Розділ 18. Оцінка захищеності інформації в інформаційно-телекомунікаційних системах (ІКС)

18.1. Оцінка захищеності інформації в інформаційно-телекомунікаційних системах згідно НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»

18.2. Концептуальна схема оцінки безпеки інформації.

18.3. Кількісна та якісна оцінки безпеки інформації.

18.1. Оцінка захищеності інформації в інформаційно-телекомунікаційних системах згідно НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»

Цей нормативний документ (далі – Критерії) – установлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу. Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

Критерії надають:

1. Порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах.

2. Базу (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

Критерії можуть застосовуватися до всього спектра комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно-орієнтовані системи та ін.

В цьому нормативному документі використовуються такі позначення і скорочення:

Загальні терміни:

– АС – автоматизована система;
– КС – комп'ютерна система;
– КЗЗ – комплекс засобів захисту;
– НСД – несанкціонований доступ;
– ОС – обчислювальна система;
– ПЗ – програмне забезпечення;
– ПЗП – постійний запам'ятовуючий пристрій;
– ПРД – правила розмежування доступу;

Позначення послуг:

– КД – довірча конфіденційність;
– КА – адміністративна конфіденційність;
– КО – повторне використання об'єктів;
– КК – аналіз прихованих каналів;
– КВ – конфіденційність при обміні;
– ЦД – довірча цілісність;
– ЦА – адміністративна цілісність;
– ЦО – відкат;
– ЦВ – цілісність при обміні;
– ДР – використання ресурсів;
– ДВ – стійкість до відмов;
– ДЗ – гаряча заміна;
– ДВ – відновлення після збоїв;
– НР – реєстрація;
– НИ – ідентифікація і автентифікація;
– НК – достовірний канал;
– НО – розподіл обов'язків;
– НЦ – цілісність КЗЗ;
– НТ – самотестування;
– НВ – автентифікація при обміні;
– НА – автентифікація відправника;
– НП – автентифікація одержувача.

Побудова і структура критеріїв захищеності інформації

В процесі оцінки спроможності комп'ютерної системи забезпечувати захист оброблюваної інформації від несанкціонованого доступу розглядаються вимоги двох видів:

– вимоги до функцій захисту (послуг безпеки);
– вимоги до гарантій.

В контексті Критеріїв комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного. Рівні починаються з першого (1) і зростають до значення n, де n – унікальне для кожного виду послуг.

Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів.

Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги треба шукати в розділі “Критерії конфіденційності”. В цьому

розділі описані такі послуги (в дужках наведені умовні позначення для кожної послуги): довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні (експорті/імпорті).

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. Якщо існують вимоги щодо обмеження можливості модифікації інформації, то відповідні послуги треба шукати в розділі "Критерії цілісності". В цьому розділі описані такі послуги: довірча цілісність, адміністративна цілісність, відкат і цілісність при обміні.

Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то відповідні послуги треба шукати в розділі "Критерії доступності". В цьому розділі описані такі послуги: використання ресурсів, стійкість до відмов, горяча заміна, відновлення після збоїв.

Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні послуги треба шукати у розділі "Критерії спостереженості". В цьому розділі описані такі послуги: реєстрація, ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, автентифікація при обміні, автентифікація відправника (невідмова від авторства), автентифікація одержувача (невідмова від одержання).

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в комп'ютерній системі, цей документ містить критерії гарантій, що дозволяють оцінити коректність реалізації послуг. Критерії гарантій включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації. В цих Критеріях вводиться сім рівнів гарантій (Г-1,..., Г-7), які є ієрархічними. Ієрархія рівнів гарантій відбиває поступово наростаючу міру певності в тому, що реалізовані в комп'ютерній системі послуги дозволяють протистояти певним загрозам, що механізми, які їх реалізують, в свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації комп'ютерної системи.

Структуру Критеріїв показано на рисунку 18.1.

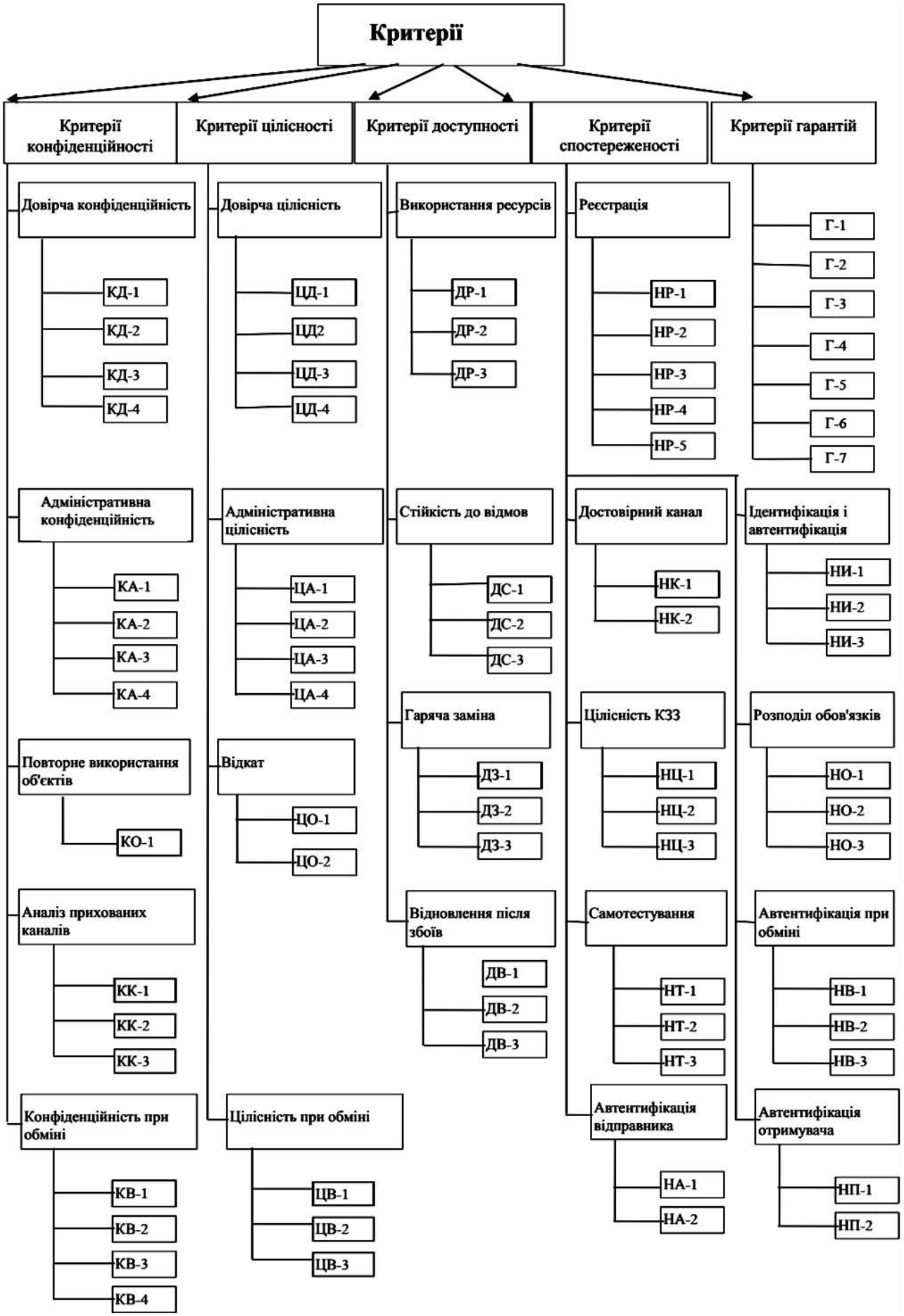

Рисунок 18.1 – Структура критеріїв

Всі описані послуги є більш-менш незалежними. Якщо ж така залежність виникає, тобто реалізація якої-небудь послуги неможлива без реалізації іншої, то цей факт відбивається як необхідні умови для даної послуги (або її рівня). За винятком послуги *аналіз прихованих каналів* залежність між функціональними послугами і гарантіями відсутня. **Рівень послуги *цілісність комплексу засобів захисту* НЦ-1 є необхідною умовою абсолютно для всіх рівнів всіх інших послуг.**

Порядок оцінки комп'ютерної системи на предмет відповідності цим Критеріям визначається відповідними нормативними документами. Експертна комісія, яка проводить оцінку комп'ютерної системи, визначає, які послуги і на якому рівні реалізовані в даній комп'ютерній системі, і як дотримані вимоги гарантій. Результатом оцінки є рейтинг, що являє собою упорядкований ряд (перелічення) буквено-числових комбінацій, що позначають рівні реалізованих послуг, в поєднанні з рівнем гарантій. Комбінації упорядковуються в порядку опису послуг в критеріях. Для того, щоб до рейтингу комп'ютерної системи міг бути включений певний рівень послуги чи гарантій, повинні бути виконані всі вимоги, перелічені в критеріях для даного рівня послуги або гарантій.

Критерії конфіденційності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям конфіденційності, КЗЗ оцінюваної КС повинен надавати послуги з захисту об'єктів від несанкціонованого ознайомлення з їх змістом (компрометації). Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні.

Довірча конфіденційність

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжуються на підставі повноти захисту і вибірковості керування.

<table>
<tr><th>КД-1. Мінімальна довірча конфіденційність</th><th>КД-2. Базова довірча конфіденційність</th><th>КД-3. Повна довірча конфіденційність</th><th>КД-4. Абсолютна довірча конфіденційність</th></tr>
<tr><td colspan="2">Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td><td colspan="2">Політика довірчої конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС</td></tr>
<tr><td colspan="4">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td>процесу і захищеного об'єкта</td><td colspan="2">користувача і захищеного об'єкта</td><td>користувача, процесу і захищеного об'єкта</td></tr>
<tr><td colspan="4">Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта</td></tr>
</table>

<table>
<tr><td colspan="4">КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити</td></tr>
<tr><td>конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td></tr>
<tr><td>—</td><td colspan="3">КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити
конкретних користувачів і/або групи користувачів, які мають право ініціювати процес
конкретних користувачів (і групи користувачів), які мають, а також тих, що не мають права ініціювати процес</td></tr>
<tr><td colspan="4">Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту</td></tr>
<tr><td colspan="2">НЕОБХІДНІ УМОВИ: НИ-1</td><td colspan="2">НЕОБХІДНІ УМОВИ: КО-1, НИ-1</td></tr>
</table>

Для усіх інших послуг існують аналогічні таблиці, які приведені у стандарті, який повністю наведений у додатку А.

Адміністративна конфіденційність

Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості управління.

Повторне використання об'єктів

Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

Аналіз прихованих каналів

Аналіз прихованих каналів виконується з метою виявлення і усунення потоків інформації, які існують, але не контролюються іншими послугами. Рівні даної послуги ранжируються на підставі того, чи виконується тільки виявлення, контроль або перекриття прихованих каналів.

Конфіденційність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Критерії цілісності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям цілісності, КЗЗ оцінюваної КС повинен надавати послуги з захисту оброблюваної інформації від несанкціонованої модифікації. Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні.

Довірча цілісність

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Адміністративна цілісність

Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Відкат

Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

Цілісність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Критерії доступності

Для того, щоб КС могла бути оцінена на відповідність критеріям доступності, КЗЗ оцінюваної КС повинен надавати послуги щодо забезпечення можливості використання КС в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність КС функціонувати у випадку відмови її компонентів. Доступність може забезпечуватися в КС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

Використання ресурсів

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

Стійкість до відмов

Стійкість до відмов гарантує доступність КС (можливість використання інформації, окремих функцій або КС в цілому) після відмови її компонента. Рівні даної послуги ранжируються на підставі спроможності КЗЗ забезпечити можливість функціонування КС в залежності від кількості відмов і послуг, доступних після відмови.

Гаряча заміна

Ця послуга дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів. Рівні даної послуги ранжируються на підставі повноти реалізації.

Відновлення після збоїв

Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

Критерії спостереженості

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям спостереженості, КЗЗ оцінюваної КС повинен надавати послуги з забезпечення відповідальності користувача за свої дії і з підтримки спроможності КЗЗ виконувати свої функції. Спостереженість забезпечується в КС такими послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача

Реєстрація

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

Ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

Достовірний канал

Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

Розподіл обов'язків

Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Цілісність комплексу засобів захисту

Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Самотестування

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

Ідентифікація і автентифікація при обміні

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

Автентифікація відправника

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

Автентифікація отримувача

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

Критерії гарантій

Критерії гарантій включають вимоги до архітектури КЗЗ, середовища розробки, послідовності розробки, середовища функціонування, документації і випробувань КЗЗ. В цих критеріях вводиться сім рівнів гарантій, які є ієрархічними. Вимоги викладаються за розділами. Для того, щоб КС одержала певний рівень гарантій (якщо вона не може одержати більш високий), повинні бути задоволені всі вимоги, визначені для даного рівня в кожному з розділів.

Архітектура

Вимоги до архітектури забезпечують гарантії того, що КЗЗ у змозі повністю реалізувати політику безпеки.

Середовище розробки

Вимоги до середовища розробки забезпечують гарантії того, що процеси розробки і супроводження оцінюваної КС є повністю керованими з боку Розробника.

Послідовність розробки

Вимоги до процесу проектування (послідовності розробки) забезпечують гарантії того, що на кожній стадії розробки (проектування) існує точний опис КС і реалізація КС точно відповідає вихідним вимогам (політиці безпеки).

Середовище функціонування

Вимоги до середовища функціонування забезпечують гарантії того, що КС поставляється Замовнику без несанкціонованих модифікацій, а також інсталюється і ініціюється Замовником так, як це передбачається Розробником.

Документація

Вимоги до документації є загальними для всіх рівнів гарантій.

У вигляді окремих документів або розділів (підрозділів) інших документів Розробник повинен подати опис послуг безпеки, що реалізуються КЗЗ, настанови адміністратору щодо послуг безпеки, настанови користувача щодо послуг безпеки.

В описі функцій безпеки повинні бути викладені основні, необхідні для правильного використання послуг безпеки, принципи політики безпеки, що реалізується КЗЗ оцінюваної КС, а також самі послуги.

Настанови адміністратору щодо послуг безпеки мають містити опис засобів інсталяції, генерації і запуску КС, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску КС, опис властивостей КС, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ, а також інструкції щодо використання адміністратором послуг безпеки для підтримки політики безпеки, прийнятої в організації, що експлуатує КС.

Настанови користувачу щодо послуг безпеки мають містити інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором).

Назва документів (розділів) не регламентується. Опис послуг безпеки може відрізнятися для користувача і адміністратора. Настанови адміністратору і настанови користувачу можуть бути об'єднані в настанови з установлення і експлуатації.

Випробування комплексу засобів захисту

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
Розробник повинен подати для перевірки програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують послуги безпеки. Мають бути представлені аргументи для підтвердження достатності тестового покриття	+	=	=	=	=	=	=
Розробник повинен подати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування	+	=	=	=	=	=	=

Розробник повинен усунути або нейтралізувати всі знайдені “слабкі місця” і виконати повторне тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові “слабкі місця ”	-	+	=	=	=	=	=
Розробник повинен виконати тести з подолання механізмів захисту і довести, що КЗЗ відносно або абсолютно стійкий до такого роду атак з боку Розробника	-	-	-	+	=	+	=

18.2. Концептуальна схема оцінки безпеки інформації

Відповідно до стандарту ISO/IEC 15408 «Критерії оцінки безпеки інформаційних технологій» (Загальні критерії) загальна схема забезпечення інформаційної безпеки, має такий вигляд (рис. 14.2). На схемі показано взаємодію основних суб’єктів та об’єктів забезпечення інформаційної безпеки. Дана схема можна використовувати як основу для побудови концептуальної моделі інформаційної безпеки (ІБ) державних інформаційних ресурсів (ДІР).

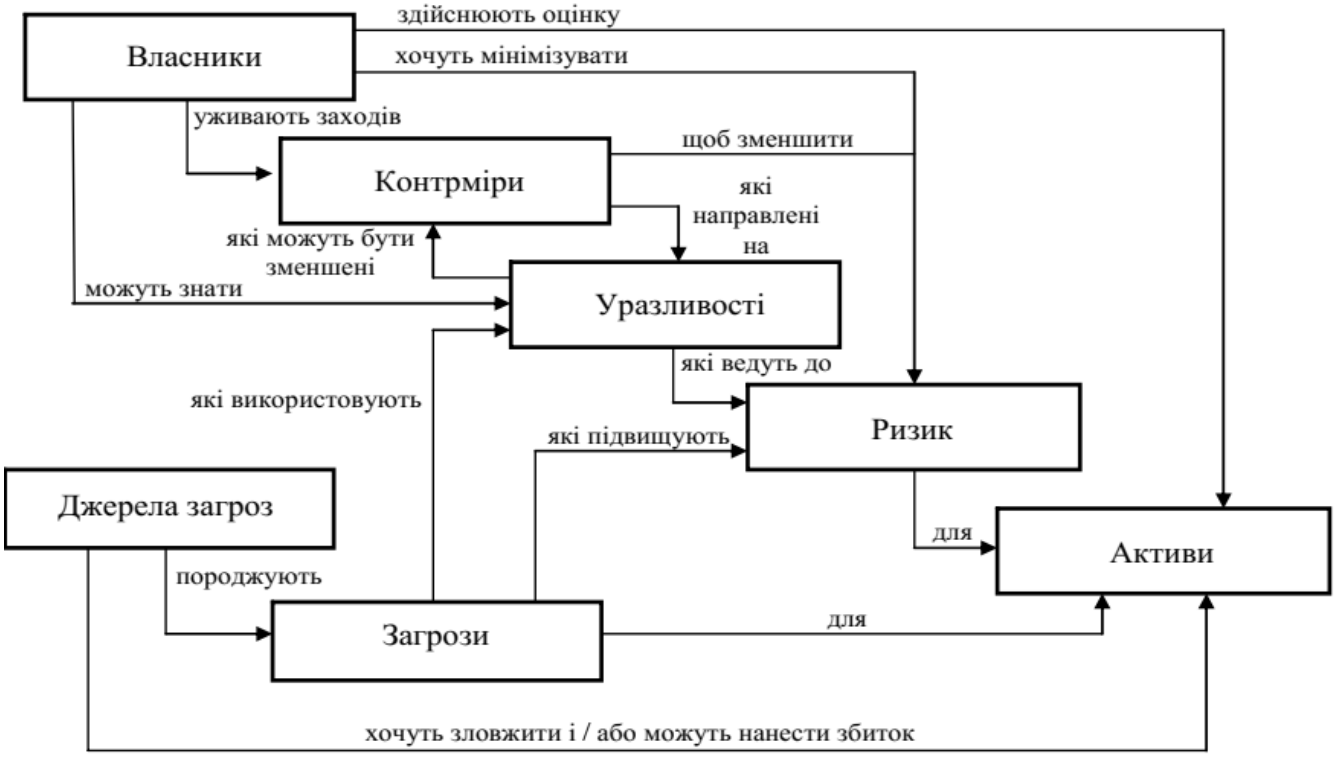

Рисунок 18.2 – Загальна схема забезпечення інформаційної безпеки відповідно до стандарту ISO/IEC 15408«Критерії оцінки безпеки інформаційних технологій»

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» (від 23 лютого 2006 року № 3475-IV зі змінами від 28.07.2022 року) державні інформаційні ресурси (ДІР) визначає наступним чином: ***державні інформаційні ресурси –*** систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень.

Крім того існує розширене визначення поняття ДІР.

Державні інформаційні ресурси – це результат інтелектуальної та практичної діяльності, що сформовані в усіх сферах життєдіяльності людини, суспільства і держави, зафіксовані і систематизовані на відповідних матеріальних носіях інформації, як окремі документи і масиви документів, банки і бази даних та знань, усі види архівів і бібліотек, музейні фонди, інформаційні ресурси які обробляються й передаються у інформаційних системах державного і/або загального призначення, інші ресурси, що містять дані, відомості і знання, які є об'єктом права власності держави незалежно від форми власності на час їх створення і мають споживчу цінність, а також такі, що призначені для розвитку і задоволення потреб громадян, суспільства, держави та підлягають захисту згідно визначеної політики безпеки й чинного законодавства.

Інформаційна безпека (ІБ) визначається як стан захищеності інформаційного середовища держави, суспільства та особистості, якій забезпечує його формування, збереження, використання і розвиток в інтересах громадян, організації чи держави. Там же наведено більш розширене визначення ІБ.

Інформаційна безпека – це стан захищеності властивостей інформації (інформаційних ресурсів), що належить державі, суспільству і особистості, за якого забезпечується її оброблення, зберігання, поширення і прогресивний розвиток незалежно від (або в умовах) наявності чи реалізації внутрішніх і зовнішніх інформаційних загроз.

До основних **компонентів концептуальної моделі ІБ ДІР** можуть бути віднесені:

– об'єкти загроз ДІР;

– загрози ДІР (нормативно-правового, організаційного, інженерно-технічного спрямування), за відповідними властивостями інформації (конфіденційність, цілісність, доступність);

– джерела загроз ДІР;

– уразливості ДІР;

– ризик реалізації загрози ДІР через уразливість;

– цілі джерел загроз ДІР;

– джерела відомостей про ДІР;

– способи неправомірного оволодіння ДІР (способи доступу до ДІР);

– напрями захисту ДІР (нормативно-правовий, організаційний, інженерно-технічний);

– способи захисту ДІР;

– засоби захисту ДІР

Об'єкти загроз ДІР (відповідно до визначеного авторами поняття ДІР) – всі інформаційні ресурси держави, суспільства або громадян, які підлягають захисту згідно визначеної політики безпеки й чинного законодавства.

Загрози ДІР – це потенційний або реальний стан небезпеки державним інформаційним ресурсам та безпосередньо їх властивостям (конфіденційності, цілісності, доступності), який може бути сформовано на основі реалізації будь-якого процесу та/або вчиненні діяння (та/або бездіяльності), спрямовано на порушення політики безпеки об'єкта інформаційної діяльності (державних інформаційних ресурсів) та такий, що завдає збитку державі. Крім того, через призму загальних напрямів забезпечення безпеки інформації (правовий захист, організаційний захист, інженерно-технічний захист) загрози ДІР можуть бути визначені як загрози відповідного спрямування:

– загрози нормативно-правового спрямування – загрози, які виникають в разі навмисного або ненавмисного порушення (впливу або/та дії на процес створення та застосування) спеціальних законів, інших нормативно-правових актів, правил, процедур та заходів, що забезпечують захист інформації на правовій основі;

– загрози організаційного спрямування – виникають у результаті навмисного або ненавмисного порушення регламентації виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, що виключає або суттєво утруднює реалізацію процесів протидії несанкціонованому порушенню властивостей інформації (інформаційних ресурсів);

– загрози інженерно-технічного спрямування – загрози, що пов'язані з використанням різноманітних фізичних, апаратних, програмних, програмно-апаратних методів та засобів, які реалізують процеси розголошення, витоку, несанкціонованого доступу, інших форм незаконного спотворення і втручання до інформаційних ресурсів, а також призводять до різних видів збитків власнику ресурсів.

Джерела загроз ДІР – носії загроз безпеці інформації ДІР (кібертерористи та кіберзловмисники, персонал підданий корупційним діям, адміністративно-управлінські органи державної влади і т. д.). У цілому всі джерела загроз безпеці інформації можна розділити на три групи обумовлені діями суб'єкта (антропогенні джерела загроз); обумовлені технічними засобами (техногенні джерела загроз); зумовлені стихійними джерелами.

Уразливості ДІР – чинники, що призводять до порушення безпеки інформації на конкретному об'єкті інформаційної діяльності.

Ризик реалізації загрози ДІР

Існує декілька визначень поняття ризику:

– Ризик – функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

– Ризик – потенційна можливість використання уразливостей активу або групи активів реальною загрозою для заподіяння збитку організації (ISO/IEC 27005:2008).

– Ризик – комбінація ймовірності події і її наслідків (BS 7799-3:2006).

Таким чином ***ризик реалізації загрози ДІР*** – потенційна можливість використання уразливостей державних інформаційних ресурсів реальною загрозою для заподіяння збитку державі, суспільству, окремому громадянину.

Цілі джерел загроз ДІР – ознайомлення з конфіденційними відомостями, їх модифікація з корисною метою, знищення для нанесення прямого матеріального збитку.

Джерела відомостей про ДІР – люди, документи та документообіг в цілому (паперовий, електронний), відкриті публікації, технічні носії інформації, технічні засоби виробничої та трудової діяльності, продукція та відходи виробництва.

Способи неправомірного оволодіння ДІР (способи доступу до ДІР) – розголошення джерелами конфіденційних відомостей, витік інформації через технічні засоби, несанкціонований доступ до відомостей, що підлягають охороні.

Напрями захисту ДІР – це нормативноправові категорії, орієнтовані на забезпечення комплексного захисту інформації від внутрішніх та зовнішніх загроз на державному рівні, на рівні підприємства або організації, а також на рівні окремої особистості. До основних напрямків захисту ДІР відносяться відповідно до комплексного підходу до захисту ДІР нормативноправовий, організаційний та інженернотехнічний.

Способи захисту ДІР – будь-які міри, шляхи, способи та дії, які забезпечують попередження протиправних дій, їх запобігання, припинення та протидію несанкціонованому доступу до ДІР.

Засоби захисту ДІР – фізичні, апаратні, програмні засоби та криптографічні методи. Криптографічні методи можуть бути реалізовані як апаратно так і змішано програмно-апаратними засобами.

Таким чином, **концептуальна модель ІБ ДІР може бути представлена у вигляді наступної схеми** (рис. 18.3).

Рисунок 18.3 – Концептуальна модель інформаційної безпеки державних інформаційних ресурсів

18.3. Кількісна та якісна оцінки безпеки інформації

Розглянемо класифікацію існуючих методів і засобів оцінки інформаційних ризиків.

Оцінка ризику – це процес, який використовується для присвоєння значень наслідків, ймовірності виникнення та рівня ризику. Вона включає в себе:

1. Оцінку ймовірності загроз і вразливостей, які можливі.
2. Розрахунок впливу, який може мати загроза на кожен актив.
3. Визначення кількісної (вимірні) або якісної (описуваної) вартості ризику.

Треба взяти до уваги те, що ці три змінні рідко незалежні одина від одної. В області інформаційної безпеки, є зв'язок між вартістю активів, впливом і ймовірністю. Наприклад, більш імовірно, що хакер буде використовувати уразливість, яка викликає більший вплив, ніж уразливість з низьким рівнем впливу. Крім того, цінний актив має більшу імовірність компрометації, ніж марний. Таким чином, в цій області повинно прийматися до уваги більше, ніж просто випадкові дії. Необхідно брати до уваги, що при наявності достатнього часу і рішучості, люди мають можливість обійти майже всі заходи безпеки. Вони можуть бути надзвичайно творчими, коли мотивовані. Таким чином, фактор мотивації повинен бути серйозно розглянутий в процесі оцінки безпеки інформаційного ризику.

На рис. 14.4 представлені три способи, за допомогою яких можна проводити оцінку інформаційних ризиків:

1. Методи.
2. Управляючі документи.
3. Інструменти.

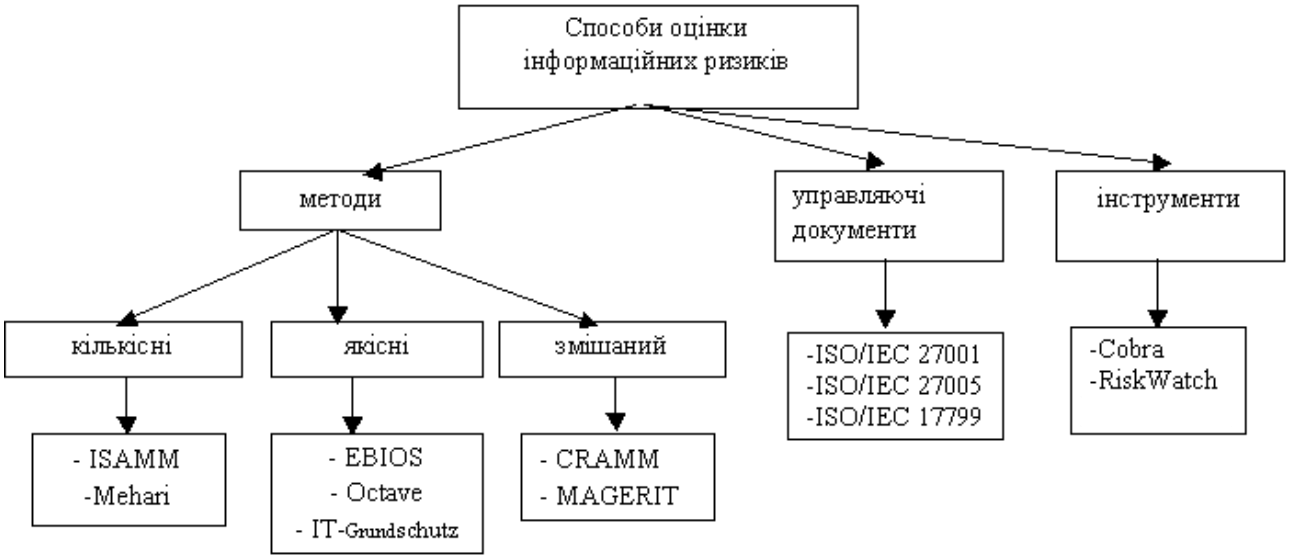

Рисунок 18.3 – Способи оцінки інформаційних ризиків

1. Методи

Метод розуміється, як систематизована сукупність кроків, дій, які необхідно зробити для вирішення певної задачі або досягти поставленої мети, в даному випадку провести оцінку ризиків. Тобто, метод мається на увазі покрокова інструкція плюс інструмент (програмний продукт) для проведення оцінки ризиків на підприємстві.

Всі методи оцінки ризику можна розділити на кількісні, якісні або комбінацію кількісних методів з якісними (змішаний).

Кількісні методи використовують вимірні, об'єктивні дані для визначення вартості активів, імовірність втрати і пов'язаних з ними ризиків. Мета полягає в тому, щоб обчислити числові значення для кожного з компонентів, зібраних в ході оцінки ризиків та аналізу витрат і переваг.

Якісні методи використовують відносний показник ризику або вартості активу на основі рейтингу або поділ на категорії, такі як низький, середній, високий, не важливо, важливо, дуже важливо, чи за шкалою від 1 до 10. Якісна модель оцінює дії й імовірності виявлених ризиків швидким і економічно ефективним способом. Набори ризиків записані і проаналізовані в якісній оцінці ризику, та можуть послужити основою для цілеспрямованої кількісної оцінки.

Раніше кількісні підходи використовувалися частіше. Однак, останнім часом використання суворо кількісних управлінь ризиками зазвичай призводить до важкої, тривалої роботи, і немає великих переваг перед якісним методом оцінки ризиків. **Комбінація кількісного і якісного методу** являє собою змішану сукупність переваг і недоліків вище згаданих методів.

Таблиця 118.1 – Переваги та недоліки методів оцінки інформаційних ризиків

	Кількісний	**Якісний**
Переваги	– ризики є пріоритетнішими фінансових наслідків; – активи є пріоритетнішими фінансових цінностей; – отримання спрощених результатів управління ризиком та поверненням інвестицій у забезпечення безпеки; – результати можуть бути виражені в управлінській специфічній термінології (наприклад, грошові значення і ймовірність виражається у вигляді певного відсотка); – точність має тенденцію до збільшення з плином часу, так як організація постійно веде записи даних.	– забезпечує прозорість і розуміння класифікації ризику; – можливість досягти консенсусу; – немає необхідності визначати фінансову вартість активів; – легше залучити людей, які не є експертами в області комп'ютерної безпеки.
Недоліки	– вплив значення, привласнених ризикам на підставі суб'єктивних думок учасників; – процес для досягнення надійних результатів і консенсусу займає багато часу; – розрахунок може бути складним і трудомістким; – результати представлені тільки в грошовому еквіваленті і їх складно інтерпретувати для «нетехнічних людей»; – процес вимагає спеціальних знань, тому складно навчити персонал.	– недостатня відмінність між важливими ризиками; – важко виправдати інвестиції в контроль реалізації, тому що немає підстав для аналізу витрат і переваг; – результати залежать від якості команди управління ризиками, яка буде створена.

Далі будуть розглянуті кращі світові методи для проведення повноцінної оцінки ризиків.

Методи оцінки ризику:

1.1. ISAMM

Виробник: Бельгія.

Опис: ISAMM була розроблена на основі Telindus. Це кількісний тип методології управління ризиками, де оцінюються ризики, виражаючи їх через щорічні очікувані збитків в грошових одиницях:

*Щорічні очікувані збитки (ALE) = [ймовірність] * [середній вплив].*

ISAMM дозволяє показувати й моделювати зниження ризику для кожного поліпшеного контролю і порівнювати з його вартістю реалізації. Ефективність методу дозволяє виконувати обґрунтовану оцінку ризику в рамках, з мінімальними витратами часу і зусиль. Останньою еволюцією в методології ISAMM є уявлення активів. Це означає, що він може бути використаний для запуску оцінки ризиків щодо активів або згрупувати набір активів. Цей метод оцінки ризиків складається з трьох основних частин: огляду; оцінки; результат розрахунків та звітність.

Метод оцінки ризику: кількісний.

Наявність допоміжних програмних інструментів: немає, але має хорошу керівну документацію.

1.2. Mehari

Виробник: Франція.

Опис: Це модель управління ризиками, з модульними компонентами і процесами. Модуль оцінки охоплює, крім інформаційної системи, організацію та її місця розташування в цілому, а також умови роботи, правові та нормативні аспекти.

Метод оцінки ризику: якісний і кількісний.

Наявність допоміжних програмних інструментів: є.

1.3. EBIOS

Виробник: Франція.

Опис: EBIOS являє собою повний набір посібників. Виробляються кращі практики, а також додатки документів, орієнтовані на кінцевих користувачів в різних контекстах. Цей метод широко використовується як в державному, так і приватному секторі. EBIOS формалізує підхід до оцінки ризику в області інформаційної безпеки систем. Метод враховує всі технічні об'єкти (програмне і апаратне забезпечення, мережі) і нетехнічні об'єкти (організації, людські аспекти, фізична безпека).

Метод оцінки ризику: якісний.

Наявність допоміжних програмних інструментів: є.

1.4. Octave

Виробник: США.

Опис: OCTAVE є самостійним підходом, що вказує на те, що персонал несе відповідальність за встановлення стратегії безпеки організації. OCTAVE вимагає аналізу в розгляді відносини між критично важливими активами, загрозами для цих активів і вразливостями (як організаційні, так і технологічні). Він визначає

пов'язані з інформацією активи, які важливі для організації і зосереджує діяльність на ці активи, тому що вони мають найбільш важливе значення для організації (акцент на кількох важливих активів, не більше п'яти). Існують різні OCTAVE методи, засновані на OCTAVE критеріях:

– OCTAVE;

– OCTAVE-S;

– OCTAVE Allegro.

Метод оцінки ризику: якісний.

Наявність допоміжних програмних інструментів: є.

1.5. IT-Grundschutz

Виробник: Німеччина.

Опис: IT-Grundschutz пропонує спосіб для створення системи управління інформаційною безпекою. Вона включає в себе як загальні рекомендації по забезпеченню безпеки IT так і допоміжні технічні рекомендації для досягнення необхідного рівня IT безпеки для конкретного домену.

У методі IT-Grundschutz представлені каталоги:

– модулі;

– каталоги загроз;

– каталоги захисту.

Метод оцінки ризику: якісний.

Наявність допоміжних програмних інструментів: є.

1.6. CRAMM

Виробник: Великобританія.

Опис: Метод CRAMM досить складно використовувати без CRAMM інструменту. У інструмента такаж назва, як і у методу – CRAMM. В основі методу CRAMM лежить комплексний підхід до оцінки ризиків, поєднуючи кількісні та якісні методи аналізу. Метод є універсальним і підходить як для великих, так і для дрібних організацій, як урядового, так і комерційного сектора. Грамотне використання методу CRAMM дозволяє отримувати дуже хороші результати, найбільш важливим з яких є можливість економічного обгрунтування витрат організації на забезпечення інформаційної безпеки та безперервності бізнесу. Економічно обгрунтована стратегія управління ризиками дозволяє, в кінцевому підсумку, заощаджувати кошти, уникаючи невиправданих витрат.

Метод оцінки ризику: якісний і кількісний.

Наявність допоміжних програмних інструментів: є.

1.7. Назва методу: Magerit

Виробник: Іспанія.

Опис: Magerit є відкритою методологією аналізу та управління ризиками пропонованої в якості основи і керівництва:

– для того, щоб особи відповідальні за інформаційні системи знали про існування ризиків і необхідність розглядати їх своєчасно;

– для пропозиції систематичного методу аналізу цих ризиків;

– для опису і планування відповідних заходів по утриманню ризику під контролем;

– для підготовки організації по процесу оцінки, аудиту, сертифікації та акредитації.

Метод оцінки ризику: кількісний і якісний.

Наявність допоміжних програмних інструментів: є.

2. Управляючі документи

Крім методів оцінки ризиків використовують управляючі документи. Де теоретично описуються і даються методичні вказівки процесу оцінки ризиків, але не дається конкретних технологій. Найвідоміші стандарти, які використовуються на території України: ISO 27001, ISO 27005, ISO 17799.

2.1. ISO/IEC 27001

Опис: Міжнародний стандарт ISO/IEC 27001 визначає процеси, що представляють можливість бізнесу встановлювати, застосовувати, переглядати, контролювати і підтримувати ефективну систему менеджменту інформаційної безпеки.

У даному стандарті регламентовані вимоги до розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення документованої системи менеджменту інформаційної безпеки в контексті існуючих бізнес ризиків організації.

Зазначені вимоги реалізуються в рамках документованих процесів менеджменту інформаційної безпеки, структурованих по моделі PDCA (Plan-Do-Check-Act). Стандарт ISO/IEC 27001 являє наочну модель менеджменту, що дозволяє здійснювати оцінку ризиків, проектування і реалізацію системи інформаційної безпеки, її менеджмент і переоцінку.

2.2. ISO/IEC 27005

Опис: Цей стандарт призначений для визначення в організації підходу до менеджменту ризиків в залежності, наприклад, від області дії СМІБ, області застосування менеджменту ризиків або сектора промисловості. Забезпечує рекомендації для менеджменту ризиків інформаційної безпеки, які включають інформацію і менеджмент ризиків безпеки технологій телекомунікації.

Стандарт підтримує загальні концепції, визначені в ISO/IEC 27001, і призначений для сприяння адекватного забезпечення інформаційної безпеки на основі підходу, пов'язаного з менеджментом ризику.

Застосуємо для організацій усіх типів (наприклад, комерційних підприємств, державних установ, некомерційних організацій), які планують здійснювати менеджмент ризиків, для компрометації інформаційної безпеки організації.

2.3. ISO/IEC 17799

Опис: У відповідності зі стандартом ISO 17799, при створенні ефективної системи безпеки особливу увагу слід приділити комплексному підходу до управління інформаційною безпекою. З цих причин в якості елементів управління розглядаються не тільки технічні, але й організаційно-адміністративні заходи, спрямовані на забезпечення наступних вимог до інформації:

– конфіденційність;
– цілісність;
– достовірність;
– доступність.

Порушення кожного з них може спричинити за собою значні втрати як у вигляді збитків, так і у вигляді неотриманого доходу.

3. Інструменти

Крім методів та управляючих документів використовують інструменти для оцінки ризиків. Інструменти являють собою програмне забезпечення з документацією про правила використання. Найвідомішими інструментами, існуючими без методики з покроковою інструкцією є: Cobra, RiskWatch.

3.1. Cobra

Виробник: Великобританія.

Опис: Cobra програмний інструмент, який дозволяє проводити оцінку ризиків у галузі безпеки.

Він оцінює відносну важливість усіх загроз і вразливостей, генерує відповідні рішення та рекомендації. Це автоматично пов'язує виявлені ризики з потенційними наслідками для бізнес-одиниці. Крім того, конкретний район або питання може бути розглянуте "самостійно", без будь-яких наслідків для організації.

3.2. RiskWatch

Виробник: США.

Опис: RiskWatch являє собою сімейство програмних продуктів, побудованих на загальному програмному ядрі, які призначені для управління різними видами ризиків та підтримки великого різновиду стандартів.

У RiskWatch в якості критеріїв для оцінки та управління ризиками використовуються:

– очікувані річні втрати (Annual Loss Expectancy, ALE);
– оцінка повернення інвестицій (Return on Investment, ROI).

RiskWatch орієнтована на точну кількісну оцінку співвідношення втрат від загроз безпеки і затрат на створення системи захисту.

Висновок

Отже, важливим кроком при побудові комплексної системи захисту інформації є вибір методів, управляючих документів та інструментів. Зазвичай організації не знають, які з існуючих способів оцінки ризиків кращі саме для їх умов. Процес оцінки повинен бути адаптований до індивідуальних особливостей організації, але в той же час узгоджений з кращими стандартами та провідними практиками. У даному розділі була розглянута класифікація основних способів оцінки інформаційних ризиків. Також наведено огляд кращих методів, керівних документів та інструментів. Вибрати найкращий спосіб оцінки ризику полягає в їх детальному порівнянні, використовуючи різні критерії. Якщо критерії, які використовуються, застосовані до всіх моделей оцінки ризиків, організація може порівняти різні моделі об'єктивно і прийняти рішення про запровадження найкращих з них.