінили можливість виявлення елементів повалених ВЧ нав’язуванням?		+	+		+	
Оцініть будь ласка можливість нейтралізації ВЧ нав’язуванням?		+	+		+	

Продовження таблиці 2.2

Питання	Менеджер	Адміністратор безпеки	Системний адміністратор	Економіст/ аналітик	Програміст	Інші
Дайте оцінку частоті можливого ВЧ нав'язування?		+	+		+	
Який на Вашу думку рівень потенційної небезпеки від ВЧ нав'язування?		+	+		+	
Як би Ви охарактеризували можливість виявлення нелегальних дій при використанні радіоканалів/глобальних інформаційних мереж?	+	+	+		+	
Як Ви оцінюєте можливість нейтралізації нелегальних дій при використанні радіоканалів/глобальних інформаційних мереж?	+	+	+		+	
Визначте частоту нелегальних дій при використанні радіоканалів/глобальних інформаційних мереж?	+	+	+		+	
Дайте оцінку рівня потенційної небезпеки від нелегальних дій при використанні радіоканалів/глобальних інформаційних мереж?	+	+	+		+	
Охарактеризуйте можливість виявлення помилок в ПО?		+	+	+	+	+
Оцініть можливість нейтралізації помилок в ПО?		+	+	+	+	+
Як Ви оцінюєте частоту виникнення помилок в ПО?		+	+	+	+	+
Як би Ви охарактеризували потенційну небезпеку від помилок в ПО?		+	+	+	+	+
Яка на Вашу думку можливість виявлення порушення режиму використання інформації?	+	+	+	+	+	+
Дайте оцінку можливості нейтралізації порушення режиму використання інформації?	+	+	+	+	+	+
Визначте частоту виникнення порушень режиму використання інформації?	+	+	+	+	+	+
Як би Ви оцінили потенційну небезпеку від порушення режиму використання інформації?	+	+	+	+	+	+
Охарактеризуйте можливість виявлення відмов і несправностей технічних засобів?	+	+	+	+	+	+
Оцініть можливість нейтралізації відмов і несправностей технічних засобів?	+	+	+	+	+	+

Продовження таблиці 2.2

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

Продовження таблиці 2.2

Питання	Менеджер	Адміністратор безпеки	Системний адміністратор	Економіст/ аналітик	Програміст	Інші
Оцініть можливість виявлення порушення режиму експлуатації технічних засобів.		+	+		+	
Дайте оцінку можливості нейтралізації порушення режиму експлуатації технічних засобів.		+	+		+	
Визначте частоту порушення експлуатації технічних засобів.		+	+		+	
Охарактеризуйте потенційну небезпеку від порушення режиму експлуатації технічних засобів.		+	+		+	
Оцініть можливість виявлення збоїв електропостачання.	+	+	+	+	+	+
Охарактеризуйте можливість нейтралізації збоїв електропостачання.	+	+	+	+	+	+
Як би Ви оцінили частоту збоїв електропостачання?	+	+	+	+	+	+
Визначте потенційну небезпеку від збоїв електропостачання?	+	+	+	+	+	+
Як Ви оцінюєте можливість виявлення старіння та розмагнічування носіїв інформації?		+	+		+	
Охарактеризуйте можливість нейтралізації старіння та розмагнічування носіїв інформації.		+	+		+	
Оцініть частоту виникнення проблем через старіння та розмагнічування носіїв інформації.		+	+		+	
Дайте оцінку рівня потенційної небезпеки від старіння і розмагнічування носіїв інформації.		+	+		+	
Як Ви оцінюєте можливість виявлення пошкодження життєзабезпечуючих комунікацій?	+	+	+	+	+	+
Визначте можливість нейтралізації пошкодження життєзабезпечуючих комунікацій.	+	+	+	+	+	+
Дайте оцінку частоти пошкоджень життєзабезпечуючих комунікацій.	+	+	+	+	+	+
Оцініть рівень потенційної небезпеки від пошкоджень життєзабезпечуючих комунікацій.	+	+	+	+	+	+
Як Ви оцінюєте можливість виявлення виникнення пожежі?	+	+	+	+	+	+
Охарактеризуйте можливість нейтралізації виникнення пожежі.	+	+	+	+	+	+

Продовження таблиці 2.2

Питання	Менеджер	Адміністратор безпеки	Системний адміністратор	Економіст/ аналітик	Програміст	Інші
Як часто виникають пожежі на Вашому підприємстві?	+	+	+	+	+	+
Як Ви оцінюєте потенційну небезпеку від пожежі на Вашому підприємстві?	+	+	+	+	+	+
Визначте можливість виявлення пожежі в районі, де знаходиться підприємство?	+	+	+	+	+	+
Як Ви оцінюєте можливість нейтралізації пожежі в районі, де знаходиться підприємство?	+	+	+	+	+	+
Яка на Вашу думку частота пожеж в районі, де знаходиться підприємство?	+	+	+	+	+	+
Охарактеризуйте потенційну небезпеку для Вашого підприємства від пожежі в районі, де воно знаходиться?	+	+	+	+	+	+
Як Ви оцінюєте можливість стихійного лиха в районі де знаходиться Ваше підприємство?	+	+	+	+	+	+
Як Ви оцінюєте можливість відновлення працездатності підприємства після стихійного лиха?	+	+	+	+	+	+
Охарактеризуйте частоту можливих стихійних лих в районі де знаходиться Ваше підприємство.	+	+	+	+	+	+
Визначте потенційну небезпеку для Вашого підприємства від стихійних лих в районі де знаходиться Ваше підприємство.	+	+	+	+	+	+
Дайте оцінку можливості виявити непередбачувані обставини?	+	+	+	+	+	+
Охарактеризуйте можливість нейтралізації непередбачуваних обставин?	+	+	+	+	+	+
Визначте частоту непередбачуваних обставин?	+	+	+	+	+	+
Як Ви оцінюєте потенційну небезпеку від непередбачуваних явищ?	+	+	+	+	+	+
Дайте оцінку можливості виявити нез’ясовані явища?	+	+	+	+	+	+
Охарактеризуйте можливість нейтралізації нез’ясованих явищ?	+	+	+	+	+	+
Визначте частоту нез’ясованих явищ?	+	+	+	+	+	+
Як Ви оцінюєте потенційну небезпеку від нез’ясованих явищ?	+	+	+	+	+	+
Дайте оцінку можливості виявити форс-мажорних обставин?	+	+	+	+	+	+

Продовження таблиці 2.2

Питання	Менеджер	Адміністратор безпеки	Системний адміністратор	Економіст/ аналітик	Програміст	Інші
Охарактеризуйте можливість нейтралізації форс-мажорних обставин?	+	+	+	+	+	+
Визначте частоту форс-мажорних обставин?	+	+	+	+	+	+
Як Ви оцінюєте потенційну небезпеку від форс-мажорних обставин?	+	+	+	+	+	+

Для визначення рівня впливу кваліфікації працівника на результати опитування була розроблена система вагових коефіцієнтів, що залежить від посади, досвіду роботи і освіти. Приклади коефіцієнтів подані у таблиці 2.3.

Таблиця 2.3 – Критерії визначення кваліфікації учасника опитування

Оцінюваний атрибут	Значення атрибуту	Числове значення
Посада	Менеджер	1,1
	Адміністратор безпеки	1,3
	Системний адміністратор	1,2
	Програміст	1,1
	Економіст	0,85
	Аналітик	0,9
	Інша посада	0,75
Стаж роботи на даному підприємстві	до 6 місяців	0,1
	6-12 місяців	0,2
	до 2 років	0,3
	до 5 років	0,4
	більше 5 років	0,5
Попередній стаж роботи в області ІБ	до 6 місяців	0,1
	6-12 місяців	0,2
	до 2 років	0,3
	до 5 років	0,4
	більше 5 років	0,5
Напрям освіта	В сфері ІБ	0,5
	В сфері ІТ	0,4
	Технічна освіта	0,3
	Інший напрям	0,2

Продовження таблиці 2.3

Оцінюваний атрибут	Значення атрибуту	Числове значення
Рівень освіти	Повна вища	0,5
	Неповна вища	0,4
	Базова вища	0,3
	Середня	0,2

Наступним етапом було створення критеріїв формалізації відповідей працівників про реалізацію загроз. Отримані результати надано в таблиці 2.4.

Таблиця 2.4 – Числові інтерпретації відповідей працівника про реалізацію загроз

Оцінюваний атрибут	Значення атрибуту	Числове значення
Можливість виявлення	Легко	1
	Можуть виникнути проблеми з виявленням	2
	Складно	3
	Дуже складно	4
	Неможливо	5
Можливість нейтралізації	Легко	1
	Нескладно	2
	Складно	3
	Дуже складно	4
	Неможливо	5
Частота	Раз на годину	5
	Раз на день	4
	Раз на тиждень	3
	Раз на місяць	2
	Раз в півроку та більш рідко	1
Потенційна небезпека	Дуже висока	5
	Висока	4
	Середня	3
	Низька	2
	Дуже низька	1

На четвертому етапі для оцінки атрибутів розробленої системи було обрано метод опитування. За допомогою опитування будуть визначатися характеристики атрибутів. В опитувальниках буде використано мінімальна опис атрибутів і одночасно цей опис буде максимально зрозумілим для персоналу. Опираючись на літературні джерела про побудову опитувальників [9] , були сформовані питання та відповіді таким чином, щоб всім працівникам було максима-

льно зрозуміло. Для окремих груп респондентів були створені окремі опитувальники, відповідно до їх посад. Це організовано через розроблення матриці запитань, яка розподіляє питання в відповідності до займаної посади. Таблиця з питаннями і матрицею питань представлені в табл. 2.2.

2.3.2 Розробка алгоритму роботи СППР

Проаналізувавши основні види СППР, були сформовані вимоги до неї. Серед яких:

- база знань заноситься до програми на етапі її розробки;
- дані повинні зберігатися в самій програмі для зменшення навантаження на технічні засоби при проведенні розрахунків, що являє собою зменшення споживаних часових ресурсів;
- це повинна бути система, яка буде надавати потрібний об’єм інформації для прийняття рішення в питаннях інформаційної безпеки;
- система має бути комплексною, оцінювати весь спектр загроз ІБ і задіювати значну частину персоналу.

Для рішення задачі дипломної роботи було обрано спосіб ризик-орієнтованої оцінки. Цей вибір був зроблений через необхідність використання розробленої системи на підприємствах різного типу.

Алгоритм розробленої системи складається з наступних етапів. Розглянемо їх детально.

1) Визначення ступеня кваліфікованості працівника у сфері ІБ.

Виходячи з відповідей працівників система отримує їх ваговий коефіцієнт. Перелік питань, на які запропоновано відповісти працівнику:

- Ваше прізвище, ім’я та по-батькові?
- Посада, яку ви займаєте?
- Стаж роботи на даному підприємстві?

- Попередній стаж роботи?
- Освіта?
- Спеціальність?

Ваговий коефіцієнт працівника розраховується за формулою (2.1):

$$R = \sum_{i=1}^{n} r_i, \quad (2.1)$$

де R – ваговий коефіцієнт працівника підприємства;

r – атрибут, що визначає кваліфікацію учасника опитування у сфері ІБ;

n – кількість атрибутів.

2) Проведення опитування респондентів

Після другого пункту цього етапу працівнику пропонується дати відповіді на питання шляхом вибору одного з запропонованих варіантів відповіді. Відповідно до посади і таблиці 2.2 та таблиці 2.4

3) Перевірка наявності відповідей на всі питання та відповідність цих відповідей визначеним варіантам.

Після заповнення анкети працівником, аудитор перевіряє наявність відповідей на кожне питання і на відповідність цієї відповіді еталону.

4) Узагальнення результатів

СППР, використовуючи ваговий коефіцієнт працівника, узагальнює всі отримані результати. Це відбувається за формулами (2.2) і (2.3):

$$U = \frac{R \cdot \sum_i u_i}{i}, \quad (2.2)$$

де U – середнє арифметичне зважене атрибуту джерела загроз;

u – інтерпретоване в числове значення відповіді працівника;

i – кількість атрибутів.

$$X = \frac{R \cdot \sum_i x_i}{i}, \quad (2.3)$$

де X – середнє арифметичне зважене атрибуту вразливості;

x – інтерпретоване в числове значення відповіді працівника;

i – кількість атрибутів.

5) Визначення рівня небезпеки.

Узагальнивши всі отримані результати, СППР переходить до визначення рівня небезпеки кожного з сценаріїв можливий атак. Це відбувається за формулою (2.4):

$$N = U \cdot \sum X_i, \tag{2.4}$$

де N – значення рівня небезпеки.

6) Отримання кінцевого результату.

СППР заносить отримані значення на попередньому кроці до підготовленої таблиці. Вихідні дані представлені у таблиці 2.5

Таблиця 2.5 – Вихідні дані

Джерело загрози	**Вразливості**		**Загроза**	**Рівень небезпеки**
І.А. Кримінальні структури	Об'єктивні	Апаратні закладки	Розкрадання	129,13
		Обумовлені місцем розташування об'єкта	Розкрадання, знищення, блокування	139,06
	Суб'єктивні	Порушення режиму захисту і охорони	Розкрадання, знищення, блокування	139,06
	Випадкові	Відмови і несправності технічних засобів(що забезпечують охорону)	Розкрадання, знищення, блокування	99,33
		Пошкодження огороджувальних конструкцій	Розкрадання, знищення, блокування	89,40
І.А. Потенційні злочинці і хакери	Об'єктивні	Електромагнітні випромінювання	Розкрадання	34,77
		Електричні випромінювання	Розкрадання	49,67
		Звукові випромінювання	Розкрадання	59,60

Продовження таблиці 2.5

Джерело загрози	**Вразливості**		**Загроза**	**Рівень небезпеки**
		Апаратні закладки	Розкрадання	64,56
		Програмні закладки	Розкрадання, знищення, модифікація, блокування	59,60
		Елементи що володіють електроакустичними перетвореннями	Розкрадання	49,67
		Елементи схильні до дії електромагнітного поля	Розкрадання	54,63
		Обумовлені організацією каналів обміну інформації	Розкрадання, знищення, модифікація, блокування, нав’язування неправдивої інформації	49,67
	Суб’єктивні	Помилки при підготовці та використанні програмного забезпечення	Розкрадання, модифікація	59,60
		Порушення режиму використання інформації	Розкрадання	54,63
	Випадкові	Відмови і несправності технічних засобів	Розкрадання, знищення, модифікація, блокування, нав’язування	54,63
		Збої ПЗ	Розкрадання, модифікація	129,13
І.А. Несумлінні партнери	Об’єктивні	Апаратні закладки	Розкрадання	258,26
		Програмні закладки	Розкрадання, модифікація	238,39
		Обумовлені місцем розташування об’єкта	Розкрадання, знищення, блокування	278,13
		Обумовлені організацією каналів обміну інформації	Розкрадання, блокування	198,66
	Суб’єктивні	Порушення режиму використання інформації	Розкрадання, модифікація	218,53
		Порушення режиму конфіденційності	Розкрадання	238,39
	Випадкові	Збої ПЗ	Розкрадання, модифікація	258,26

Продовження таблиці 2.5

Джерело загрози	**Вразливості**		**Загроза**	**Рівень небезпеки**
І.А. Технічний персонал постачальників телематичних послуг	Об'єктивні	Апаратні закладки	Розкрадання	193,69
		Програмні закладки	Розкрадання, модифікація	178,80
		Елементи що володіють електроакустичними перетвореннями	Розкрадання	149,00
		Обумовлені організацією каналів обміну інформації	Розкрадання, блокування, відмова	149,00
	Суб'єктивні	При підготовці та використанні програмного забезпечення	Розкрадання, знищення	178,80
		Порушення режиму охорони та захисту	Розкрадання, знищення, модифікація, нав'язування неправдивої інформації	208,59
	Випадкові	Відмови і несправності технічних засобів	Розкрадання, нав'язування неправдивої інформації	163,90
		Пошкодження огороджуючих конструкцій	Розкрадання	134,10
І.А. Представники наглядових організацій та аварійних служб	Об'єктивні	Апаратні закладки	Розкрадання	64,56
	Суб'єктивні	Порушення режиму охорони та захисту	Розкрадання, знищення, модифікація, нав'язування неправдивої інформації	69,53
	Випадкові	Пошкодження огороджуючих конструкцій	Розкрадання	44,70
І.А. Представники силових структур	Об'єктивні	Електромагнітні випромінювання	Розкрадання	34,77
		Електричні випромінювання	Розкрадання	49,67
		Звукові випромінювання	Розкрадання	59,60
		Апаратні закладки	Розкрадання	64,56
		Елементи схильні до дії електромагнітного поля	Розкрадання	54,63
		Обумовлені місцем розташування об'єкта	Розкрадання, знищення, блокування	69,53
		Обумовлені організацією каналів обміну інформації	Розкрадання, блокування	49,67

Продовження таблиці 2.5

Джерело загрози	Вразливості		Загроза	Рівень небезпеки
	Суб'єктивні	Порушення режиму охорони та захисту	Розкрадання, знищення, модифікація, нав'язування неправдивої інформації	69,53
	Випадкові	Пошкодження огороджуючих конструкцій	Розкрадання	44,70
І.А. Конкуренти	Об'єктивні	Електромагнітні випромінювання	Розкрадання	13,93
		Електричні випромінювання	Розкрадання	19,90
		Звукові випромінювання	Розкрадання	23,88
		Апаратні закладки	Розкрадання	25,87
		Обумовлені місцем розташування об'єкта	Розкрадання, знищення, блокування	27,86
		Обумовлені організацією каналів обміну інформації	Розкрадання, блокування	19,90
	Суб'єктивні	Порушення режиму охорони та захисту	Розкрадання, знищення, модифікація, нав'язування неправдивої інформації	27,86
	Випадкові	Пошкодження огороджуючих конструкцій	Розкрадання	17,91
І.В. Основний персонал	Об'єктивні	Апаратні закладки	Розкрадання	109,76
		Програмні закладки	Розкрадання, модифікації, блокування	101,32
	Суб'єктивні	Помилки при підготовці та використанні програмного забезпечення	Розкрадання, модифікації, блокування	101,32
		Помилки при управлінні складними системами	Блокування, нав'язування неправдивої інформації	75,99
		Помилки при експлуатації технічних засобів	Розкрадання, блокування	118,20
		Порушення режиму охорони та захисту	Розкрадання, знищення	118,20
		Порушення режиму експлуатації технічних засобів	Блокування	101,32
		Порушення режиму використання інформації	Розкрадання, модифікація	92,87
		Порушення режиму конфіденційності	Розкрадання	101,32

Продовження таблиці 2.5

Джерело загрози	**Вразливості**		**Загроза**	**Рівень небезпеки**
	Випадкові	Збої ПЗ	Розкрадання, модифікація, блокування	109,76
		Пошкодження огороджувальних конструкцій	Розкрадання	75,99
І.В. Представники служби захисту інформаці	Об’єктивні	Апаратні закладки	Розкрадання	109,76
		Програмні закладки	Розкрадання, модифікації, блокування	101,32
	Суб’єктивні	Помилки при підготовці та використанні програмного забезпечення	Розкрадання, модифікації, блокування	101,32
		Помилки при управлінні складними системами	Блокування, нав’язування неправдивої інформації	75,99
		Помилки при експлуатації технічних засобів	Розкрадання, блокування	118,20
		Порушення режиму охорони та захисту	Розкрадання, знищення	118,20
		Порушення режиму експлуатації технічних засобів	Блокування	101,32
		Порушення режиму використання інформації	Розкрадання, модифікація	92,87
		Порушення режиму конфіденційності	Розкрадання	101,32
І.В. Допоміжний персонал	Об’єктивні	Апаратні закладки	Розкрадання	109,76
	Суб’єктивні	Порушення режиму охорони та захисту	Розкрадання	118,20
		Порушення режиму експлуатації технічних засобів	Розкрадання	101,32
		Порушення режиму використання інформації	Розкрадання	92,87
		Порушення режиму конфіденційності	Розкрадання	101,32
І.В. Технічний персонал	Об’єктивні	Апаратні закладки	Розкрадання	109,76
	Суб’єктивні	Помилки при експлуатації технічних засобів	Розкрадання, блокування	118,20
		Порушення режиму використання інформації	Розкрадання	92,87
		Порушення режиму конфіденційності	Розкрадання	101,32

Продовження таблиці 2.5

Джерело загрози	**Вразливості**		**Загроза**	**Рівень небезпеки**
	Випадкові	Пошкодження огороджувальних конструкцій	Розкрадання	75,99
II. А. Засоби зв'язку	Об'єктивні	Електромагнітні випромінювання	Розкрадання	139,06
		Електричні випромінювання	Розкрадання	198,66
		Звукові випромінювання	Розкрадання	238,39
	Випадкові	Збої електропостачання	Блокування	238,39
II. А. Мережі інженерних комунікацій	Об'єктивні	Електромагнітні випромінювання	Розкрадання	173,83
		Електричні випромінювання	Розкрадання	248,33
		Звукові випромінювання	Розкрадання	297,99
		Обумовлені місцем розташування об'єкта	Розкрадання	347,66
II. А. Транспорт	Об'єктивні	Обумовлені місцем розташування об'єкта	Блокування	69,53
II. В. Неякісні технічні засоби обробки інформації	Об'єктивні	Електромагнітні випромінювання	Розкрадання, модифікація	139,06
		Електричні випромінювання	Розкрадання, модифікація	198,66
		Елементи схильні до дії електромагнітного поля	Розкрадання, знищення	218,53
	Суб'єктивні	Помилки при підготовці та використанні ПЗ	Модифікація, блокування	238,39
		Помилки при управлінні складними системами	Модифікація, блокування	178,80
		Помилки при експлуатації технічних засобів	Модифікація, блокування	278,13
		Порушення режиму експлуатації технічних засобів	Блокування	238,39
	Випадкові	Відмови і несправності технічних засобів	Блокування	218,53
		Старіння та розмагнічування носіїв інформації	Знищення	218,53

Продовження таблиці 2.5

Джерело загрози	Вразливості		Загроза	Рівень небезпеки
		Збої електропостачання	Знищення, блокування	238,39
		Пошкодження життєзабезпечуючих комунікацій	Знищення, блокування	238,39
II. А. Неякісні програмні засоби обробки інформації	Суб'єктивні	Помилки при підготовці та використанні ПЗ	Розкрадання, модифікація, блокування	119,20
		Помилки при управлінні складними системами	Модифікація, блокування	89,40
		Помилки при експлуатації технічних засобів	Модифікація, блокування	139,06
		Порушення режиму використання інформації	Модифікація, блокування	109,26
		Порушення режиму конфіденційності	Розкрадання	119,20
		Збої ПЗ	Блокування	129,13
Допоміжні засоби	Об'єктивні	Звукові випромінювання	Розкрадання	119,20
		Елементи що володіють електроакустичними перетвореннями	Розкрадання	99,33
		Елементи схильні до дії електромагнітного поля	Розкрадання	109,26
	Суб'єктивні	Порушення режиму експлуатації технічних засобів	Розкрадання, блокування	119,20
II. А. Інші технічні засоби, що застосовуються в установі	Об'єктивні	Електромагнітні випромінювання	Розкрадання	69,53
		Електричні випромінювання	Розкрадання	99,33
		Звукові випромінювання	Розкрадання	119,20
		Елементи що володіють електроакустичними перетвореннями	Розкрадання	99,33
		Елементи схильні до дії електромагнітного поля	Розкрадання	109,26
	Суб'єктивні	Помилки при експлуатації технічних засобів	Блокування	139,06
		Порушення режиму експлуатації технічних засобів	Блокування	119,20

Продовження таблиці 2.5

Джерело загрози	**Вразливості**		**Загроза**	**Рівень небезпеки**
	Випадкові	Відмови і несправності технічних засобів	Блокування	109,26
III. А. Пожежі	Випадкові	Порушення режиму охорони і захисту	Розкрадання, знищення	122,57
		Обумовлені місцем розташування об’єкта	Знищення, блокування	122,57
III. А. Землетрус, повінь, ураган	Об’єктивні	Обумовлені місцем розташування об’єкта	Знищення, блокування	133,71
III. А. Різні непередбачувані обставини	Об’єктивні	Обумовлені місцем розташування об’єкта	Знищення, блокування	122,57
III. А. Нез’ясовані явища	Об’єктивні	Обумовлені місцем розташування об’єкта	Знищення, блокування	133,71
III. А. Інші форс-мажорні обставини	Об’єктивні	Обумовлені місцем розташування об’єкта	Знищення, блокування	122,57

Вихідні значення оцінюються відповідно до школи критичності, яка представлена в таблиці 2.6.

Таблиця 2.6 – Шкала критичності загроз

Низький рівень загрози	Рівень загрози нижче середнього	Середній рівень загрози	Рівень загрози вище середнього	Високий рівень загрози	Критична загроза	Катастрофічна загроза
0-40	41-80	81-110	111-135	136-165	166-185	186-200

2.4 Модель процесу підтримки прийняття рішень

Виходячи з загального виду процесу і елементів процесу представлений в першому розділі на рис 1.1 і рис. 1.2 було побудовано модель процесу роботи СППР, яка представлена на рис. 2.1.

Отримана модель складається з:

- вхідних даних, які включають в себе призначення СППР, об’єкти дослідження і вид оцінки;
- фактори, котрі впливають на процес оцінки, які включають в себе модель, критерії і обмеження по ролям;
- процесів, що відбуваються в самій програмі;
- вихідних даних, які представлені в нашій СППР сформованою моделлю загроз.

Рисунок 2.1 – Модель СППР

2.5 Задачі та функціональні можливості системи підтримки прийняття рішень для оцінки загроз інформаційній безпеці

Дана робота присвячена опису системи підтримки прийняття рішень для оцінки загроз інформаційній безпеці.

Керуючись класифікацією, наданою у підрозділі 2.1, на рівні користувача подана система відноситься до пасивних – систем, які допомагають процесу прийняття рішення, але не можуть винести пропозицію, яке рішення прийняти. На концептуальному рівні ця система керована знаннями. Крім того, на техніч-

ному рівні систему, що розглядається, можна віднести до настільних (обслуговує лише один комп'ютер користувача). Залежно від даних, з якими працює система, СППР можна віднести до стратегічних – орієнтовані на аналіз значних обсягів різнорідної інформації, яка збирається з різних джерел.

СППР володіє такими функціональними можливостями:

- на підставі інформації про працівників, такої як посада; досвід; освіта; формує ваговий коефіцієнт кожного працівника;
- ґрунтуючись на інформації отриманій від персоналу підприємства методом анкетування розраховує значення атрибутів моделі загроз;
- враховуючи інформацію про значення атрибутів формується список загроз ранжируваний по рівню небезпеки.

2.6 Апробація розробленої СППР

Апробацію розробленої СППР було проведено на приватному комерційному підприємстві.

Розглянутий об'єкт є сервісним центром з ремонту побутової техніки

Так як діяльність підприємства не пов'язана з прямим виробництвом товарів, а лише їх обслуговуванням, графік роботи підприємства для більшості співробітників з 09.00 до 18.00. Також діяльність підприємства передбачає роботу з клієнтами, а значить, передбачає, що в робочий час можливе знаходження на території об'єкта осіб, які не працюють на виробництві.

На підприємстві відсутні відомості, що становлять державну таємницю, але ведеться робота з комерційною таємницею і конфіденційною інформацією.

Розроблена СППР була впроваджена на підприємстві. До анкетування були залучені 10 співробітників даного підприємства. Серед них:

- директор підприємства – 1 люд.;
- системний адміністратор – 1 люд;
- бухгалтер – 2 люд.;

- аналітик – 1 люд.;
- програміст – 2 люд.;
- менеджер – 3 люд.

Персонал був ознайомлений з правилами заповнення анкет і пройшов тестування. В результаті було отримано ранжований список з 10 найбільш критичних загроз, представлено в таблиці 2.7 і рекомендовано забезпечити захист від даних загроз.

Таблиця 2.7 – Результати апробації

Джерела загроз	**Вразливості інформаційної системи**	**Загрози інформації**	**Рівень небезпеки**
I.A. Несумлінні партнери	Програмні закладки	Розкрадання, модифікація	**161,4**
I.A. Технічний персонал постачальників послуг	Порушення режиму охорони та захисту	Розкрадання, знищення, модифікація, нав'язування неправдивої інформації	**152, 4**
I.A. Несумлінні партнери	Апаратні закладки	Розкрадання	**150,8**
I.A. Потенційні злочинці і хакери	Програмні закладки	Розкрадання, знищення, модифікація, блокування	**147,6**
I.B. Основний персонал	Порушення режиму використання інформації	Розкрадання, модифікація	**130,7**
I.A. Технічний персонал постачальників послуг	Апаратні закладки	Розкрадання	**123,7**
I.B. Технічний персонал	Порушення режиму використання інформації	Розкрадання	**120,2**
I.A. Потенційні злочинці і хакери	Порушення режиму використання інформації	Розкрадання	**109,8**
I.B. Основний персонал	Порушення режиму конфіденційності	Розкрадання	**101,32**
I.A. Потенційні злочинці і хакери	Звукові випромінювання	Розкрадання	**90,6**

2.7 Висновок

В цьому розділі для вирішення задач дипломної роботи було проаналізовано основні СППР і методи врахування експертних оцінок. Аналіз дав можливість сформулювати необхідні вимоги до СППР і методу врахування експертних оцінок. На основі результатів аналізу було розроблено алгоритм роботи і модель СППР, на основі яких розроблений програмний комплекс підтримки прийняття рішень щодо оцінки рівнів небезпеки загроз інформаційній безпеці підприємства.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Вступ

Апробацію розробленої СППР було проведено на малому приватному комерційному підприємстві ТОВ «Альва сервіс», що займається ремонтом побутової техніки за адресою м. Дніпро, вул. Грушевського 14.

На підприємстві відсутні відомості, що становлять державну таємницю, але ведеться робота з комерційною таємницею і конфіденційною інформацією.

Розроблена СППР була впроваджена на підприємстві. До анкетування були залучені 10 співробітників даного підприємства. Серед них:

- директор підприємства – 1 люд.;
- системний адміністратор – 1 люд;
- бухгалтер – 2 люд.;
- аналітик – 1 люд.;
- програміст – 2 люд.;
- менеджер з обслуговування клієнтів (майстер) – 3 люд.

Запропонований ранжований список з 10 найбільш критичних загроз представлено в табл. 2.7.

3.2 Визначення трудомісткості розробки СППР для оцінки загроз інформаційної безпеки підприємства (анкетування)

Трудомісткість створення системи підтримки прийняття рішень визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста):

$$t = t_{mз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{д} = 20+72+72+168+72+72=476 \text{ годин}, \quad (3.1)$$

де $t_{mз}$ = 20 – тривалість складання технічного завдання на розробку СППР;

$t_{в}$ = 72 – тривалість вивчення ТЗ, літературних джерел за темою тощо;

$t_{а}$ = 72 – тривалість розробки блок-схеми алгоритму;

$t_{пр}$ = 168 – тривалість програмування за готовою блок-схемою;

$t_{опр}$ = 72 – тривалість опрацювання програми на ПК;

$t_{д}$ = 72 – тривалість підготовки технічної документації на ПЗ.

Витрати на створення СППР Ксппр складаються з витрат на заробітну плату виконавця СППР Ззп і вартості витрат машинного часу, що необхідний для опрацювання системи на ПК Змч:

$$К_{сппр} = З_{зп} + З_{мч}=11640+1091=12731. \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування єдиного соціального внеску (22%) и визначається за формулою:

$$З_{ЗП} = t \cdot З_{пр} =476*24,40=11\ 640, \text{ грн}, \quad (3.3)$$

де t = 476 – загальна тривалість створення СППР, годин

$З_{пр}$ = 24,4 – мінімальна заробітна плата спеціаліста з нарахуваннями, грн/годину.

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

$$З_{мч} = t \cdot С_{мч} =476*2,29=1091, \text{ грн}, \quad (3.4)$$

де $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_{д}$ – трудомісткість підготовки документації на ПК, годин;

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

Ліцензійного програмного забезпечення не потрібно. Всі розрахунки виконувались на безкоштовному програмного забезпеченні Office 365. Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = Р \cdot t_{нал} \cdot С_{е} + \frac{Ф_{зал} \cdot Н_{а}}{F_{р}} = =(0,6*1.65)+(5000*0,5)/1920=2.29 \text{ грн,/год} \quad (3.5)$$

де P = 0,6 –встановлена потужність ПК, кВт;

$С_{е}$ = 1,65 – тариф на електричну енергію, грн/кВт*година;

$Ф_{зал}$ = 5000 – залишкова вартість ПК на поточний рік, грн.;

$Н_{а}$ = 0,5 – річна норма амортизації на ПК, частки одиниці;

F_p = 1920 – річний фонд робочого часу (за 40-годинного робочого тижня F_p = 1920).

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

Визначена таким чином вартість створення СППР (Ксппр) є частиною одноразових капітальних витрат, що може бути використана на будь-якої кількості підприємств.

3.3 Визначення витрат на проведення анкетування на підприємстві

Для проведення анкетування необхідно 1 година робочого часу всіх співробітників, що будуть опитуватися. Годинна заробітна плата цих співробітників наведена у табл. 3.1.

Про проведення анкетування по СППР підприємство буде оплачувати простої працівників за звичайним тарифом з урахуванням кількості задіяних робітників та податків, що необхідно донараховувати до заробітної плати. Ці витрати повинні враховуватися як вартість впровадження запропонованої СППР.

Таблиця 3.1 – Розрахунок витрат на опитування

Посади співробітників	Кількість, люд.	Місячний оклад	Годинна заробітна платня, грн./год	Вартість опитування з урахуванням простою та податків, грн
директор підприємства	1	10000	62,50	76,25
системний адміністратор	1	8500	53,125	64,18
бухгалтер	2	6000	37,50	91,5
аналітик	1	6500	49,56	60,49
програміст	2	8500	53,125	129,63
менеджер з обслуговування клієнтів (майстер)	3	7500	46,88	171,56
Всього				595

Використання запропонованої СППР дозволить зекономити на розробці системи інформаційної безпеки в цілому на підприємстві. Так за результатами анкетування найбільшим джерелом загрозу представляють несумлінні партнери і технічний персонал постачальників послуг (див. табл. 2.7).

3.4 Економічне обґрунтування використання СППР

Економічний ефект від використання даного програмного продукту полягає в тому, що підприємство може не використовувати інші комерційні та державні структури при проведенні експертної оцінки інформаційної безпеки на своєму підприємстві. Так при користування послугами ДП "Українські спеціальні системи" економічний ефект буде досягнений при умові, що вартість їх послуг буде більше ніж 595+ 12721 = 13316 грн.

Якщо вартість експертної оцінки інформаційної безпеки спеціалістів ДП "Українські спеціальні системи" буде коштувати менше, то розробка та проведення СППР окупляться при проведенні експертної оцінки у декількох підприємств. Розрахунки наведені у табл.3.2.

Таблиця 3.2 – Розрахунок терміну окупності запропонованої СППР

Вартість послуг сторонньої компанії, грн.	Вартість проведення експертної оцінки з урахуванням частки вартості розробки СППР, грн	Кількість підприємств
1000	595+405, де 405 = 12721/32	32
1500	595+905, де 905 =12721/15	15
1800	595+1205, де 1205 = 12721/11	11

3.5 Висновки

В Економічному розділі було приведено обґрунтування економічної доцільності розробки та впровадження СППР. Капітальні витрати становлять приблизно 12721 грн. Вартість проведення експертного опитування на малому комерційному підприємстві склала 595 грн.

При вартості експертної оцінки 1500 грн., що буде проведена сторонньою компанією, запропонована СППР окупиться при проведенні аналогічного по собівартості анкетування у 15 підприємств.

ВИСНОВКИ

Підчас виконання дипломної роботи проаналізовано методи оцінки стану ІБ та принципи побудови моделі загроз. В результаті були побудовані сценарії реалізації загроз ІБ. Зважаючи на великий обсяг інформації та різних факторів, які необхідно враховувати при оцінці ризиків реалізації загроз, актуальним є застосування системи підтримки прийняття рішень (СППР).

Базуючись на результатах аналізу існуючих СППР та методів збору та обробки експертної інформації, розроблений алгоритм прийняття рішень та побудована модель СППР. На базі побудованої моделі реалізований програмний комплекс підтримки прийняття рішень. Розроблена СППР дозволяє зменшити фінансові витрати на експертів і часових ресурсів при проведенні процесу оцінки і володіє таким функціональними можливостями:

- на підставі інформації про працівників, такої як посада, досвід, освіта – формує ваговий коефіцієнт кожного працівника;
- ґрунтуючись на інформації отриманій від персоналу підприємства методом анкетування розраховує значення атрибутів моделі загроз;
- враховуючи інформацію про значення атрибутів формується список загроз ранжируваний по рівню небезпеки.

Результати дослідження можуть бути застосовані на комерційних підприємствах під час проведення первинного аналізу загроз інформації.

СПИСОК ЛІТЕРАТУРИ

1 Оценка информационной безопасности бизнеса (Електрон. ресурс) /Спосіб доступу: URL: http://www.cfin.ru/appraisal/business/special/ infosec. shtml?printversion – Загол. з екрану.

2 Огляд та систематизація типових моделей загроз безпеці персональних даних, які обробляються в спеціалізованих інформаційних системах підприємств (Електрон. ресурс)/Спосіб доступу: URL: http://archive.nbuv.gov.ua/portal/soc_gum/vsunu/2012_8_1/title/16.pdf – Загол. з екрану.

3 Классификация угроз информационной безопасности (Електрон. ресурс)/Спосіб доступу: URL: http://www.cnews.ru/reviews/free/oldcom/ security/elvis_class.shtml– Загол. з екрану.

4 Классификация угроз безопасности web-серверов / Спосіб доступу: URL: http://www.nestor.minsk.by/kg/2006/06/kg60619.html. – Загол. з екрана.

5 Bonczek, R.H. Foundation of Decision Support Systems [text] / R.H. Bonczek, C. Holsapple, A.B.Whinston; – New York: Academic Press, 1981. – 186p.

6 Marakas, G.M. Decision support systems in the twenty-first century. [text] / G.M. Marakas – Upper Saddle River, N.J.: Prentice Hall, 1999. – 248 p.

7 Згуровский, М.З. Системный анализ. Проблемы. Методология. Приложения [текст] / М.З. Згуровский, Н.Д. Панкратова. – К.: Наукова думка, 2011 – 726 с.

8 Тикунов, В.С. Геоинформатика. Системы поддержки принятия решений (СППР) [текст] / В.С. Тикунов. – М.: Академия, 2005. — 480 с.

9 Keen P.G.W. Decision Support Systems: The next decades [text] / Keen P.G.W. // Decision Support Systems, 1987. – V. 3. – pp. 253 – 265.

10 Побудова анкети (методичні рекомендації) (Електрон. ресурс)/Спосіб доступу: URL: http://psyclub.at.ua/load/pobudova_a nket i _metodichni_rekomendaciji/2-1-0-27– Загол. з екрану

11 Бешелев С.Д., Гурвич Ф.Г. Экспертные оценки. М.: Наука, 1973. 246 с.

12 Литвак Б.Г. Экспертная информация: методы получения и анализа; М.; Радио и связь, 1982-184с.

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

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

15 Основи економічної теорії / С.В. Мочерний, С.А Єрохін, Л.О. Канищенко та ін. – К.: Академія, 1997. – 463 с.

16 Закон України «Про господарські товариства».

17 Закон України «Про підприємства в Україні».

18 Податковий кодекс України.

19 ДСТУ 3008-95. Документація. Звіти у сфері науки і техніки. Структура і правила оформлення видавничої справи. Бібліографічний запис. Бібліографічний опис. Загальні.

20 ДСТУ ГОСТ 7.1:2006. Система стандартів з інформації, бібліотечної та вимоги та правила складання (ГОСТ 7.1-2003, IDT).

ДОДАТОК А. Перелік матеріалів дипломної роботи

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Список використаної літератури.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

Презентація.pptx

ДОДАТОК Б. Відгуки керівників розділів

Б.1 Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК В. ВІДГУК

на дипломну роботу магістра на тему:

«Синтез системи підтримки прийняття рішень для оцінки загроз інформаційної безпеки підприємства»

студента групи 125м-16-1

Затуливітер Володимир Анатолійович

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 107 сторінках та містить 5 рисунків і 9 таблиць та 20 джерел.

Мета дипломної роботи є актуальною, оскільки вона направлена на забезпечення потрібного рівню точності аналізу загроз при зменшенні витрат на спеціалістів та зниження витрат часових ресурсів при оцінці загроз інформації

При виконанні роботи автор продемонстрував відмінний рівень теоретичних знань і практичних навичок, запропонована система підтримки прийняття рішень для оцінки загроз інформаційної безпеки підприємства.

Наукова новизна полягає у розробці системи підтримки прийняття рішень для оцінки загроз інформації, з метою підвищення рівня інформаційної безпеки підприємства та зменшення фінансових затрат на проведення експертної оцінки.

В цілому дипломна робота задовольняє усім вимогам і може бути допущена до захисту, а її автор Затуливітер Володимир Анатолійович заслуговує на оцінку «_____» та присвоєння кваліфікації «професіонал з організації інформаційної безпеки».

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

Керівник спец. част.,
ст. викл. І.І. Начовний

Р Е Ц Е Н З І Я

на дипломну роботу магістра на тему:

«Синтез системи підтримки прийняття рішень для оцінки загроз інформаційної безпеки підприємства»

студента групи 125м-16-1

Затуливітер Володимир Анатолійович

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 107 сторінках, та містить 5 рисунків, 9 таблиць і 20 джерел.

Актуальність роботи полягає у зниження витрат часових ресурсів при оцінці загроз інформації та забезпечення потрібного рівню точності аналізу загроз.

У спеціальній частині проаналізовані основні класи та види систем підтримки прийняття рішень. Розроблена система підтримки прийняття рішень щодо оцінки актуальних загроз інформації на підприємстві на підставі даних опитування співробітників підприємства.

У роботі наведені:

- методика оцінки інформаційної безпеки;
- класифікація компонентів моделі загроз;
- алгоритм системи підтримки прийняття рішень;
- вихідні дані роботи системи підтримки прийняття рішень.

Наукова новизна полягає у розробці системи підтримки прийняття рішень для оцінки загроз інформації, з метою підвищення рівня інформаційної безпеки підприємства та зменшення фінансових затрат на проведення експертної оцінки.

В цілому дипломна робота задовольняє усім вимогам, а її автор Затуливітер Володимир Анатолійович заслуговує на оцінку «_____».

Рецензент