Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Дослідження шляхів оптимізації комплексу засобів захисту на об'єкті інформатизації
(тема)

Виконала:
студентка 2 курсу, групи АМСЗІм-21-2
Румянцева О.В.
(прізвище, ініціали)

Спеціальність: 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)

Керівник: доцент кафедри ІКІ ім. В.В. Поповського
Пшеничних С.В.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2023 р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентці Румянцевої Ользі Володимирівні
(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження шляхів оптимізації комплексу засобів захисту на об'єкті інформатизації
затверджена наказом по університету від «23» березня 2023р. №292 Ст.
2. Термін подання студентом роботи до екзаменаційної комісії 19.05.2023р.
3. Вихідні дані до роботи: нормативні документи щодо створення комплексної системи захисту інформації, сучасні методи та засоби захисту інформації.
4. Перелік питань, що потрібно опрацювати в роботі:
1) Аналіз підходів до побудови комплексної системи захисту інформації на об’єкті інформатизації.
2) Аналіз методів оцінки ефективності комплексних систем захисту інформації.
3) Розробка варіантів систем захисту інформації для об’єкта інформатизації.
4) Оцінка ефективності розроблених систем захисту інформації та вибір оптимальної системи захисту інформації для об’єкта інформатизації.

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: демонстраційний матеріал у вигляді ppt-презентації.

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	доцент Пшеничних Сергій Васильович		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	15.02.2023	Виконано
2	Збір матеріалів для дослідження	01.03.2023	Виконано
3	Розробка 1 розділу	20.03.2023	Виконано
4	Розробка 2 розділу	07.04.2023	Виконано
5	Розробка 3 розділу	15.04.2023	Виконано
6	Розробка 4 розділу	22.04.2023	Виконано
7	Оформлення кваліфікаційної роботи	30.04.2023	Виконано

Дата видачі завдання 15 лютого 2023 року

Студентка _____ Румянцева О.В.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доцент Пшеничних С.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 82 с., 8 рис., 8 табл., 5 додатків, 28 джерел.

ОПТИМІЗАЦІЯ, СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНІ РЕСУРСИ, РИЗИКИ, ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ.

Об’єкт дослідження – процес проектування комплексних систем захисту інформації на об'єкті інформатизації.

Предмет дослідження – методи формування оптимального складу комплексу засобів захисту інформації.

Мета роботи – визначення шляхів формування оптимального складу комплексу засобів захисту інформації та оцінки його ефективності при побудові комплексної системи захисту інформації на об'єкті інформатизації.

Методи досліджень – емпіричний аналіз, формалізація та порівняння.

На даний час одним з найважливіших завдань оптимальної побудови комплексної системи захисту інформації є вибір із безлічі наявних засобів такого їх набору, який дозволить забезпечити нейтралізацію всіх потенційно можливих інформаційних загроз із найкращою якістю та мінімально можливими витраченими на це ресурсами.

У роботі виконаний аналіз підходів до побудови комплексних системи захисту інформації на об’єкті інформатизації та методів оцінки їх ефективності. На основі аналізу був запропонований новий показник ефективності та критерій оптимізації вибору засобів захисту по кожному каналу витоку інформації. Також був запропонований показник ефективності та критерій оптимізації складу комплексу засобів захисту інформації для комплексної системи захисту в цілому.

З використанням запропонованих показників ефективності був проведений порівняльний аналіз варіантів захисту інформації від витоку по каналу побічних електромагнітних випромінювань на об'єкті інформатизації.

ABSTRACT

The report contains: 82 p., 8 fig., 8 tables, 5 application, 28 sources.

OPTIMIZATION, INFORMATION PROTECTION SYSTEM, INFORMATION RESOURCES, RISKS, INFORMATION SECURITY CONTROLS.

Object of research – the process of designing complex information protection systems at the object of informatization.

Subject of research – methods of forming the optimal composition of the information security complex.

Objective – determining the ways of forming the optimal composition of the complex of information security tools and evaluating its effectiveness when building a comprehensive information security system at the object of informatization.

Research methods – empirical analysis, formalization, and comparison.

Currently, one of the most important tasks of the optimal construction of a complex information protection system is the selection of a set of such tools from among the many available tools, which will ensure the neutralization of all potentially possible information threats with the best quality and the least possible resources spent on it.

The paper analyzes approaches to building complex information protection systems at the object of informatization and methods for evaluating their effectiveness. On the basis of the analysis, a new efficiency indicator and criterion for optimizing the selection of protection means for each channel of information leakage was proposed. An efficiency indicator and a criterion for optimizing the composition of the complex of information protection tools for the complex protection system as a whole were also proposed.

Using the proposed efficiency indicators, a comparative analysis of options for protecting information from leakage through the channel of side electromagnetic radiation at the informatization facility was conducted.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

АС – автоматизована система
БД – база даних
ЕЦП – електронний цифровий підпис
ЗІ – захист інформації
ІС – інформаційна система
КС – комплексна система
КСЗІ – комплексна система захисту інформації
ОІ – об’єкт інформатизації
ОС – операційна система
ПЕМВН – побічне електромагнітне випромінювання та наведення
ПЕМВ – побічне електромагнітне випромінювання
ПЗ – програмне забезпечення
ПК – персональний комп’ютер
ФОП – фізична особа підприємець
GDPR – General Data Protection Regulation
HDD – Hard Drive Disk
HTTP – Hypertext Transfer Protocol
TCP – Transfer Control Protocol
TCSEC – Trusted Computer System Evaluation Criteria
VPN – Virtual Private Network

ВСТУП

В сучасному світі, де інформаційні технології проникають у всі сфери життя, захист інформаційних об'єктів стає дедалі важливішим завданням. Комплекс засобів захисту на об'єкті інформатизації відіграє ключову роль у забезпеченні конфіденційності, цілісності та доступності цінної інформації. Однак, з кожним днем зростає кількість загроз та атак на інформаційні системи, що ставить під загрозу безпеку даних.

Сучасний світ все більше стає цифровим, а це означає, що питання захисту інформації стають все більш актуальними. Зокрема, це стосується об'єктів інформатизації - систем, які обробляють, зберігають та передають інформацію. Сучасні технології дозволяють здійснювати ці процеси з високою швидкістю і ефективністю, але вони також створюють нові можливості для зловмисників.

В результаті, необхідно постійно оновлювати і оптимізувати засоби захисту, щоб вони відповідали сучасним викликам. Це може включати в себе внесення змін у фізичні засоби захисту, оновлення програмного забезпечення, а також підготовку персоналу до роботи з новими технологіями і загрозами.

Дослідження шляхів оптимізації комплексу засобів захисту на об'єкті інформатизації є актуальною проблемою в сучасному світі. Це напрямок досліджень, спрямований на пошук ефективних рішень для захисту інформаційних систем від широкого спектру загроз, включаючи хакерські атаки, віруси, фішинг та інші види кіберзлочинності.

Оптимізація комплексу засобів захисту включає в себе пошук найбільш ефективних технологій, методів і підходів до захисту інформації. Це може включати розробку імунітету до нових загроз, вдосконалення систем виявлення інцидентів, швидку реакцію на кібератаки та відновлення після них, а також підвищення усвідомленності та навичок користувачів щодо кібербезпеки.

Оптимізація засобів захисту не тільки забезпечує більш ефективне використання ресурсів, але й дозволяє підвищити рівень безпеки об'єкта інформатизації. Це, у свою чергу, сприяє збільшенню довіри до інформаційної системи з боку користувачів, що є важливим фактором її успішної експлуатації.

Дослідження шляхів оптимізації комплексу засобів захисту на об'єкті інформатизації має великий потенціал для покращення безпеки інформаційних систем. Воно сприяє розробці нових технологій, стандартів та процедур, які дозволяють виявляти, запобігати і реагувати на кібератаки більш ефективно та швидко. Шляхи оптимізації можуть включати в себе удосконалення алгоритмів шифрування та аутентифікації, розробку інтелектуальних систем виявлення загроз, використання машинного навчання та штучного інтелекту для автоматизації процесів захисту, а також впровадження принципів безпеки на рівні архітектури інформаційних систем.

Оптимізація комплексу засобів захисту також передбачає врахування особливостей конкретного об'єкта інформатизації, його потреб у захисті та ресурсних обмежень. Використання цілеспрямованих стратегій та аналізу ризиків дозволяє розробити оптимальні рішення, що враховують конкретні вимоги безпеки.

Необхідність дослідження шляхів оптимізації комплексу засобів захисту на об'єкті інформатизації обумовлена необхідністю постійного вдосконалення захисту в умовах зростаючих загроз при мінімально можливих витрачених на це ресурсах. Тільки шляхом постійних досліджень, інновацій та оптимізації можна забезпечити високий рівень захисту інформаційних об'єктів.

Таким чином, дослідження шляхів оптимізації комплексу засобів захисту на об'єкті інформатизації має на меті посилення безпеки інформаційних систем шляхом розробки та впровадження ефективних стратегій, технологій та процедур. Це важлива складова у розвитку сучасного інформаційного суспільства, де надійний захист даних є необхідним умовою для забезпечення довіри, конфіденційності та стабільності інформаційних процесів.

1 АНАЛІЗ ПІДХОДІВ ДО ПОБУДОВИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАТИЗАЦІЇ

1.1 Мета, завдання та принципи побудови комплексної системи захисту інформації

Об’єктами інформатизації (ОІ) є об’єкти інформаційної діяльності, на яких здійснюється озвучення та/або обробка інформації з обмеженим доступом розташованими на них засобами електронно-обчислювальної техніки інформаційних (автоматизованих), телекомунікаційних або інформаційно-телекомунікаційних систем та/або іншими технічними засобами. Як виконавча структура інформаційної сфери організації об'єкт інформатизації – це сукупність інформаційних ресурсів, засобів і систем обробки інформації, що використовуються згідно заданої інформаційної технології. До складу об'єкта інформатизації входять всі засоби життєзабезпечення об'єкту інформатизації (будівлі, споруди, приміщення, що забезпечують технічні засоби і системи), які необхідні для встановлення та експлуатації засобів і систем обробки інформації, а також приміщення та об'єкти, призначені для ведення конфіденційних переговорів.

Обробка великих обсягів інформації з обмеженим доступом на ОІ здійснюється в умовах найрізноманітніших загроз. Забезпечення інформаційної безпеки на об'єкті потребує залучення досить великого арсеналу засобів захисту. Однак максимальний ефект може бути досягнутий, коли всі заходи, методи та засоби захисту об'єднуються в єдиний цілісний механізм – комплексну систему захисту інформації. При цьому функціонування системи має контролюватись, оновлюватись та доповнюватись в залежності від зміни зовнішніх та внутрішніх умов.

Комплексна система захисту інформації (КСЗІ) – сукупність організаційних, інженерних і технічних заходів та засобів, призначених для захисту від витоку інформації з обмеженим доступом технічними каналами на об’єктах інформаційної діяльності [1].

Організаційно-правові заходи включають створення концепції інформаційної безпеки, а також:

– складання посадових інструкцій для користувачів та обслуговуючого персоналу;

– створення правил адміністрування компонентів інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;

– розробку планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;

– навчання правилам інформаційної безпеки користувачів.

У разі потреби в рамках проведення організаційно-правових заходів може бути створена служба інформаційної безпеки, режимно-пропускний відділ, проведена реорганізація системи діловодства та зберігання документів.

Інженерно-технічні заходи – це сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно-технічних заходів залежить від рівня безпеки інформації, який необхідно забезпечити. Інженерно-технічні заходи для захисту інформаційної інфраструктури організації можуть включати використання захищених підключень, міжмережевих екранів, розмежування потоків інформації між сегментами мережі, використання засобів шифрування та захисту від несанкціонованого доступу. У разі потреби, у рамках проведення інженерно-технічних заходів, може здійснюватися встановлення у приміщеннях систем охоронно-пожежної сигналізації, систем контролю та управління доступом. Окремі приміщення можуть бути обладнані засобами захисту від витоку акустичної (мовної) інформації.

Основною метою КСЗІ є забезпечення безперервного та стійкого функціонування ОІ та запобігання загрозам його безпеці.

КСЗІ спрямована на захист інформації від [2]:

– витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;

– несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою

використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм, використання комп’ютерних вірусів та інше;

– спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Для кожної конкретної інформаційної системи (ІС) склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом ІС та умовами її експлуатації.

Виходячи з цілей КСЗІ, можна визначити завдання, що стоять перед нею. До них відносяться [3]:

– управління доступом користувачів до ресурсів автоматизованої системи з метою її захисту від неправомірного випадкового або умисного втручання в роботу системи та несанкціонованого (з перевищенням наданих повноважень) доступу до її інформаційних, програмних та апаратних ресурсів з боку сторонніх осіб, а також осіб із числа персоналу організації та користувачів;

– захист даних, що передаються каналами зв'язку;

– реєстрація, збирання, зберігання, обробка та видача відомостей про всі події, що відбуваються в системі та мають відношення до її безпеки;

– контроль роботи користувачів системи з боку адміністрації та оперативне оповіщення адміністратора безпеки про спроби несанкціонованого доступу до ресурсів системи;

– контроль та підтримання цілісності критичних ресурсів системи захисту та середовища виконання прикладних програм;

– забезпечення замкненого середовища перевіреного програмного забезпечення з метою захисту від безконтрольного впровадження в систему потенційно небезпечних програм та засобів подолання системи захисту, а також від впровадження та розповсюдження комп'ютерних вірусів;

– управління засобами системи захисту.

На основі теоретичних досліджень і практичних робіт у сфері захисту інформації (ЗІ) сформульований системно-концептуальний підхід до ЗІ [4]. Під системністю як основною частиною системно-концептуального підходу розуміється:

– системність цільова, захищеність інформації розглядається як основна частина загального поняття якості інформації;

– системність просторова, яка пропонує взаємопов'язані рішення всіх питань захисту на всіх компонентах підприємства;

– системність тимчасова, що означає безперервність робіт із ЗІ, що здійснюються відповідно до планів;

– системність організаційна, що означає єдність організації всіх робіт із ЗІ і управління ними.

Концептуальність підходу передбачає розробку єдиної концепції як повної сукупності науково обґрунтованих поглядів, положень і рішень, необхідних і достатніх для оптимальної організації та забезпечення надійності захисту інформації, а також цілеспрямованої організації всіх робіт щодо ЗІ.

Захист інформації в ІС повинен ґрунтуватися на таких основних принципах [3, 4, 5]:

– системності;

– комплексності;

– безперервності захисту;

– своєчасності;

– спадкоємності та вдосконалення;

– розумної достатності;

– гнучкості управління і застосування;

– відкритості алгоритмів і механізмів захисту;

– простоти застосування заходів та засобів захисту.

Комплексний (системний) підхід до побудови системи захисту інформації на ОІ – це принцип розгляду проекту, у якому аналізується система загалом, а чи не її окремі частини. Основне завдання – оптимізація усієї системи. Комплексний підхід включає наступні етапи [4].

1) Аналіз об'єкта захисту, постановку цілей, завдання критеріїв оптимізації системи захисту та управління нею.

2) Окреслення меж системи захисту та розроблення її первинної структури. На цьому етапі вся сукупність об'єктів та процесів, що мають відношення до

поставленої мети, розбивається на два класи – власне досліджувану систему та зовнішнє середовище як джерело загроз безпеці.

3) Складання математичної моделі системи, що вивчається, а саме - параметризація системи, завдання області визначення параметрів, встановлення залежностей між введеними параметрами.

4) Дослідження побудованої моделі, а саме - прогноз розвитку досліджуваної системи з урахуванням її моделі, аналіз результатів моделювання, оцінку економічної доцільності.

5) Вибір оптимального управління для приведення системи в бажаний (цільовий) стан.

Сутність системного підходу полягає у тому, що КСЗІ, як об'єкт проектування чи управління сприймається як єдність взаємозалежних елементів, які утворюють єдине ціле і діють у сфері реалізації єдиної мети. Системний підхід вимагає розглядати кожен елемент системи у взаємозв'язку та взаємозалежності з іншими елементами, розкривати закономірності, властиві даної конкретної системі, виявляти оптимальний режим її функціонування. Дослідження чи опис окремих елементів системи проводиться з урахуванням ролі та місця кожного елемента у всій системі.

Принцип безперервності полягає в тому, що захист інформації є реалізацією безперервного процесу, що здійснюється на всіх етапах життєвого циклу систем обробки інформації при комплексному використанні всіх засобів захисту. При цьому всі засоби, методи та заходи, що використовуються для СЗІ, найбільш раціонально об'єднуються в єдиний цілісний механізм.

Принцип своєчасності передбачає запобіжний характер заходів для забезпечення безпеки інформації.

Принцип спадкоємності та вдосконалення передбачає постійне вдосконалення заходів та засобів захисту інформації в міру вдосконалення інформаційних технологій та збільшення числа користувачів.

Принцип розумної достатності передбачає відповідність рівня витрат на забезпечення безпеки інформації цінності інформаційних ресурсів та величині можливої шкоди.

Принцип гнучкості управління і застосування передбачає те, що для забезпечення можливості варіювання рівня захищеності при зміні зовнішніх умов і вимог з плином часу засоби захисту повинні мати певну гнучкість;

Принцип відкритості алгоритмів і механізмів захисту полягає в тому, що захист не повинен забезпечуватися тільки за рахунок таємності структурної організації та алгоритмів функціонування її підсистем. Знання алгоритмів роботи системи захисту не повинно давати можливості її подолання. Однак це не означає, що інформація про конкретну систему захисту має бути загальнодоступною.

Принцип простоти застосування заходів та засобів захисту полягає в тому, що механізми захисту повинні бути інтуїтивно зрозумілі і прості у використанні, без залучення значних додаткових трудозатрат.

Враховуючи все вищесказане, можна сформулювати висновки.

1) Система ЗІ може бути забезпечена лише при комплексному використанні всього арсеналу наявних засобів захисту, що поєднує в собі такі напрями захисту, як правова, організаційна та інженерно-технічна.

2) Ніяка система ЗІ не забезпечить безпеку інформації без належної підготовки користувачів та дотримання ними всіх правил захисту.

3) Ніяку систему захисту не можна вважати абсолютно надійною, тому, що завжди може знайтися зловмисник, який знайде лазівку для доступу до інформації.

4) Система захисту повинна бути адаптованою до умов, що постійно змінюються.

1.2 Підходи до проектування комплексних систем захисту інформації

На сьогоднішній день склалися певні підходи до побудови систем захисту інформації (СЗІ), які можна розділити на два основні класи: побудова індивідуальних систем захисту, що найбільш повно враховують умови функціонування об'єкта інформатизації, що захищається, структуру та вимоги до його інформаційної системи, та побудова систем захисту з використанням типових проектних рішень. Підходи проектування СЗІ представлені на рисунку 1.1.

Рисунок 1.1 – Підходи до проектування комплексних систем захисту інформації

Індивідуальне проектування СЗІ з використанням типових засобів захисту інформації застосовується в рамках попереджувальної стратегії, коли система захисту будується на етапі проектування. Воно дозволяє більш глибоко проаналізувати можливий вплив на інформаційні ресурси об'єкта внутрішніх та зовнішніх факторів, що дестабілізують, вибрати оптимальний набір механізмів захисту від них, визначити організаційну побудову СЗІ. Тому можна стверджувати, що застосування зазначеного підходу дозволяє досягти максимального рівня безпеки інформації. Основною проблемою при реалізації такого підходу проектування стає значне порівняно з типовим підходом збільшення часових ресурсів та необхідність залучення для цього вищого рівня спеціалістів. І, як наслідок, веде до суттєвого подорожчання системи захисту, що не завжди буває виправданим.

Найчастіше невеликі організації без потреби захисту своїх інформаційних ресурсів не готові до великих вкладень у створення системи захисту. Це відбувається, коли вартість активів організації (величина потенційних збитків) невелика порівняно

з витратами на їх захист. У цих умовах найбільш доцільним є створення СЗІ з використанням типових засобів захисту. Водночас пропонується визначати склад засобів захисту, виходячи з індивідуальних особливостей ОІ, аналізу його складу та загроз.

На сьогоднішній день проектування КСЗІ полягає у виборі відповідного комплексу засобів із існуючого різноманіття окремих засобів.

Засоби захисту інформації, присутні у теперішній час на ринку умовно можна поділити на декілька груп [5]:

– активні та пасивні технічні засоби, що забезпечують захист від витоку інформації за різними фізичними полями, що виникають при функціонуванні засобів їх обробки;

– програмні, організаційні та програмно-технічні засоби, що забезпечують розмежування доступу до інформації на різних рівнях, ідентифікацію та аутентифікацію користувачів;

– програмні та програмно-технічні засоби, що забезпечують захист інформації та підтвердження її справжності при передачі каналами зв'язку;

– програмно-апаратні та організаційні засоби, що забезпечують цілісність програмного продукту та захист від несанкціонованого копіювання;

– програмні засоби, які забезпечують захист від програм-вірусів та інших шкідливих програм;

– програмні та технічні засоби виявлення мережевих атак;

– програмні та технічні засоби захисту від розкриття параметрів системи.

Особливе місце займають загальносистемні програмні продукти, що виключають можливість використання недекларованих можливостей.

Поява нових загроз неминуче тягне за собою появу засобів захисту від них. Таким чином, ринок засобів захисту інформації постійно розвивається, а отже очікується подальше збільшення номенклатури цих засобів.

Аналіз літератури [5] показав, що на сьогоднішній день теорія захисту інформації знаходиться на теоретико-концептуальному етапі розвитку, при цьому завдання захисту перетікає в завдання забезпечення комплексного захисту об'єкта

інформатизації. Еволюція постановки завдання захисту інформації представлена у таблиці 1.1.

Таблиця 1.1 – Еволюція постановки завдання захисту інформації

Номер этапа	Еволюція постановки завдання захисту	Періоди розвитку теорії захисту інформації
1	Забезпечення комп'ютерної безпеки	Емпіричний
2	Комплексне забезпечення комп'ютерної безпеки	Концептуально-емпіричний
3	Комплексне забезпечення безпеки об'єкту	Теоретично-концептуальний
4	Забезпечення інформаційної безпеки	Загальнотеоретичний

Необхідність комплексного вирішення завдань захисту випливає з припущення про усвідомленість діяльності зловмисника щодо подолання системи захисту, а також наявністю безлічі загроз природного походження (аварії, збої, помилки, стихійні лиха тощо).

Цілий спектр загроз впливає на інформацію, що циркулює в рамках певного об'єкта інформатизації, який можна визначити як сукупність інформаційних ресурсів, засобів та систем обробки інформації, що використовуються з певною інформаційною технологією, засобів забезпечення об'єктів інформатизації, приміщень або об'єктів (будівель, споруд, технічних засобів), у яких вони розміщені, або приміщення чи об'єкти, призначені для проведення конфіденційних переговорів [5]. Приклад типового об'єкта інформатизації представлено на рисунку 1.2.

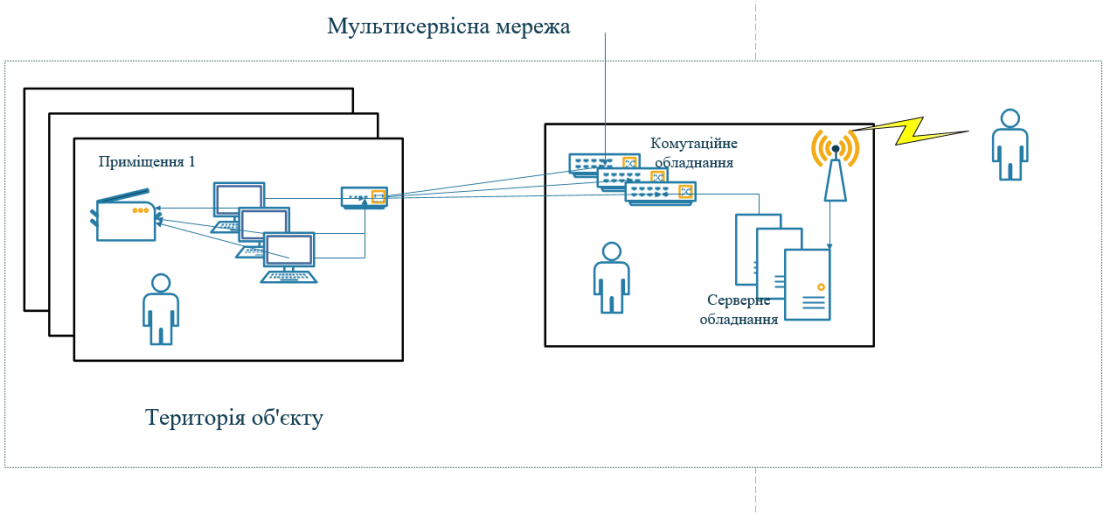

Рисунок 1.2 – Структура типового об'єкта інформатизації

Вочевидь до складу об'єкта інформатизації поряд з інформаційними системами та технологіями, що є основним джерелом сучасних інформаційних загроз, входять традиційні носії інформації та люди, утворюючи єдину соціотехнічну систему.

Таким чином, у складі об'єкта інформатизації поряд з загрозами інформації характерними для комп'ютерних систем необхідно розглядати і класичні загрози [4] (витік інформації по технічних каналах, порушення цілісності та доступності інформації внаслідок об'єктивних та суб'єктивних причин тощо).

1.3 Аналіз нормативно-методичної бази щодо проектування комплексних систем захисту інформації

В сьогоднішній день питання побудови комплексних систем захисту інформації для різних об'єктів інформатизації вирішується на міжнародному, державному та відомчому рівнях. Так останнім часом створено безліч стандартів, що регламентують вимоги до систем захисту інформації та описують кращі практики в галузі побудови захищених інформаційних систем [5]. Структура нормативно-методичного забезпечення захисту інформації представлена рисунку 1.3.

Рисунок 1.3 – Структура нормативно-методичного забезпечення процесу проектування систем захисту інформації

Як можна побачити з рисунка 1.3, до нормативно-методичної баз включені державні нормативні документи: НД ТЗІ 2.5-007-2007, НД ТЗІ 1.1-005-07, НД ТЗІ 3.3-001-07, НД ТЗІ 2.1-002-07, НД ТЗІ 3.1-001-07 та НД ТЗІ 3.7-003-2005. Аналіз цих документів представлено в додатку А.

1.3.1 Аналіз Закону України «Про інформацію».

Закон України «Про інформацію» є основним законодавчим актом, який регулює відносини, що виникають у зв'язку зі збиранням, зберіганням, обробкою, поширенням, пошуком та наданням інформації.

У пункті 1 статті 1 Закону України «Про інформацію» визначено поняття «інформація», яке охоплює будь-які відомості незалежно від форми їх представлення та способу подання.

У пункті 2 статті 2 Закону України «Про інформацію» встановлено право на інформацію, яке є конституційним правом громадян та стосується отримання, зберігання та поширення інформації.

У пункті 2.5 статті 5 Закону України «Про інформацію» встановлено вимогу щодо забезпечення доступу до інформації у відкритому вигляді. Згідно з цим положенням, органи державної влади та місцевого самоврядування зобов'язані надавати інформацію у відкритому вигляді, який не вимагає спеціального запиту або заяви [6].

У пункті 2.7 статті 5 Закону України «Про інформацію» встановлено право на отримання інформації у зручній для отримання формі. Згідно з цим положенням, органи державної влади та місцевого самоврядування зобов'язані надавати інформацію у формі, яка є зручною для отримання та використання.

У пункті 1 статті 6 Закону України «Про інформацію» встановлено вимогу щодо захисту інформації, яка міститься в документах, які становлять державну таємницю. Відповідно до цього положення, державна таємниця захищається законодавством України та забороняється доступ до неї осіб, які не мають на це дозволу [6].

У пункті 2 статті 10 Закону України «Про інформацію» встановлено вимогу щодо надання інформації про фізичних та юридичних осіб. Згідно з цим положенням, інформація про фізичних та юридичних осіб може надаватися тільки з їх згоди або на підставі закону.

У пункті 2 статті 12 Закону України «Про інформацію» встановлено вимогу щодо права на користування авторськими та суміжними правами. Згідно з цим положенням, автор твору має право на визнання його авторством, захист від несанкціонованого використання та право на винагороду за використання твору.

Закон України «Про інформацію» встановлює правові засади збирання, зберігання, обробки, поширення та надання інформації в Україні. Вимоги до захисту інформації, права на інформацію та користування авторськими та суміжними правами є важливими засадами регулювання інформаційних відносин в Україні.

1.3.2 Аналіз Закону України «Про захист персональних даних» та General Data Protection Regulation для використання при побудові комплексної системи захисту інформації.

Закон України «Про захист персональних даних» є законодавчим актом, який встановлює правові засади збору, зберігання, використання, захисту та передачі персональних даних в Україні.

У пункті 1 статті 2 Закону України «Про захист персональних даних» визначено поняття «персональні дані», яке охоплює будь-яку інформацію, яка стосується прямо чи опосередковано визначеної або визначуваної фізичної особи.

У пункті 1 статті 6 Закону України «Про захист персональних даних» встановлено вимогу щодо збору та обробки персональних даних, згідно з якою збір та обробка персональних даних можливі лише за згодою суб'єкта персональних даних або на підставі закону.

У пункті 1 статті 7 Закону України «Про захист персональних даних» встановлено вимогу щодо захисту персональних даних, згідно з якою оператори персональних даних повинні забезпечувати їх захист від несанкціонованого доступу, знищення, втрати чи недостовірного використання.

У пункті 1 статті 8 Закону України «Про захист персональних даних» встановлено вимогу щодо передачі персональних даних, згідно з якою передача персональних даних дозволяється лише за згодою суб'єкта персональних даних або на підставі закону.

У пункті 1 статті 17 Закону України «Про захист персональних даних» встановлено вимогу щодо права суб'єкта персональних даних на доступ до своїх персональних даних. Згідно з цим положенням, суб'єкт персональних даних має право на доступ до своїх персональних даних та отримання інформації про їх використання [7].

Закон України «Про захист персональних даних» встановлює правові засади збору, зберігання, використання, захисту та передачі персональних даних в Україні. Вимоги до зберігання та обробки персональних даних, а також обмеження їх передачі та захисту, є важливими засадами регулювання відносин, пов'язаних з персональними даними в Україні.

У пункті 1 статті 21 Закону України «Про захист персональних даних» встановлено вимогу щодо відповідальності за порушення законодавства про захист персональних даних, згідно з якою за порушення законодавства про захист персональних даних встановлюється відповідальність відповідно до закону.

У пункті 2 статті 22 Закону України «Про захист персональних даних» встановлено вимогу щодо права на захист персональних даних, згідно з якою суб'єкт

персональних даних має право на захист своїх прав та інтересів у випадку порушення законодавства про захист персональних даних [7].

Закон України «Про захист персональних даних» встановлює правові засади збору, зберігання, використання, захисту та передачі персональних даних в Україні. Вимоги до збереження та обробки персональних даних, а також обмеження їх передачі та захисту, є важливими засадами регулювання відносин, пов'язаних з персональними даними в Україні. Особлива увага приділяється відповідальності за порушення законодавства про захист персональних даних та праву суб'єкта персональних даних на захист своїх прав та інтересів.

Ключовим аспектом є також інтеграція системи захисту інформації з міжнародними стандартами та рекомендаціями, такими як General Data Protection Regulation (GDPR), що дозволяє підтримувати відповідність національного законодавства та враховувати вимоги міжнародних партнерів. Переваги дотримання Закону України «Про захист персональних даних» разом з GDPR приведені нижче.

1) GDPR встановлює високі стандарти захисту персональних даних, які визнані та застосовуються в багатьох країнах світу. Відповідність GDPR може покращити репутацію організації на міжнародному рівні.

2) Якщо організація співпрацює з партнерами або клієнтами в Європейському Союзі (ЄС) або обробляє дані громадян ЄС, дотримання GDPR є обов'язковим. Недотримання може призвести до суттєвих штрафів та втрати довіри.

3) Врахування вимог обох законодавчих актів допоможе створити комплексну систему захисту інформації, яка забезпечує найвищий рівень захисту персональних даних.

4) Недотримання будь-якого з цих законів може призвести до відповідальності та штрафів. Створення комплексної системи захисту інформації, яка дотримується вимог обох законодавчих актів, допоможе уникнути таких проблем.

5) Забезпечення відповідності вимогам як Закону України «Про захист персональних даних», так і GDPR допомагає врахувати інтереси всіх сторін, задіяних у процесі обробки персональних даних, включаючи користувачів, клієнтів, співробітників та партнерів. Це може забезпечити більшу довіру до організації та підвищити лояльність клієнтів та партнерів організації.

Отже, дотримання вимог Закону України «Про захист персональних даних» та GDPR при побудові комплексної системи захисту інформації має низку переваг, що включають міжнародне визнання, відповідність регулятивним вимогам, підвищення довіри та конкурентоспроможності організації.

Для побудови комплексної системи захисту інформації з урахуванням Закону України «Про захист персональних даних» та GDPR, слід враховувати вимоги, які приведені нижче.

1) Розуміння основних положень та вимог обох законів є ключовим аспектом побудови ефективної системи захисту інформації.

2) Потрібно ідентифікувати всі види персональних даних, які обробляються організацією, та забезпечити належний рівень захисту відповідно до категорій даних.

3) Потрібно сформувати політики та процедури щодо збору, обробки, зберігання та передачі персональних даних відповідно до вимог Закону України «Про захист персональних даних» та GDPR.

4) Необхідно розробити та впровадити технічні та організаційні заходи, які сприяють забезпеченню безпеки персональних даних, такі як шифрування, регулярне резервне копіювання, контроль доступу та інше [8].

5) Потрібно забезпечити постійне навчання та освіту співробітників з питань захисту персональних даних, та пов'язане з вимогами Закону України «Про захист персональних даних» та GDPR.

6) Система захисту інформації повинна враховувати права суб'єктів даних, такі як право на доступ, виправлення, видалення, обмеження обробки, та право на переносимість даних [8].

7) Потрібно регулярно оцінювати ризики, пов'язані з обробкою персональних даних, та вживати необхідних заходів для їх зменшення. Також потрібно виконувати перевірки безпеки та переглядати політики та процедури захисту інформації, щоб вони відповідали поточним вимогам Закону України «Про захист персональних даних» та GDPR.

8) Необхідно забезпечити належну адресацію відгуків та скарг від суб'єктів даних та контролюючих органів, та відповідати на них оперативно та відповідно до вимог обох законів.

9) Якщо організація передає персональні дані між країнами, необхідно врахувати вимоги щодо міжнародної передачі даних, які встановлені Законом України «Про захист персональних даних» та GDPR. Також потрібно вживати необхідних заходів для захисту даних під час передачі.

10) Необхідно утримувати добрі відносини з контролюючими органами, такими як Уповноважений з прав людини у сфері захисту персональних даних в Україні та відповідні органи ЄС. Потрібно бути готовими надавати їм інформацію про систему захисту інформації та відповідати на їх запити.

Забезпечення відповідності комплексної системи захисту інформації вимогам Закону України «Про захист персональних даних» та GDPR вимагає систематичного та відповідального підходу. Враховуючи ці кроки, організація зможе створити комплексну систему захисту інформації, яка дотримується вимог обох законодавчих актів, тим самим забезпечуючи безпеку персональних даних та довіру клієнтів та партнерів.

1.3.3 Аналіз стандарту ISO/IEC 27001.

ISO/IEC 27001 є міжнародним стандартом, який встановлює вимоги до систем управління інформаційною безпекою. Він надає рамки для захисту конфіденційної інформації та дотримання вимог законодавства з питань інформаційної безпеки.

У пункті 1 стандарту ISO/IEC 27001 встановлюється загальний контекст інформаційної безпеки, що охоплює конфіденційність, цілісність та доступність інформації, а також визначається вимога до управління ризиками інформаційної безпеки.

У пункті 4 стандарту ISO/IEC 27001 встановлюється вимога до контексту організації, зокрема до визначення зовнішніх та внутрішніх факторів, які можуть вплинути на інформаційну безпеку, а також до визначення стейкхолдерів та їх вимог.

У пункті 5 стандарту ISO/IEC 27001 встановлюється вимога до керування лідерством організації, зокрема до визначення політики інформаційної безпеки, призначення відповідальних за інформаційну безпеку, а також до забезпечення необхідних ресурсів для здійснення заходів із захисту інформації.

У пункті 6 стандарту ISO/IEC 27001 встановлюється вимога до планування, зокрема до визначення процесів та процедур, необхідних для здійснення заходів із захисту інформації [9].

У пункті 7 стандарту ISO/IEC 27001 встановлюється вимога до підтримки, зокрема до забезпечення ресурсів, навчання та свідомості співробітників щодо інформаційної безпеки, а також до здійснення контролю за дотриманням дозволів на доступ до інформації.

У пункті 8 стандарту ISO/IEC 27001 встановлюється вимога до експлуатації, зокрема до забезпечення безпеки інформації в процесі експлуатації інформаційних систем, а також до здійснення моніторингу та аналізу інформаційної безпеки.

У пункті 9 стандарту ISO/IEC 27001 встановлюється вимога до оцінки та покращення, зокрема до здійснення оцінки ризиків та визначення заходів із зниження ризику, а також до здійснення постійного вдосконалення системи управління інформаційною безпекою [9].

ISO/IEC 27001 є важливим стандартом для забезпечення інформаційної безпеки в організаціях. Він надає рамки для управління інформаційною безпекою та захисту конфіденційної інформації. Організації, які прагнуть отримати сертифікацію ISO/IEC 27001, повинні дотримуватись встановлених вимог та забезпечити належний рівень інформаційної безпеки.

1.4 Постановка завдання вибору оптимального варіанта комплексу засобів захисту при проектуванні захищеного об'єкта інформатизації

Комплексна система захисту інформації, що циркулює на об'єкті, зазвичай складається з набору інструментів інформаційного захисту, які виконують відповідні функції для запобігання різноманітних деструктивних впливів, об'єднаних системою керівництва (ядром СЗІ) [10]. Існують два ключові підходи до розробки складних систем: зростаюче та спадне проектування. Від порядку виконання стадій проектування залежить розподіл на зростаюче (проектування знизу вгору) та спадне (проектування зверху вниз) проектування. Зростаюче проектування характеризується розв'язанням проблем нижчих ієрархічних рівнів перед рішеннями вищих рівнів, тоді як спадне проектування зосереджується на використанні схемних рішень,

оптимальних для конкретного пристрою або елемента автоматизації, і пов'язане з розробкою оригінальних основних схем та структур компонентів.

Незважаючи на те, що окремий проект СЗІ, який включає розробку спеціалізованих засобів захисту, допомагає досягти найвищого рівня захисту інформації на об'єкті інформатизації, він може виявитися недостатньо ефективним через високу витратність ресурсів. Вже створено багато інструментів інформаційного захисту, і розробка інтегрованої системи захисту інформації часто полягає в виборі відповідного комплекту засобів захисту з наявних різноманітних інструментів. Рішення проблеми вибору комплексу засобів захисту вимагає розробки належної методичної основи. Проте аналіз сучасної методичної бази процесу проектування комплексних систем захисту інформації свідчить про недостатню методичну підтримку, зокрема щодо апріорної оцінки ефективності різних проектних варіантів комплексу засобів захисту.

Постановка завдання вибору оптимального варіанта комплексу засобів захисту при проектуванні захищеного об'єкта інформатизації полягає в розробці стратегії та плану захисту інформації, які забезпечать максимальний рівень безпеки від різноманітних загроз та вразливостей [11].

Для постановки завдання вибору оптимального варіанта комплексу засобів захисту необхідно виконати етапи, які описані нижче.

1) Визначення мети проекту. На цьому етапі визначається, які інформаційні ресурси будуть захищатися та від яких загроз ці інформаційні ресурси потрібно захистити.

2) Аналіз загроз та вразливостей. На цьому етапі необхідно виконати аналіз загроз та вразливостей, які можуть виникнути в процесі експлуатації об'єкта інформатизації. Цей аналіз включає в себе визначення типів загроз та вразливостей, їх серйозності та ймовірності виникнення.

3) Вибір засобів захисту. Після аналізу загроз та вразливостей потрібно вибрати найбільш ефективні засоби захисту, які відповідають потребам проекту. Вибір засобів захисту повинен включати в себе вибір технічних та організаційних заходів, таких як фізичний захист, криптографічні методи, заходи мережевої безпеки тощо.

4) Розробка стратегії захисту. Після вибору засобів захисту необхідно розробити стратегію захисту, яка включатиме в себе визначення послідовності застосування засобів захисту, розподіл заходів захисту між різними компонентами системи, розробку процедур контролю доступу

Розробка КСЗІ потребує значних зусиль та часу. Така система має тривалий термін експлуатації, протягом якого її технічні компоненти можуть зазнавати змін декілька разів. Тому одним з ключових аспектів, які розробник КСЗІ має вирішити, є оптимізація складу компонентів системи для забезпечення стабільної ефективності протягом її життєвого циклу. Оптимізація компонентів системи під час проектування є одним з найскладніших завдань.

Відповідно, необхідно розробити методологічний інструментарій, який дозволить серед різноманітних стандартних інструментів захисту інформації доступних на ринку, сформувати комплексний набір рішень, які найефективніше вирішуватимуть завдання захисту відповідно до встановленого рівня потенційних втрат, характеристик ймовірного зловмисника та ресурсів інформаційного об'єкта.

Враховуючи завдання створення оптимальної системи інформаційної безпеки як завдання проектування складного технічного об'єкта, його математичну постановку можна представити наступним чином.

Нехай маємо складний технічний об'єкт інформаційної системи, який має захищатися від різноманітних загроз та вразливостей. При проектуванні системи захисту необхідно визначити множину можливих заходів захисту, яку можна визначити як $S = \{S_1, S_2, \dots, S_i\}$, де S_i – окремий захід захисту.

Далі, необхідно визначити множину загроз та вразливостей, які можуть виникнути в процесі експлуатації інформаційної системи. Цю множину можна позначити як $T = \{T_1, T_2, \dots, T_i\}$, де T_i – окрема загроза або вразливість.

Також необхідно визначити множину ефективності заходів захисту, яку можна позначити як $E = \{E_1, E_2, \dots, E_i\}$, де E_i – ефективність заходу захисту S_i в умовах відповідного типу загрози або вразливості T_i.

Для побудови оптимального комплексу системи захисту ($E_{опт}$) необхідно вирішити задачу максимізації ефективності заходів захисту, при врахуванні впливу на кожен захід захисту загроз та вразливостей. Це можна виразити у вигляді математичної моделі:

$$E_{опт} = MAX\ (\sum_{i} E_i \cdot X_i), \quad (1.1)$$

де E_i – ефективність заходу захисту S_i в умовах відповідного типу загрози або вразливості T_i;

X_i – булеві змінні, які вказують, чи має бути включений захід захисту S_i в комплекс системи захисту.

Якщо $X_i = 1$, то захід захисту включений в комплекс системи захисту, інакше $X_i = 0$.

При цьому є наступні обмеження:

$$\sum (E_i \cdot X_i) \geq E_{min}, \quad (1.2)$$

де E_i – ефективність заходу захисту S_i в умовах відповідного типу загрози або вразливості T_i;

X_i – булеві змінні, які вказують, чи має бути включений захід захисту S_i в комплекс системи захисту;

E_{min} – мінімальний допустимий рівень ефективності захисту.

Обмеження, що вказане в формулі (1.2) гарантує, що комплекс системи захисту має відповідати вимогам безпеки інформації:

$$\sum (X_i) \leq N, \quad (1.3)$$

де X_i – булеві змінні, які вказують, чи має бути включений захід захисту S_i в комплекс системи захисту;

N – максимальна кількість заходів захисту, яку можна включити в комплекс системи захисту.

Обмеження, що вказане у формулі (4.3) гарантує, що кількість заходів захисту в комплексі не перевищує допустиму максимальну кількість.

За умови (1.1) необхідно знайти оптимальний комплект засобів захисту (X_{opt}) такий, що:

$$X_{opt} = \arg\max E(X, Y, t), \quad (1.4)$$

де E(X,Y,t) – узагальнений показник ефективності функціонування комплексу засобів захисту при множині загроз Y.

Потрібно сформувати склад засобів захисту інформації з багатьох доступних, які забезпечують виконання всіх необхідних функцій за умови досягнення оптимуму обраного критерію та виконання відповідних обмежень. Крім того, такий набір засобів захисту повинен задовольняти вимогам нормативних документів та вимогам сумісності.

При цьому приймаються такі припущення та обмеження:

– час аналізу захищеності поставлено (t = T);

– множина потенційно можливих загроз Y визначена і є кінцевою;

– зловмисник є інформаційним суб'єктом, здатним до навчання;

– витрати на експлуатацію КСЗІ постійні, а їх надійність абсолютна;

– випадки появи різних ненавмисних загроз є незалежними випадковими подіями.

Загальні підходи до оцінювання ефективності КСЗІ на об’єкті інформатизації розглянуто в низці робіт. З'ясовано, що завдання розробника полягає в забезпеченні максимального рівня захищеності інформації в ІС за мінімальної вартості КСЗІ і максимальної вартості інформації, що захищається. Крім того, система захисту інформації повинна бути адекватною - витрати на безпеку не повинні перевищувати вартості самої інформації і розмірів можливих втрат, які викликані успішною реалізацією загроз. Тому, при оцінюванні ефективності КСЗІ треба враховувати не тільки зменшення збитків від реалізації можливих загроз, але й витрати на її створення та експлуатацію.

При вирішенні задачі побудови оптимального комплексу системи захисту необхідно мати достатні знання про множину можливих заходів та засобів захисту, множину загроз та вразливостей, а також множину ефективності заходів та засобів захисту в умовах різних загроз та вразливостей. Отже, для успішного вирішення цієї задачі необхідно провести детальний аналіз загроз та вразливостей, вибрати найбільш ефективні заходи та засоби захисту та розробити стратегію їх застосування.

2 АНАЛІЗ МЕТОДІВ ОЦІНКИ ЕФЕКТИВНОСТІ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Аналіз вихідних даних для побудови моделі комплексної системи захисту інформації

Розробка КСЗІ починається з аналізу загроз безпеки інформації, аналізу комплексної системи (КС), що захищається, та аналізу конфіденційності та важливості інформації в КС [12]. Насамперед, проводиться аналіз конфіденційності та важливості інформації, яка має оброблятися, зберігатися та передаватися до КС. За підсумками аналізу робиться висновок доцільність створення КСЗИ. Якщо інформація не конфіденційна і легко може бути відновлена, то створювати КСЗІ немає необхідності. Не має сенсу також створювати КСЗІ у КС, якщо втрата цілісності та конфіденційності інформації пов'язана з незначними втратами. У таких випадках достатньо використовувати штатні кошти КС і, можливо, страхування втрати інформації.

При аналізі інформації визначаються потоки конфіденційної інформації, елементи КС, де вона обробляється і зберігається. На цьому етапі розглядаються питання розмежування доступу до інформації окремих користувачів і цілих сегментів КС. На основі аналізу інформації визначаються вимоги щодо її захищеності. Вимоги задаються шляхом визначення певного грифу конфіденційності, встановлення правил розмежування доступу [13].

При аналізі інформації, необхідно враховувати між якими підрозділами організації вона циркулює. У типовій компанії можуть бути різні відділи, залежно від розміру компанії, специфіки та сфери діяльності. Але виділяють деякі загальні відділи, які зазвичай зустрічаються в організаціях:

- відділ керівництва;
- фінансовий відділ;
- юридичний відділ;
- відділ маркетингу;
- відділ продажів;

- відділ розробки та виробництва продукта;
- відділ IT;
- відділ інформаційної безпеки;
- відділ кадрів.

У типовій організації взаємозв'язок між відділами та обмін інформацією між ними є фундаментальним для забезпечення ефективності бізнес-процесів та інформаційної безпеки. Успішне функціонування організації залежить від належної координації роботи різних відділів та своєчасного обміну важливою інформацією.

Відділ продажів тісно взаємодіє з відділом маркетингу для вивчення ринкових тенденцій, аналізу конкурентів та визначення найбільш ефективних стратегій просування продуктів та послуг компанії.

Відділ маркетингу також співпрацює з виробничим відділом для отримання інформації про нові та існуючі продукти, їх переваги та особливості.

Відділ кадрів спілкується з керівниками інших відділів для забезпечення своєчасного підбору, наймання та звільнення персоналу, а також проведення регулярних оцінок ефективності співробітників.

Фінансовий відділ взаємодіє з з відділом керівництва організації для планування бюджетів, контролю витрат та забезпечення фінансової стабільності організації.

Юридичний відділ співпрацює з керівництвом компанії та іншими відділами для забезпечення дотримання законодавства, регулятивних вимог та захисту інтелектуальної власності. Це включає надання консультацій, підготовку контрактів та угод, а також розв'язання юридичних спорів.

Всі відділи організації взаємодіють між собою за допомогою різних каналів коммунікації та обмінюються інформацією обженого доступу та загальнодоступною інформацією. У таблиці 2.1 представленні інформаційні ресурси, які циркулюють та зберігаються у підрозділах типової організації.

Таблиця 2.1 – Інформаційні ресурси типової компанії

Інформаційний ресурс	Тип інформації (загальнодоступна / обмеженого доступу)	Відділи компанії, які допущені до інформації	Приміщення, в яких зберігається та оброблюється інформація	Види носіїв, на яких зберігається та оброблюється інформація
1	2	3	4	5
Публікації про новини організації у соціальних мережах	Загальнодоступна інформація	Немає обмежень	Відділ маркетингу	Мобільні пристрої, персональні комп’ютери (ПК) з Hard Disk Drive (HDD) або з Solid-State Drive (SSD) накопичувачеми
Плани рекламних кампаній та публікацій у соціальних мережах	Інформація обмеженого доступу	Відділ маркетингу, відділ керівництва	Відділ маркетингу, відділ керівництва	ПК з HDD або SSD накопичувачами, хмарні сховища
Документи з інформацією про замовлення організації	Інформація обмеженого доступу	Відділ продажів, фінансовий відділ, відділ керівництва	Відділ продажів, фінансовий відділ, відділ керівництва	Паперові носії, ПК з HDD або SSD накопичувачами

Продовження таблиці 2.1

1	2	3	4	5
Документи з інформацією про замовлення організації	Інформація обмеженого доступу	Відділ продажів, фінансовий відділ, відділ керівництва	Відділ продажів, фінансовий відділ, відділ керівництва	Паперові носії, ПК з HDD або SSD накопичувачами
Фінансовий стан компанії, дані грошових переказів	Інформація обмеженого доступу	Фінансовий відділ, відділ керівництва	Фінансовий відділ, відділ керівництва	Паперові носії, ПК з HDD або SSD накопичувачами
Відомості про закупівлі технічного обладнання та спеціалізованого програмного забезпечення (ПО)	Загальнодоступна інформація	Немає обмежень	Відділ ведення фінансів, відділ керівництва, відділ інформаційної безпеки	Паперові носії, ПК з HDD або SSD накопичувачами
Інформація, що стосується продуктів організації	Загальнодоступна інформація	Немає обмежень	Відділ продажів, відділ керівництва, відділ маркетингу	Паперові носії, ПК з HDD або SSD накопичувачами

Продовження таблиці 2.1

1	2	3	4	5
Вимоги до продукта, , напрацювання для нових продуктів та покращення вже наявних продуктів	Інформація обмеженого доступу	Відділ виробництва та розробки продукта, відділ керівництва, відділ маркетингу, відділ продажів	Відділ виробництва та розробки продукта	ПК з HDD або SSD накопичувачами
Вакансії компанії	Загальнодоступна інформація	Немає обмежень	Відділ кадрів, відділ керівництва, відділ інформаційної безпеки	Паперові носії, ПК з HDD або SSD накопичувачами
Запити працівників на закупівлю матеріалів, технічного обладнання та спеціалізованого програмного забезпечення	Загальнодоступна інформація	Немає обмежень	Відділ продажів, відділ керівництва, фінансовий відділ, відділ інформаційної безпеки	Паперові носії, ПК з HDD або SSD накопичувачами

Продовження таблиці 2.1

1	2	3	4	5
Інструкції для працівників всіх відділів	Інформація обмеженого доступу	Інформація обмежена межами організації	Всі відділи організації	Паперові носії, ПК з HDD або SSD накопичувачами, хмарні сховища
Спеціальні інструкції для кожного відділу	Інформація обмеженого доступу	Інформація обмежена межами відділу	Для кожного відділу розповсюдженні свої інструкції	Паперові носії, ПК з HDD або SSD накопичувачами, хмарні сховища
Накази і розпорядження керівництва компанії	Інформація обмеженого доступу	Розповсюджується між всіма відділами, яких стосується	Розповсюджена між всіма відділами, яких стосується	Паперові носії, ПК з HDD або SSD накопичувачами
Інформація про конкурентів компанії	Інформація обмеженого доступу	Відділ керывництва, відділ інформаційної безпеки	Відділ інформаційної безпеки, відділ керівництва	ПК з HDD або SSD накопичувачами

Продовження таблиці 2.1

1	2	3	4	5
Договори про найм співробітників	Інформація обмеженого доступу	Відділ керівництва, відділ фінансів, юридичний відділ, відділ кадрів, відділ інформаційної безпеки	Відділ кадрів	Паперові носії, ПК з HDD або SSD накопичувачами
Персональні дані працівників компанії (паспортні дані, адреса і т.д.)	Інформація обмеженого доступу	Відділ керівництва, юридичний відділ, відділ кадрів, відділ інформаційної безпеки	Відділ кадрів, відділ інформаційної безпеки	Паперові носії, ПК з HDD або SSD накопичувачами
Документи які містять конфігурації обладнання працівників	Загальнодоступна інформація	Відділ інформаційної безпеки, відділ IT	Відділ інформаційної безпеки, відділ IT	ПК з HDD або SSD накопичувачами

Аналіз загроз безпеки одна із обов'язкових умов побудови КСЗІ. За результатами проведеного аналізу будується модель загроз безпеки інформації в КС, яка містить систематизовані дані про випадкові та навмисні загрози безпеки інформації в конкретній КС. Систематизація даних моделі передбачає наявність відомостей про всі можливі загрози, їх небезпеку, часових рамок дії, ймовірність реалізації. В таблиці 2.2 вказані загрози та вразливості для інформаційних ресурсів з таблиці 2.1.

Таблиця 2.2 – Загрози та вразливості інформаційних ресурсів типової організації

Загрози	Уразливості	Інформаційні ресурси
1	2	3
Прослуховування інформації	Підслуховування інформації працівниками компанії через недостатню систему шумоізоляції	Плани рекламних кампаній та публікацій у соціальних мережах; фінансовий стан компанії, дані грошових переказів; накази і розпорядження керівництва компанії; інформація про конкурентів компанії.
	Прослуховування інформації за допомогою прослуховувальних пристроїв через недостатній захист від витоку інформації акустичним шляхом	
Перехоплення інформації віброакустичним шляхом	Перехоплення інформації лазерними мікрофонами, датчиками вібрації тощо через відсутність захисту або недостатній захист від перехоплення інформації віброакустичним шляхом	Документи з інформацією про замовлення організації; фінансовий стан компанії, дані грошових переказів; інструкції для працівників всіх відділів.

Продовження таблиці 2.2

1	2	3
Перехоплення побічного електромагнітного випромінювання (ПЕМВ)	Перехоплення інформації за допомогою радіочастотних приймачів, антен тощо через відсутність захисту або недостатній захист від перехоплення ПЕМВ	Документи з інформацією про замовлення організації; фінансовий стан компанії, дані грошових переказів; вимоги до продукта, напрацювання для нових продуктів та покращення вже наявних продуктів; спеціальні інструкції для кожного відділу; накази і розпорядження керівництва компанії.
Пошкодження або знищення інформації працівником компанії	Незадоволення працівника компанією	Плани рекламних кампаній та публікацій у соціальних мережах; документи з інформацією про замовлення організації
	Відсутність навчання працівників по роботі з інформацією	
	Відсутність резервного копіювання даних	
Пошкодження або знищення інформації за допомогою шкідливого програмного забезпечення (ПЗ)	Недостатній контроль доступу	Документи з інформацією про замовлення організації; фінансовий стан компанії, дані грошових переказів; вакансії компанії; спеціальні інструкції для кожного відділу.
	Відсутність або неналежна реалізація резервного копіювання даних	
	Відсутність антивірусного ПЗ	

Продовження таблиці 2.2

1	2	3
Копіювання інформації на зовнішній носій	Відсутність навчання працівників з інформаційної безпеки	Плани рекламних кампаній та публікацій у соціальних мережах; документи з інформацією про замовлення організації; фінансовий стан компанії, дані грошових переказів; спеціальні інструкції для кожного відділу; договори про найм співробітників; персональні дані працівників компанії; документи, які містять конфігурації обладнання працівників.
	Незадоволення працівника компанією	
Перешкоджання доступу до ПК	Відсутність або слабка політика паролів	Вимоги до продукта, напрацювання для нових продуктів та покращення вже наявних продуктів; інструкції для працівників всіх відділів; документи, які містять конфігурації обладнання працівників.
	Несанкціонований фізичний доступ до комп'ютера	
	Використання неоновленого або вразливого ПЗ	

Продовження таблиці 2.2

1	2	3
Знищення носіїв інформації	Відсутність або неправильне використання системи контролю доступу до приміщень, де знаходяться носіїв інформації	Фінансовий стан компанії, дані грошових переказів; вимоги до продукта, напрацювання для нових продуктів та покращення вже наявних продуктів; накази і розпорядження керівництва компанії; інформація про конкурентів компанії.
	Невідповідні умови для зберігання носіїв інформації	
	Відсутність резервного копіювання даних	
Модифікація інформації на носіях інформації	Відсутність або неправильне використання шифрування інформації	Плани рекламних кампаній та публікацій у соціальних мережах; документи з інформацією про замовлення організації; інструкції для працівників всіх відділів; спеціальні інструкції для кожного відділу; персональні дані працівників компанії.
	Відсутність або слабкий механізм аутентифікації	
	Відсутність або неправильне використання системи контролю доступу до приміщень, де знаходяться носіїв інформації	
	Недостатнє аудитування та моніторинг активності користувачів	

Продовження таблиці 2.2

1	2	3
Перешкоджання доступу до бази даних (БД)	Слабкий механізм аутентифікації та авторизації користувачів БД	Інструкції для працівників всіх відділів; фінансовий стан компанії, дані грошових переказів; договори про найм співробітників
	Недостатній захист від DoS або DDoS атак	
	Відсутність резервного копіювання даних	

2.2 Аналіз методів моделювання комплексних систем захисту інформації

Оцінка ефективності функціонування КСЗІ є складним науково-технічним завданням. Комплексна СЗІ оцінюється у процесі розробки комплексної системи, у період експлуатації та при створенні (модернізації) СЗІ для вже існуючих КС. Під час розробки складних систем поширеним методом проектування є синтез із наступним аналізом. Система синтезується шляхом узгодженого об'єднання блоків, пристроїв, підсистем та аналізується (оцінюється) ефективність отриманого рішення. З безлічі синтезованих систем вибирається найкраща за результатами аналізу, що здійснюється за допомогою моделювання [13].

Моделювання КСЗІ полягає в побудові образу (моделі) системи, що з певною точністю відтворює процеси, що відбуваються в реальній системі. Реалізація моделі дозволяє отримувати та досліджувати характеристики реальної системи.

Для оцінки систем використовуються аналітичні та імітаційні моделі. У аналітичних моделях функціонування досліджуваної системи записується у вигляді математичних чи логічних співвідношень. Для цього використовується потужний математичний апарат: алгебра, функціональний аналіз, різноманітні рівняння, теорія ймовірностей, математична статистика, теорія множин, теорія графів, теорія масового обслуговування, теорія зв'язку тощо [14].

При імітаційному моделюванні система, що моделюється, представляється у вигляді деякого аналога реальної системи. У процесі імітаційного моделювання на

ЕОМ реалізуються алгоритми зміни основних характеристик реальної системи відповідно до еквівалентних реальних процесів математичними та логічними залежностями [15].

Моделі поділяються також на детерміновані та стохастичні. Моделі, що оперують із випадковими величинами, називаються стохастичними. Так як на процеси захисту інформації основний вплив мають випадкові чинники, то моделі систем захисту є стохастичними.

2.3 Підходи до оцінки ефективності комплексних систем захисту інформації

Ефективність КСЗІ оцінюється як на етапі розробки, так і у процесі експлуатації. В оцінці ефективності КСЗІ, залежно від використовуваних показників та способів їх отримання, можна виділити три підходи [16]:

– класичний;
– офіційний;
– експериментальний.

Під класичним підходом до оцінки ефективності мають на увазі використання критеріїв ефективності, отриманих за допомогою показників ефективності. Значення показників ефективності утворюється шляхом моделювання або обчислюються за характеристиками реальної КС. Такий підхід використовується для розробки та модернізації КСЗІ.

При класичному підході для оцінки ефективності КСЗІ та отримання критерію ефективності при використанні деякої множини n показників використовують ряд методів [4].

1) Вибирається один головний показник, і оптимальною вважається система, для якої цей показник досягає екстремуму. За умови, що решта показників задовольняє системі обмежень, заданих у вигляді нерівностей.

2) Методи, засновані на ранжируванні показників за важливістю. При порівнянні систем однойменні показники ефективності зіставляються в порядку зменшення їх важливості за певними алгоритмами.

3) Мультиплікативні та адитивні методи отримання критеріїв ефективності ґрунтуються на об'єднанні всіх або частини показників за допомогою операцій

множення або додавання до узагальнених показників. Якщо в добуток включається частина показників, то інші приватні показники включаються до обмежень.

4) Метод Парето: під час використання n показників ефективності системі відповідає точка в n-мірному просторі. У n-вимірному просторі будується область парето-оптимальних рішень, що містить незрівнянні рішення, для яких поліпшення будь-якого показника неможливе без погіршення інших показників ефективності. Вибір найкращого рішення з-поміж парето-оптимальних може здійснюватися за різними правилами.

У сучасних нормативних документах з інформаційної безпеки використовується класифікаційний підхід. Даний підхід до визначення ефективності КСЗІ умовно можна назвати офіційним чи нормативним. Політика безпеки інформаційних технологій проводиться державою та має спиратися на нормативні акти. У цих документах необхідно визначити вимоги до захищеності інформації різних категорій конфіденційності та важливості [4].

Вимоги можуть задаватися переліком механізмів захисту інформації, які необхідно мати у КС, щоб вона відповідала певному класу захисту. Використовуючи такі документи можна оцінити ефективність КСЗІ. І тут критерієм ефективності КСЗІ є її клас захищеності. Безперечною перевагою таких класифікаторів (стандартів) є простота використання. Основним недоліком нормативного підходу до визначення ефективності систем захисту є те, що не визначається ефективність конкретного механізму захисту, а констатується лише факт його наявності чи відсутності. Цей недолік певною мірою компенсується завданням у деяких документах докладних вимог до цих механізмів захисту.

У всіх розвинених країнах розроблено свої стандарти захищеності комп'ютерних систем критичного застосування. Так, у міністерстві оборони США використовується стандарт Department of Defence Trusted Computer System Evaluation Criteria (TCSEC), який відомий як «Помаранчева книга». Відповідно до цієї книги для оцінки інформаційних систем розглядається чотири групи безпеки: A, B, C, D [17]. У деяких випадках групи безпеки діляться додатково на класи безпеки.

1) Група А (гарантований або контрольований захист) забезпечує гарантований рівень безпеки. Методи захисту, реалізовані у системі, можна перевірити формальними методами. У цій групі лише один клас – А1.

2) Група B (повноважний або повний захист) представляє повний захист КС. У цій групі виділено класи безпеки:

– B1 (захист через грифи чи мітки), який забезпечується використанням у КС грифів секретності, що визначають доступ користувачів до частин системи;

– B2 (структурований захист), який досягається поділом інформації на захищені та незахищені блоки та контролем доступу до них користувачів;

– B3 (області або домени безпеки), який передбачає поділ КС на підсистеми з різним рівнем безпеки та контролем доступу до них користувачів.

3) Група C (виборчий захист) представляє вибірковий захист підсистем з контролем доступу користувачів до них. У цій групі виділено класи безпеки:

– C1 (виборчий захист інформації), який передбачає поділ користувачів та даних у КС. Цей клас забезпечує найнижчий рівень захисту КС;

– C2 (захист через керований чи контрольований доступ), який забезпечується окремим доступом користувачів до даних.

4) Групу D (мінімальної безпеки) складають КС, перевірені на безпеку, але які не можуть бути віднесені до класів A, B або C.

Організація захисту інформації в обчислювальних мережах міністерства оборони США здійснюється відповідно до вимог керівництва «The Trusted Network Interpretation of Department of Defense. Trusted Computer System Evaluation Guidelines». Цей документ отримав назву «Червона книга».

Подібні стандарти захищеності КС ухвалено і в інших розвинутих країнах. Так, 1991 року Франція, Німеччина, Нідерланди та Великобританія прийняли узгоджені «Європейські критерії», в яких розглянуто 7 класів безпеки від E0 до E6. Найнижчий клас – сьомий, найвищий – перший. Класи поділяються на чотири групи, що відрізняються якісним рівнем захисту:

– перша група містить лише один сьомий клас;

– друга група характеризується дискреційним захистом та містить шостий та п'ятий класи;

– третя група характеризується мандатним захистом та містить четвертий, третій та другий класи;

– четверта група характеризується верифікованим захистом і містить лише перший клас.

Крім вимог щодо захищеності окремих елементів, у керівному документі наведено вимоги до захищеності автоматизованих систем (АС). Автоматизовані системи є функціонально орієнтованими. При створенні АС враховуються особливості інформації користувача, технологія обробки, зберігання та передачі інформації, конкретні моделі загроз. Встановлюється дев'ять класів безпеки АС від несанкціонованого доступу до інформації. Класи поділяються на три групи, що відрізняються особливостями обробки інформації в АС. Третя група класифікує АС, з якими працює один користувач, допущений до інформації АС, розміщеної на носіях одного рівня конфіденційності. Група містить два класи – 3Б та 3А. До другої групи зведено АС, користувачі яких мають однакові права доступу до всієї інформації АС. Група містить два класи – 2Б та 2А. Першу групу складають розраховані на багато користувачів АС, в яких користувачі мають різні права доступу до інформації. Група включає п'ять класів – 1Д, 1Г, 1В, 1Б, 1А. До кожного з дев'яти класів захищеності АС висуваються свої вимоги.

Під експериментальним підходом розуміється організація процесу визначення ефективності існуючих КСЗІ шляхом спроб подолання захисних механізмів системи фахівцями, які знаходяться у ролі зловмисників.

Складається план проведення експерименту. У ньому визначаються черговість та матеріально-технічне забезпечення проведення експериментів щодо визначення слабких місць у системі захисту. Служба безпеки до моменту подолання захисту «зловмисниками» має запровадити в КСЗІ нові механізми захисту (змінити старі), щоб уникнути «зламування» системи захисту.

Функціональне тестування є об'єктивним видом оцінки ефективності КСЗІ. Воно призначене для перевірки фактичної працездатності реалізованих механізмів безпеки, їх відповідності вимогам, а також забезпечує отримання статистичних даних.

З огляду на те, що засоби безпеки мають обмежені можливості протидії загрозам, завжди існує ймовірність порушення захисту, навіть якщо під час тестування механізми безпеки не були обійдені або блоковані. Для оцінки цієї ймовірності мають проводитися додаткові дослідження. У методичному плані визначення ефективності КСЗІ повинне полягати у виробленні судження щодо

придатності способу дій персоналу чи пристосованості технічних засобів до досягнення мети захисту на основі вимірювання відповідних показників при функціональному тестуванні.

Ефективність оцінюється на вирішення наступних задач:

– ухвалення рішення про допустимість практичного використання КСЗІ у конкретній ситуації;

– виявлення вкладів різних факторів у досягнення мети;

– встановлення шляхів підвищення ефективності КСЗІ;

– порівняння альтернативних варіантів систем.

Вирішенням проблеми комплексної оцінки ефективності КСЗІ може стати використання системного підходу, що дозволяє ще на стадії проектування кількісно оцінити рівень безпеки та створити механізм управління ризиками. Однак цей шлях слід реалізовувати за наявності відповідної системи показників та критеріїв.

Високий ступінь невизначеності вихідних даних при проектуванні КСЗІ є причиною того, що її ефективність не може бути адекватно виражена та описана детермінованими показниками. Тому об'єктивною характеристикою якості КСЗІ може бути лише ймовірність, що характеризує ступінь відповідності системи, що оцінюється, своєму призначенню – досягненню необхідного рівня безпеки в умовах реального впливу випадкових факторів при заданому комплексі умов. Така характеристика називається ймовірністю виконання завдання системою. Ця ймовірність має бути покладена в основу комплексу показників та критеріїв оцінки ефективності КСЗІ. При цьому критеріями оцінки є поняття придатності та оптимальності. Придатність означає виконання всіх встановлених до КСЗІ вимог, а оптимальність – досягнення однієї з характеристик екстремального значення при дотриманні обмежень та умов інших властивостей системи. При виборі конкретного критерію необхідне його узгодження з метою КСЗІ.

2.4 Визначення показників ефективності та критеріїв оптимальності комплексної системи захисту інформації

З точки зору забезпечення безпеки, що циркулює на ОІ, доцільно оцінювати якість системи захисту інформації такими показниками:

– результативність;
– неперервність захисту;
– ресурсоємність захисту.

Результативність виражається захищеністю інформації від сукупності загроз конфіденційності, цілісності та доступності. Даний показник має імовірнісну природу, тому пропонується в якості нього використовувати ймовірність успішної реалізації будь-якого деструктивного впливу на заданому інтервалі часу або значення потенційної шкоди (ризику).

Безперервність захисту інформації визначається через показники технічної надійності КСЗ, що оцінюється середнім часом безвідмовної роботи, ймовірністю відмови за деякий час t, ймовірністю знаходження КСЗ у працездатному стані на час t або коефіцієнтом технічної готовності $К_г$.

Ресурсоємність захисту інформації може виражатися в економічних витратах на реалізацію та обслуговування КСЗ, а також у витратах телекомунікаційних, обчислювальних, організаційних ресурсів.

Система показників, що характеризують ефективність захисту інформації та їх взаємозв'язок з показниками якості окремих засобів захисту інформації представлена на рисунку 2.1 [18].

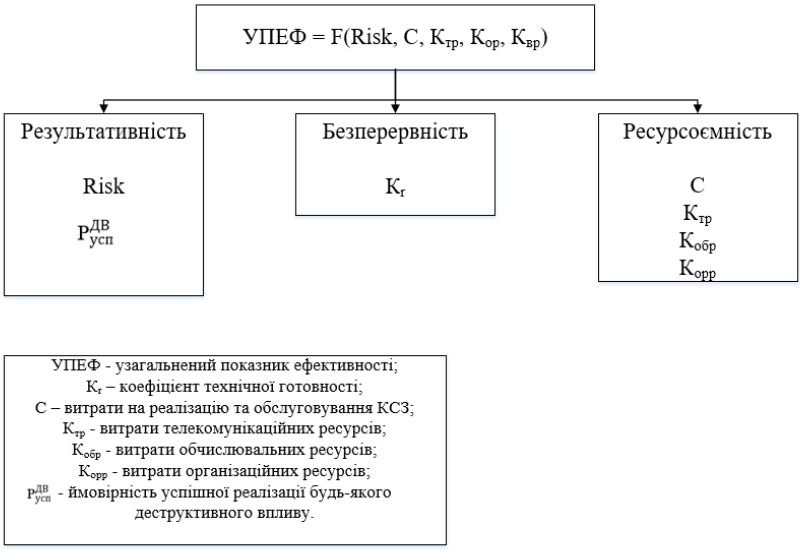

Рисунок 2.1 – Система показників якості комплексної системи захисту інформації

Припускаючи, що технічна та експлуатаційна надійність КСЗ забезпечується при виконанні вимог щодо встановлення та експлуатації окремих засобів захисту інформації і при цьому K_r близький до 1, показник безперервності надалі не враховуватимемо.

У ряді робіт, присвячених питанням оцінки ефективності захисту інформації як показника, розглядається залишковий ризик — величина шкоди з урахуванням ймовірності реалізації події, що призводить до цієї шкоди.

$$R = \sum P_i \cdot C_i, \tag{2.1}$$

де R – величина шкоди з урахуванням ймовірності реалізації події, що призводить до цієї шкоди;

P_i – ймовірність реалізації і-ї загрози;

C_i – величина збитків від реалізації і-ї загрози.

Величини P_i та C_i визначаються методом експертних чи аналітичних оцінок. Розмір шкоди є випадковою величиною з функцією розподілу F(C), де $C \in [0, \infty]$, а як міра шкоди у виразі (2.1) приймають математичне очікування величини шкоди.

Часто щодо ризику враховують витрати на реалізацію захисних заходів – S, тоді вираз (2.1) перетворюється на вид [18]:

$$R = \sum P_i \cdot (C_i + S_i), \tag{2.2}$$

де R – ризик, який характеризує потенційні втрати чи шкоду від витоку інформації;

P_i – ймовірність виникнення витоку інформації через канал і;

C_i, – величина шкоди від реалізації і-ої загрози;

S_i – вартість реалізації захисних механізмів від тієї ж загрози.

Однак при такому підході витрати на впровадження та експлуатацію засобів захисту прирівнюються до збитків від реалізації загрози, що не завжди є коректним.

У роботах [18, 19] як показник ефективності розробки КСЗІ використовується величина запобіжних збитків за вирахуванням витрат на впровадження та експлуатацію засобів безпеки:

$$E = \sum_{i=1}^{K}(C_i - C_i^*) - \sum_{b=1}^{B}(S_b^{ВП} + S_b^{ек}), \qquad (2.3)$$

де E – ефективність розробки КСЗІ;

C_i – величина збитків від реалізації і-ї загрози до впровадження КСЗІ;

C_i^* – величина збитків від реалізації і-ї загрози після впровадження КСЗІ;

$S_b^{вп}$ – витрати на впровадження b-го засобу безпеки;

$S_b^{ек}$ – витрати на експлуатацію b-го засобу безпеки.

При такому підході не враховується ймовірності реалізації загроз, що дозволяє оптимальним чином вибрати адекватні методи і засоби захисту. Доцільно таким чином формувати комплексну систему захисту (КСЗ), щоб витрати на безпеку були адекватні потенційним загрозам. Подібна ситуація визначає необхідність оцінки та врахування ймовірності реалізації загроз.

Оцінка ймовірності реалізації загроз та пов'язана з цим оцінка можливих втрат є найскладнішою та найвідповідальнішою частиною всього процесу забезпечення безпеки. Від того, наскільки, з одного боку, досить повно виявлено реальні та прогнозовані (потенційні) загрози, залежить, зрештою, ступінь захищеності об'єкта. З іншого боку, свідоме перевищення достатності при врахуванні тих загроз, вплив яких безпосередньо на функціонування об'єкта малоймовірний або локалізація яких неможлива або малоефективна, призведе до значного підвищення витрат на безпеку і може суттєво позначитися на економічної ефективності захисту, що реально досягається [20].

Звідси постає завдання оптимізації рівня захищеності об'єкта від загроз, що дозволяє досягти максимальної ефективності обраного варіанта комплексу захисних заходів. При цьому необхідно враховувати дуже важливе обмеження: незважаючи на наявність прямої залежності між розмірами виділених на захист засобів і ефективністю захисту, існує гранично допустима величина витрат, що визначається

рентабельністю проектованої системи захисту – нормою прибутку на кошти, що інвестуються в неї.

Підвищення рентабельності захисту можливе, як з допомогою обгрунтованої економії витрат за її організацію та експлуатацію, так і за допомогою їх раціонального розподілу у просторі загроз.

Через фізичну природу виникнення, існуючі на ОІ канали витоку інформації умовно можна поділити на залежні та незалежні. Кожному каналу витоку можна протиставити окрему сукупність методів та засобів захисту. Деякі методи та засоби дозволяють забезпечити захист від кількох загроз по декількох залежних каналах витоку інформації. Наприклад, просторове акустичне зашумлення дозволяє блокувати витік мовної інформації з акустичного, віброакустичного, акустоелектричного та параметричного каналів на ОІ. Подібним чином просторове електромагнітне зашумлення виключає витік інформації каналом ПЕМВ, а також каналом наведень на шину заземлення, на всі провідні лінії і всі струмопровідні інженерні комунікації, які є на ОІ. Однак при цьому необхідно оцінити достатність зазначених заходів захисту з урахуванням усіх факторів, зокрема ергономічного та людського.

Оптимізація вибору методів та засобів захисту для кожного каналу витоку дає змогу економічно обґрунтувати склад комплексу спеціальних технічних засобів для об'єкта загалом. Критерієм оптимальності цієї композиції може бути обрано суму середніх втрат від реалізації загроз і витрат на систему захисту.

Припустимо, що на ОІ в ході спеціального обстеження виявлено М каналів витоку інформації та К інформаційних ресурсів, що захищаються. Для кожного каналу визначено загрози та вразливості для відповідного інформаційного ресурсу та є набір засобів та методів захисту. Завдання полягає у виборі складу засобів та методів відповідно до деякого критерію оптимальності.

Позначимо ймовірність реалізації j-ї загрози щодо ресурсу, що захищається, по m-му каналу витоку за умови невикористання засобів захисту P_{jm}, а збиток компанії від її реалізації – C_{jm}. Тоді ризик реалізації jm-й загрози (R_{jm}) дорівнює:

$$R_{jm} = P_{jm} \cdot C_{jm}, \qquad (2.4)$$

де R_{jm} – ризик реалізації jm-й загрози;

P_{jm} – ймовірність реалізації j-ї загрози щодо ресурсу, що захищається, по m-му каналу витоку за умови невикористання засобів захисту;

C_{jm} – збиток компанії від її реалізації jm-й загрози.

Після використання засобу захисту (X_i) величина ризику стане рівною:

$$R_{jm}(X_i) = P_{jm}(X_i) \cdot C_{jm} \quad (2.5)$$

де $R_{jm}(X_i)$ – ризик реалізації jm-й загрози за умови використання X_i засобу захисту;

$P_{jm}(X_i)$ – ймовірність реалізації j-ї загрози щодо ресурсу, що захищається, по m-му каналу витоку за умови використання X_i засобу захисту;

C_{jm} – збиток компанії від її реалізації jm-й загрози.

З урахуванням вартості цього засобу захисту (S_i) пропонується використовувати наступний показник ефективності:

$$E_{jm}(X_i)[\%] = \left(\frac{R_{jm} - R_{jm}(X_i)}{R_{jm}} \cdot 100\right) - \left(\frac{S_i}{R_{jm}} \cdot 100\right) \quad (2.6)$$

де $E_{jm}(X_i)$ – ефективність засобу захисту (X_i) при реалізації j-ї загрози щодо ресурсу, що захищається, по m-му каналу витоку;

R_{jm} – ризик реалізації jm-й загрози;

$P_{jm}(X_i)$ – ймовірність реалізації j-ї загрози щодо ресурсу, що захищається, по m-му каналу витоку за умови використання X_i засобу захисту;

S_i – вартість засобу захисту X_i.

У абсолютному грошовому еквіваленті показник (2.6) має наступний вигляд:

$$E_{jm}(X_i)[₴] = R_{jm} - R_{jm}(X_i) - S_i = \Delta R_{jm}(X_i) - S_i, \quad (2.7)$$

де $E_{jm}(X_i)$ – ефективність засобу захисту (X_i) при реалізації j-ї загрози щодо ресурсу, що захищається, по m-му каналу витоку;

R_{jm} – ризик реалізації jm-й загрози;

$P_{jm}(X_i)$ – ймовірність реалізації j-ї загрози щодо ресурсу, що захищається, по m-му каналу витоку за умови використання X_i засобу захисту;

S_i – вартість засобу захисту X_i.

Показник (2.7) відображає зменшення ризику в грошовому еквіваленті за рахунок використання засобу захисту (X_i) у разі реалізації j-ї загрози щодо ресурсу, що захищається, по m-му каналу витоку інформації з урахуванням вартості заходу щодо захисту (з урахуванням вартості апаратури, її встановлення та експлуатації).

Завдання оптимізації полягає у виборі такого засобу з множини $X= \{X_1, X_2, \ldots, X_i\}$, для якого буде виконуватись умова:

$$X_{jm}^{opt} = \arg\max E_{jm}(X_i), \tag{2.8}$$

де X_{jm}^{opt} – оптимальний засіб захисту інформації при реалізації j-ї загрози щодо ресурсу, що захищається, по m-му каналу витоку;

$E_{jm}(X_i)$ – ефективність засобу захисту (X_i) при реалізації j-ї загрози щодо ресурсу, що захищається, по m-му каналу витоку.

Іншими словами, цей засіб (захід) повинен забезпечувати максимальне зменшення ризику при мінімальних витратах. У деяких випадках максимальне значення параметра $E_{jm}(X_i)$ може приймати значення близькі до нуля, що є прийнятним. Однак, якщо максимальне значення параметра оптимізації набуває негативних значень, це свідчить про перевищення витрат і необхідність використання більш дешевих засобів та методів захисту.

Загалом для комплексу засобів захисту за всіма M каналами витоку інформації, які виявлені на ОІ в ході попереднього спеціального обстеження вираз для параметра ефективності можна записати в наступному вигляді:

$$E(X) = \sum_{m=1}^{M} \sum_{j=1}^{Y} E_{jm}(X_i), \tag{2.9}$$

де E(X) – ефективність комплексу засобів захисту за всіма M каналами витоку інформації, які виявлені на об'єкті інформатизації;

$E_{jm}(X_i)$ – ефективність засобу захисту (X_i) при реалізації j-ї загрози щодо ресурсу, що захищається, по m-му каналу витоку.

Однак, тут не враховується те, що один і той самий засіб (захід) може забезпечувати захист інформації відразу по кількох каналах витоку. У такій ситуації пропонується використати наступний показник ефективності:

$$E(X)[\%] = \left(\frac{R_{old} - R_{nev}(X)}{R_{old}} \cdot 100\right) - \frac{\sum_{i=1}^{K} S_i}{R_{old}} \cdot 100, \qquad (2.10)$$

де E(X) – ефективність комплексу засобів захисту за всіма M каналами витоку інформації, які виявлені на об'єкті інформатизації;

R_{old} – ризик для ОІ до впровадження КСЗІ;

$R_{nev}(X_i)$ – ризик для ОІ після впровадження КСЗІ;

S_i – витрати на впровадження та експлуатацію і-го засобу безпеки.

K – загальна кількість засобів (заходів), що використовуються в КСЗІ.

У абсолютному грошовому еквіваленті показник (2.10) має наступнтй вигляд:

$$E(X)[₴] = R_{old} - R_{nev}(X) - \sum_{i=1}^{K} S_i, \qquad (2.11)$$

де E(X) – ефективність комплексу засобів захисту в абсолютному грошовому еувіваленті за всіма M каналами витоку інформації, які виявлені на об'єкті інформатизації;

R_{old} – ризик для ОІ до впровадження КСЗІ;

$R_{nev}(X_i)$ – ризик для ОІ після впровадження КСЗІ;

S_i – витрати на впровадження та експлуатацію і-го засобу безпеки.

K – загальна кількість засобів (заходів), що використовуються в КСЗІ.

Оцінку ризиків для ІС до і після впровадження КСЗІ проводитимемо за методикою компанії «Digital Securit» [21].

Згідно з цим критерієм, витрати на безпеку ІС не повинні перевищувати величину ризику, який існував до впровадження КСЗІ. Якщо ця умова не

виконується, необхідно зменшувати кількість заходів із захисту чи шукати інші засоби і методи.

Рішенням оптимізаційної задачі для КСЗІ буде знаходження складу комплексу засобів $X_{opt}= \{X_1,X_2, \ldots, X_i\}$, для якого буде виконуватись умова:

$$X_{opt} = \arg\max E(X, Y, P, C, S), \qquad (2.12)$$

де $Y= \{Y_1,Y_2, \ldots, Y_j\}$ – множина загроз;

$P= \{P_1,P_2, \ldots, P_j\}$ – ймовірності реалізації загроз;

$C= \{C_1,C_2, \ldots, C_j\}$ – збитки від реалізації загроз;

$S= \{S_1,S_2, \ldots, S_i\}$ – вартості реалізації засобів захисту.

Таким чином було розроблено алгоритм вирішення задачі оптимізації КСЗІ. Для кожного каналу витоку інформації засоби захисту підбираються відповідно до критерію (2.7) з використанням показника (2.6). Для КСЗІ загалом оптимальність перевіряється за критерієм (2.10). Алгоритм у вигляді блок-схеми представлений на рисунку 2.2.

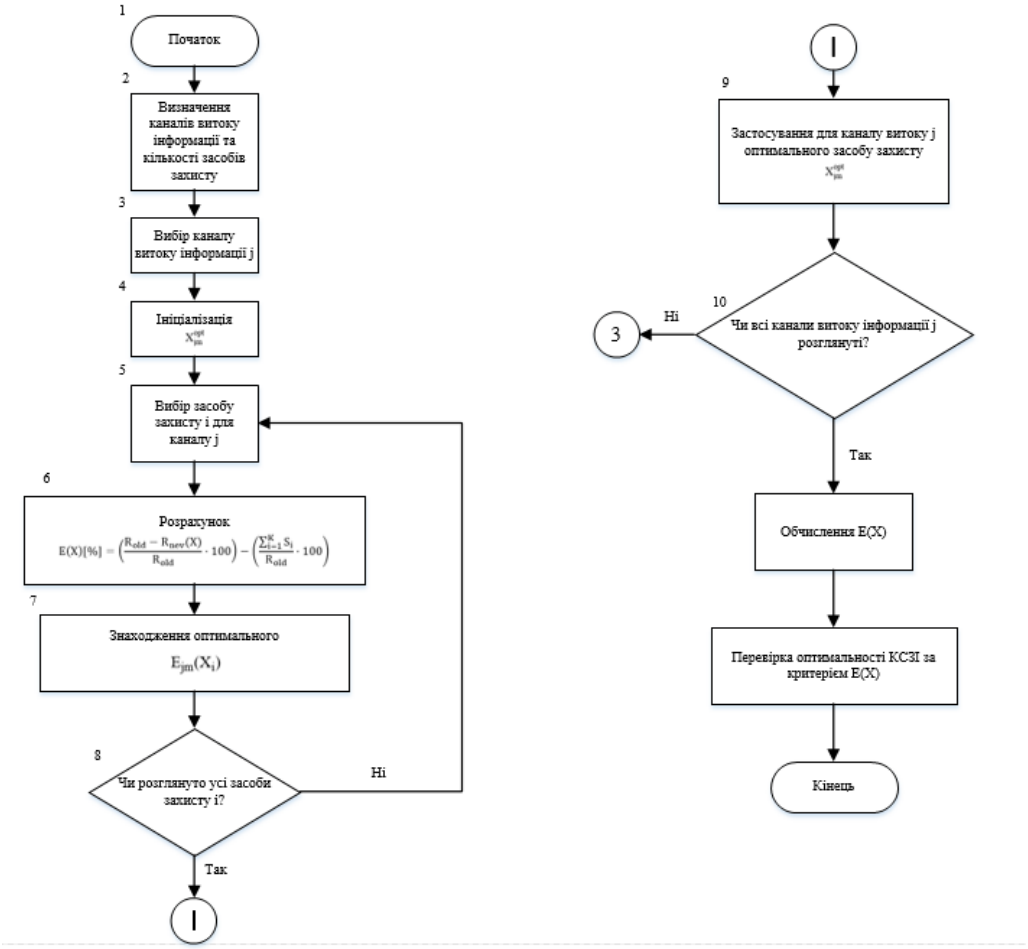

Рисунок 2.2 – Блок-схема алгоритму вирішення задачі оптимізації комплексної системи захисту інформації

Принцип дії алгоритму представленого у вигляді блоку схеми на рисунку 2.2 полягає в наступному:

– на кроці 2 визначаються можливі канали витоку інформації та доступні засоби захисту;

– на кроці 3 вибирається один із каналів витоку інформації j для подальшої оптимізації;

– на кроці 4 значення X_{jm}^{opt} ініціалізується для поточного каналу витоку j;

– на кроці 5 вибирається один із доступних засобів захисту інформації i для застосування до поточного каналу витоку j;

– на кроці 6 розраховується показник ефективності $E_{jm}(X_i)$ для вибраного засобу захисту i та поточного каналу витоку j;

– на кроці 7 якщо поточне значення $E_{jm}(X_i)$ краще оптимального значення $E_{jm}(X_i)$, то значення X_{jm}^{opt} оновлюється і новим оптимальним значенням $E_{jm}(X_i)$, стає поточне значення $E_{jm}(X_i)$;

– на кроці 8 перевіряється чи всі засоби захисту і розглянуті, якщо так, то переходимо до кроку 9, якщо ні то повертаємось до кроку 5 для розгляду наступного засобу захисту;

– на кроці 9 застосовується оптимальний засіб захисту X_{jm}^{opt} до поточного каналу витоку j;

– на кроці 10 відбувається перевірка чи розглянуті всі канали витоку j, якщо так, то переходимо до кроку 11, якщо ні, то повертаємося на крок 3 для оптимізації наступного каналу витоку інформації;

– на кроці 11для всієї КСЗІ розраховується загальний показник ефективності E(X) після застосування оптимальних засобів захисту до кожного каналу витоку інформації;

– на кроці 12 відбувається перевірка, чи отримане рішення є оптимальним з точки зору критерію E(X).

В алгоритмі ітеративно розглядаються всі канали витоку інформації та для кожного каналу визначається найефективніший засіб захисту, за допомогою критерію X_{jm}^{opt}. Для кожного засобу захисту і та каналу витоку j обчислюється показник ефективності $E_{jm}(X_i)$, який є різницею між вихідним ризиком R_{jm} і ризиком після застосування засобу захисту $R_{jm}(X_i)$, а також враховує вартість засобу захисту S_i.

В алгоритмі послідовно переглядаються всі доступні засоби захисту кожного каналу витоку, порівнюючи їх ефективність та вибираючи найефективніший засіб захисту для кожного каналу.

Після того, як для всіх каналів витоку визначено оптимальні засоби захисту, в алгоритмі обчислюється загальний показник ефективності (E(X)) КСЗІ в цілому. Потім перевіряється оптимальність КСЗІ за критерієм (E(X)), який є різницею між вихідним загальним ризиком (R_{old}) і загальним ризиком після застосування оптимальних засобів захисту ($R_{nev}(X)$), враховуючи сумарну вартість всіх застосованих засобів захисту.

3 РОЗРОБКА ВАРІАНТІВ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ОБ’ЄКТА ІНФОРМАТИЗАЦІЇ

3.1 Аналіз існуючої комплексної системи захисту інформації

ІТ-компанія «DIAgency» – це компанія яка зарєстрована згідно Українського законодавства, а саме за Господарським Кодексом України № 1183-IX від 03.02.2021, ВВР, 2021, № 19, ст.170 № 1396-IX від 15.04.2021.

Компанія «DIAgency» займається розробкою, тестуванням та підтримкою програмного забезпечення. Також для компанії «DIAgency» важливо зберегти конфіденційні дані працівників компанії та забезпечити безпечну передачу даних замовнику, а також безпечне зберігання даних проекту. План офісу компанії «DIAgency» представлено на рисунку Б.1 в додатку Б.

В компанії «DIAgency» вже впроваджена комплексна система захисту інформації.

1) Для доступу в приміщення офісу встановлено електронно-механічний кодовий замок Atis SS-K4.

2) Для шифрування даних персонального комп'ютера встановлено засіб шифрування даних на дисках TrueCrypt.

3) Для видалення даних с дисків встановлена програма для безповоротного видалення файлів з дисків Eraser.

4) Для захисту від шкідливого ПО встановлено антивірус ESET Smart Security Suite.

5) Для захищеної роботи у внутрішній мережі встановлено VPN-з'єднання.

6) Для організації електронного документообігу впроваджено за допомогою засобу для формування електронного цифрового підпису (ЕЦП) – «КАРМА» від компанії «НетКом Текнолоджи».

7) Для захисту програмного забезпечення та конфіденційної інформації від несанкціонованого копіювання впроваджено індивідуальний електронний ключ eToken Pro 32.

8) Для захисту від знімання інформації по акустичним та оптичним каналам розроблена СЗІ від знімання по акустичному і оптичному каналу. Більш детально СЗІ від знімання по акустичному і оптичному каналу описана у додатку В.

9) Впроваджена система відеоспостереження. Більш детально система відеоспостереження описана у додатку Г.

При аналізі моделі загроз та вразливостей, та при аналізі СЗІ компанії «DIAgency» було виявлено, що відсутній захист від побічного електромагнітного випромінювання та наведення (ПЕМВН), що може спричинити значні порушення в роботі електронних пристроїв та систем обробки інформації, зокрема приладів збору, обробки та зберігання даних. Як наслідок, може бути витік інформації, а також інформація може бути модифікована або знищена, що може призвести до серйозних фінансових, організаційних та правових наслідків. Відтак, у модель загроз та вразливостей компанії «DIAgency» були додані загрози та вразливості витоку інформаціїї каналами ПЕМВН. Оновлена модель загроз та вразливостей з врахуванням вже існуючих засобів захисту та їх вартості представлена у таблиці Д.2 додатку Д.

Також на основі цього було прийнято рішення про впровадження комплексної системи захисту інформації, що враховує захист від ПЕМВН, стає необхідною умовою для забезпечення безпеки та конфіденційності інформації. Компанія «DIAgency» відповідає найвищим стандартам безпеки та якості своєї продукції, тому впровадження захисту від ПЕМВН є важливим кроком у забезпеченні надійного захисту інформаційних ресурсів компанії.

Для компанії «DIAgency» впровадження СЗІ від витоку каналами ПЕМВН необхідна, тому що, без цього є доволі високий ризик витоку інформації

Серед інформаційних ресурсів компанії «DIAgency», які можуть бути пошкоджені, модифіковані або вкрадені за допомогою ПЕМВН є:

– інформація про фінансовий стан компанії, дані грошових переказів;
– документи, що стосуються роботи компанії;
– накази і розпорядження керівництва компанії;
– документи з інформацією про замовлення організації;
– вимоги до продукту, напрацювання для нових продуктів та покращення вже наявних продуктів.

Отже, впровадження захисту від ПЕМВН є важливим кроком для компанії «DIAgency» у забезпеченні безпеки та конфіденційності інформаційни ресурсів. Тому було прийнято рішення розробити оптимальну систему захисту від витоку інформації каналами ПЕМВН, яка буде забезпечувати максимальне зниження ризику витоку інформації при мінімальних витратах.

Відділ розробки у компанії «DIAgency» розміщений у двох приміщеннях. Тому для того, щоб зменшити витрати при побудові СЗІ прийнято рішення по перенесенню відділу розробки в одне приміщення, а звільнене приміщення було виділено для обробки інформації, що піддається ризику витоку каналами ПЕМВН. Це було зроблено для того, щоб зменшити витрати на побудову СЗІ від витоку каналами ПЕМВН. План офісу після перенесення відділу розробки в одне приміщення та виділення приміщення для роботи з інформацією чутливою до витоку каналами ПЕМВН представлений на рисунку Д.1 у додатку Д.

Виділення окремого приміщення для обробки інформації, що піддається ризику витоку каналами ПЕМВН має ряд переваг при побудові СЗІ.

1) Захист всіх приміщень офісу буде дорогою та трудоємкою задачею. Побудова СЗІ від витоку інформації каналами ПЕМВН в одному приміщенні дозволяє концентрувати ресурси та забезпечити більш високий рівень захисту.

2) Контролювати доступ до одного приміщення легше, ніж до цілого офісу. Це дозволяє забезпечити доступ до цього приміщення тільки авторизованим працівникам компанії, яким надали доступ до приміщення, де обробляються інформаційні ресурси, які піддаються ризику витоку каналами ПЕМВН.

3) Зосередження обробки інформації в одному місці допомагає зменшити ризик витоку інформації каналами ПЕМВН. Коли інформація циркулює в декількох приміщеннях, існує більший ризик витоку інформації каналами ПЕМВН.

4) Моніторинг функціонування СЗІ у одному приміщенні є більш простим та ефективним ніж моніторинг СЗІ розміщеної у декількох приміщеннях.

5) СЗІ потребують обслуговування та підтримки. Підтримка СЗІ розміщеної у одному приміщенні є більш простою та більш дешевою ніж підтримка СЗІ розміщеної у декількох приміщеннях.

Побудова оптимальної СЗІ від витоку каналами ПЕМВН — це складна і багатоаспектна задача. Для розробки оптимального рішення необхідно врахувати ряд

факторів, включаючи специфіку діяльності компанії, характер оброблюваної інформації, особливості інфраструктури тощо.

Основою побудови ефективної СЗІ є розробка декількох варіантів захисту, кожен з яких має використовувати різні засоби та методи захисту від ПЕМВН. Для цього можна використовувати різні пасивні і активні засоби захисту інформації від витоку каналами ПЕМВН. Кожен варіант системи захисту має бути детально проаналізований з точки зору ефективності захисту та вартості впровадження.

3.2 Розробка системи захисту інформації з використанням генераторів радіочастотного шуму

Так як вартість СЗІ є важливим показником для компанії «DIAgency», було вирішено розробити СЗІ від витоку каналами ПЕМВН, в якій будуть використані генератори радіочастотного шуму.

СЗІ від витоку каналами ПЕМВН, що базується на генераторах радіочастотного шуму може бути ефективним рішенням з кількох причин.

1) Використання генераторів радіочастотного шуму є більш економічно виправданим варіантом, ніж встановлення більш складних та коштовних систем захисту.

2) Якщо «DIAgency» часто змінює розташування або має кілька віддалених офісів, якщо компанія вирішить змінити розташування офісу, генератори радіочастотного шуму можуть бути легко перенесені та встановлені в новому місці.

При розробці СЗІ розглядались генератори радіочастотного шуму «PIAC-1M» та «PIAC-1C», технічні характеристики яких наведені в таблиці 3.1.

Таблиця 3.1 – Технічні характеристики генераторів радіочастотного шуму «PIAC-1M» та «PIAC-1C»

Характеристика	Значення
1	2
Генератор радіочастотного шуму «PIAC-1M»	
Коефіцієнт якості шуму	Не менше 0.8

Продовження таблиці 3.1

1	2
Коефіцієнт міжспектральних кореляційних зв'язків	Не менше 2.0
Спектральна щільність напруженості електричної Еш та магнітної рНш компонент електромагнітного поля шуму (дБ/мкв*м-1*кГц-0,5) щодо 1 мкВ на відстані 1 м від антени	В діапазонах частот: від 10 кГц до 500 МГц – не менше 50 дБ; від 500 МГц до 1000МГц – не менше 40 дБ; від 1000 МГц до 1500 МГц – не менше 30 дБ.
Індикація контролю функціонування	Звукова та світлова
Нормований рівень спектральної щільності напруги електричного та магнітного компонентів нормованого електромагнітного поля шуму	Не менше 30 дБ
Максимальне інтегральне значення вихідної потужності	Не менше 5 Вт
Час технічної готовності	Не більше 1 сек
Потужність, що споживається від мережі змінного струму	Не більше 20 Вт
Маса приладу	Не більше 1,5 кг
Склад приладу	Генератор високочастотного шуму мобільний «РІАС–1ГМ», антени дипольні телескопічні «РІАС–1АД»
Генератор радіочастотного шуму «РІАС-1С»	
Коефіцієнт якості шуму	Не менше 0.8
Коефіцієнт міжспектральних кореляційних зв'язків	Не менше 2.0

Продовження таблиці 3.1

1	2
Спектральна щільність напруженості електричної Еш та магнітної рНш компонент електромагнітного поля шуму (дБ/мкв*м-1*кГц-0,5) щодо 1 мкВ на відстані 1 м від антени	В діапазоні частот від 10 кГц до 1000 МГц – не менше 60 дБ
	В діапазоні частот від 1000 МГц до 2000МГц – не менше 50 дБ
	В діапазоні частот від 2000 МГц до 2500 МГц – не менше 40 дБ
Індикація контролю функціонування	Звукова та світлова
Нормований рівень спектральної щільності напруги електричного та магнітного компонентів нормованого електромагнітного поля шуму	Не менше 30 дБ
Максимальне інтегральне значення вихідної потужності	Не менше 5 Вт
Час технічної готовності	Не більше 1 сек
Потужність, що споживається від мережі змінного струму	не більше 20 Вт
Маса приладу	не більше 2,5 кг
Склад приладу	Генератор високочастотного шуму стаціонарний «РІАС–1ГС»
	Антени рамкові м’ягкі «РІАС–1АМ»

Так як до складу генератора радіочастотного шуму «РІАС-1С» входять рамочні антени, які мають кращу направленість ніж дипольні телескопічні антени, а до складу

генератора радіочастотного шуму «PIAC-1M» входять дипольні телескопічні антени, то для побудови СЗІ компанії «DIAgency» обрали генератор радіочастотного шуму «PIAC-1C». Розміщення генератора радіочастотного шуму «PIAC-1C» у приміщенні виділеному для розробки СЗІ представлено на рисунку 3.1.

Рисунок 3.1 – Розміщення генератору радіочастотного шуму у приміщенні

3.3 Розробка системи захисту інформації з використанням екранованої камери

Екрановані камери є одним із найефективніших засобів захисту інформації від витоку каналами ПЕМВН. Вони створюють фізичний бар'єр між обладнанням всередині камери та впливом зовні, що зменшує ризик зйому інформації.

Для компанії «DIAgency», для якої важливо зберегти конфіденційні дані та забезпечити безпечну передачу даних, а також безпечне зберігання даних,

використання екранованих камер є одним з варінтів зниження ризику витоку інформації каналами ПЕМВН.

Серед переваг екранованої камери можна виділити:

– надання високого рівня захисту від витоку інформації каналами ПЕМВН;

– забезпечення захисту не тільки від радіочастотного впливу, але й від електромагнітних полів, що можуть впливати на обладнання всередині;

– можливість створення контрольованого середовища для обладнання, знижуючи ризик впливу зовнішніх чинників.

Однак при використанні екранованих камер потрібно враховувати також їх недоліки. До недоліків впровадження екранованих камер у СЗІ можна виділити:

– вартість екранованих камер, так як вони можуть бути досить дорогими для встановлення і обслуговування;

– досить великий розмір приміщення для розміщення екранованої камери, так як вони зазвичай вимагають більше місця, ніж інші рішення;

– затрати часу та грошей на обслуговування екранованої камери, так як вони можуть вимагати регулярного обслуговування та інспекції, щоб гарантувати, що вони продовжують ефективно функціонувати.

Так як для компанії «DIAgency» при побудові СЗІ від витоку каналами ПЕМВН є важливим забезпечити максимальне зниження ризику витоку інформації при мінімальних витратах, було розроблено екрановану камеру, яка має наступні технічні характеристики:

– робочий діапазон частот – від 10 кГц до 1000 МГЦ;

– ефективність екранування - до 80 дБ.

Розроблена екранована камера має наступну конструкцію:

– модулі стін і перекриттів зі сталі товщиною 1,5 мм;

– екранований дверний блок;

– уведення кабелів;

– фільтри (хвильоводні та мережні).

Також у комплектацію розробленої екранованої камери входять:

– модулі стін і перекриттів;

– екрановані дверні блоки (стандартні одинарні або підвійні, з'єднані тамбуром);

– хвилеводні фільтри;

– електричні перешкододавлюючі фільтри;

– ригельний механізм замикання;

– замки (механічний та кодовий).

Розміщення екранованої камери у приміщенні офісу представлено на рисунку 3.2.

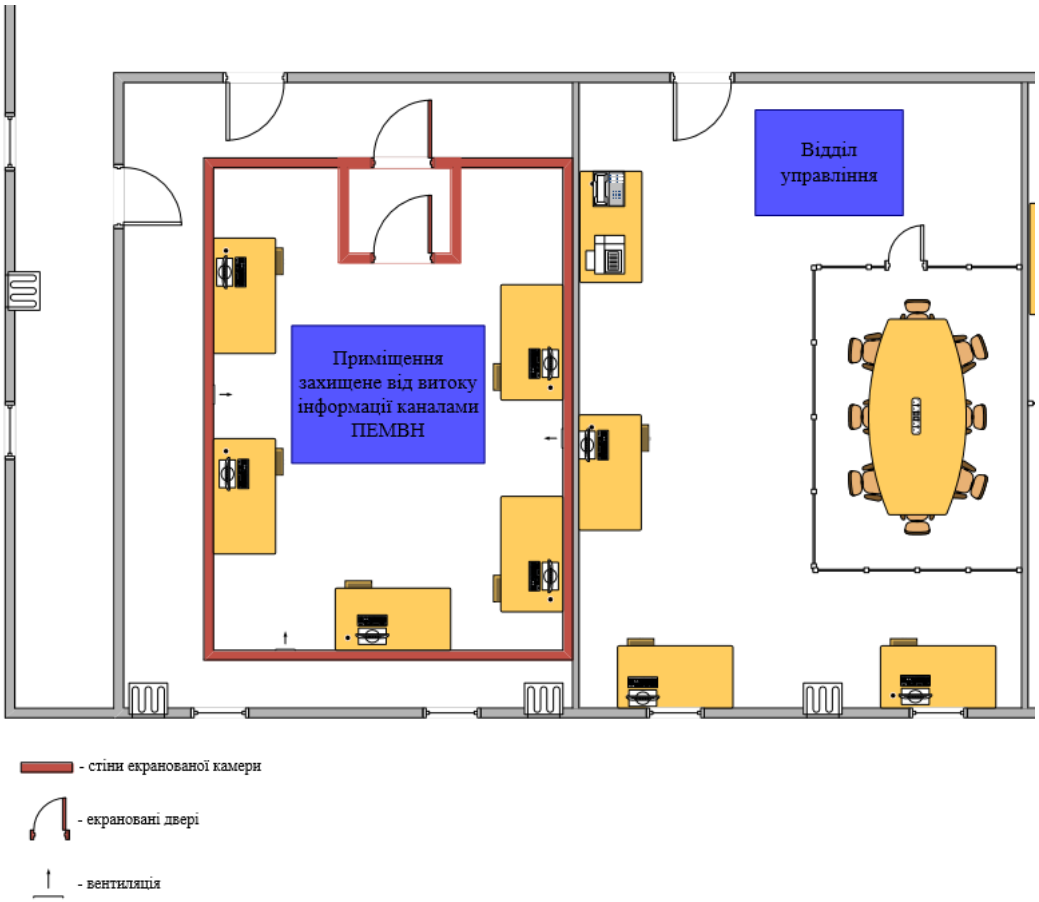

Рисунок 3.2 – Розміщення екранованої камери у приміщенні офісу

3.4 Розробка системи захисту інформації з використанням екранованих персональних комп’ютерів

Для компанії «DIAgency», для якої важливо зберегти конфіденційні дані та забезпечити безпечну передачу даних, а також безпечне зберігання даних, використання екранованих ПК може бути ефективним рішенням.

Екрановані ПК представляють собою спеціалізовані комп'ютери, корпуси яких оброблені таким чином, щоб зменшити або виключити можливість випромінювання чутливої інформації через електромагнітні поля. Екранування може включати в себе металеві корпуси, спеціальні герметичні роз'єми і шлейфи для з'єднання, а також додаткові засоби захисту, такі як фільтри та заглушки на портах.

Основною перевагою екранованих ПК є те, що вони надають безпосередній та ефективний захист від витоку інформації через електромагнітні поля, які можуть генеруватися при нормальній роботі комп'ютера. Вони також дозволяють зменшити залежність від додаткових засобів захисту ПЕМВН, таких як екрановані приміщення, які є більш дорогим методом захисту.

Крім того, екрановані ПК можуть підвищити гнучкість СЗІ. Вони можуть бути встановлені майже в будь-якому приміщенні. Тому якщо б в компанії «DIAgency» не було б можливості виділити окреме приміщення для роботи з інформацією, для якої високий ризик зйому за ПЕМВ, то цей варіант захисту був би одним з найефективніших, так як кількість засобів пасивного захисту каналами ПЕМВН суттєво б зменшилась.

Серед недоліків екранованих ПК можна виділити їх вартість, так як вони є доволі дорогими. Вони також можуть вимагати спеціалізованого обслуговування та підтримки, що може додатково збільшити вартість.

При розробці СЗІ від витоку каналами ПЕМВН для компанії «DIAgency» було обрано екранований моноблок «Expert», який виробляє українська компанія «ЕПОС». Моноблок «Expert» – це екранований ПК, який виконаний у спеціальному корпусі та має ряд особливостей, які підходять під вимоги до СЗІ компанії «DIAgency».

1) Моноблок з розмірами, що практично не перевищують розміри звичайного TFT-монітора.

2) Використання моноблочної конструкції з оптичними розв'язками основних вузлів ПК дозволяє досягти низьких рівнів електромагнітних випромінювань, що відповідають сучасним вимогам НД ТЗІ.

3) Захищена клавіатура та комп'ютерна миша підключаються за допомогою оптичних кабелів. Підтримується підключення захищених принтера та інших периферійних пристроїв за допомогою оптичних подовжувачів. Захищений порт USB для підключення флеш-накопичувача.

4) Опціонально може бути обладнаний оптичним мережевим адаптером для використання в локальній мережі.

5) Можливість підключення до локальної мережі по оптоволоконному кабелю для побудови АС класу «2».

6) Можливість заміни периферійних пристроїв (клавіатура, комп'ютерна миша, принтер, сканер тощо) в процесі експлуатації без проведення додаткових спеціальних досліджень.

Описані вище особливості роблять екранований моноблок «Expert» гнучким та адаптивним до змін у вимогах до обладнання протягом часу, що дозволяє забезпечити тривалу ефективність системи захисту інформації.

Розміщення екранованих моноблоків «Expert» у приміщенні офісу компанії «DIAgency» представлено на рисунку 3.3.

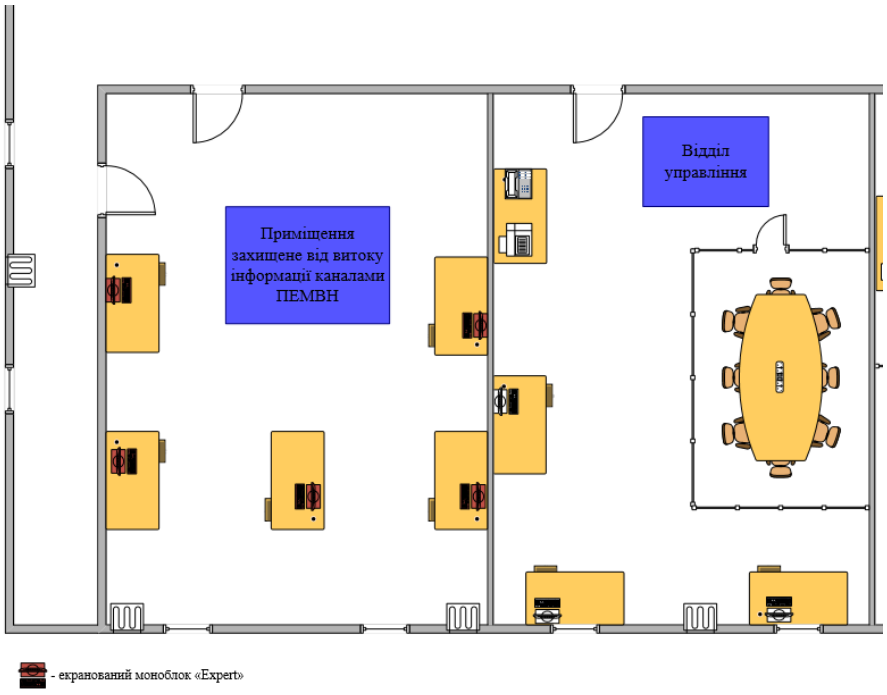

Рисунок 3.3 – Розміщення екранованих моноблоків «Expert» у приміщенні офісу

4 ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ТА ВИБІР ОПТИМАЛЬНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТІ ІНФОРМАТИЗАЦІЇ

При розробці СЗІ важливим кроком є розрахунок та порівняння ефективності розроблених рішень захисту інформації. Визначення ефективності допомагає визначити, наскільки добре кожна система може запобігти витоку інформації та який рівень захисту вона надає.

Ефективність СЗІ вимірюється за допомогою ряду параметрів. Згідно з алгоритму пошуку оптимальної СЗІ представленого на рисунку 2.2, для розрахунку ефективності комплексу засобів захисту або СЗІ було обрано формулу (2.6). Але для розрахунку ефективності комплексу засобів захисту спочатку необхідно розрахувати ризик реалізації загрози за умови невикористання засобів захисту (R_{jm}) інформації за формулою (2.4). Для розрахунку використовувались значення ймовірності реалізації загрози щодо ресурсу (P_{jm}) взяті з таблиці Д.4 додатку Д та збиток компанії від реалізації загрози щодо ресурсу (C_{jm}) вказаний компанією «DIAgency». Результати розрахунку ризику реалізації загрози за умови невикористання засобів захисту інформації (R_{jm}) представлено у таблиці 4.1.

Таблиця 4.1 – Розрахунок ризику реалізації загрози щодо ресурсу за умови невикористання засобів захисту

Загроза /Вразливість	Ймовірність реалізації j-ї загрози щодо ресурсу, по m-му каналу витоку за умови невикористання засобів захисту, P_{jm}	Збиток компанії від реалізації j-ї загрози щодо ресурсу (грн.), C_{jm}	Ризик реалізації jm-й загрози щодо ресурсу (грн.), R_{jm}
Ресурс 1. Інформація про фінансовий стан компанії, дані грошових переказів			
Загроза 5/Вразливість 6	0,5	1000000 грн.	500000 грн.
Ресурс 2. Документи, що стосуються роботи компанії			
Загроза 9/Вразливість 11	0,4	400000 грн.	160000 грн.
Ресурс 3. Накази і розпорядження керівництва компанії			
Загроза 12/Вразливість 14	0,5	300000 грн.	150000 грн.
Ресурс 10. Документи з інформацією про замовлення організації			
Загроза 29/Вразливість 35	0,6	700000 грн.	420000 грн.
Ресурс 11. Вимоги до продукту, напрацювання для нових продуктів та покращення вже наявних продуктів			
Загроза 31/Вразливість 37	0,7	3000000 грн.	2100000 грн.

Після розрахунку ризику реалізації загрози за умови невикористання засобів захисту інформації, для розрахунку ефективності комплексу засобів захисту, необхідно зробити розрахунок ризику реалізації загрози щодо ресурсу за умови використання засобів захисту за формулою (2.5). Ризик реалізації загрози щодо ресурсу за умови використання засобів захисту було розраховано для кожної розробленої СЗІ. Результати розрахунку ризику реалізації загрози за умови використання засобів захисту інформації представлено у таблиці 4.2.

Таблиця 4.2 – Розрахунок ризику реалізації загрози щодо ресурсу за умови використання засобів захисту

Назва СЗІ	Загроза /Вразливість	Ймовірність реалізації j-ї загрози щодо ресурсу, по m-му каналу витоку за умови використання засобів захисту, P_{jm}	Збиток компанії від реалізації j-ї загрози щодо ресурсу (грн.), C_{jm}	Ризик реалізації jm-й загрози щодо ресурсу (грн.), $R_{jm}(X_i)$
1	2	3	4	5
СЗІ від витоку каналами ПЕМВН з використанням генераторів радіочастотного шуму	Ресурс 1. Інформація про фінансовий стан компанії, дані грошових переказів			
	Загроза 5/Вразливість 6	0,25	1000000 грн.	250000 грн.
	Ресурс 2. Документи, що стосуються роботи компанії			
	Загроза 9/Вразливість 11	0,23	400000 грн.	92000 грн.
	Ресурс 3. Накази і розпорядження керівництва компанії			
	Загроза 12/Вразливість 14	0,27	300000 грн.	81000 грн.
	Ресурс 10. Документи з інформацією про замовлення організації			
	Загроза 29/Вразливість 35	0,3	700000 грн.	210000 грн.
	Ресурс 11. Вимоги до продукту, напрацювання для нових продуктів та покращення вже наявних продуктів			
	Загроза 31/Вразливість 37	0,33	3000000 грн.	990000 грн.

Продовження таблиці 4.2

1	2	3	4	5
СЗІ від витоку каналами ПЕМВН з використанням екранованої камери	Ресурс 1. Інформація про фінансовий стан компанії, дані грошових переказів			
	Загроза 5/Вразливість 6	0,11	1000000 грн.	110000 грн.
	Ресурс 2. Документи, що стосуються роботи компанії			
	Загроза 9/Вразливість 11	0,1	400000 грн.	40000 грн.
	Ресурс 3. Накази і розпорядження керівництва компанії			
	Загроза 12/Вразливість 14	0,13	300000 грн.	39000 грн.
	Ресурс 10. Документи з інформацією про замовлення організації			
	Загроза 29/Вразливість 35	0,14	700000 грн.	98000 грн.
	Ресурс 11. Вимоги до продукту, напрацювання для нових продуктів та покращення вже наявних продуктів			
	Загроза 31/Вразливість 37	0,16	3000000 грн.	480000 грн.

Продовження таблиці 4.2

1	2	3	4	5
СЗІ від витоку каналами ПЕМВН з використанням екранованих ПК	Ресурс 1. Інформація про фінансовий стан компанії, дані грошових переказів			
	Загроза 5/Вразливість 6	0,155	1000000 грн.	155000 грн.
	Ресурс 2. Документи, що стосуються роботи компанії			
	Загроза 9/Вразливість 11	0,12	400000 грн.	48000 грн.
	Ресурс 3. Накази і розпорядження керівництва компанії			
	Загроза 12/Вразливість 14	0,13	300000 грн.	39000 грн.
	Ресурс 10. Документи з інформацією про замовлення організації			
	Загроза 29/Вразливість 35	0,15	700000 грн.	105000 грн.
	Ресурс 11. Вимоги до продукту, напрацювання для нових продуктів та покращення вже наявних продуктів			
	Загроза 31/Вразливість 37	0,17	3000000 грн.	510000 грн.

При визначенні ефективності систем захисту інформації одним з ключових чинників, які необхідно врахувати, є вартість розробки та впровадження СЗІ, а саме розрахунок вартості засобів захисту інформації, які використовувались при розробці СЗІ. Розрахунок вартості кожної СЗІ та кількісний склад засобів захисту для кожної СЗІ представлено у таблиці 4.3.

Таблиця 4.3 – Розрахунок вартості розроблених систем захисту інформації

Назва СЗІ	Засіб захисту інформації	Кількість (шт.)	Вартість за 1шт. (грн.)	Вартість за запроваджені засоби захисту інформації
СЗІ від витоку каналами ПЕМВН з використанням генераторів радіочастотного шуму	Генератор радіочастотного шуму «PIAC-1C»	1 шт.	14760 грн.	14760 грн.
СЗІ від витоку каналами ПЕМВН з використанням екранованої камери	Екранована камера	1 шт.	600000 грн.	600000 грн.
СЗІ від витоку каналами ПЕМВН з використанням екранованих ПК	Екранований моноблок «Expert»	5 шт.	130000 грн.	650000 грн.

Для визначення ефективності комплексу засобів захисту інформації згідно з формулою (2.6) будуть використовуватись значення ризику витоку інформації за умови невикористання засобів захисту $\sum R_{jm}$ по всім інформаційним ресурсам чутливих до витоку каналами ПЕМВН, ризику витоку інформації за умови використання засобів захисту $\sum R_{jm}(X_i)$ також по всім інформаційним ресурсам чутливих до витоку каналами ПЕМВН та вартість розроблених СЗІ.

Поєднуючи ці параметри в формулі (2.6), отримується обчислювана метрика ефективності для кожної СЗІ. При цьому важливо врахувати, що найбільш ефективна система буде та, яка більше за всі інші знижує значення ризику витоку інформації каналами ПЕМВН. Розрахунок ефективності розроблених систем захисту інформації $E(X_i)$ представлено у таблиці 4.4.

Таблиця 4.4 – Розрахунок ефективності розроблених систем захисту інформації

Назва СЗІ	Ризик витоку інформації за умови невикористання засобів захисту (грн.), $\sum R_{jm}$	Ризик витоку інформації за умови використання засобів захисту (грн.), $\sum R_{jm}(X_i)$	Вартість СЗІ (грн.), $\sum S_i$	Ефективність комплексу засобів захисту (%), $E(X_i)$
СЗІ від витоку каналами ПЕМВН з використанням генераторів радіочастотного шуму	3330000 грн.	1623000 грн.	14760 грн.	50,86%
СЗІ від витоку каналами ПЕМВН з використанням екранованої камери	3330000 грн.	767000 грн.	600000 грн.	59,09%
СЗІ від витоку каналами ПЕМВН з використанням екранованих ПК	3330000 грн.	857000 грн.	650000 грн.	54,75%

Враховуючи ефективність комплексу засобів захисту $E(X_i)$ за формулою (2.8) визначається оптимальна СЗІ з множини, розроблених згідно з алгоритмом вирішення задачі вибору оптимальної СЗІ представленому на рисунку 2.2. Згідно з формулою (2.8) оптимальна СЗІ – це та СЗІ, яка надає найвищий рівень захисту за найкращою

ціною та вартістю обслуговування. Така система повинна бути не тільки ефективною, але й практичною для використання, враховуючи конкретні потреби та обмеження компанії. Але згідно з формулою (2.8) також найоптимальнішим рішенням захисту інформації є те рішення, у якого найбільша ефективність комплексу засобів захисту $E(X_i)$.

Як можна побачити з таблиці 4.4 СЗІ від витоку каналами ПЕМВН з використанням екранованої камери має найвищу ефективність серед усіх розроблених СЗІ, але і найбільшу вартість впровадження. Але при розрахунках ефективності комплексу засобів захисту $E(X_i)$ враховується також остатковий ризик після впровадження СЗІ, і якщо скласти вартість СЗІ і остатковий ризик після впровадження СЗІ і вважати цей показник за вартість, то у СЗІ від витоку каналами ПЕМВН з використанням екранованої камери буде найменша вартість так як остатковий ризик даної СЗІ найменший з запропонованих.

ВИСНОВКИ

У ході роботи було досліджено шляхи оптимізації комплексу засобів захисту інформації на об’єкті інформатизації. Для цього було проведено аналіз сучасних підходів до створення систем захисту інформації та нормативно-правової бази, що регулює процес побудови та впровадження систем захисту інформації. Це дозволило виділити переваги та недоліки існуючих підходів до створення комплексних систем захисту інформації, а також оцінити можливості їх використання для конкретного об'єкта інформатизації. В результаті аналізу нормативно-правової бази, було виявлено ключові вимоги, які пред'являються до СЗІ та яким повинна відповідати оптимізована СЗІ. Також встановлено основні орієнтири для створення власної системи захисту інформації.

Також було проаналізовано ряд показників ефективності та вибору оптимального складу засобів захисту інформації задля того, щоб вибрати найбільш точні показники вирішення задачі оптимізації комплексу засобів захисту інформації на об’єкті інформатизації. Використовуючи обрані показники було розроблено алгоритм найбільш оптимальної системи захисту інформації. Згідно з цим алгоритмом оптимальна система захисту інформації повинна забезпечувати найвищий рівень захисту за найкращою вартістю. Така система захисту інформації повинна бути не тільки ефективною, але й практичною для використання, враховуючи потреби та обмеження, що висуваються на конкретних об'єктах інформатизації.

Детально було проаналізовано існуючу комплексну систему захисту інформації, її структуру, механізми захисту, модель загроз та вразливостей компанії «DIAgency». Особливу увагу було приділено моделі загроз і вразливостей, яка дозволила визначити основні джерела загроз, потенційні канали витоку інформації, а також місця, де виявлені вразливості можуть бути використані зловмисниками.

Аналіз виявив, що в компанії існують значні загрози та вразливості витоку інформації каналами ПЕМВН, які на сьогоднішній день не захищені належним чином. Тому було прийняте рішення про розробку системи захисту інформації від витоку каналами ПЕМВН.

Для компанії «DIAgency» було розроблено декілька варіантів систем захисту інформації від витоку каналами ПЕМВН, які включають такі засоби захисту, як екрановані камери, генератори радіочастотного шуму, екрановані моноблоки. Кожний варіант був детально проаналізований з позицій ефективності захисту, вартості впровадження та обслуговування. Опрацювання кожного з варіантів дозволило вибрати ту систему захисту, яка найкращим чином відповідає потребам та можливостям компанії, а також забезпечує максимальний рівень захисту інформації.

Внаслідок розрахунків ефективності та показника оптимальності, оптимальною системою захисту інформації було визначено систему захисту інформації, що включає в себе екрановану камеру. Рівень захищенності даної системи захисту інформації від витоку каналами ПЕМВН є найвищим серед розглянутих. Так як система складається з пасивних засобів захисту інформації, то серед переваг системи можна виділити забезпечення постійного рівня захисту. Але серед недоліків серед недолікуів даної системи було виявлено високу вартість.

Ця система була обрана оптимальною при своїй досить великій вартості, так як після впровадження даної системи захисту інформації, остатковий ризик був найменшим, через що дана система захисту інформації є також і економічно вигідною.

Загалом, результати проведеного дослідження дозволили покращити рівень захисту інформації на об'єкті інформатизації, розробивши та оптимізувавши впровадженні засоби протидії витоку інформації каналами ПЕМВН.

Отже, дане дослідження дозволило розробити ефективну, вартісно оптимальну систему захисту інформації на об'єкті інформатизації, що покращує її безпеку та надійність. Дослідження може бути використане для підвищення ефективності та безпеки інформаційних систем в інших об'єктах інформатизації.

Окремі результати роботи були представлені на наукових конференціях. Одна з робот була представлена на всеукраїнській науково-практичній Internet-конференції «Моделювання та інформаційні технології в науці, техніці, кібербезпеці та освіті» та була опублікована у збірнику цієї конференції [12]. Дві роботи були представлені на конференціях 27-го міжнародного молодіжного форуму «Радіоелектроніка та молодь в XXI столітті» [14, 20] та були опубліковани у збірнику за результатами конференцій.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Комплексні системи захисту інформації : навч. посіб. / Ю. Яремчук та ін. Вінниця : Вінницький національний технічний університет, 2018. 143 с.
2. Гатчин Ю. А., Климова Е. В. Введение в комплексную защиту объектов информатизации. Санкт-Петербург : Научно-технический центр информационных технологий, 2011. 319 с.
3. Колтик М. А. Проблеми масової побудови комплексної системи захисту інформації (КСЗІ) та шляхи їх вирішення. *Проблеми програмування*. 2011. № 11. С. 69–78.
4. Малюк А. А. Методи захисту інформації. *Інформаційна безпека: концептуальні та методологічні основи захисту інформації* : навч. посіб. 2004. С. 79–87.
5. Основы организационного обеспечения информационной безопасности объектов информатизации / С. Н. Сёмкин и др. Москва : ГелиосАРВ, 2005. 305 с.
6. Закон України «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 20.04.2023).
7. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 20.04.2023).
8. General Data Protection Regulation. URL: https://gdpr-info.eu/ (date of access: 20.04.2023).
9. ISO/IEC 27001:2013(en) Information technology – Security techniques – Information security management systems – Requirements. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en (date of access: 20.04.2023).
10. Корнюшин П. Н., Костерин С. С. Информационная безопасность : учеб. пособ. Владивосток : ТИДОТ ДВГУ, 2003. 182 с.
11. Голев Д. В., Кононович В. Г., Хомич С. В. Методики оцінки інформаційної захищеності телекомунікацій : навч. посіб. Одеса : ОНАЗ ім. О.С. Попова, 2013. 206 с.
12. Румянцева О. В. Аналіз методів класифікації вразливостей та загроз інформаційної системи. *Всеукраїнська науково-практична Internet-конференція*

«Моделювання та інформаційні технології в науці, техніці, кібербезпеці та освіті». 2022. С. 52–56.

13. Ротштейн О. П. Моделювання та оптимізація надійності багатовимірних алгоритмічних процесів. Вінниця : УНІВЕРСУМ-Вінниця, 2007. 309 с.

14. Румянцева О. В. Аналіз моделей систем захисту інформації, побудованих з використанням теорії графів. *27-ий Міжнародний молодіжний форум «Радіоелектроніка та молодь в XXI столітті»*. 2023. С. 46–47.

15. Малышев Н. Г., Бернштейн Л. С., Боженюк А. В. Нечеткие модели для экспертных систем в САПР. Москва : Энергоиздат, 1991. 384 с.

16. Комплексные системы защиты информации предприятия : учеб. пособ. / В. Т. Еременко и др. Орел : ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», 2016. 270 с.

17. NIST Computer Security Resource Center | CSRC. URL: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf (дата звернення: 23.04.2023)..

18. Горохов Д. Е. Методика формирования рационального состава комплекса средств защиты информации на основе априорной оценки риска : автореф. дис. … канд. тех. наук. Орел, 2010. 140 с.

19. Домарев В. В. Безопасность информационных технологий, системный подход. Санкт-Петербург : ТИД «ДС», 2004. 317 с.

20. Румянцева О. В. Застосування ігрової моделі для дослідження оптимальності систем захисту інформації. *27-ий Міжнародний молодіжний форум «Радіоелектроніка та молодь в XXI столітті»*. 2023. С. 48–49.

21. Методика оценки риска ГРИФ 2005 из состава Digital Security Office. URL: http://citforum.ru/products/dsec/grif/ (дата звернення: 20.04.2023).

22. НД ТЗІ 2.5-007-07. Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробці в автоматизованих системах класу 1. Чинний від 2007-12-12. Вид. офіц. Київ : Державна служба спеціального зв'язку України, 2007. 9 с.

23. НД ТЗІ 1.1-005-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

Чинний від 2007-12-12. Вид. офіц. Київ : Державна служба спеціального зв'язку України, 2007. 7 с.

24. НД ТЗІ 3.3-001-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації. Чинний від 2007-12-12. Вид. офіц. Київ : Державна служба спеціального зв'язку України, 2007. 9 с.

25. НД ТЗІ 2.1-002-07. Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення. Чинний від 2007-12-12. Вид. офіц. Київ : Державна служба спеціального зв'язку України, 2007. 9 с.

26. НД ТЗІ 3.1-001-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. Чинний від 2007-12-12. Вид. офіц. Київ : Державна служба спеціального зв'язку України, 2007. 12 с.

27. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Чинний від 2005-11-08. Вид. офіц. Київ : Державна служба спеціального зв'язку України, 2005. 22 с.

28. Румянцева О. В. Забезпечення комплексного захисту інформаційних ресурсів компанії : кваліфікаційна робота першого (бакалаврського) рівня вищої освіти : 125. Харків, ХНУРЕ, 2021. 50 с.