Міністерство освіти і науки України

Одеська національна академія зв'язку ім. О.С. Попова

Кафедра інформаційної безпеки та передачі даних

С.М. Горохов, Н. В. Кондратьєва, В.Г. Кононович, С.В. Стайкуца

ПРОГРАМИ ТА МЕТОДИКИ ДЕРЖАВНОЇ ЕКСПЕРТИЗИ ІНФОРМАЦІЙНОЇ ЗАХИЩЕНОСТІ ТЕЛЕКОМУНІКАЦІЙ

Навчальний посібник у галузі знань 1701 «Інформаційна безпека» за спеціальностями 7.17010201, 8.17010201 Системи технічного захисту інформації, автоматизація її обробки

За ред. чл.-кор. МАЗ В.Г. Кононовича

Одеса 2013

УДК 004.056.5(075.8); 681.336; 342.4 План НМВ 2013 р.
ББК 32.81; 32.88
П 78

Рецензенти:
Баранов П.Ю., д.т.н., професор, директор Інституту радіоелектроніки та телекомунікацій ОНІПУ, завідувач кафедри радіотехнічних систем.
Климаш М.М., д.т.н., професор кафедри «Телекомунікації», Національний університет «Львівська Політехніка»
Кадацький А.Ф., д.т.н., професор кафедри «Безпеки виробничих процесів та електроживлення систем зв'язку», Одеська національна академія зв'язку ім. О.С. Попова

П 78 Програми та методики державної експертизи інформаційної захищеності телекомунікацій : навч. посіб. / **С.М. Горохов, Н. В. Кондратьєва, В.Г. Кононович, С.В. Стайкуца;** за ред. чл.-кор. МАЗ **В.Г. Кононовича**. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – 252 с.

ISBN 978-617-582-005-6

У навчальному посібнику розглянуто основні положення, теоретичні засади та практичні аспекти методик оцінки інформаційної захищеності. Пояснюються моделі та принципи оцінки ефективності захисту від несанкціонованого доступу. Розглядаються методи оцінки забезпечення гарантій безпеки. Описані теорія та методи експертних оцінок у дослідженні систем безпеки інформаційних технологій. Розглядаються основні цілі, задачі та порядок проведення державної експертизи комплексних систем технічного захисту інформації в інфокомунікаціях. Розглядаються методичні основи оцінки ефективності захисту інформаційних ресурсів інформаційної безпеки у галузі інфокомунікацій. Навчальний посібник містить теоретичну частину та питання для самоконтролю.

Навчальний посібник призначено для студентів, які здобувають вищу освіту за напрямом „Інформаційна безпека". Посібник буде також корисним для аспірантів, викладачів, слухачів післядипломної освіти та працівників підприємств галузі зв'язку, а також студентам старших курсів вищих навчальних закладів.

СХВАЛЕНО
кафедрою інформаційної безпеки та передачі даних і рекомендовано до друку.
Протокол № 10 від 21 травня 2012 р..

ЗАТВЕРДЖЕНО
методичною радою академії зв'язку
Протокол № 16 від 23.03.2012 р.

ISBN 978-617-582-005-6

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CRAMM – *UK Goverment Risk Analysis and Managment Method.* Метод аналізу та контролю ризиків (стандарт). Розроблено службою безпеки Великобританії (*UK Security Service*). Російський аналог – ГРИФ

CCITSE *Common Criteria foi- Information Technology Security Evaluation.* Загальні критерії оцінювання безпеки інформаційних технологій

DoS – *Danial of Service.* Відмова в обслуговуванні

DDoS – *Distributed Danial of Service.* Розподілена відмова в обслуговуванні

ETSI – *European Telecommunications Standards Institute*. Європейський інститут зі стандартизації в області телекомунікацій

FC – *Functional Classes.* Функціональні класи

IEC *International Electrotechnical Commission/* Міжнародна електротехнічна комісія

ISO – *International Organization for Standardization*. Міжнародна організація зі стандартизації

ITU-T – *International Telecommunication Union*. Міжнародний союз телекомунікацій – сектор телекомунікацій

QUEST – *Qualitative Utility Estimates for Science and Technology.* Метод кількісних оцінок корисності науки та техніки

PP – *Protection Profile.* Профіль захисту

SEER	–	*System for Event Evaluation and Review.* Система оцінок й огляду подій
ST	–	*Security Target.* Проект захисту
АС	–	Автоматизована система
ВГБ	–	Вимоги гарантій безпеки
ЕОМ	–	Електронно-обчислювальна машина
ІзОД	–	Інформація з обмеженим доступом
ІТ	–	Інформаційні технології
ІТС	–	Інформаційно-телекомунікаційна система
КЗЗ	–	Комплекс засобів захисту
КСЗІ	–	Комплексна система захисту інформації
КЦД	–	Конфіденційність, цілісність, доступність
ЛОМ	–	Локальна обчислювальна мережа
НСД	–	Несанкціонований доступ
НД ТЗІ	–	Нормативний документ технічного захисту інформації
ОЕ		Об’єкт експертизи
ОПР		Особа, що приймає рішення
ОС	–	Операційна система
ПЕМВН	–	Побічні електромагнітні випромінювання та наводки
ПЕОМ	–	Персональна електронно-обчислювальна машина
ПІБ	–	Політика інформаційної безпеки
ПЗ	–	Програмне забезпечення
СЗІ	–	Служба захисту інформації
ТЗІ	–	Технічний захист інформації
ФПБ	–	Функціональні послуги безпеки
ФПЗ	–	Функціональні послуги захисту

ВСТУП

Навчальний посібник з нормативної дисципліни «Методики оцінки інформаційної захищеності телекомунікацій» повинен допомогти студентам, які навчаються за напрямами підготовки 1601, 1801 у галузі знань «Інформаційна безпека» оволодіти теоретичними знаннями та практичними навиками забезпечення кібербезпеки підприємства та звернути увагу на проблеми, які виникають у процесі створення комплексної системи кібербезпеки на підприємствах зв'язку.

У цьому навчальному посібнику розглядаються методи експертної оцінки захищеності інформаційних ресурсів інфокомунікацій від несанкціонованого доступу.

Контроль захищеності інформації проводиться у рамках створення комплексних системи захисту інформації (КСЗІ), передбачений Конституцією України, Законами України «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», іншими законами та підзаконними нормативно-правовими актами, міжнародними договорами України.

Відповідно до ст. 4 Постанови Кабінету Міністрів України від 29 березня 2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» захисту в системі підлягає:

1. Відкрита інформація, яка є власністю держави й у визначенні Закону України "Про інформацію" належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі - відкрита інформація).
2. Конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу (далі – конфіденційна інформація);
3. Інформація, що становить державну або іншу передбачену законом таємницю (далі – таємна інформація).

Згідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [2] інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися у системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи у порядку, встановленому законодавством. Відповідальність за забезпечення захисту інформації у системі покладається на власника системи. Особи, винні у порушенні законодавства про захист інформації у системі, несуть відповідальність згідно із законом.

На практиці реалізують наступні види послуг у сфері створення КСЗІ:

1. Встановлення та налаштування програмного або програмно-апаратного комплексу засобів захисту інформації від несанкціонованого доступу та за необхідності прикладного програмного забезпечення.

2. Створення КСЗІ в автоматизованих системах класу 1 і класу 2 на об'єктах інформаційної діяльності різних категорій і підготовка пакета документів на КСЗІ.

3. Супроводження державної експертизи КСЗІ до отримання Експертного висновку й Атестату відповідності та проведення Державної експертизи КСЗІ АС для отримання Атестату відповідності.

Згідно з «Положенням про державну експертизу у сфері технічного захисту інформації» [3], затвердженого Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93, – державна експертиза у сфері технічного захисту інформації (далі – експертиза) проводиться з метою дослідження, перевірки, аналізу та оцінки об'єктів експертизи щодо відповідності до вимог норм технічного захисту інформації.

Головними розділами навчального посібника є моделі та принципи оцінки ефективності захисту інформації та методи оцінки забезпечення гарантій безпеки. У результаті вивчення дисципліни слухачі набувають наступні знання та вміння:

– знання призначення, параметрів, обладнання й особливостей проведення вимірювання захищеності інформації від витоку технічними каналами;

– знання призначення, параметрів й особливостей застосування експертних методів оцінки функціональних послуг безпеки у засобах захисту інформації від несанкціонованого доступу, а також оцінки рівня гарантій безпеки у засобах захисту від несанкціонованого доступу;

– знання порядку та методики проведення атестації комплексів технічного захисту інформації та порядку й методики проведення державної експертизи комплексних систем технічного захисту інформації в інфокомунікаціях;

– уміння проводити експертні оцінки реалізації функціональних вимог інформаційної захищеності та виконувати оцінки рівня гарантій безпеки у засобах захисту від несанкціонованого доступу.

Майбутні спеціалісти можуть здійснювати типові задачі діяльності, а саме готувати та брати участь у проведенні атестації комплексів технічного захисту інформації й участь у проведенні державної експертизи комплексних систем технічного захисту інформації в інфокомунікаціях.

Викладення матеріалу навчального посібника засновано на вітчизняних і міжнародних стандартах. Навчальний посібник містить основний матеріал і питання для самоконтролю.

Навчальний посібник підготували: Н.В. Кондратьєва (розд. 1.1, 4), к.т.н., доцент В.Г. Кононович (вступ, розд. 1, 2, 5), к.ф.н. С.В. Стайкуца (розд. 2, 5.1, 5.4). Основну термінологію, перелік скорочень складені спільно.

Автори будуть вдячні за конструктивні зауваження та побажання.

Розділ 1
МОДЕЛІ ТА ПРИНЦИПИ ОЦІНКИ ЕФЕКТИВНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

1.1 Модель і методи оцінювання ефективності заходів захисту за Рекомендацією МСЕ – Т серії Х.800

Міжнародна організація зі стандартизації у сфері телекомунікацій – Міжнародний союз електрозв'язку (МСЕ, ITU – International Telecommunication Union) вперше поставив задачу забезпечення безпеки телекомунікацій у період з 1983 по 1988 рр., під час розробки моделі взаємодії відкритих систем у телекомунікаціях [11, с. 7, с. 31]. А вже у 1991 р. була розроблена Рекомендація Х.800 (ISO 7498-2), де описані аспекти забезпечення інформаційної безпеки та викладені загальні вимоги до архітектури безпеки елементів і протоколів телекомунікацій [1]. Ці рекомендації офіційно не перекладались російською мовою, що не сприяло усвідомленню важливості забезпечення інформаційної безпеки у телекомунікаційних системах і мережах Радянського Союзу.

У подальшому всі рекомендації та міжнародні стандарти, які стосувались нових телекомунікаційних технологій, як правило, містять розділи з вимогами до забезпечення інформаційної безпеки телекомунікацій.

Базові положення архітектури безпеки у моделі архітектури взаємодії відкритих систем детально розглянуті у [12, с. 56 - 76]; технічна експлуатація механізмів безпеки в архітектурі взаємодії відкритих систем [12, с. 77 - 94]. Модель архітектури інформаційної безпеки для систем передачі інформації з кінця в кінець подана у навчальному посібнику [12, с. 95 - 113]. Серед нових телекомунікаційних технологій у тому ж навчальному посібнику висвітлено модель архітектури, структура та механізми інформаційної безпеки піринговых мереж [12, с. 114 - 136].

У цілому, підходи до оцінки інформаційної захищеності зводяться до наступного [1, с. 35]. Перед проектуванням системи безпеки (безпечної системи), спочатку необхідно ідентифікувати конкретні загрози, проти яких потрібен захист. Це називають оцінкою загроз. Система вразлива у багатьох відношеннях, але використовуються лише деякі з уразливостей, тому що атакуючому недостає сприятливих можливостей, або тому, що результат не виправдовує зусилля і є ризик виявлення атаки. Проблеми оцінки загроз у широкому плані включають:

– ідентифікацію (визначення) вразливостей системи;

– аналіз імовірності загроз, що націлюється на експлуатацію цієї вразливості;

– оцінювання наслідків, якщо кожна загроза могла успішно здійснюватися;

– обчислення (оцінювання) вартості кожної атаки;

– оцінювання вартості потенційних контрзаходів;

– вибір механізмів безпеки, які обґрунтовані, можливо за допомогою використання аналізу вартості отриманої вигоди.

Повна технічна безпека, подібно повній фізичній безпеці, неможлива. Задача, таким чином, у тому, щоб зробити вартість атаки достатньо високою, так щоб скоротити ризик до прийнятного рівня.

Оцінку інформаційної захищеності необхідно проводити на всіх стадіях життєвого циклу системи, а саме на стадіях:

- прийняття рішення щодо захисту;
- складання технічного завдання на систему захисту;
- розробки технічного та робочого проекту;
- будівництва системи захисту та здачі в експлуатацію після атестації та/чи державної експертизи;
- технічної експлуатації системи захисту;
- утилізації системи при виведенні системи захисту з експлуатації.

У фізичному телекомунікаційному середовищі оцінка захищеності інформації здійснюється інструментальними засобами, шляхом вимірювання фізичних величин: сили або напруги струму, напруженості електромагнітного або акустичного поля, звукового тиску тощо. Для оцінки захищеності обчислюється відношення або логарифм відношення фізичної величини до такої ж величини завад. Головними оцінками є обчислена величина захищеності та величина похибки оцінки, які визначають разом певний рівень довіри до оцінки.

У віртуальних комп'ютерних середовищах ми маємо багатоплановий та надзвичайно широкий діапазон фізичних і логічних процесів оцінки захищеності інформаційних ресурсів. Інструментальні вимірювання складають незначну частину засобів оцінки інформаційної захищеності та мають лише допоміжне значення. Основну роль відіграють розвинені методи експертних оцінок. Експерти дають якісну оцінку певних явищ, процесів, властивостей тощо у певних умовних «шкалах». Довіра до таких оцінок досягається не величиною похибки вимірювань, а чітким дотриманням науково обґрунтованої процедури проведення експертизи.

Розроблено численні міжнародні та вітчизняні стандарти, методики, рекомендації з оцінки інформаційної захищеності.

Адміністрування засобів безпеки. Адміністрування засобів безпеки включає у себе керування та ведення інформації, необхідної для роботи послуг і механізмів безпеки, а також збирання й аналіз інформації щодо їх функціонування. Приклади: установка значень параметрів захисту, ведення журналу подій, розповсюдження криптографічних ключів тощо.

Основою адміністрування є інформаційна база керування безпекою, де зберігається інформація, необхідна для реалізації обраної політики безпеки.

Відповідно до рекомендацій X.800, робота адміністратора засобів безпеки повинні розподілятися за трьома напрямами:

- адміністрування інформаційної системи у цілому;
- адміністрування послуг безпеки;
- адміністрування механізмів безпеки.

Серед дій, що стосуються системи у цілому, відзначають забезпечення дотримання політики безпеки, взаємодію з іншими адміністративними

службами, реагування на події, що відбуваються, аудит і безпечне відновлення системи.

Адміністрування послуг безпеки включає у себе визначення об’єктів, що підлягають захисту, вироблення правил підбору механізмів безпеки (при наявності альтернатив), комбінування механізмів для реалізації послуг, взаємодія з іншими адміністраторами для забезпечення узгодженої роботи.

Обов’язки адміністратора безпеки визначаються переліком задіяних механізмів і включають у себе:

– керування ключами (генерація та розподіл);

– керування шифруванням (установлення та синхронізація криптографічних параметрів). До керування шифруванням можна віднести й адміністрування механізмів цифрового підпису. Керування цілісністю, якщо воно забезпечується криптографічними засобами, також відноситься до даного напряму:

– адміністрування керування доступом (розподіл інформації, необхідної для керування – паролів, списків доступу тощо);

– керування автентифікацією (розподіл інформації, необхідної для автентифікації паролів, ключів тощо);

– керування доповненням трафіка (вироблення та підтримка правил, що задають характеристики додаткових повідомлень частоти відправки, розмір повідомлення тощо). У подальшому ця послуга була вилучена;

– керування маршрутизацією (виділення довірених шляхів);

– керування нотаризацією (розповсюдження інформації щодо нотаріальних служб, адміністрування цих служб).

Детально функції та засоби адміністратора безпеки розглядаються у навчальному посібнику [13, с. 20 - 28].

Класифікація моделей керування доступом. Керування доступом має на меті забезпечення властивостей інформації конфіденційності, цілісності та доступності за умови підтримання неперервної спостережності процесів функціонування інформаційної системи та системи захисту інформації в інформаційній системі. Під *політикою безпеки* розуміють набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації та спрямовані на захист її від певних загроз. Корисно звернути увагу на те, що визначення політики безпеки [14, с. 94]:

1) це набір правил;

2) чітко визначених;

3) достатньо повних й узгоджених між собою;

4) таких, що призначені для реалізації на практиці.

Керування доступом – це сукупність заходів із визначення повноважень і прав доступу, контролю за дотриманням правил розмежування доступу.

Розмежування доступу до інформації – це сукупність заходів, які передбачають поділ інформації на групи за категоріями її важливості й організація доступу до груп інформації посадових осіб згідно з їхніми функціональними обов’язками та повноваженнями.

Система розмежування доступу – це сукупність процедур, що реалізують перевірку запитів на доступ, оцінювання можливості надання доступу на підставі правил розмежування доступу та надає можливість доступу.

Правила розмежування доступу – це частина політики безпеки, що регламентує порядок доступу користувачів і процесів до пасивних об'єктів.

У теорії захищених систем винайдені такі види керування доступом:

- мандатне (Mandatory Access Control);
- дискреційне (Discretionary Access Control);
- рольове (Role based).

За мандатного керування доступом передбачається виконання таких умов:

- усі суб'єкти й об'єкти системи ідентифіковані;
- задано набір міток таємності інформації, що утворює решітку цінностей;
- кожному об'єкту системи надається мітка таємності (або ще говорять рівень таємності), яка відповідає цінності інформації, що міститься в ньому;
- кожному суб'єкту системи надається мітка таємності (або рівень доступу), якою визначається максимальній рівень таємності об'єктів, до яких суб'єкт має доступ. Основною метою мандатного керування доступом є попередження витоку інформації від суб'єктів і об'єктів із високим рівнем доступу до суб'єктів і об'єктів з низьким рівнем доступу.

За дискреційного керування доступом мають бути такі властивості:

- усі суб'єкти й об'єкти системи ідентифіковані;
- права доступу суб'єкта до об'єкта системи визначаються власником об'єкта на основі певних правил.

Рольове керування доступом є компромісом переваг та недоліків між мандатним і дискреційним керуванням. У рольовій моделі використані поняття «користувач», «роль», «повноваження» та «сеанс». Користувач – це особа, що працює із системою, виконуючи певні обов'язки. *Роль* – це логічно зв'язаний набір повноважень, необхідний для здійснення певної активної діяльності у системі, наприклад, спеціальні повноваження адміністратора системи. Ролі записуються у таблицях доступу.

У нормативних документах технічного захисту України (НД ТЗІ) застосовані поняття довірчого та адміністративного керування доступом.

За *довірчого керування доступом* звичайним користувачам надається право (довіряється) керувати потоками інформації між іншими користувачами й об'єктами свого домену, наприклад на підставі права володіння об'єктами. Система, що реалізує довірче керування доступом, дозволяє звичайному користувачеві модифікувати та створювати нові потоки інформації у системі.

За *адміністративного керування доступом* управління потоками інформації між користувачами й об'єктами здійснюється лише спеціально авторизованими користувачами. Наприклад, механізм захисту для надавання доступу може використати атрибути доступу, які містять мітки, що відображають міру конфіденційності інформації та рівень допуску користувача. Комплекс засобів захисту, порівнюючи мітки об'єкта та користувача, може визначити можливість користувача виконувати доступ до інформації. Система, що реалізує адміністративне керування доступом, має гарантувати, що потоки інформації у

системі визначаються адміністратором і не можуть бути змінені звичайним користувачем.

1.2 Модель оцінювання інформаційної захищеності системи керування доступом

Розглянемо модель комплексної системи захисту, що покладена в основу пакета нормативних документів сфери ТЗІ України [15 – 24], який починається з НД ТЗІ 1.1-002-99. Комплексна система захисту інформації (КСЗІ) – це сукупність організаційних й інженерних засобів, програмно-апаратних засобів, які забезпечують захист інформації в інформаційно-телекомунікаційній системі (ІТС) [15, с. 8]. Згідно з теорією захищених систем, до складу КСЗІ входять компоненти ІТС, які призначені для реалізації політики безпеки (наприклад, засоби ізоляції процесів або керування потоками інформації) та допоміжні компоненти, які забезпечують функціонування перших.

Загальні положення моделі. Відповідно до НД ТЗІ 1.1-002-99 усі ресурси ІТС, що знаходяться під керуванням КСЗІ називаються об'єктами. Як об'єкти вони характеризуються логічним поданням (зміст, семантика, значення) та фізичним (форма, синтаксис). Об'єкт має свій стан, що характеризується атрибутами та поведінкою, яка визначає способи зміни стану. Наприклад, об'єктами операційної системи є процеси, файли, кластери, сектори дисків, сегменти пам'яті тощо. Усе, що підлягає захисту відповідно до політики безпеки, має бути визначене як об'єкт.

Об'єкти можуть перебувати у трьох станах, точніше, бути:

- *пасивним об'єктом,* який у конкретному акті доступу є пасивним компонентом системи, над яким виконується дія та/або який служить джерелом чи приймачем інформації;
- *об'єктом-процесом,* тобто програмою, що виконується у даний момент і повністю характеризується своїм контекстом (поточним станом регістрів процесора, адресним простором, повноваженнями тощо);
- *об'єктом-користувачем*, який є поданням фізичного користувача в ІТС, що створюється у процесі входження користувача у систему та повністю характеризується своїм контекстом (псевдонімом, ідентифікаційним кодом, повноваженнями тощо).

Сукупність користувача та процесу, який він здійснює, у зарубіжній літературі називають суб'єктом.

Перехід між станами означає, що об'єкт просто розглядається в іншому контексті. Пасивний об'єкт переходить у стан об'єкта-користувача, коли особа (фізична особа-користувач) «входить» у систему. Цей об'єкт-користувач виступає для комплексу засобів захисту як образ фізичною користувача. За ініціативою користувача йде активізація об'єкта-процесу. Цей об'єкт-процес є керуючим для пасивних об'єктів усередині домену користувача.

Взаємодія двох об'єктів ІТС створює потік інформації між об'єктами та/або змінює стан системи. Потоком інформації є будь-яка порція інформації, що передається між об'єктами ІТС.

Основні принципи керування доступом

Керування доступом має такі види: довірче керування доступом адміністрування, контроль за цілісністю й інші види, які розглянуто вище.

Принцип безперервності захисту. Захист інформації повинен забезпечуватися протягом усього періоду її існування. Згідно з головним постулатом теорії захищених інформаційних технологій, рівень захищеності об'єкта інформаційної діяльності визначається рівнем захищеності найменш захищеної ланки його системи захисту. Має бути забезпечена:

нерозривність захисту у просторі (необхідна кругова оборона об'єкта);

нерозривність захисту за множиною загроз інформаційним ресурсам (система захисту має протистояти всім без винятку виявленим загрозам);

нерозривність захисту у фізичній структурі системи (об'єктами захисту мають бути всі елементи розподіленої інфокомунікаційної системи: абонентські пристрої та робочі станції, вузли комутації та програмні комутатори, канали зв'язку, бази даних, підсистеми керування, синхронізації та сигналізації);

нерозривність захисту за всіма логічними рівнями взаємодії та стека протоколів (фізичним, канальним, мережним, транспортним, сеансовим, представницьким і прикладним рівням і відповідним протоколам);

безперервність захисту у часі (захист інформації повинен бути забезпеченим на всіх стадіях життєвого циклу системи, на стадіях: прийняття рішення щодо захисту, складання технічного завдання на систему захисту, розробки технічного та робочого проекту, будівництва системи захисту та здачі в експлуатацію після атестації та/чи державної експертизи, її технічної експлуатації, утилізації системи при виведенні системи захисту з експлуатації).

З моменту створення об'єкта ІТС або його імпорту до системи й аж до його знищення або експорту із системи всі запити на доступ до об'єкта й об'єкт і на доступ до інших об'єктів мають контролюватися КСЗІ.

З принципу безперервності захисту випливає необхідність того, щоб абсолютно всі запити на доступ до об'єктів контролювалися комплексом засобів захисту та не існувало можливості обійти цей контроль (отримати доступ в обхід КСЗІ). Для захисту об'єктів комплекс засобів захисту повинен у першу чергу забезпечувати свою цілісність і керованість.

Крім того, особливого значення набуває визначення діючих за замовчуванням правил, що визначають початкові умови, за яких починається існування об'єкта всередині ІТС.

Принцип використання атрибутів доступу. Для реалізації політики безпеки КСЗІ має забезпечити ізоляцію об'єктів усередині сфери керування та гарантувати розмежування запитів доступу й керування потоками інформації між об'єктами. Для цього з об'єктами ІТС має бути пов'язана інформація, що дозволяла б комплексу засобів захисту ідентифікувати об'єкти та перевіряти легальність запитів доступу. Такою інформацією є атрибути доступу.

Атрибут доступу – це термін, що використовується для опису будь-якої інформації, яка використовується за керування доступом і пов'язана з користувачами, процесами або пасивними об'єктами. Відповідність атрибутів

доступу й об’єкта може бути як явною, так і неявною. Атрибути доступу об’єкта є частиною його подання в ІТС.

Кожен об’єкт комп’ютерної системи повинен мати певний набір атрибутів доступу, який включає унікальний ідентифікатор й іншу інформацію, що визначає його права доступу та/або права доступу до нього. Коли користувачі або процеси намагаються отримати доступ до пасивних об’єктів, механізми, що реалізують керування доступом, можуть визначити легальність запиту на підставі політики безпеки та перевірки атрибутів доступу.

Для реалізації функцій розмежування доступу використовується концепція матриці доступу. *Матриця доступу* являє собою таблицю, у кожному виміру якої відкладені ідентифікатори об’єктів ІТС, а як елементи матриці виступають дозволені або заборонені режими доступу. Матриця доступу може бути двовимірною (наприклад, користувачі/пасивні об’єкти або процеси/пасивні об’єкти) або тривимірною (користувачі/процеси/пасивні об’єкти). Повна тривимірна матриця доступу дозволяє точно описати, хто (ідентифікатор користувача), через що (ідентифікатор процесу), до чого (ідентифікатор пасивного об’єкта), який вид доступу може отримати.

Види вимог до оцінки спроможності ІТС забезпечити захист. Утворення додаткових потоків інформації може бути зумовлене: модифікацією атрибутів доступу користувача, процесу або пасивного об'єкта: створенням нових об’єктів, копіюванням існуючих; експортом або імпортом об'єктів.

Відповідно до НД ТЗІ 1.1-002-99 у 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 безпеки.

Систему критеріїв оцінки інформації у комп’ютерних системах від несанкціонованого доступу викладено у НД ТЗІ 2.1-004-99 [17].

1.3 Методи оцінки коректності реалізації функціональних критеріїв захисту інформації

Функціональні критерії НД ТЗІ 2.5-004-99. У критеріях НД ТЗІ 2.5-004-99 інформаційно-телекомунікаційна система (ІТС) розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати кілька рівнів. Чим вищий 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, цілісність, доступність, спостережність.

Конфіденційність. Характеристика безпеки інформації, що відображає її властивість не виявляємості та не доступності без відповідних повноважень [25, с. 102]. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги потрібно шукати у розд. «Критерії конфіденційності» НД ТЗІ 2.5-004-99. Це стосується всіх інших типів вимог до послуг відповідно.

Цілісність. Характеристика безпеки інформації, що відображає її властивість протистояти несанкціонованій модифікації. Наприклад, користувач, що накопичує інформацію, має право очікувати, що зміст його файлів залишається незмінним, незважаючи на цілеспрямовані впливи, а також відмови програмних або апаратних засобів [25, с. 242].

Доступність, готовність, наявність. Характеристика безпеки інформації, що відображає її властивість, яка полягає у можливості її використання в заданий момент часу відповідно до заданих повноважень [25, с. 40]. Основними загрозами доступності є відмова у доступі (*DoS, DDoS*) або збої обладнання чи програмного забезпечення.

Спостережність, підзвітність, обліковість. Властивість ІТС фіксувати та надавати відповідальним за захист інформації особам звіти про хід порушення або спробу порушення безпеки [25, с. 13]. Під *безпекою* (*safety*) розуміють властивість системи, яка полягає у тому, що вона ніколи й нічого не зробить погано. Ідентифікація та контроль за діями користувачів або легальністю доступу, керованість ІТС, контроль за спроможністю комплексу засобів захисту виконувати свої функції становлять предмет послуг спостережності та керованості.

Ідентифікатори рівнів функціональних критеріїв наведені у табл. 1.1

Ранжирування вимог критеріїв конфіденційності

Для того, щоб ІТС могла бути оцінена на предмет відповідності критеріям конфіденційності, КСЗІ оцінюваної системи має надавати послуги із захисту об’єктів від несанкціонованого ознайомлення з їх змістом (компрометації). Конфіденційність забезпечується такими послугами: КД – довірча конфіденційність, КА – адміністративна конфіденційність, КО – повторне використання об’єктів, КК – аналіз прихованих каналів, КВ – конфіденційність при обміні.

Довірча конфіденційність. Послуга довірчої конфіденційності дозволяє користувачу керувати потоками інформації від захищених об’єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту та вибірковості керування: КД-1 – мінімальна довірча конфіденційність; КД-2 – базова довірча конфіденційність; КД-3 – повна довірча конфіденційність; КД-4 – абсолютна довірча конфіденційність.

Спільними для всіх рівнів вважаються такі вимоги:

– запити на зміну прав доступу до об’єкта повинні оброблятися КСЗІ на підставі атрибутів доступу користувача, що ініціює запит, й об’єкта;

– права доступу до кожного захищеного об’єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої

конфіденційності повинні бути представлені правила збереження атрибутів доступу об’єктів під час їх експорту й імпорту.

Таблиця 1.1 – Ідентифікатори рівнів функціональних критеріїв захищеності інформації

Загальний ідентифікатор	Найменування ідентифікатора	Рівні ідентифікатора
Критерії конфіденційності		
КД	Довірча конфіденційність	КД-1, КД-2, КД-3, КД-4
КА	Адміністративна конфіденційність	КА-1, КА-2, КА-3, КА-4
КО	Повторне використання об’єктів	КО-1
КК	Аналіз прихованих каналів	КК-1, КК-2, КК-3
КВ	Конфіденційність при обміні	КВ-1, КВ-2, КВ-3, КВ-4
Критерії цілісності		
ЦД	Довірча цілісність	ЦД-1, ЦД-2, ЦД-3, ЦД-4
ЦА	Адміністративна цілісність	ЦА-1, ЦА-2, ЦА-3, ЦА-4
ЦО	Відкіт	ЦО-1, ЦО-2
ЦВ	Цілісність при обміні	ЦВ-1, ЦВ-2, ЦВ-3
Критерії доступності		
ДР	Використання ресурсів	ДР-1, ДР-2, ДР-3
ДС	Стійкість до відмов	ДС-1, ДС-2, ДС-3
ДЗ	Гаряча заміна	ДЗ-1, ДЗ-2, ДЗ-3
ДВ	Відновлення після збоїв	ДВ-1, ДВ-2, ДВ-3
Критерії спостережності		
НР	Реєстрація	НР-1, НР-2, НР-3, НР-4, НР-5
НИ	Ідентифікація й автентифікація	НИ-1, НИ-2, НИ-3
НО	Розподіл обов’язків	НО-1, НО-2, НО-3
НВ	Автентифікація при обміні	НВ-1, НВ-2, НВ-3
НП	Автентифікація отримувача	НП-1, НП-2
НК	Достовірний канал	НК-1, НК-2
НЦ	Цілісність комплексу засобів захисту	НЦ-1, НЦ-2, НЦ-3
НТ	Самотестування	НТ-1, НТ-2, НТ-3
НА	Автентифікація відправника	НА-1, НА-2

Рівень КД-1 «Мінімальна довірча конфіденційність» включає у себе такі вимоги:

– політика довірчої конфіденційності, що реалізується КСЗІ, має визначати множину об’єктів ІТС, яких вона стосується;

– КСЗІ має здійснювати розмежування доступу на підставі атрибутів доступу процесу й захищеного об’єкта;

– КСЗІ має надавати користувачу можливість для кожного захищеного об’єкта, що належить його домену, визначати конкретні процеси і/або групи процесів, які мають право отримувати інформацію від об’єкта.

Необхідна умова: НИ-1.

Рівень КД-2 «Базова довірча конфіденційність» включає у себе такі вимоги:

– політика довірчої конфіденційності, що реалізується КСЗІ, має визначати множину об’єктів ІТС, яких вона стосується;

– КСЗІ має здійснювати розмежування доступу на підставі атрибутів користувача й захищеного об’єкта;

– КСЗІ має надавати користувачу можливість для кожного захищеного об’єкта, що належить його домену, визначати конкретних користувачів та/або групи користувачів, які мають право отримувати інформацію від об’єкта;

– КСЗІ має надавати користувачу можливість для кожного процесу, що належить його домену, визначати конкретних користувачів та/або групи користувачів, які мають право ініціювати процес.

Необхідна умова: ІШ-1.

Рівень КД-3 «Повна довірча конфіденційність» включає у себе такі вимоги:

– політика довірчої конфіденційності, що реалізується КСЗІ, має стосуватися всіх об’єктів ІТС;

– КСЗІ має здійснювати розмежування доступу на підставі атрибутів користувача й захищеного об’єкта;

– КСЗІ має надавати користувачу можливість для кожного захищеного об’єкта, що належить його домену, визначати конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають право отримувати інформацію від об’єкта;

– КСЗІ має надавати користувачу можливість для кожного процесу, що належить його домену, визначати конкретних користувачів (і групи користувачів), які мають, а також тих, що не мають право ініціювати процес.

Необхідні умови: КО-1, НИ-1.

Рівень КД-4 «Абсолютна довірча конфіденційність» включає у себе такі вимоги:

– політика довірчої конфіденційності, що реалізується КСЗІ, має стосуватися всіх об’єктів ІТС;

– КСЗІ має здійснювати розмежування доступу на підставі атрибутів користувача, процесу й захищеного об’єкта;

– КСЗІ має надавати користувачу можливість для кожного захищеного об’єкта, що належить його домену, визначати конкретних користувачів і процеси (і групи користувачів, і процесів), які мають, а також тих, які не мають право отримувати інформацію від об’єкта;

– КСЗІ має надавати користувачу можливість для кожного процесу, що належить його домену, визначати конкретних користувачів (і групи користувачів), які мають, а також тих, що не мають право ініціювати процес.

Необхідні умови: КО-1, НИ-1.

Адміністративна конфіденційність. Послуга адміністративної конфіденційності дозволяє адміністратору або спеціально авторизованому користувачеві керувати потоками інформації від захищених об’єктів до користувачів. Рівні даної послуги ранжируються на підставі повноти захисту й вибірковості керування: КА-1 – мінімальна адміністративна конфіденційність, КА-2 – базова адміністративна конфіденційність, КА-3 – повна адміністративна конфіденційність, КА-4 – абсолютна адміністративна конфіденційність.

Спільними для всіх рівнів вважаються такі вимоги:

– запити на зміну прав доступу повинні оброблятися КСЗІ тільки у тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження;

– права доступу до кожного захищеного об’єкта мають установлюватися у момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об’єктів під час їх експорту й імпорту.

Рівень КА-1 «Мінімальна адміністративна конфіденційність» включає у себе такі вимоги:

– політика адміністративної конфіденційності, що реалізується КСЗІ, повинна визначати множину об’єктів ІТС, яких вона стосується;

– КСЗІ має здійснювати розмежування доступу на підставі атрибутів доступу процесу й захищеного об’єкта;

– КСЗІ має надавати можливість адміністратору або користувачу з відповідними повноваженнями, для кожного захищеного об’єкта, шляхом керування належністю користувачів, процесів і об’єктів до відповідних доменів, визначати конкретні процеси і/або групи процесів, які мають право отримувати інформацію від об’єкта.

Необхідні умови: НО-1, НИ-1.

Рівень КА-2 «Базова адміністративна конфіденційність» включає у себе такі вимоги:

– політика, адміністративної конфіденційності, що реалізується КСЗІ, повинна визначати множину об’єктів ІТС, яких вона стосується;

– КСЗІ має здійснювати розмежування доступу на підставі атрибутів доступу користувача й захищеного об’єкта;

– КСЗІ має надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об’єкта, шляхом керування належністю користувачів», процесів і об’єктів до відповідних доменів, визначити конкретних користувачів і/або групи користувачів, які мають право отримувати інформацію від об’єкта;

– КСЗІ має надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу, через керування належністю користувачів і процесів до відповідних доменів, визначати конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Необхідні умови: НО-1, НИ-1.

Рівень КА-3 «Повна адміністративна конфіденційність» включає у себе такі вимоги:

– політика адміністративної конфіденційності, що реалізується КЗЗ, має стосуватися всіх об’єктів ІТС;

– КСЗІ має здійснювати розмежування доступу на підставі атрибутів доступу користувача й захищеного об’єкта;

– КСЗІ має надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об’єкта, шляхом керування належністю користувачів, процесів і об’єктів до відповідних доменів, визначати

конкретних користувачів (і групи користувачів), які мають, а також тих. які не мають право отримувати інформацію від об’єкта;

– КСЗІ має надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів, визначати конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають право ініціювати процес.

Необхідні умови: КО-1, НО-1, НИ-1.

Рівень КА-4 «Абсолютна адміністративна конфіденційність» включає у себе такі вимоги:

– політика адміністративної конфіденційності, що реалізується КСЗІ, має стосуватися всіх об’єктів ІТС;

– КСЗІ має здійснювати розмежування доступу на підставі атрибутів доступу користувача, процесу й захищеного об’єкта;

– КСЗІ має надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожною захищеного об’єкта, шляхом керування належністю користувачів, процесів і об’єктів до відповідних доменів, визначати конкретних користувачів і процеси (і групи користувачів, і процесів), які мають, а також тих, які не мають право отримувати інформацію від об’єкта;

– КСЗІ має надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу, через керування належністю користувачів і процесів до відповідних доменів, визначати конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають право ініціювати процес.

Необхідні умови: КО-1, НО-1, НИ-1.

Повторне використання об’єктів. Послуга повторного використання об’єктів дозволяє забезпечити коректність повторного використання розділюваних об’єктів, гарантуючи, що у разі, якщо розділюваний об’єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

Рівень КО-1 «Повторне використання об’єктів» включає у себе такі вимоги:

– політика повторного використання об’єктів, що реалізується КСЗІ, має стосуватися всіх об’єктів ІТС;

– перш ніж користувач або процес зможе отримати у своє розпорядження звільнений іншим користувачем або процесом об’єкт, установлені для попереднього користувача або процесу права доступу до даного об’єкта повинні бути скасовані;

– перш ніж користувач або процес зможе отримати у своє розпорядження звільнений іншим користувачем або процесом об’єкт, уся інформація, що міститься у даному об’єкті, повинна стати недосяжною.

Аналіз прихованих каналів. Аналіз прихованих каналів виконується з метою виявлення й 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: КК-1 – виявлення прихованих каналів, КК-2 – контроль прихованих каналів, КК-3 – перекриття прихованих каналів.

Спільною для всіх рівнів є послуга: має бути виконаний аналіз прихованих каналів.

Рівень КК-1 «Виявлення прихованих каналів» включає у себе такі вимоги:

– усі приховані канали, які існують в апаратному та програмному забезпеченні, а також у програмах на постійних запам’ятовувальних пристроях, мають бути документовані;

– має бути документована максимальна пропускна здатність кожного знайденого прихованого каналу, отримана на підставі теоретичної оцінки або вимірів;

– для прихованих каналів, які можуть бути використані спільно, повинна бути документована сукупна пропускна здатність.

Необхідні умови: КО-1, Г-3.

Рівень КК-2 "Контроль прихованих каналів» включає у себе такі вимоги:

– усі приховані канали, які існують в апаратному та програмному забезпеченні, а також у програмах на постійних запам’ятовуючих пристроях, мають бути документовані;

– має бути документована максимальна пропускна здатність кожного знайденого прихованого каналу, отримана на підставі теоретичної оцінки або вимірів;

– для прихованих каналів, які можуть бути використані спільно, має бути документована сукупна пропускна здатність;

– КСЗІ має забезпечувати реєстрацію використання затвердженої підмножини знайдених прихованих каналів.

Необхідні умови: КО-1, НР-1, Г-3.

Рівень КК-3 «Перекриття прихованих каналів» включає вимогу: усі знайдені під час аналізу приховані канали мають бути усунені.

Необхідні умови: КО-1, Г-3.

Конфіденційність при обміні. Послуга конфіденційності при обміні 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 та вибірковості керування: КВ-1 – мінімальна конфіденційність при обміні, КВ-2 – базова конфіденційність при обміні, КВ-3 – повна конфіденційність при обміні, КВ-4 – абсолютна конфіденційність при обміні.

Спільними для всіх рівнів вважаються такі вимоги:

– політика конфіденційності при обміні, що реалізується КСЗІ, має визначати рівень захищеності, який забезпечується механізмами, що використовуються, та спроможність користувачів і/або процесів керувати рівнем захищеності;

– КСЗІ має забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об’єкті, який передається.

Рівень КВ-1 «Мінімальна конфіденційність при обміні» включає у себе вимогу: політика конфіденційності при обміні, що реалізується КСЗІ, має визначати множину об’єктів й інтерфейсних процесів, яких вона стосується.

Рівень КВ-2 «Базова конфіденційність при обміні» включає у себе такі вимоги:

– політика конфіденційності при обміні, що реалізується КСЗІ, повинна визначати множину об’єктів та інтерфейсних процесів, яких вона стосується;

– запити на призначення або зміну рівня захищеності мають оброблятися КСЗІ тільки у тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надано відповідні повноваження;

– запити на експорт захищеного об’єкта мають оброблятися передавальним КСЗІ на підставі атрибутів доступу інтерфейсного процесу;

– запити на імпорт захищеного об’єкта мають оброблятися приймальним КСЗІ на підставі атрибутів доступу інтерфейсного процесу.

Необхідна умова: НО-1.

Рівень КВ-3 «Повна конфіденційність при обміні» включає у себе такі вимоги:

– політика конфіденційності при обміні, що реалізується КСЗІ, має стосуватися всіх об’єктів й існуючих інтерфейсних процесів;

– запити на призначення або зміну рівня захищеності мають оброблятися КСЗІ тільки у тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження;

– запити на експорт захищеного об’єкта мають оброблятися передавальним КСЗІ на підставі атрибутів доступу інтерфейсного процесу та приймальника об’єкта;

– запити на імпорт захищеного об’єкта мають оброблятися приймальним КСЗІ на підставі атрибутів доступу інтерфейсного процесу та джерела об’єкта;

– представлення захищеного об’єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об’єкта, а також його джерела та приймальника.

Необхідні умови: НО-1, НВ-1.

Рівень КВ-4 «Абсолютна конфіденційність при обміні» включає у себе такі вимоги:

– політика конфіденційності при обміні, що реалізується КСЗІ, має стосуватися всіх об’єктів й існуючих інтерфейсних процесів;

– запити на призначення або зміну рівня захищеності мають оброблятися КСЗІ тільки у тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження;

– запити на експорт захищеного об’єкта мають оброблятися передавальним КСЗІ на підставі атрибутів доступу інтерфейсного процесу та приймальника об’єкта;

– запити на імпорт захищеного об’єкта мають оброблятися приймальним КСЗІ на підставі атрибутів доступу інтерфейсного процесу та джерела об’єкта;

– представлення захищеного об’єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об’єкта, а також його джерела та приймача;

– політика конфіденційності при обміні має включати у себе опис інформації. яку можливо отримати шляхом одночасного аналізу низки отриманих об’єктів;

– має бути виконано аналіз прихованих каналів обміну. Усі знайдені приховані канали обміну та максимальна пропускна здатність кожного із них мають бути документовані. Має бути забезпечена реєстрація використання затвердженої підмножини знайдених прихованих каналів, їх часткове перекриття або усунення.

Необхідні умови: НО-1, НВ-1, НР-1, Г-3.

Ранжирування вимог критеріїв цілісності

Для того, щоб ІТС могла бути оцінена на предмет відповідності критеріям цілісності, КСЗІ оцінюваної системи має надавати послуги із захисту оброблюваної інформації від несанкціонованої модифікації. Цілісність забезпечується такими послугами: ЦД – довірча цілісність, ЦА – адміністративна цілісність, ЦО – відкіт, ЦВ – цілісність при обміні.

Довірча цілісність. Послуга довірчої цілісності дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об’єктів, що належать його доменам. Рівні даної послуги ранжируються на підставі повноти захисту та вибірковості керування: ЦД-1 – мінімальна довірча цілісність, ЦД-2 – базова довірча цілісність, ЦД-3 – повна довірча цілісність, ЦД-4 – абсолютна довірча цілісність.

Спільними для всіх рівнів вважаються такі вимоги:

– запити на зміну прав доступу до об’єкта мають оброблятися КСЗІ на підставі атрибутів доступу користувача, що ініціює запит, і об’єкта;

– права доступу до кожного захищеного об’єкта мають встановлюватися у момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об’єктів під час їх експорту й імпорту.

Рівень ЦД-1 «Мінімальна довірча цілісність» включає у себе такі вимоги:

– політика довірчої цілісності, що реалізується КСЗІ, має визначати множину об’єктів ІТС, яких вона стосується;

– КСЗІ має здійснювати розмежування доступу на підставі атрибутів доступу користувача та захищеного об’єкта;

– КСЗІ має надавати користувачу можливість для кожного захищеного об’єкта, що належить його домену, визначати конкретних користувачів і/або групи користувачів, які мають право модифікувати об’єкт.

Необхідна умова: НИ-1.

Рівень ЦД-2 «Базова довірча цілісність» включає у себе такі вимоги:

– політика довірчої цілісності, що реалізується КСЗІ, має визначати множину об’єктів ІТС, яких вона стосується;

– КСЗІ має здійснювати розмежування доступу на підставі атрибутів доступу процесу та захищеного об’єкта;

– КСЗІ має надавати користувачу можливість для кожного захищеного об’єкта, що належить його домену, визначати конкретні процеси та/або групи процесів, які мають право модифікувати об’єкт;

– КСЗІ має надавати користувачу можливість для кожного процесу, що належить його домену, визначати конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Необхідна умова: НИ-1.

Рівень ЦД-3 «Повна довірча цілісність» включає у себе такі вимоги:

– політика довірчої цілісності, що реалізується КСЗІ, має стосуватися всіх об'єктів ІТС;

– КСЗІ має здійснювати розмежування доступу на підставі атрибутів доступу процесу та захищеного об'єкта;

– КСЗІ має надавати користувачу можливість для кожного захищеною об'єкта, що належить його домену, визначати конкретні процеси (і групи процесів), які мають, а також тих, що не мають право модифікувати об'єкт;

– КСЗІ має надавати користувачу можливість для кожного процесу, що належить його домену, визначати конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають право ініціювати процес.

Необхідні умови: КО-1, НИ-1.

Рівень ЦЦ-4 «Абсолютна довірча цілісність» включає у себе такі вимоги:

– політика довірчої цілісності, що реалізується КСЗІ, має стосуватися всіх об'єктів ІТС;

– КСЗІ має здійснювати розмежування доступу на підставі атрибутів доступу процесу, користувача та захищеного об'єкта;

– КСЗІ має надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначати конкретних користувачів і процеси (і групи користувачів, і процесів), які мають, а також тих, що не мають право модифікувати об'єкт;

– КСЗІ має надавати користувачу можливість для кожного процесу, що належить його домену, визначати конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають право ініціювати процес.

Необхідні умови: КО-1, НИ-1.

Адміністративна цілісність. Послуга адміністративної цілісності дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні цієї послуги ранжируються на підставі повноти захисту та вибірковості керування: ЦА-1 – мінімальна адміністративна цілісність, ЦА-2 – базова адміністративна цілісність, ЦА-3 – повна адміністративна цілісність, ЦА-4 – абсолютна адміністративна цілісність.

Спільними для всіх рівнів вважаються такі вимоги:

– запити на зміну прав доступу мають оброблятися КСЗІ лише у тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження;

– права доступу до кожного захищеного об'єкта мають встановлюватися у момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єкта під час їх експорту й імпорту.

Рівень ЦА-1 «Мінімальна адміністративна цілісність» включає у себе такі вимоги:

– політика адміністративної цілісності, що реалізується КСЗІ, має визначати множину об’єктів ІТС, яких вона стосується;

– КСЗІ має здійснювати розмежування доступу на підставі атрибутів доступу користувача та захищеного об’єкта;

– КСЗІ має надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об’єкта шляхом керування належністю користувачів, процесів і об’єктів до відповідних доменів визначати конкретних користувачів і/або групи користувачів, які мають право модифікувати об’єкт.

Необхідні умови: НО-1, НИ-1.

Рівень ЦА-2 «Базова адміністративна цілісність» включає у себе такі вимоги:

– політика адміністративної цілісності, що реалізується КСЗІ, має визначати множину об’єктів ІТС, яких вона стосується;

– КСЗІ має здійснювати розмежування доступу на підставі атрибутів доступу процесу та захищеного об’єкта;

– КСЗІ має надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об’єкта шляхом керування належністю користувачів, процесів і об’єктів до відповідних доменів визначати конкретні процеси і/або групи процесів, які мають право модифікувати об’єкт;

– КСЗІ має надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначати конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Необхідні умови: НО-1. НИ-1.

Рівень ЦА-3 «Повна адміністративна цілісність» включає у себе такі вимоги:

– політика адміністративної цілісності, що реалізується КСЗІ, має стосуватися всіх об’єктів ІТС;

– КСЗІ має здійснювати розмежування доступу на підставі атрибутів доступу процесу та захищеного об’єкта;

– КСЗІ має надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об’єкта шляхом керування належністю користувачів, процесів і об’єктів до відповідних доменів визначати конкретні процеси (і групи процесів), які мають, а також тих, які не мають право модифікувати об’єкт;

– КСЗІ має надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного пронесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають право ініціювати процес.

Необхідні умови: КО-1, НО-1, НИ-1.

Рівень ЦА-4 «Абсолютна адміністративна цілісність» включає у себе такі вимоги:

– політика адміністративної цілісності, що реалізується КСЗІ, має стосуватися всіх об'єктів ІТС;

– КСЗІ має здійснювати розмежування доступу на підставі атрибутів доступу процесу, користувача та захищеного об'єкта;

– КСЗІ має надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначати конкретних користувачів і процеси (і групи користувачів, і процесів), які мають, а також тих, які не мають право модифікувати об'єкт;

– КСЗІ має надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначати конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес.

Необхідні умови: КО-1, НО-1, НИ-1.

Відкіт. Послуга відкоту забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкотити) захищений об'єкт до попереднього етапу. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкіт: ЦО-1 – обмежений відкіт, ЦО-2 – повний відкіт.

Спільною для всіх рівнів вважається вимога: політика відкоту, що реалізується КСЗІ, має визначати множину об'єктів ІТС, яких вона стосується.

Рівень ЦО-1 «Обмежений відкіт» включає у себе таку вимогу: мають існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкотити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

Необхідна умова: НИ-1.

Рівень ЦО-2 «Повний відкіт» включає у себе таку вимогу: мають існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкотити або відмінити всі операції, виконані над захищеним об'єктом за певний проміжок часу. Необхідна умова: НИ-1.

Цілісність при обміні. Послуга цілісності при обміні дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься у них, під час їх експорту імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту та вибірковості керування: ЦВ-1 – мінімальна цілісність при обміні, ЦВ-2 – базова цілісність при обміні, ЦВ-3 – повна цілісність при обміні.

Спільною для всіх рівнів вважається вимога: політика цілісності при обміні, що реалізується КСЗІ, має визначати множину об'єктів ІТС та інтерфейсних процесів, яких вона стосується, рівень захищеності, що забезпечується використаними механізмами, та спроможність користувачів і/або процесів керувати рівнем захищеності.

Рівень ЦВ-1 «Мінімальна цілісність при обміні» включає у себе таку вимогу: КСЗІ має забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається.

Рівень ЦВ-2 «Базова цілісність при обміні» включає у себе такі вимоги:

– КСЗІ має забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається, а також фактів його видалення або дублювання;

– запити на експорт захищеного об'єкта мають оброблятися передавальним КСЗІ на підставі атрибутів доступу інтерфейсного процесу;

– запити на імпорт захищеного об'єкта мають оброблятися приймальним КСЗІ на підставі атрибутів доступу інтерфейсного процесу;

– запити на присвоєння або зміну рівня захищеності мають оброблятися КСЗІ тільки у тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження. Необхідна умова: НО-1.

Рівень ЦВ-3 «Повна цілісність при обміні» включає у себе такі вимоги:

– КСЗІ має забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається, а також фактів його видалення або дублювання;

– запити на експорт захищеного об'єкта мають оброблятися передавальним КСЗІ на підставі атрибутів доступу інтерфейсного процесу та приймальника об'єкта;

– запити на імпорт захищеного об'єкта мають оброблятися приймальним КСЗІ на підставі атрибутів доступу інтерфейсного процесу та джерела об'єкта;

– запити на присвоєння або зміну рівня захищеності мають оброблятися КСЗІ тільки у тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження;

– представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела та приймальника.

Необхідні умови: НО-1, НВ-І.

Ранжирування вимог критеріїв доступності

Для того, щоб ІТС могла бути оцінена на предмет відповідності критеріям доступності, КСЗІ оцінюваної ІТС має надавати послуги щодо забезпечення можливості використання ІТС у цілому, окремих функцій або оброблюваної інформації на певному проміжку часу та гарантувати здатність системи функціонувати у випадку відмови її компонентів. Доступність може забезпечуватися для ІТС такими послугами: ДР – використання ресурсів, ДС – стійкість до відмов, ДЗ – гаряча заміна, ДВ – відновлення після збоїв.

Використання ресурсів. Послуга використання ресурсів дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту та вибірковості керування доступністю послуг ІТС: ДР-1 – квоти, ДР-2 – недопущення захоплення ресурсів, ДР-3 – пріоритетність використання ресурсів.

Загальною для усіх рівнів вважається вимога: запити на зміну встановлених обмежень мають оброблятися КСЗІ тільки у тому випадку, якщо вони

надходять від адміністраторів або від користувачів», яким надані відповідні повноваження.

Необхідна загальна умова: НО-1.

Рівень ДР-1 «Квоти» включає у себе такі вимоги:

– політика використання ресурсів, що реалізується КСЗІ, має визначати множину об'єктів ІТС, яких вона стосується;

– політика використання ресурсів має визначати обмеження, які можна накладати на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачеві.

Рівень ДР-2 «Недопущення захоплення ресурсів» включає у себе такі вимоги:

– політика використання ресурсів, що реалізується КСЗІ, має стосуватися всіх об'єктів ІТС;

– політика використання ресурсів має визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу;

– має існувати можливість установлювати обмеження таким чином, щоб КСЗІ мав можливість запобігти діям, які можуть призвести до неможливості доступу інших користувачів до функцій КСЗІ або захищених об'єктів. КСЗІ має контролювати такі дії, здійснювані з боку окремого користувача.

Рівень ДР-3 «Пріоритетність використання ресурсів» включає у себе такі вимоги:

– політика використання ресурсів, що реалізується КСЗІ, має стосуватися всіх об'єктів ІТС;

– політика використання ресурсів має визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу та довільним групам користувачів;

– має існувати можливість установлювати обмеження таким чином. щоб КСЗІ мав можливість запобігти діям, які можуть призвести до неможливості доступу інших користувачів до функцій КСЗІ або захищених об'єктів. КСЗІ має контролювати такі дії, здійснювані з боку окремого користувача та довільних груп користувачів.

Стійкість до відмов. Послуга, стійкості до відмов гарантує доступність системи (можливість використання інформації, окремих функцій або системи у цілому) після відмови її компонента. Рівні даної послуги ранжируються на підставі здатності КСЗІ забезпечити можливість функціонування ІТС залежно від кількості відмов і послуг, доступних після відмови: ДС-1 – стійкість при обмежених відмовах, ДС-2 – стійкість при погіршенні характеристик обслуговування, ДС-3 – стійкість без погіршення характеристик обслуговування.

Спільними для всіх рівнів вважаються вимоги:

– розробник має провести аналіз відмов компонентів ІТС;

– мають бути чітко вказані рівні відмов, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги;

– мають бути чітко вказані рівні відмов, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги.

Необхідна загальна умова: НО-1.

Рівень ДС-1 «Стійкість при обмежених відмовах» включає у себе такі вимоги:

– політика стійкості до відмов, що реалізується КСЗІ, має визначати множину компонентів ІТС, яких вона стосується, і типи їхніх відмов, після яких ІТС спроможна продовжувати функціонування;

– відмова одного захищеного компонента не має призводити до недоступності всіх послуг, а має у найгіршому випадку проявлятися у зниженні характеристик обслуговування.

Рівень ДС-2 «Стійкість при погіршенні характеристик обслуговування» включає у себе такі вимоги:

– політика стійкості до відмов, що реалізується КСЗІ, має стосуватися всіх компонентів ІТС;

– відмова одного захищеного компонента не має призводити до недоступності всіх послуг, а має у гіршому випадку проявлятися у зниженні характеристик обслуговування.

Рівень ДС-3 «Стійкість без погіршення характеристик обслуговування» включає у себе такі вимоги;

– політика стійкості до відмов, що реалізується КСЗІ, має стосуватися всіх компонентів ІТС;

– відмова одного захищеного компонента не має призводити до недоступності всіх послуг або до зниження характеристик обслуговування.

Гаряча заміна. Послуга гарячої заміни дозволяє гарантувати доступність ІТС (можливість використання інформації, окремих функцій або системи у цілому) у процесі заміни окремих компонентів. Рівні даної послуги ранжируються на підставі повноти реалізації: ДЗ-1 – модернізація, ДЗ-2 – обмежена гаряча заміна, ДЗ-3 – гаряча заміна будь-якого компонента.

Рівень ДЗ-1 «Модернізація» включає у себе такі вимоги:

– політика гарячої заміни, що реалізується КСЗІ, має визначати політику проведення модернізації ІТС;

– адміністратор або користувач, який має відповідні повноваження, повинні мати можливість провести модернізацію (*upgrade*) ІТС. Модернізація системи не має призводити до необхідності ще раз проводити інсталяцію системи або до переривання виконання КСЗІ функцій захисту.

Необхідна умова: НО-1.

Рівень ДЗ-2 «Обмежена гаряча заміна» включає у себе такі вимоги:

– політика гарячої заміни, що реалізується КСЗІ, має визначати множину компонентів ІТС, які можуть бути замінені без переривання обслуговування;

– адміністратор або користувач, який має відповідні повноваження, повинні мати можливість замінити будь-який захищений компонент. Необхідні умови: НО-1, ДС-1.

Рівень ДЗ-3 «Гаряча заміна будь-якого компонента» включає у себе такі вимоги:

– політика гарячої заміни, що реалізується КСЗІ, має забезпечувати можливість заміни будь-якого компонента без переривання обслуговування;

– адміністратор або користувач, який має відповідні повноваження, повинні мати можливість замінити будь-який захищений компонент.

Необхідні умови: НО-1. ДС-1.

Відновлення після збоїв. Послуга відновлення після збоїв забезпечує повернення ІТС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі ступеня автоматизації процесу відновлення: ДВ-І – ручне відновлення, ДВ-2 – автоматизоване відновлення, ДВ-3 – вибіркове відновлення.

Спільною для всіх рівнів вважається вимога: політика відновлення, що реалізується КСЗІ, має визначати множину типів відмов ІТС і переривання обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Мають бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція системи.

Необхідна загальна умова: НО-1.

Рівень ДВ-1 «Ручне відновлення» включає у себе такі вимоги:

– після відмови ІТС або переривання обслуговування КСЗІ має перевести систему до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувач, який має відповідні повноваження;

– мають існувати ручні процедури, за допомогою яких можна безпечним чином повернути систему до нормального функціонування.

Рівень ДВ-2 «Автоматизоване відновлення» включає у себе такі вимоги:

– після відмови ІТС або переривання обслуговування КСЗІ має бути здатним визначити, чи можуть бути використані автоматизовані процедури для повернення системи до нормального функціонування безпечним чином. Якщо такі процедури можуть бути використані, то КСЗІ має бути здатним виконати їх і повернути систему до нормального функціонування;

– якщо автоматизовані процедури не можуть бути використані, то КСЗІ має перевести систему до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувач, який має відповідні повноваження;

– мають існувати ручні процедури, за допомогою яких можна безпечним чином повернути ІТС до нормального функціонування.

Рівень ДВ-3 «Вибіркове відновлення» включає у себе такі вимоги:

– після будь-якої відмови ІТС або переривання обслуговування, що не призводить до необхідності заново інсталювати систему, КСЗІ має бути здатним виконати необхідні процедури та безпечним чином повернути систему до нормального функціонування або, у найгіршому випадку, до функціонування у режимі з погіршеними характеристиками обслуговування;

– якщо автоматизовані процедури не можуть бути використані, то КСЗІ має перевести ІТС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувач, який має відповідні повноваження;

– мають існувати ручні процедури, за допомогою яких можна безпечним чином повернути ІТС із режиму з погіршеними характеристиками обслуговування у режим нормального функціонування.

Ранжирування вимог критеріїв спостережності

Для того, щоб ІТС могла бути оцінена на предмет відповідності критеріям спостережності, КСЗІ оцінюваної ІТС має надавати послуги щодо забезпечення відповідальності користувача за свої дії та з підтримки здатності КСЗІ виконувати свої функції. Спостереженість забезпечується у системі такими послугами: НР – реєстрація (аудит), НИ – ідентифікація й автентифікація, НО – розподіл обов'язків, НВ – ідентифікація й автентифікація при обміні, НП – автентифікація отримувача, НК – достовірний канал, НЦ – цілісність КСЗІ, НТ – самотестування, НА – автентифікація відправника.

Реєстрація. Послуга «Реєстрація» дозволяє контролювати небезпечні для ІТС події. Рівні даної послуги ранжируються залежно від повноти та вибірковості контролю, складності засобів аналізу даних журналів реєстрації та здатності вияву потенційних порушень: НР-1 – зовнішній аналіз, НР-2 – захищений журнал, НР-3 – сигналізація про небезпеку, НР-4 – детальна реєстрація, НР-5 – аналіз у реальному часі

Спільними для всіх рівнів вважаються такі вимоги:

– політика реєстрації, що реалізується КСЗІ, має визначати перелік подій, що реєструються;

– журнал реєстрації має містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації має містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що стосувалися кожної зареєстрованої події.

Рівень НР-1 «Зовнішній аналіз» включає у себе такі вимоги:

– КСЗІ має бути здатним здійснювати реєстрацію подій, які мають безпосереднє відношення до безпеки;

– КСЗІ має бути здатним передавати журнал реєстрації в інші системи з використанням певних механізмів захисту.

Необхідна умова: НИ-1.

Рівень НР-2 «Захищений журнал» включає у себе такі вимоги:

– КСЗІ має бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки;

– КСЗІ має забезпечувати захист журналу реєстрації під несанкціонованого доступу, модифікації або руйнування. Адміністратори та користувачі, яким надані відповідні повноваження, повинні мати у своєму розпорядженні засоби перегляду й аналізу журналу реєстрації.

Необхідні умови: 1ИИ-1, НО-І.

Рівень НР-3 «Сигналізація про небезпеку» включає у себе такі вимоги:

– КСЗІ має бути здатним здійснювати реєстрацію подій, що безпосередньо стосуються безпеки;

– КСЗІ має забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори та користувачі, яким

надані відповідні повноваження, повинні мати у своєму розпорядженні засоби перегляду й аналізу журналу реєстрації;

– КСЗІ має бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки КС. КСЗІ має бути здатним негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій.

Необхідні умови: НИ-1, НО-1.

Рівень НР-4 «Детальна реєстрація» включає у себе такі вимоги:

КСЗІ має бути здатним здійснювати реєстрацію подій, що безпосередньо або непрямо стосуються безпеки;

– КСЗІ має забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори та користувачі, яким надані відповідні повноваження, новині мати у своєму розпорядженні засоби перегляду й аналізу журналу реєстрації;

– КСЗІ має бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки КС. КСЗІ має бути здатним негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій. Необхідні умови: НИ-1, НО-1.

Рівень НР-5 «Аналіз у реальному часі» включає у себе такі вимоги:

– КСЗІ має бути здатним здійснювати реєстрацію подій, що безпосередньо або непрямо стосуються безпеки;

– КСЗІ має забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори та користувачі, яким надані відповідні повноваження, повинні мати у своєму розпорядженні засоби перегляду й аналізу журналу реєстрації;

– КСЗІ має бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки КС. КСЗІ має бути здатним негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій;

– КСЗІ має бути здатним виявляти й аналізувати несанкціоновані дії у реальному часі.

Необхідні умови: НИ-1, НО-1.

Ідентифікація й автентифікація. Послуга «Ідентифікація й автентифікація» дозволяє КСЗІ визначити та перевірити особу користувача, що намагається отримати доступ до ІТС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації: НИ-1 – зовнішня ідентифікація й автентифікація, НИ-2 – поодинока ідентифікація й автентифікація, НИ-3 – множинна ідентифікація й автентифікація.

Спільною для всіх рівнів вважається вимога: політика ідентифікації й автентифікації, що реалізується КСЗІ, має визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожен користувач має однозначно ідентифікуватися КСЗІ.

Рівень НИ-1 «Зовнішня ідентифікація й автентифікація» включає у себе таку вимогу: перш, ніж дозволити будь-якому користувачу виконувати будь-які контрольовані КСЗІ дії, КСЗІ має з використанням захищеного механізму отримати від деякого зовнішнього джерела автентифікований ідентифікатор цього користувача.

Рівень НИ-2 «Поодинока ідентифікація й автентифікація» включає у себе такі вимоги:

– перш ніж дозволити будь-якому користувачу виконувати будь-які контрольовані КСЗІ дії, КСЗІ має автентифікувати цього користувача з використанням захищеного механізму;

– КСЗІ має забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

Необхідна умова: НК-1.

Рівень НИ-3 «Множинна ідентифікація й автентифікація» включає у себе такі вимоги:

– перш ніж дозволити будь-якому користувачу виконувати будь-які контрольовані КСЗІ дії, КСЗІ має автентифікувати цього користувача з використанням захищених механізмів двох або більше типів;

– КСЗІ має забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

Необхідна умова: НК-1.

Достовірний канал. Послуга «Достовірний канал» дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КСЗІ. Рівні даної послуги ранжируються залежно від гнучкості надання можливості КСЗІ або користувачу ініціювати захищений обмін: НК-1 – однонапрямлений достовірний канал, НК-2 – двонапрямлений достовірний канал.

Спільною для всіх рівнів вважається вимога: політика достовірного каналу, що реалізується КСЗІ, має визначати механізми встановлення достовірного зв’язку між користувачем і КСЗІ.

Рівень НК-1 «Однонапрямлений достовірний канал» включає у себе таку вимогу: достовірний канал має бути використаним для початкової ідентифікації й автентифікації. Зв’язок із використанням даного каналу має ініціюватися виключно користувачем.

Рівень НК-2 «Двонапрямлений достовірний канал» включає у себе такі вимоги:

– достовірний канал має бути використаний для початкової ідентифікації й автентифікації та у випадках, коли необхідний прямий зв’язок користувач – КСЗІ або КСЗІ – користувач. Зв’язок із використанням даного каналу має ініціюватися користувачем або КСЗІ;

– обмін із використанням достовірного каналу, що ініціює КСЗІ, має бути однозначно ідентифікований і має відбутися тільки після позитивного підтвердження готовності до обміну з боку користувача.

Розподіл обов'язків. Послуга «розподіл обов'язків» дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача й обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів й адміністраторів: НО-1 – виділення адміністратора, НО-2 – розподіл обов'язків адміністратора, НО-3 – розподіл обов'язків на підставі привілеїв.

Спільними для всіх рівнів вважаються такі вимоги:

– політика розподілу обов'язків, що реалізується КСЗІ, має визначати ролі адміністратора та звичайного користувача та притаманні ним функції;

– користувач повинен мати можливість виступати у певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття ним цієї ролі.

Необхідна загальна умова: НИ-1.

Рівень НО-1 «Виділення адміністратора» включає у себе спільні для всіх рівнів вимоги й умову.

Рівень НО-2 «Розподіл обов'язків адміністратора» включає у себе таку вимогу: політика розподілу обов'язків має визначати мінімум дві адміністративні ролі: адміністратора й адміністратора безпеки. Функції, притаманні кожній із ролей, мають бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі.

Рівень НО-3 «Розподіл обов'язків адміністратора на підставі привілеїв» включає у себе такі вимоги:

– політика розподілу обов'язків має визначати мінімум дві адміністративні ролі: адміністратора й адміністратора безпеки. Функції, притаманні кожній із ролей, мають бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі;

– політика розподілу обов'язків має визначати множину ролей користувачів.

Цілісність комплексу засобів захисту. Ця послуга визначає міру здатності КСЗІ захищати себе та гарантувати свою здатність керувати захищеними об'єктами. Включає у себе такі рівні: НЦ-1 – КСЗІ із контролем цілісності, НЦ-2 – КСЗІ із гарантованою цілісністю, НЦ-3 – КСЗІ із функціями диспетчера доступу.

Рівень НЦ-1 «КСЗІ з контролем цілісності» включає у себе такі вимоги:

– політика цілісності КСЗІ має визначати склад КСЗІ та механізми контролю цілісності компонентів, що входять до складу КСЗІ;

– у разі виявлення порушення цілісності будь-якого зі своїх компонентів КСЗІ має повідомити адміністратора та/або автоматично відновити відповідність компонента еталону або перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувач, якому надані відповідні повноваження;

– мають бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КСЗІ та всі запити на доступ до захищених об'єктів контролюються КСЗІ.

Необхідні умови: НР-1, НО-1.

Рівень НЦ-2 «КСЗІ з гарантованою цілісністю» включає у себе такі вимоги:

– політика цілісності КСЗІ має визначати домен КСЗІ й інші домени, а також механізми захисту, що використовуються для реалізації розподілу доменів;

– КСЗІ має підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування;

– мають бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КСЗІ і всі запити на доступ до захищених об'єктів контролюються КСЗІ.

Рівень НЦ-3 «КСЗІ зі функціями диспетчера доступу» включає у себе такі вимоги:

– політика цілісності КСЗІ має визначати домен КСЗІ й інші домени, а також механізми захисту, що використовуються для реалізації розподілу доменів;

– КСЗІ має підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації та/або втрати керування;

– КСЗІ має гарантувати, що послуги безпеки доступні тільки через інтерфейс КСЗІ та всі запити на доступ до захищених об'єктів контролюються КСЗІ.

Самотестування. Самотестування дозволяє КСЗІ перевірити та на підставі цього гарантувати правильність функціонування та цілісність певної множини функцій КС. Рівні даної послуги ранжируються на підставі можливості виконання тестів у процесі запуску або штатної роботи: НТ-1 – самотестування за запитом, НТ-2 – самотестування при старті, НТ-3 – самотестування у реальному часі.

Спільною для всіх рівнів вважається наступна вимога: політика самотестування, що реалізується КСЗІ, має описувати властивості ІТС і реалізовані процедури, які можуть бути використані для оцінювання правильності функціонування КСЗІ. Необхідна загальна умова: Н-01.

Рівень НТ-1 «Самотестування за запитом» включає у себе таку вимогу: КСЗІ має бути здатним виконувати набір тестів із метою оцінювання правильності функціонування своїх критичних функцій. Тести мають виконуватися за запитом користувача, що має відповідні повноваження.

Рівень НТ-2 «Самотестування на старті» включає у себе таку вимогу: КСЗІ має бути здатним виконувати набір тестів із метою оцінювання правильності функціонування своїх критичних функцій. Тести мають виконуватися при ініціалізації КСЗІ за запитом користувача, що має відповідні повноваження.

Рівень НТ-3 «Самотестування у реальному часі» включає у себе таку вимогу: КСЗІ має бути здатним виконувати набір тестів із метою оцінювання правильності функціонування своїх критичних функцій. Тести мають виконуватися при ініціалізації КСЗІ та у процесі штатного функціонування за запитом користувача, що має відповідні повноваження.

Ідентифікація й автентифікація при обміні. Ця послуга дозволяє одному КСЗІ ідентифікувати інший КСЗІ (встановити та перевірити його ідентичність)

та забезпечити іншому КСЗІ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації: НВ-1 – автентифікація вузла, НВ-2 – автентифікація джерела даних, НВ-3 – автентифікація підтвердження.

Спільними для всіх рівнів вважаються такі вимоги:

– політика ідентифікації й автентифікації при обміні, що реалізується КСЗІ, має визначати множину атрибутів КСЗІ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КСЗІ;

– КСЗІ, перш ніж почати обмін даними з іншим КСЗІ, має ідентифікувати й автентифікувати цей КСЗІ з використанням захищеного механізму;

– підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

Рівень НВ-1 «Автентифікація вузла» включає у себе загальні вимоги.

Рівень НВ-2 «Автентифікація джерела даних» включає у себе таку вимогу: КСЗІ має використовувати захищені механізми для встановлення джерела кожного об’єкта, що експортується чи імпортується.

Рівень НВ-3 «Автентифікація з підтвердженням» включає у себе такі вимоги:

– КСЗІ має використовувати захищені механізми для встановлення джерела кожного об’єкта, що експортується чи імпортується;

– використаний протокол автентифікації має забезпечувати можливість однозначного підтвердження джерела об’єкта незалежною третьою стороною.

Автентифікація відправника. Послуга «автентифікація відправника» дозволяє забезпечити захист від заперечення свого авторства й 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: НЛ-1 – базова автентифікація відправника, НА-2 – автентифікація відправника з підтвердженням.

Спільними для всіх рівнів вважаються такі вимоги:

– політика автентифікації відправника, що реалізується КСЗІ, має визначати множину властивостей й атрибутів об’єкта, що передається, користувача-відправника й інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об’єкт був відправлений (створений) певним користувачем;

– встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації.

Необхідна загальна умова: НИ-1.

Рівень НА-1 «Базова автентифікація відправника» включає у себе спільні вимоги та необхідну загальну умову.

Рівень НА-2 «Автентифікація відправника з підтвердженням» включає у себе такі вимоги:

– додатково мають бути визначені ті властивості, атрибути та процедури, які можуть бути використані для однозначного підтвердження належності об’єкта незалежною третьою стороною;

– використаний протокол автентифікації має забезпечувати можливість однозначного підтвердження належності об’єкта незалежною третьою стороною.

Автентифікація отримувача. Послуга «автентифікація отримувача» дозволяє забезпечити захист від заперечення отримання та дозволяє однозначно встановити факт отримання певного об’єкта певним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною: НП-1 – базова автентифікація отримувача, НП-2 – автентифікація отримувача з підтвердженням.

Спільними для всіх рівнів вважаються такі вимоги:

– політика автентифікації отримувача, що реалізується КСЗІ, має визначати множину властивостей і атрибутів об’єкта, що передається, користувача-отримувача й інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об’єкт був отриманий певним користувачем;

– встановлення належності отримувача має виконуватися на підставі затвердженого протоколу автентифікації.

Необхідна загальна умова: НИ-1.

Рівень НП-1 «Базова автентифікація отримувача» включає у себе спільні вимоги та необхідну загальну умову.

Рівень НП-2 «Автентифікація отримувача з підтвердженням» включає у себе такі вимоги:

– додатково мають бути визначені ті властивості, атрибути та процедури, які можуть бути використані незалежною третьою стороною для однозначного підтвердження факту отримання об’єкта;

– використаний протокол автентифікації має забезпечувати можливість однозначного підтвердження незалежною третьою стороною факту отримання об’єкта.

Далі можемо порівняти викладені критерії із підходами до оцінки захищеності у міжнародних стандартах.

1.4 Класифікація та функціональні профілі захищеності інформаційно-комунікаційних систем

Складність архітектури та різноманітність інформаційно-комунікаційних систем (ІТС) – локальні, корпоративні, глобальні – вимагають створити їхні класи безпеки та приводять до втілення концепції функціональних профілів безпеки. У НД ТЗІ 2.5-005-99 [18] встановлюються принципи класифікації автоматизованих систем (тобто ІТС за сучасною термінологією) й утворення стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу.

Класифікація автоматизованих систем у НД ТЗІ 2.5-005-99. Мета введення класифікації ІТС і стандартних функціональних профілів захищеності полягає у полегшенні задачі зіставлення вимог до комплексу засобів захисту (КЗЗ) обчислювальної системи ІТС зі характеристиками ІТС.

Автоматизована система, з погляду кібербезпеки, являє собою організаційно-технічну систему, що об'єднує операційну систему (ОС), фізичне середовище, персонал й оброблювану інформацію.

Вимоги до функціонального складу комплексу засобів захисту (КЗЗ) залежать від характеристик оброблюваної інформації, самої ОС, фізичного середовища, персоналу й організаційної підсистеми.

Вимоги до гарантій визначаються насамперед характером (важливістю) оброблюваної інформації та призначенням ІТС.

У цьому документі за сукупністю характеристик ІТС (конфігурація апаратних засобів ОС та їх фізичне розміщення, кількість різноманітних категорій оброблюваної інформації, кількість користувачів і категорій користувачів) виділено три ієрархічні класи ІТС, вимоги до функціонального складу КЗЗ яких істотно відрізняються.

Клас 1 – це одномашинний однокористувацький комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності. Істотні особливості:

– у кожен момент часу з комплексом може працювати лише один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але всі вони повинні мати однакові повноваження (права) щодо доступу до інформації, яка обробляється;

– технічні засоби (носії інформації та засоби вводу/виводу) з точки зору захищеності належать до однієї категорії та всі можуть бути використані для збереження та/або вводу, виводу всієї інформації.

Приклад: автономна персональна ЕОМ, доступ до якої контролюється з використанням організаційних заходів, або надбудованою системою заходів захисту.

Клас 2 – локалізований багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відміна від попереднього класу – наявність користувачів із різними повноваженнями по доступу та/або технічних засобів, які можуть одночасно здійснювати оброблення інформації різних категорій конфіденційності.

Приклад: локальна обчислювальна мережа.

Клас 3 – розподілений багатомашинний багатокористувцький комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відміна від попереднього класу – необхідність передачі інформації через незахищене середовище або, у загальному випадку, наявність вузлів, що реалізують різну політику безпеки. Приклад: глобальна обчислювальна мережа.

В межах кожного класу ІТС класифікуються на підставі вимог до забезпечення певних властивостей інформації. З точки зору безпеки інформація характеризується трьома властивостями: конфіденційністю, цілісністю та доступністю. У зв'язку з цим, у кожному класі ІТС виділяються такі підкласи:

– автоматизована система, в якій підвищено вимоги до забезпечення конфіденційності оброблюваної інформації (підкласи х.К);

– автоматизована система, в якій підвищено вимоги до забезпечення цілісності оброблюваної інформації (підкласи х.Ц);

– автоматизована система, в якій підвищено вимоги до забезпечення доступності оброблюваної інформації (підкласи х.Д);

– автоматизована система, в якій підвищено вимоги до забезпечення конфіденційності та цілісності оброблюваної інформації (підкласи х.КЦ);

– автоматизована система, в якій підвищено вимоги до забезпечення конфіденційності та доступності оброблюваної інформації (підкласи х.КД);

– автоматизована система, в якій підвищено вимоги до забезпечення цілісності та доступності оброблюваної інформації (підкласи х.ЦД);

– автоматизована система, в якій підвищено вимоги до забезпечення конфіденційності, цілісності та доступності оброблюваної інформації (підкласи х.КЦД).

Для кожного з підкласів кожного класу вводиться деяка кількість ієрархічних стандартних функціональних профілів, яка може бути різною для кожного класу та підкласу ІТС. Профілі є ієрархічними у тому розумінні, що їх реалізація забезпечує зростаючу захищеність від загроз відповідного типу (конфіденційності, цілісності та доступності). Зростання рівня захищеності може досягатись як підсиленням певних послуг, тобто включенням до профілю більш високого рівня послуги, так і включенням до профілю нових послуг.

Така класифікація корисна для полегшення вибору переліку функцій, які повинен реалізувати КЗЗ ОС, проектованої або існуючої ІТС. Цей підхід дозволяє мінімізувати витрати на початкових етапах створення комплексної системи захисту інформації ІТС. Для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної ІТС, необхідне проведення у повному обсязі аналізу загроз й оцінки ризиків.

Функціональні профілі захищеності. Визначення та призначення

Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізувати КЗЗ обчислювальної системи, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється у даній ІТС. Стандартні функціональні профілі будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред’являються.

Політика безпеки ІТС, що реалізує певний стандартний профіль, має бути "успадкована" з відповідних документів, що встановлюють вимоги до порядку обробки певної інформації в ІТС. Так один і той самий профіль захищеності може бути використано для опису функціональних вимог із захисту оброблюваної інформації та для ОС, і для СУБД у той час, як їхня політика безпеки, зокрема, визначення об’єктів, буде різною.

Єдина вимога, якої слід дотримуватися при утворенні нових профілів – це дотримання описаних у НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації у комп’ютерних системах від несанкціонованого доступу» необхідних умов для кожної із послуг, що включаються у профіль.

Функціональні профілі можуть бути використані також для порівняння оцінки функціональності КС за критеріями інших держав із оцінкою за національними критеріями.

Семантики профілю. Опис профілю складається з трьох частин: літерно-числового ідентифікатора, знака рівності та переліку рівнів послуг, взятого у фігурні дужки. Ідентифікатор у свою чергу включає: позначення класу ІТС (1, 2 або 3), літерну частину, що характеризує види загроз, від яких забезпечується захист (К, і/або Ц. і/або Д), номер профілю та необов'язкове літерне позначення версії. Всі частини ідентифікатора відділяються одна від одної крапкою.

Наприклад, 2.К.4 – функціональний профіль номер чотири, що визначає вимоги до ІТС класу 2, призначених для обробки інформації, основною вимогою щодо захисту якої є забезпечення конфіденційності.

Версія може служити, зокрема, для вказівки на підсилення певної послуги всередині профілю. Наприклад, нарощування можливостей реєстрації приведе до появи нової версії.

Стандартні профілі. Класифікація ІТС, у якій надані стандартні профілі захищеності для різних класів ІТС, що описують вимоги до КЗЗ обчислювальних систем, які входять до складу цих ІТС, наведені у [18]. Оскільки класифікація ІТС достатньо умовна, той факт, що деякий профіль не потрапив до наведеного нижче переліку, не означає, що він некоректний або гірший за перелічені. Наведені профілі відповідають тим видам КС, потреба в яких найактуальніша.

До всіх профілів включені послуги спостережності, оскільки, з одного боку, реалізація багатьох із них є необхідною умовою для реалізації інших послуг, а з іншого, спостережність і керованість важливі для будь-якої системи, що реалізує будь-які функції захисту інформації.

***Приклад функціонального профілю для ІТС класу* «1».** Комплекс засобів захисту від несанкціонованого доступу (НСД) «Гриф» призначено для захисту опрацьовуваної на ПЕОМ інформації від несанкціонованого ознайомлення, модифікування, вилучення. КЗЗ дозволяє створити безпечне технологічне середовище для систем електронного документообігу, банківських й інших систем, для яких ключовою вимогою є дотримання конфіденційності опрацьовуваної інформації та технології її опрацювання. КЗЗ є спеціалізованою надбудовою над стандартною операційною системою типу MS Windows 95/98 і її наступними версіями ОС і доповнює її функціями розмежування доступу. Комплекс дозволяє створити захищене автоматизоване робоче місце з обмеженим колом користувачів, які мають різні повноваження щодо доступу до ресурсів. Сукупність реалізованих у комплексі функцій і механізмів захисту інформації забезпечує рівень захищеності інформації, достатній для опрацьовування інформації, яка становить як державну, так і комерційну таємницю.

Згідно НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу", КЗЗ від НСД може реалізувати функціональний профіль:

{КА-2, КО-0, ЦА-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-1, НТ-2}. Найчастіше розроблення виконують відповідно до вимог щодо рівня гарантій Г-3.

КЗЗ системи автоматизації обраного функціонального профілю захищеності має реалізувати такі послуги із захисту інформації:

1) надавати послуги із захисту об'єктів від несанкціонованого ознайомлення з їхнім змістом (компрометації). Конфіденційність забезпечується такими послугами: КА-1 – мінімальна адміністративна конфіденційність, КО-1 – повторне використання об'єктів;

2) надавати послуги із захисту опрацьовуваної інформації від несанкціонованого модифікування. Цілісність може забезпечуватись послугою ЦА-1 – мінімальна адміністративна цілісність;

3) надавати послуги із забезпечення можливості використання системи автоматизації у цілому, окремих функцій чи опрацьовуваної інформації на певному проміжку часу та гарантувати здатність системи автоматизації функціонувати у разі відмови її компонентів. Доступність може забезпечуватися послугою ДВ-1 – ручне відновлення після збоїв;

4) надавати послуги із забезпечення відповідальності користувача за свої дії та за підтримування здатності КЗЗ виконувати свої функції. Спостережність забезпечується у системі автоматизації такими послугами: НР-2 – реєстрування (аудит), (захищений журнал), НИ-2 – одиночне ідентифікування й автентифікування, НК-1 – односпрямований вірогідний канал, НО-1 – розподіл обов'язків, а саме виокремлення адміністратора, НЦ-1 – КЗЗ із контролем цілісності, НТ-2 – самотестування при стартуванні.

Поданий функціональний профіль є зумовлений призначенням комплексу та сформований на підставі попередньо проведеного аналізування загроз і ризиків із урахуванням таких моментів:

– комплекс призначено для автономної (відімкненої від локальної мережі та не виступаючої у ролі сервера) ПЕОМ, на якій водночас не можуть працювати кілька користувачів чи виконуватися процеси інших користувачів, що значно скорочує перелік загроз, а отже, й вимоги до набору послуг безпеки;

– комплекс за визначенням є надбудований над програмно-апаратною платформою імпортного виробництва, що накладає низку обмежень на перелік і рівні послуг, які не можна здолати принципово; цим фактом, зокрема, обмежено й рівень гарантій;

– реалізація додаткових послуг та/чи їхніх більш високих рівнів, які забезпечують захист від малоймовірних загроз, чи подальше зниження рівня ризику потребує значних витрат.

Зазначений функціональний профіль досягається лише у тому разі, якщо виконується низка умов й обмежень, зокрема обов'язковим є використання апаратного захисту від несанкціонованого завантаження.

Приклад функціонального профілю для ІТС класу «2». До класу «2» ІТС відносять локальні обчислювальні мережі (ЛОМ), сполучувальні лінії між комп'ютерами якої не виходять за межі контрольованої зони. Нормативним документом НД ТЗІ 2.5-008-2002 [20] визначаються наведені нижче стандартні

функціональні профілі захищеності інформації під час застосування технології, яка потребує підвищених вимог до забезпечування:

– конфіденційності опрацьовуваної інформації:

2.К.3 = {КД-2, КА-2, КО-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2};

– конфіденційності та цілісності опрацьовуваної інформації:

2.КЦ.3 = {КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2};

– конфіденційності та доступності опрацьовуваної інформації:

2.КД.1а = {КД-2, КА-2, КО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2};

– конфіденційності, цілісності та доступності опрацьовуваної інформації:

2.КЦД.2а = {КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2}.

Позначення послуг безпеки подано згідно табл. 1.1:

ДВ-1 – ручне відновлення;

* ДЗ-1 – модернізація;

ДР-1 – квоти;

* ДС-1 – стійкість за обмежених відмовлень;

КА-2 – базова адміністративна конфіденційність;

* КД-2 – базова довірча конфіденційність;

* КО-1 – повторне використання об’єктів;

НИ-2 – поодиноке ідентифікування й автентифікування;

НК-1 – односпрямований вірогідний канал;

\+ НО-2 – розподіл обов’язків адміністраторів (для WEB-сторінки буде обиратись НО-1);

\+ НТ-2 – самотестування при старті (для WEB-сторінки обирають НТ-1);

НР-2 – захищений журнал;

\+ НЦ-2 – комплекс засобів захисту з гарантованою цілісністю (для WEB-сторінки буде обиратись НЦ-1);

ЦА-1 – мінімальна адміністративна цілісність;

* ЦА-2 – базова адміністративна цілісність;

* ЦД-1 – мінімальна довірча цілісність;

ЦО-1 – обмежений відкіт.

Зірочкою* позначено послуги безпеки, які пов’язані з більш високою категорією захищуваної конфіденційної інформації. Значком “+” зазначено послуги з підвищеним рівнем захищеності інформації, що є пов’язано із захистом інформації вищого грифу таємності.

При виборі функціонального профілю захисту інформації слід врахувати нижчеподані особливості:

1. У разі, коли у ЛОМ усіх користувачів допущено до опрацювання конфіденційної інформації, реалізування послуги безпеки КО-1 не є обов’язкове.

2. Реалізування послуг безпеки, базованих на довірчому принципі розмежування доступу (КД і ЦД), може здійснюватися у разі:

- якщо політикою безпеки передбачено створення груп користувачів із однаковими повноваженнями щодо роботи з конфіденційною інформацією для розмежування доступу у межах цих груп;

- для розмежування доступу до об'єктів, які потребують захисту, але не містять конфіденційної інформації.

В усіх інших випадках розмежування доступу здійснюється згідно з адміністративним принципом (послуги безпеки КА й ЦА).

3. Рівень ЦА-2 послуги безпеки "адміністративна цілісність" реалізується під час опрацювання конфіденційної інформації, розміщеної у сильнопов'язаних об'єктах. Для опрацювання конфіденційної інформації, розміщеної у слабкопов'язаних об'єктах, реалізується рівень послуги ЦА-1.

У разі необхідності для конкретної ЛОМ до функціональних профілів захищеності можуть вводитися додаткові послуги безпеки, а також підвищуватись рівень будь-якої з наведених послуг.

За певних обставин у КСЗІ вимоги щодо політики впровадження окремих послуг безпеки можуть частково забезпечуватися організаційними чи іншими заходами захисту. Рівень такої послуги, що входить до профілю захищеності, може бути знижено. Послуга безпеки може не реалізуватись, якщо її політика у повному обсязі відповідно до моделі захисту інформації спрямована на нейтралізацію лише неістотних загроз, визначених моделлю загроз для інформації в автоматизованій системі.

***Приклади функціонального профілю для ІТС класу* «3».**

Приклад 1. Під час створення WEB-сторінки та визначення операторів, вузли яких будуть використані для приєднання до Інтернету, слід керуватися законами України, іншими нормативно-правовими актами, які встановлюють вимоги з технічного захисту інформації. Запровадження організаційних, технічних і програмно-технічних заходів захисту за технічної експлуатації систем захисту WEB-сторінок базується на НД ТЗІ 2.5-010-03 "Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу", законах і указах щодо захисту інформації, яка є власністю держави, й інших нормативно-правових актах.

Залежно від способу передавання інформації від сервера до робочої станції розрізнюють дві технології:

– технологія Т1, коли WEB-сервер і робочі станції розташовуються на території установи-власника WEB -сторінки чи на території оператора;

– технологія Т2, коли WEB-сервер розташовується на території оператора, а робочі станції – на території власника WEB-сторінки, взаємодія яких із WEB-сервером здійснюється з використанням мереж передавання даних.

Технологія Т1 відрізняється від технології Т2 способом передавання інформації від робочої станції до WEB-сервера, а саме: наявністю у другому випадку незахищеного й не контрольованого середовища та додатковими вимогами щодо ідентифікування й автентифікування між комплексом засобів захисту робочої станції й комплексом засобів захисту WEB-сервера під час спроби розпочати обмін інформацією та забезпечування цілісності інформації при обміні.

З урахуванням особливостей надавання доступу до інформації WEB-сторінки, типових характеристик середовищ функціонування й особливостей технологічних процесів опрацювання інформації рекомендуються такі мінімально необхідні рівні послуг безпеки для забезпечування захисту інформації від загроз:

– за умови технології Т1 мінімально необхідний функціональний профіль є КА-2, ЦА-1, ЦО-1, ДВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1;

– за умови технології Т2 мінімально необхідний функціональний профіль визначається КА-2, КВ-1, ЦА-1, ЦО-1, ЦВ-1, ДВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-1,НЦ-1, НТ-1, НВ-1.

Використовуються такі позначення послуг, які використовуються у функціональних профілях:

– *за критерієм доступності:*

ДВ-1 - ручне відновлювання після збоїв;

ДР-1 - квоти;

– *за критерієм конфіденційності:*

КА-2 - базова адміністративна конфіденційність;

КВ-1[*)] - мінімальна конфіденційність при обміні;

– *за критерієм спостережності:*

НВ-1[*)] - автентифікування вузла;

НИ-2 - одиночне ідентифікування й автентифікування;

НК-1 - односпрямований вірогідний канал;

НО-1 - розподіл обов'язків;

НР-2 - захищений журнал;

НТ-1 - самотестування за запитом;

НЦ-1 – комплекс засобів захисту з контролем цілісності;

– *за критерієм цілісності:*

ЦА-1 - мінімальна адміністративна цілісність;

ЦВ-1[*)] - мінімальна цілісність при обміні;

ЦО-1 - обмежений відкіт.

Зірочкою [*)] позначено послуги безпеки КВ-1, ЦВ-1, НВ-1 – конфіденційності, цілісності при обміні й автентифікування вузла, що належать до характерної особливості технології Т2, тобто до необхідності передавання інформації через незахищене середовище та наявності вузлів, які реалізують різну політику безпеки.

З функціональних профілів видно, що до системи захисту інформації WEB-сторінки пред'являються дещо підвищені вимоги стосовно конфіденційності та спостережності.

Як буде показано далі, конфіденційність КА-2 стосується обмеження доступу до технологічної інформації мережі, а спостережність (НИ-2, НР-2) – необхідності контролю за діями користувачів в умовах боротьби зі тероризмом.

У разі, коли в автоматизованих системах вимоги щодо політики впровадження будь-якої із послуг безпеки забезпечуються організаційними чи іншими заходами захисту, які у повному обсязі відповідають установленим НД-ТЗІ-2.5-004-99 специфікаціям для певного рівня послуги безпеки, то рівень

такої послуги у профілі захищеності може бути знижено на відповідну величину.

Приклад 2. Порядок створення та функціонування системи інформаційної безпеки у телекомунікаційних мережах визначаються міжнародними та вітчизняними рекомендаціями та нормативними документами. Зокрема, вимоги з інформаційної безпеки входять у документи ITU-T серії Е: «Загальна експлуатація мережі, функціонування служб і людські фактори, керування мережею». Нові проблеми інформаційної безпеки є порівняно складними та мають охоплювати декілька рівнів і сфер діяльності: мережне адміністрування, фізичну безпеку, моніторинг, програмне забезпечення телекомунікацій, інструменти забезпечення безпеки, аудит безпеки. Міжнародна Рекомендація МСЕ Е.408 визначає перелік функціональних вимог, послуги, які ці вимоги забезпечують (табл. 1.2) й особливості реалізації послуг безпеки за рівнями моделі взаємодії відкритих систем [26].

Таблиця 1.2. – Взаємозв’язок вимог до безпеки та послуг безпеки

Функціональна вимога	**Послуга безпеки**
Підтвердження ідентифікаційної інформації	Автентифікація: користувача, рівноправного об’єкта, джерела даних
Керований доступ й авторизація	Керування доступом
Захист цілісності системи	Керування доступом
Захист конфіденційності даних, які зберігаються	Керування доступом
Захист конфіденційності даних, які переносяться	Конфіденційність
Захист цілісності даних, які зберігаються	Керування доступом
Захист цілісності даних, які переносяться	Цілісність
Звітність	Захист від невизнання участі
Реєстрація дій	Аудиторський журнал
Аварійне сповіщення безпеки	Аварійний сигнал безпеки
Аудит безпеки	Аудиторський журнал і відновлення

Визначення та характеристику функціональних вимог і послуг безпеки дано у навчальному посібнику [12, розд. 4…7]. Практичне значення Рекомендації ITU-T Е.408 полягає також у тому, що у ній визначені функціональні класи (*Functional Classes*, *FC*), за якими можна класифікувати заходи безпеки.

Функціональний клас – це послідовний комплекс заходів безпеки для задоволення вимог до безпеки на різних функціональних рівнях. Запропоновані функціональні класи на трьох рівнях безпеки: мінімальний функціональний клас (*FC* 1), базовий функціональний клас (*FC* 2) й удосконалений функціональний клас (*FC* 3) (табл. 1.3).

Факультативність послуг конфіденційності згідно вітчизняної нормативної бази означає, що послуга конфіденційності може надаватись оператором телекомунікацій лише за спеціальним договором із власником інформаційної мережі, для якої надаються телекомунікаційні послуги.

Функціональний клас послуг безпеки базового рівня може бути впроваджено у телекомунікаційних мережах шляхом деякої реорганізації служби технічної експлуатації.

Таблиця 1.3 – Функціональні класи послуг безпеки

***FC* 1**	***FC* 2**	***FC* 3**
Основна увага надається цілісності зберіганих керованих ресурсів	Основна увага надається цілісності зберіганих керованих ресурсів і цілісності даних, які передаються	Як *FC* 2 плюс звітність за операціями керування
Автентифікація (рівноправного об'єкта або користувача). Керування доступом до домену адміністративного правління. Керування доступом до керованого ресурсу. Аварійний сигнал безпеки, перевірка й відновлення	Автентифікація (рівноправного об'єкта й користувача). Керування доступом до домену адміністративного управління. Керування доступом до керованого ресурсу Автентифікація джерела даних. Вибіркова цілісність поля. Цілісність з'єднання. Аварійний сигнал безпеки, перевірка й відновлення	Автентифікація (рівноправного об'єкта й користувача). Керування доступом до домену адміністративного управління. Керування доступом до керованого ресурсу. Автентифікація джерела даних. Вибіркова цілісність поля. Цілісність з'єднання. Захист від невизнання участі джерела. Захист від невизнання участі отримувача. Аварійний сигнал безпеки, перевірка й відновлення
Факультативно: - цілісність з'єднання; - конфіденційність з'єднання	Факультативно: - конфіденційність з'єднання; - вибіркова конфіденційність поля	Факультативно: - конфіденційність з'єднання; - вибіркова конфіденційність поля

Задачі захисту інформаційних ресурсів знаходяться у тісному зв'язку та істотно залежать від (показників) якості, характеристик доставки інформації, надійності мереж. Останні є предметом піклування системи технічної експлуатації.

Міжнародні рекомендації однозначно визначають функціонування систем інформаційної безпеки у складі системи загальної експлуатації мережі й керування мережею з урахуванням людського фактора.

1.5 Основні положення «Загальних критеріїв оцінювання безпеки інформаційних технологій»

Міжнародний стандарт ISO/IEC 15408 «Інформаційні технології – Методи захисту – Критерії оцінювання ІТ-безпеки» часто називають «Загальні критерії оцінювання безпеки інформаційних технологій [Common Criteria foi-Information Technology Security Evaluation (CCITSE)]. Цей стандарт було прийнято в Україні як державний стандарт [27 – 29] і рекомендовано для широкого впровадження, головним чином, у підприємствах й організаціях різної форми власності. Стандарт продовжує активно розвиватись, його версії випускались у 2002 – 2005 рр. Остання версія підготовлена у 2011 р. Вона скасовує та замінює попередні версії стандарту.

ISO/IEC 15408 складається із трьох частин:

Частина 1. Вступ і загальна модель.

Частина 2. Функціональні компоненти безпеки.

Частина 3. Компоненти гарантій безпеки.

Стандарт ISO/IEC 15408 застосовується сумісно зі стандартом ISO/IEC 180045-2008 «Інформаційна технологія – Методи та засоби забезпечення безпеки – Методологія оцінки безпеки інформаційних технологій».

Загалом стандарт ISO/IEC 15408 розвиває попередні міжнародні документи щодо критеріїв оцінки безпеки та представляє єдину основу для формулювання розробниками, користувачами й оцінювачами (експертами) інформаційних технологій вимог, метрик і гарантій безпеки. Стандарт ISO/IEC 15408 корисний як настанова для розробки, оцінювання та/або придбання ІТ-продуктів, що мають засоби кібербезпеки.

Основними компонентами стандарту ISO/IEC 15408 є:

- потенційні загрози безпеці;
- завдання захисту;
- політика безпеки;
- продукт інформаційних технологій;
- профіль захисту (PP – Protection Profile);
- проект захисту (ST – Security Target);
- функціональні вимоги безпеки;
- вимоги гарантій безпеки;
- рівні гарантій.

Матеріали стандарту являють собою енциклопедію вимог і гарантій з інформаційної безпеки, які можуть обиратися та реалізуватися у функціональні профілі захисту для конкретних систем, мереж і засобів як постачальниками, що пропонують засоби захисту, так і користувачами, розробниками й операторами мереж (по відношенню до того, що вони гарантують у продукті, який реалізується).

Стандарт ISO/IEC 15408 сконцентровано на захисті інформаційних ресурсів від несанкціонованого розкриття (конфіденційності) модифікації (цілісності) або неможливості використання (доступності). ISO/IEC 15408 можна застосувати для оцінювання антропогенних ризиків (зловмисних або інших дій) і ризиків що не пов’язані з діяльністю людини.

ISO/IEC 15408 розраховано на споживачів, розробників і оцінювачів безпечних ІТ-продуктів. Вони можуть використовувати стандарт таким чином:

- споживачі обирають компоненти для вираження функціональних вимог, що задовольняють цілі безпеки, виражені у профілі захисту – PP, або проекті захисту – ST). ISO/IEC 15408-1 надає докладну інформацію про відношення між цілями безпеки та вимогами до захисту;
- розробники, що задовольняють отримані від споживачів вимоги безпеки у побудові об'єкта оцінки, можуть задіяти стандартний метод тлумачення цих вимог. Вони можуть використати конвент стандарту як базис подальшого визначення функціональної безпеки об'єкта оцінки та механізмів, що виконують ці вимоги;
- оцінювачі, що використовують функціональні вимоги, визначені у стандарті, під час верифікації виконання вимог об'єкта оцінки, що виражені у профілі захисту – PP, або проекті захисту – ST); цілей безпеки ІТ-систем, а також обліку й усіх залежностей. Оцінювачі мають використовувати стандарт у вирішенні, чи задовольняє об'єкт оцінки заявленим вимогам.

Кваліфікування рівня безпеки

Кваліфікаційний аналіз – це аналіз ІТС із метою визначення рівня її захищеності та відповідності вимогам безпеки на основі критеріїв стандарту інформаційної безпеки.

Для проведення кваліфікаційного аналізу розробник продукту повинен надати наступні матеріали:

- профіль захисту (PP – Protection Profile);
- проект захисту (ST – Security Target);
- обґрунтування та підтвердження властивостей і можливостей ІТ-продукту, отримані розробником;
- сам ІТ-продукт;
- додаткові відомості, отримані шляхом проведення різноманітних незалежних експертиз.

Процес кваліфікаційного аналізу включає такі три стадії:

- аналіз профілю захисту на предмет його повноти, несуперечності, реалізованості та можливості використання у вигляді набору вимог для продукту, що аналізується;
- аналіз проекту захисту на предмет його відповідності профілю захисту, а також повноти, несуперечності, реалізованості та можливості використання у вигляді еталона при аналізі ІТ-продукту;
- аналіз ІТ-продукту на предмет відповідності проекту захисту. Результатом кваліфікаційного аналізу є висновок про те, що підданий аналізу ІТ-продукт відповідає представленому проекту захисту.

Потенційні загрози безпеці

Загрози безпеці обчислювальної системи – це впливи на обчислювальну систему, які прямо або побічно можуть нанести шкоду її безпеці. Розробники вимог безпеки та засобів захисту виділяють три види загроз:

- загрози порушення конфіденційності інформації;
- загрози порушення цілісності інформації;

- загрози порушення працездатності системи (відмови в обслуговуванні).

Загрози порушення конфіденційності – загрози безпеці обчислювальної системи, спрямовані на розголошення інформації з обмеженим доступом.

Загрози порушення цілісності – загрози безпеці обчислювальної системи, що полягають у спотворенні або зміні неавторизованим користувачем інформації, що зберігається або передається. Цілісність інформації може бути порушена як зловмисником, так і у результаті об'єктивних впливів зі боку середовища експлуатації системи. Найбільш актуальна ця загроза для систем передавання інформації – комп'ютерних мереж і систем телекомунікації.

Загрози порушення працездатності – загрози безпеці обчислювальної системи, спрямовані на створення ситуацій, коли у результаті навмисних дій знижується працездатність обчислювальної системи або її ресурси стають недоступними.

Типові завдання захисту

Завдання захисту декларуються наступним чином:

- захист від загроз порушення конфіденційності (несанкціонованого отримання) інформації з усіх каналів її витоку, особливо за рахунок каналів *ПЕМВН* і *прихованих* (таємних) каналів зв'язку;
- захист від загроз порушення цілісності (несанкціонованого змінювання інформації);
- захист від загроз порушення доступності інформації (несанкціонованого або випадкового обмеження інформації та ресурсів самої системи);
- захист від загроз аудиту системи (наприклад, загрози несанкціонованих вторгнень у систему, маніпуляцій з протоколами обміну й аудиту, із загальносистемним програмним забезпеченням).

Політика безпеки

Політика безпеки - це сукупність законів, норм і правил, що регламентують порядок оброблення, захисту та розповсюдження інформації комп'ютерної системи.

У системах зв'язку політика безпеки є частиною загальної політики безпеки оператора зв'язку та може включати, зокрема, положення державної політики у галузі захисту інформації.

Для кожної системи (підсистеми) зв'язку політика безпеки може бути індивідуальною та може залежати від технології передавання, оброблення та зберігання інформації, що реалізується, від особливостей системи зв'язку, середовища експлуатації та від багатьох інших факторів. Політика має визначати ресурси системи зв'язку, які потребують захисту, зокрема, встановлювати категорії інформації, яка передається, обробляється та зберігається у системі. Мають бути сформульовані основні загрози для системи зв'язку, персоналу, інформації різних категорій і вимоги до захисту від цих загроз.

Складовими частинами загальної політики безпеки у системі зв'язку мають бути політики забезпечення конфіденційності, цілісності та доступності інформації, що передається, обробляється та зберігається. Відповідальність персоналу за виконання положень політики безпеки має бути персоніфікована.

Частина політики безпеки, яка регламентує правила доступу користувачів і процесів системи зв'язку, складає правила розмежування доступу.

Продукт інформаційних технологій (ІТ-продукт)

ІТ-продукт - це сукупність апаратних і/(або) програмних засобів, які поставляються кінцевому споживачеві як готовий до використання засіб оброблення інформації. Сукупність ІТ-продуктів об'єднується у функціонально закінчений комплекс (продукт) для вирішення конкретного прикладного завдання у системі оброблення інформації.

ІТ-продукт звичайно розробляється для використання у багатьох системах оброблення інформації, тому його розробник орієнтується тільки на найзагальніші вимоги до середовища його експлуатації (умови його застосування та потенційні загрози інформації).

Навпаки, система оброблення інформації розробляється вузько спеціалізованою для вирішення конкретних прикладних задач і під конкретні вимоги споживачів, що дозволяє повною мірою врахувати специфіку впливу з боку конкретного середовища експлуатації. Саме тому ІТ-продукт, а не система оброблення інформації, декларується у стандарті як універсальний компонент безпеки.

Профіль захисту

Профіль захисту - це спеціальний нормативний документ. що регламентує сукупність завдань захисту, функціональних вимог безпеки, вимог гарантій безпеки та їхнє обґрунтування. За допомогою профілю захисту споживачі формують свої вимоги до розробників ІТ-продуктів.

Профіль захисту має такий зміст.

1) Вступ. Це розділ профілю захисту, який містить всю інформацію для пошуку профілю захисту в бібліотеці профілів. Вступ складається з:

1.1) ідентифікатора профілю захисту, що являє собою унікальне ім'я для його пошуку серед подібних йому профілів і позначення посилань на нього;

1.2) огляду змісту профілю захисту, що містить коротку анотацію профілю захисту, на основі якої споживач може зробити висновок про придатність даного профілю захисту.

2) Опис ІТ-продукту. Це розділ профілю захисту, який містить коротку характеристику ІТ-продукту, призначення, принцип роботи, методи використання тощо. Ця інформація не підлягає кваліфікаційному аналізу та сертифікації, але подається розробникам й експертам для пояснення вимог безпеки та визначення їхньої відповідності до завдань, що вирішуються за допомогою ІТ-продукту.

3) Середовище експлуатації. Це розділ профілю захисту, який містить опис усіх аспектів функціонування ІТ-продукту, пов'язаних із безпекою. у середовищі експлуатації описуються:

3.1) умови експлуатації. Опис умов експлуатації ІТ-продукту повинен містити вичерпну характеристику середовища його експлуатації з точки зору безпеки, зокрема обмеження на умови його застосування;

3.2) загрози безпеці. Опис загроз безпеці, що діють у середовищі експлуатації, яким повинен протистояти захист ІТ-продукту. Для кожної загрози має бути вказане її джерело, метод і об'єкт впливу;

3.3) політика безпеки. Опис політики безпеки повинен визначати та за необхідності пояснювати правила політики безпеки, яка повинна бути реалізована в ІТ-продукті.

4) Завдання захисту. Це розділ профілю захисту, що відображає потреби користувачів у протидії потенційним загрозам безпеці та (або) реалізації політики безпеки. До складу завдань захисту входять:

4.1) завдання захисту ІТ-продукту, які повинні визначати та регламентувати потреби у протидії потенційним загрозам безпеці та/або у реалізації політики безпеки;

4.2) інші завдання захисту, які повинні регламентувати потреби у протидії потенційним загрозам безпеці та/або у реалізації політики безпеки інших компонентів ІТС, що не відносяться до сфери інформаційних технологій.

5) Вимоги безпеки. Це розділ профілю захисту, що містить вимоги, яким повинен задовольняти ІТ-продукт для вирішення завдань захисту (типових, спеціальних тощо). У розділі подаються:

5.1) функціональні вимоги безпеки. Функціональні вимоги мають містити типові вимоги, передбачені відповідними розділами «Загальних критеріїв». Необхідно забезпечити такий рівень деталізації вимог, який дозволяє продемонструвати їх відповідність до завдань захисту. Функціональні вимоги можуть дозволяти або забороняти використання конкретних методів і засобів захисту;

5.2) вимоги гарантій безпеки. Вимоги гарантій містять посилання на типові вимоги рівнів гарантій, проте допускають і визначення додаткових вимог гарантій (див. розд. 5.3 цього навчального посібника);

5.3) вимоги до середовища експлуатації. Вимоги до середовища експлуатації є необов'язковими та можуть містити функціональні вимоги та вимоги гарантій, яким повинні задовольняти компоненти інформаційних технологій, що складають середовище експлуатації ІТ-продукту. На відміну від попередніх розділів, використання типових вимог «Загальних критеріїв» є бажаними, але не обов'язковими.

6) Додаткові відомості. Це необов'язковий розділ профілю захисту, що містить будь-яку додаткову інформацію, корисну для проектування, розроблення, кваліфікаційного аналізу та сертифікації ІТ-продукту.

7) Обґрунтування. Це розділ профілю захисту, який повинен демонструвати, що профіль захисту містить повну й пов'язану множину вимог і що ІТ-продукт, який задовольняє їм, буде протистояти загрозам безпеці середовища експлуатації. Розділ складається з:

7.1) обґрунтування завдань захисту. Обґрунтування завдань захисту повинно демонструвати, що завдання, які пропонуються у профілі, відповідають параметрам середовища експлуатації, а їх вирішення дозволить ефективно протистояти загрозам безпеці та реалізувати політику безпеки;

7.2) обґрунтування вимог безпеки. Обґрунтування вимог безпеки показує, що вимоги безпеки дозволяють ефективно вирішувати завдання захисту, оскільки:

- сукупність цілей окремих функціональних вимог безпеки відповідає встановленим завданням захисту;
- вимоги безпеки є пов'язаними, тобто не суперечать, а взаємно підсилюються, також вибір вимог є виправданим (особливо це відноситься до додаткових вимог);
- обраний набір функціональних вимог і рівень гарантій відповідають завданням захисту.

Профіль захисту є керівництвом для виробника та розробника ІТ-продукту, які повинні на основі його та технічних рекомендацій, що запропоновані ним, розробити проект захисту, який є керівництвом для кваліфікаційного аналізу та сертифікації ІТ-продукту.

Проект захисту

Проект захисту – це нормативний документ, який включає вимоги та завдання захисту ІТ-продукту, а також описує рівень функціональних можливостей, реалізованих у ньому засобів захисту, їх обґрунтування та підтвердження ступеня їхніх гарантій. Проект захисту, з одного боку, є відправного точкою для розробника системи, а з іншого, являє собою еталон системи у ході кваліфікаційного аналізу.

Проект захисту містить вступ, опис ІТ-продукту, середовище експлуатації, завдання захисту, вимоги безпеки, загальні специфікації ІТ-продукту, заявку на відповідність профілю захисту, обґрунтування.

Багато розділів проекту захисту збігаються з однойменними розділами профілю захисту.

1) Вступ – це розділ проекту захисту, який містить інформацію, необхідну для ідентифікації проекту захисту, визначення призначення, а також огляд його змісту та заявку на відповідність вимогам «Загальних критеріїв»:

1.1) ідентифікатор проекту захисту – унікальне ім'я проекту захисту для його пошуку й ідентифікації, а також відповідного ІТ-продукту;

1.2) огляд змісту проекту захисту – достатньо докладна анотація проекту захисту, що дозволяє споживачам визначати придатність ІТ-продукту для вирішення завдань;

1.3) заявка на відповідність «Загальним критеріям» – це опис усіх властивостей ІТ-продукту, що підлягають кваліфікаційному аналізу на основі «Загальних критеріїв».

2) Опис ІТ-продукту – це розділ проекту захисту, який містить коротку характеристику ІТ-продукту, призначення, принцип роботи, методи використання тощо. Ця інформація не підлягає кваліфікаційному аналізові та сертифікації, але подається розробникам і експертам для пояснення вимог безпеки та визначення їхньої відповідності завданням, то вирішуються за допомогою ІТ-продукту.

3) Середовище експлуатації – це розділ проекту захисту, що містить опис усіх аспектів функціонування ІТ-продукту, пов'язаних із безпекою. У середовищі експлуатації описуються:

3.1) умови експлуатації. Опис умов експлуатації ІТ-продукту повинен містити вичерпну характеристику середовища його експлуатації з точки зору безпеки, у тому числі обмеження на умови його застосування;

3.2) загрози безпеці. Опис загроз безпеці, що діють у середовищі експлуатації, яким повинен протистояти захист ІТ-продукту. Для кожної загрози повинно бути вказане її джерело, метод і об'єкт впливу;

3.3) політика безпеки. Опис політики безпеки повинен визначати та за необхідності пояснювати правила політики безпеки, яка повинна бути реалізована в ІТ-продукті.

4) Завдання захисту – це розділ проекту захисту, що відображає потреби користувачів у протидії потенційним загрозам безпеці та/або реалізації політики безпеки. До складу задач захисту входять:

4.1) завдання захисту ІТ-продукту. Завдання захисту ІТ-цродукту повинні визначати та регламентувати потреби у протидії потенційним загрозам безпеці та/або у реалізації політики безпеки;

4.2) інші завдання захисту. Інші завдання захисту повинні регламентувати потреби у протидії потенційним загрозам безпеці та/або у реалізації політики безпеки інших компонентів ІТС, що не відносяться до сфери інформаційних технологій.

5) Вимоги безпеки – це розділ проекту захисту, що містить вимоги безпеки до ІТ-продукту, якими керувався виробник у ході його розроблення. Цей розділ дещо відрізняється від аналогічного розділу профілю захисту та має зміст:

5.1) розділ функціональних вимог безпеки до ІТ-продукту на відміну від відповідного розділу профілю захисту допускає використання, крім типових вимог й інших, специфічних для даного продукту та середовища його експлуатації. При описі таких спеціальних вимог необхідно зберігати стиль «Загальних критеріїв» і забезпечувати властивий їм ступінь деталізації;

5.2) розділ вимог гарантій безпеки може включати рівні гарантій, не передбачені у «Загальних критеріях». У даному випадку опис рівня гарантій повинен бути чітким, несуперечним і мати ступінь деталізації, що допускає його використання у ході кваліфікаційного аналізу. При цьому бажано використати стиль і деталізації опису рівнів гарантій, прийняті у «Загальних критеріях»;

5.3) вимоги до середовища експлуатації є необов'язковими та можуть містити функціональні вимоги та вимоги гарантій, яким повинні задовольняти компоненти інформаційних технологій, що складають середовище експлуатації ІТ-продукту.

6) Загальні, специфікації ІТ-продукту – це розділ проекту захисту, який описує механізми реалізації завдань захисту за допомогою визначення багаторівневих специфікацій засобів захисту у відповідності з

функціональними вимогами безпеки та вимогами гарантій безпеки, що пред'являються. Загальні специфікації складаються зі:

6.1) специфікацій функцій захисту;

6.2) специфікацій рівня гарантій.

7) Заявка на відповідність профілю захисту – це необов'язковий розділ проекту захисту, який містить матеріали, необхідні для підтвердження заявки. Для кожного профілю захисту, на реалізацію якого претендує проект захисту, цей розділ повинен містити:

7.1) посилання на профіль захисту, яке однозначно ідентифікує профіль захисту, на реалізацію якого претендує проект захисту, із зазначенням випадків, у яких рівень захисту, що забезпечується, перевершує вимоги профілю з коректною реалізацією усіх його вимог без виключення;

7.2) відповідність профілю захисту, що визначає можливості ІТ-продукту, які реалізують завдання захисту та вимоги профілю захисту;

7.3) удосконалення профілю захисту, що відображає можливості ІТ-продукту, які виходять за рамки завдань захисту та вимог, установлених у профілі захисту.

8) Обґрунтування – це розділ проекту захисту, який повинен показувати, що проект захисту містить повну та зв'язну множину вимог, що ІТ-продукт, який реалізує їх, буде ефективно протистояти загрозам безпеці. Крім того, обґрунтування містить підтвердження заявленої відповідності профілю захисту. Розділ деталізується так.

Обґрунтування завдань захисту повинно демонструвати, що завдання захисту, заявлені у проекті захисту, відповідають властивостям середовища експлуатації, тобто їх вирішення дозволить ефективно протидіяти загрозам безпеці та реалізувати обрану для них політику безпеки.

Обґрунтування вимог безпеки показує, що виконання цих вимог дозволяє вирішити завдання захисту, тому що:

- сукупність функціональних вимог безпеки та вимог гарантій безпеки, а також умов експлуатації ІТ-продукту відповідають завданням захисту;
- усі вимоги безпеки є несуперечними та взаємно підсилюють одна одну;
- вибір вимог є оправданим;
- рівень функціональних можливостей засобів захисту відповідає завданням захисту.

Обґрунтування загальних специфікацій ІТ-продукту повинно демонструвати, що засоби захисту та методи забезпечення їхніх гарантій відповідають вимогам, що пред'являються, оскільки:

- сукупність засобів захисту задовольняє функціональним вимогам;
- необхідний рівень безпеки та надійності захисту забезпечується засобами, що запропоновані;
- заходи, спрямовані на забезпечення гарантій реалізації функціональних вимог, відповідають вимогам гарантій.

Обґрунтування відповідності профілю захисту показує, що вимоги проекту захисту підтримують всі вимоги профілю захисту. Для цього повинно бути показано, що:

- усі удосконалення завдань захисту порівняно зі профілем захисту реалізовані коректно у напряму їхнього розвитку та конкретизації;

- усі удосконалення вимог безпеки порівняно зі профілем захисту реалізовані коректно у напряму їхнього розвитку та конкретизації;

- усі завдання захисту профілю захисту успішно реалізовані й усі вимоги профілю захисту задоволені;

- ніякі додатково введені у проект захисту спеціальні завдання захисту та вимоги безпеки не суперечать профілю захисту.

Функціональні вимоги до засобів захисту

Функціональні вимоги безпеки регламентують функціонування компонентів ІТ-продукту, що забезпечують безпеку, та визначають можливості засобів захисту. Функціональні вимоги згруповано на основі ролей, які вони виконують, або цілей безпеки, які вони обслуговують. Всього є 11 функціональних класів, поділених на три групи, 66 сімейств, 135 компонентів.

1. Перша група визначає елементарні послуги безпеки:

- FAU – аудит, вимоги до послуг, протоколювання;

- FIA – ідентифікація й автентифікація;

- FRU – контроль використання ресурсів для забезпечення відмовостійкості.

2. Друга група класів описує похідні послуги, що реалізовані на базі елементарних:

- FCO – безпека причетності до передавання/приймання;

- FPR – приватність (захист персональних даних або конфіденційність роботи у системі);

- FDP – захист даних користувача;

- FPT – захист функцій безпеки об’єкта захисту.

3. Третя група класів пов’язана з інфраструктурою об’єкта оцінки:

- FCS – підтримка криптографії, керування ключами та криптоопераціями;

- FMT – менеджмент безпеки;

- FTA – контроль доступу до системи, керування сеансами роботи користувача;

- FTP – довірений маршрут/канал.

Прикладом поділу на сімейства може бути клас FAU. Він включає у себе шість сімейств:

- FAU_GEN – генерація даних аудиту безпеки (реєстрація й облік подій);

- FAU_SEL – відбір подій для реєстрації й обліку;

- FAU_STG – протокол аудиту;

- FAU_SAR – доступ до протоколу аудиту;

- FAU_SAA – аналіз протоколу аудиту;

- FAU_ARP – автоматичне реагування на спроби порушення безпеки.

Прикладом компонента візьмемо сімейство FAU. Призначення двох компонент цього сімейства наступне:

- FAU_GEN1 - генерація даних аудита;

- FAU_GEN2 – асоціація ідентифікатора користувача.

Вивчення функціональних класів безпеки, сімейств і компонентів безпеки рекомендується самостійно за текстами самих стандартів [5 - 7] або [27 - 39].

Зауважимо, що значного рівня ІТ-безпеки можна досягти за допомогою, чи підтримуючи адміністративні заходи, наприклад, управління організаційними, персональними, фізичними та процедурними факторами, які реалізуються поза ІТ-системою. Тому міжнародний стандарт ISO/IEC 15408 не підтримує ці та низку наступних заходів:

- не охоплено оцінювання техніко-фізичних аспектів ІТ-безпеки, зокрема електромагнітне випромінювання та наведення;
- не описує методологію оцінювання відповідності, у рамках якої необхідно застосувати критерії;
- не описує правові рамки задіювання критеріїв органами оцінювання відповідності. Ці рамки визначаються національним законодавством;
- не охоплює оцінювання критеріїв властивостей криптографічних алгоритмів.

На закінчення цього розділу розглянемо методологію оцінювання функціональних послуг безпеки, що прийнята у вітчизняній нормативній базі.

1.6 Методологія оцінювання функціональних послуг безпеки у засобах захисту інформації від несанкціонованого доступу

Методологія оцінювання функціональних послуг безпеки описується у НД ТЗІ 2.7-009-99. Якщо в інформаційно-телекомунікаційній системі (ІТС) планується оброблення інформації, порядок захисту якої регламентується законами України або іншими нормативно-правовими актами (інформації, що є власністю держави або становить державну таємницю), обов'язковим є незалежне підтвердження (оцінювання) відповідності реалізованих засобів і заходів захисту встановленим вимогам і нормам. Результатом проведеного оцінювання має бути відповідний висновок, на підставі якого власники ІТС і оброблюваних у них інформаційних ресурсів можуть приймати рішення щодо прийнятності та достатності вжитих заходів і реалізованих засобів.

Вироблена наступна термінологія.

Критерії оцінки – це сукупність вимог (шкала оцінки), яка використовується для оцінювання ефективності функцій захисту інформації та коректності їх реалізації. В Україні як критерії оцінки використовуються критерії, встановлені НД ТЗІ 2.5-004-99, а також вимоги діючих НД ТЗІ щодо забезпечення захисту інформації в ІТС різного призначення. Вони надають:

- порівняльну шкалу для оцінювання ефективності функцій і механізмів захисту інформації від несанкціонованого доступу (НСД), реалізованих в ІТС, а також коректності їх реалізації. Згідно вимог НД ТЗІ 2.5-004-99, окремо оцінюються реалізовані функції захисту (функціональні послуги безпеки) та рівень гарантій коректності їх реалізації (рівень гарантій);
- базу (орієнтири) для розроблення засобів захисту інформації, оброблюваної в ІТС, від НСД.

Система оцінювання – це адміністративно-правова структура, у рамках якої у певному співтоваристві органи, що здійснюють оцінювання, застосовують критерії оцінки. Система оцінювання в Україні функціонує на основі

«Положення про державну експертизу у сфері технічного захисту інформації». Згідно вимог цього документа, оцінювання відповідності реалізованих засобів і заходів захисту встановленим вимогам і нормам здійснюється шляхом проведення експертизи.

Методологія оцінювання визначає послідовність (алгоритм) дій, що виконуються експертами при оцінюванні ефективності функцій захисту інформації та коректності їх реалізації, а також форму подання результатів.

Загальні положення

Суб'єктами експертизи є:

- юридичні та фізичні особи, що є замовниками експертизи;
- Державна служби спеціального зв'язку та захисту інформації України, а також підприємства, установи й організації, які проводять експертизу за її дорученням (організатори експертизи);
- фізичні особи – виконавці експертних робіт із ТЗІ (експерти).

Об'єктами експертизи (ОЕ) у частині, що стосується оцінювання функціональних послуг безпеки, можуть бути комплекси засобів захисту (КЗЗ) комплексних систем захисту інформації (КСЗІ), засоби технічного захисту інформації від НСД, а також захищені від НСД компоненти обчислювальної системи.

Методологія оцінювання функцій захисту (функціональних послуг безпеки) передбачає виконання таких етапів робіт:

- попередній аналіз оцінюваного ОЕ;
- розроблення програми випробувань функціональних послуг безпеки;
- розроблення методики випробувань функціональних послуг безпеки;
- проведення випробувань;
- аналіз, документування та затвердження результатів випробувань.

Попередній аналіз об'єкта експертизи

Головною метою етапу попереднього аналізу є прийняття рішення щодо можливості проведення робіт із експертизи ОЕ, визначення обсягів і плану робіт. Послідовність і обсяг робіт експерта на цьому етапі залежать від варіанта подання ОЕ на експертизу. Об'єкт експертизи у вигляді КЗЗ КСЗІ, або ЗТЗІ від НСД, або захищеного компонента обчислювальної системи може бути подано на експертизу розробником у таких варіантах:

- розробником разом із проектною й експлуатаційною документацією, при цьому в проектній документації розробником визначено функціональні специфікації об'єкта експертизи (перелік реалізованих в об'єкті експертизи функціональних послуг безпеки згідно НД ТЗІ 2.5-004-99 і опис їхньої політики);
- розробником, який володіє інформацією щодо особливостей реалізації в об'єкті експертизи функцій захисту, разом із експлуатаційною документацією, при цьому розробником не визначено функціональні специфікації об'єкта;
- представником розробника (заявником), який не володіє інформацією щодо особливостей реалізації в об'єкті експертизи функцій захисту, разом із експлуатаційною документацією, при цьому розробником не визначено функціональні специфікації об'єкта експертизи.

Етап проведення попереднього аналізу оцінюваного об’єкта експертизи передбачає виконання таких дій:

1) дослідження оцінюваного об’єкта експертизи з метою перевірки його готовності до виконання робіт із експертизи;

2) визначення (ідентифікація) або уточнення множини випробовуваних функціональних послуг безпеки, їх рівнів і політики;

3) документування отриманих результатів і прийняття рішення щодо проведення подальших етапів робіт.

У процесі дослідження оцінюваного ОЕ експертом має бути сформовано чітке уявлення про:

- інформаційну модель процесів оброблення інформації в об’єкті експертизи;
- оброблювані інформаційні ресурси та можливі загрози цим ресурсам;
- функціональні вимоги до оцінюваного об’єкта експертизи, у тому числі ті, що стосуються забезпечення захисту інформації від можливих загроз;
- засоби керування оцінюваним об’єктом експертизи.

При цьому необхідна інформація може бути отримана шляхом ознайомлення з наданою документацією, або анкетуванням розробників оцінюваного об’єкта експертизи, або дослідженням експертами об’єкта.

На основі результатів дослідження об’єкта експертизи, у випадку, якщо отримані результати підтверджують його готовність до проведення подальших робіт, має бути здійснено визначення або уточнення множини випробовуваних функціональних послуг безпеки, їхніх рівнів і політики.

При цьому, за наявності у проектній або експлуатаційній документації чітко визначених функціональних специфікацій об’єкта експертизи, таке уточнення можна здійснювати шляхом аналізу відповідності формальних вимог до функціональних послуг безпеки (функцій захисту) й опису порядку реалізації відповідних функцій, наведеного у проектній документації, а також результатів анкетування розробників із використанням переліку спеціальних запитань.

За відсутності у проектній документації чітко визначених функціональних специфікацій об’єкта експертизи таке уточнення можна здійснювати шляхом проведення експертами досліджень об’єкта експертизи, метою яких є виявлення наявності механізмів захисту та реалізованих ними функціональних послуг безпеки, оцінювання можливості запобігання ними певним загрозам інформації з подальшим уточненням політики функціональних послуг безпеки з використанням переліку спеціальних запитань. Методичні рекомендації щодо здійснення ідентифікації функціональних послуг безпеки, уточнення їх рівнів і політики викладено у розд. 4.3 – 4.6 цього навчального посібника.

Результатом етапу попереднього аналізу має бути звіт, в якому експерти, що здійснювали аналіз, повинні викласти свою думку з приводу повноти та вмісту наданих матеріалів, обґрунтувати рішення щодо можливості та доцільності проведення подальших робіт із експертизи, а у випадку позитивного рішення – навести пропозиції щодо плану та послідовності проведення подальших робіт.

Крім цього, у випадку позитивного рішення щодо проведення подальших робіт, результатом цього етапу має також бути узгоджений із розробником або

заявником документ, що містить уточнений опис переліку та політики функціональних послуг безпеки, на відповідність яким здійснюватиметься перевірка, наприклад, у вигляді технічних вимог до оцінюваного об'єкта експертизи у частині реалізації функціональних послуг безпеки й опису порядку реалізації цих вимог. Цей документ, у випадку успішного завершення експертизи, має бути поданий як невід'ємний додаток до експертного висновку щодо відповідності оцінюваного об'єкта експертизи вимогам НД ТЗІ.

Проведення попереднього аналізу оцінюваного об'єкта експертизи у випадку подання розробником на експертизу об'єкта експертизи з визначеними у проектній документації функціональними специфікаціями. У цьому випадку подання розробником на експертизу об'єкта експертизи з визначеними у проектній документації функціональними специфікаціями експерт на етапі попереднього аналізу повинен використовувати оцінюваний об'єкт експертизи у працездатному стані та проектну документацію (наприклад, матеріали передпроектних досліджень, технічне завдання, технічні вимоги, матеріали ескізного, технічного та робочого проектів тощо), яка, зокрема, містить функціональні специфікації об'єкта експертизи у вигляді переліку реалізованих функціональних послуг безпеки згідно НД ТЗІ 2.5-004-99 і опису їх політики. Крім того, необхідно використовувати експлуатаційну документацію на оцінюваний об'єкт експертизи (наприклад, опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову адміністратора; настанову користувача тощо).

При цьому послідовність (алгоритм) дій експерта на етапі попереднього аналізу має бути такою:

Крок 1.1 – початок етапу аналізу наданого розробником об'єкта експертизи з визначеними функціональними специфікаціями.

Крок 1.2 – перевірка факту надання експлуатаційної документації на об'єкт експертизи (опису засобу або системи; опису процедур інсталяції, генерації та запуску; настанови адміністратора; настанови користувача тощо) та наявності в ній відомостей, необхідних для виконання подальших робіт із оцінювання працездатності об'єкта експертизи. У випадку відсутності документації, подальші роботи мають припинятися (перехід на крок 1.15, інакше на крок 1.3).

Крок 1.3 – оцінювання працездатності поданого об'єкта експертизи (з використанням отриманої експлуатаційної документації) та визначення його придатності для виконання подальших робіт. У випадку виявлення непрацездатності об'єкта експертизи, подальші роботи мають припинятися (перехід на крок 1.15, інакше на крок 1.4).

Крок 1.4 – перевірка наявності проектної документації на об'єкт експертизи (матеріалів передпроектних досліджень, технічного завдання, технічних вимог, матеріалів ескізного, технічного та робочого проектів тощо) та наявності в ній функціональних специфікацій об'єкта експертизи у вигляді переліку реалізованих функціональних послуг безпеки згідно НД ТЗІ 2.5-004-99 і опису їх політики. У випадку відсутності документації або відсутності в ній функціональних специфікацій об'єкта експертизи має розглядатися як такий, що наданий розробником без визначеної функціональної специфікації (перехід

до початку іншого алгоритму, крок 2.1, інакше на крок 1.5).

Крок 1.5 – перевірка наявності у наведеній функціональній специфікації об'єкта експертизи послуги безпеки «Цілісність КЗЗ» рівня НЦ-1 або вище. У випадку, якщо така функціональна послуга безпеки відсутня у функціональній специфікації об'єкта експертизи, подальші роботи мають припинятися (перехід на крок 1.15, інакше на крок 1.6).

Крок 1.6 – перевірка наявності у наведеній функціональній специфікації об'єкта експертизи функціональних послуг безпеки певного рівня, наявність яких, згідно вимог НД ТЗІ 2.5-004-99, є необхідною умовою для реалізації інших послуг. Якщо такі функціональні послуги є, то перехід на крок 1.8, інакше, перехід на крок 1.7.

Крок 1.7 – вилучення із заявленого переліку функціональних послуг тих, необхідні умови реалізації яких відсутні.

Крок 1.8 – прийняття (після консультацій із розробником) рішення про прийнятність уточненого переліку реалізованих функціональних послуг безпеки та продовження робіт.

Крок 1.9 – уточнення, із залученням розробника, фактів реалізації та політики всіх функціональних послуг безпеки, що містяться в їх уточненому переліку.

Крок 1.10 – перевірка наявності в уточненому переліку реалізованих в об'єкті експертизи функціональних послуг безпеки послуги «Цілісність КЗЗ» рівня НЦ-1 або вище. У випадку, якщо така функціональна послуга безпеки відсутня в уточненому переліку, подальші роботи мають припинятися (перехід на крок 1.15, інакше на крок 1.11).

Крок 1.11 – перевірка наявності в уточненому переліку реалізованих в об'єкті експертизи функціональних послуг безпеки послуг певного рівня, наявність яких, згідно вимог НД ТЗІ 2.5-004-99, є необхідною умовою для реалізації інших послуг. Якщо такі функціональні послуги є, то перехід на крок 1.13, інакше, перехід на крок 1.12.

Крок 1.12 – вилучення з уточненого переліку функціональних послуг тих, необхідні умови реалізації яких відсутні.

Крок 1.13 – прийняття (після консультацій із розробником) рішення про прийнятність уточненого переліку реалізованих функціональних послуг безпеки, наявність яких має бути підтверджено у процесі експертизи, та про продовження робіт.

Крок 1.14 - розроблення (із залученням розробника) й узгодження з розробником документа, який містить уточнений опис переліку та політики функціональних послуг безпеки, на відповідність яким здійснюватиметься перевірка об'єкта експертизи, наприклад, у вигляді технічних вимог до оцінюваного об'єкта експертизи у частині реалізації функціональних послуг безпеки й опису порядку реалізації цих вимог.

Крок 1.15 – кінець алгоритму.

Проведення попереднього аналізу оцінюваного об'єкта експертизи у випадку подання розробником на експертизу об'єкта експертизи без визначених функціональних специфікацій. У цьому випадку експерт на етапі

попереднього аналізу повинен використовувати оцінюваний об’єкт експертизи у працездатному стані й експлуатаційну документацію на оцінюваний об’єкт (наприклад, опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову адміністратора; настанову користувача тощо).

При цьому послідовність (алгоритм) дій експерта на етапі попереднього аналізу має бути такою:

Крок 2.1 – початок етапу аналізу наданого розробником об’єкта експертизи без визначених функціональних специфікацій.

Крок 2.2 - перевірка факту надання експлуатаційної документації на об’єкт експертизи (опису засобу або системи; опису процедур інсталяції, генерації та запуску; настанови адміністратора; настанови користувача тощо) та наявності в ній відомостей, необхідних для виконання подальших робіт із оцінювання працездатності об’єкта експертизи. У випадку відсутності документації, подальші роботи мають припинятися (перехід на крок 2.9, інакше на крок 2.3).

Крок 2.3 - оцінювання працездатності поданого об’єкта експертизи (з використанням отриманої експлуатаційної документації) та визначення його придатності для виконання подальших робіт. У випадку виявлення непрацездатності об’єкта експертизи, подальші роботи мають припинятися (перехід на крок 2.9, інакше на крок 2.4).

Крок 2.4 - проведення, із залученням розробника, ідентифікації фактів реалізації й уточнення політики функціональних послуг безпеки.

Крок 2.5 - перевірка наявності у складеному переліку реалізованих в об’єкті експертизи функціональних послуг безпеки послуги «Цілісність КЗЗ» рівня НЦ-1 або вище. У випадку, якщо така функціональна послуга безпеки відсутня у складеному переліку, подальші роботи мають припинятися (перехід на крок 2.9, інакше на крок 2.6.

Крок 2.6 - перевірка наявності у складеному переліку реалізованих в об’єкті експертизи функціональних послуг безпеки послуг певного рівня, наявність яких, згідно вимог НД ТЗІ 2.5-004-99, є необхідною умовою для реалізації інших послуг. У випадку, якщо таких послуг нема, то перехід на крок 2.7, інакше на крок 2.8.

Крок 2.7 - з вилученням із переліку функціональних послуг тих, необхідні умови реалізації яких відсутні.

Крок 2.8 - прийняття (після консультацій із розробником) рішення про прийнятність уточненого переліку реалізованих функціональних послуг безпеки, наявність яких має бути підтверджено у процесі експертизи, та про продовження робіт. Якщо перелік послуг не прийнято, то припинення робіт, перехід на крок 2.10, інакше перехід на крок 2.9.

Крок 2.9 - розроблення (із залученням розробника) й узгодження з розробником документа, який містить уточнений опис переліку та політики функціональних послуг безпеки, на відповідність яким здійснюватиметься перевірка об’єкта експертизи, наприклад, у вигляді уточнених технічних вимог до оцінюваного об’єкта експертизи у частині реалізації функціональних послуг безпеки й опису порядку реалізації цих вимог.

Крок 2.9 – кінець алгоритму.

Проведення попереднього аналізу об'єкта експертизи у випадку подання на експертизу представником розробника (заявником) об'єкта експертизи без визначених функціональних специфікацій. У цьому випадку, експерт на етапі попереднього аналізу має використовувати об'єкт експертизи у працездатному стані, наданий для аналізу й експлуатаційну документацію на оцінюваний об'єкт експертизи (наприклад, опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову адміністратора; настанову користувача тощо).

Послідовність (алгоритм) дій експерта на етапі попереднього аналізу має складатись із таких кроків:

Крок 3.1 – початок етапу попереднього аналізу наданого представником розробника (заявника) об'єкта експертизи без визначених функціональних специфікацій.

Крок 3.2 – перевірка факту надання експлуатаційної документації на ОЕ (опису засобу або системи; опису процедур інсталяції, генерації та запуску; настанови адміністратора; настанови користувача тощо) та наявності в ній відомостей, необхідних для виконання подальших робіт із оцінювання працездатності об'єкта експертизи. У випадку відсутності документації, подальші роботи мають припинятися (перехід на крок 3.10, інакше на крок 3.3).

Крок 3.3 – оцінювання працездатності наданого об'єкта експертизи (з використанням отриманої експлуатаційної документації) та визначення його придатності для виконання подальших робіт. У випадку виявлення непрацездатності об'єкта експертизи, подальші роботи мають припинятися (перехід на крок 3.10, інакше на крок 3.4).

Крок 3.4 – виконання власними силами дослідження об'єкта експертизи з метою ідентифікації фактів реалізації й уточнення політики функціональних послуг безпеки.

Крок 3.5 – перевірка наявності у складеному переліку реалізованих в об'єкті експертизи функціональних послуг безпеки послуги «Цілісність КЗЗ» рівня НЦ-1 або вище. У випадку, якщо така функціональна послуга безпеки відсутня у складеному переліку, подальші роботи мають припинятися (перехід на крок 3.10, інакше на крок 3.6).

Крок 3.6 – перевірка наявності у складеному переліку реалізованих в об'єкті експертизи функціональних послуг безпеки послуг певного рівня, наявність яких, згідно вимог НД ТЗІ 2.5-004-99, є необхідною умовою для реалізації інших послуг. Якщо зазначені вимоги відсутні, то перехід на крок 3.7, інакше перехід на крок 3.8.

Крок 3.7 – вилучення з переліку функціональних послуг тих, необхідні умови реалізації яких відсутні.

Крок 3.8 – прийняття (після консультацій із заявником) рішення про прийнятність уточненого переліку реалізованих функціональних послуг безпеки, наявність яких має бути підтверджено у процесі експертизи, та про продовження робіт. Якщо перелік функціональних послуг не підтверджено, то припинення робіт і перехід на крок 3.10, інакше перехід на крок 3.9.

Крок 3.9 – розроблення й узгодження із заявником документа, який містить уточнений опис переліку та політики функціональних послуг безпеки, на відповідність яким здійснюватиметься перевірка об’єкта експертизи, наприклад, у вигляді технічних вимог до оцінюваного об’єкта експертизи у частині реалізації функціональних послуг безпеки й опису порядку реалізації цих вимог.

Крок 3.10 – завершення етапу.

Розроблення програми випробувань функціональних послуг безпеки

Головною метою етапу розроблення програми проведення випробування функціональних послуг безпеки є розроблення та узгодження цієї програми. Експертом мають бути використані такі матеріали у залежності від варіанта подання об’єкта експертизи на експертизу:

- проектна документація (за наявності) на об’єкт експертизи (наприклад, матеріали передпроектних досліджень, технічне завдання, технічні вимоги, матеріали ескізного, технічного та робочого проектів тощо), яка, зокрема, містить функціональні специфікації об’єкта у вигляді переліку реалізованих у ньому функціональних послуг безпеки згідно НД ТЗІ 2.5-004-99 і опису їх політики;
- документація (за наявності), що містить результати проведених розробником випробувань об’єкта експертизи (програма випробувань, методика випробувань, протоколи випробувань тощо);
- підготовлений на етапі попереднього аналізу документ, який містить уточнений опис переліку та політики функціональних послуг безпеки, наприклад, у вигляді уточнених технічних вимог до об’єкта експертизи, на відповідність яким має здійснюватися перевірка цього об’єкта.

Основний зміст програми випробувань, яка розробляється на цьому етапі, становить опис того, які властивості оцінюваного об’єкта експертизи мають бути перевірені під час проведення випробувань із метою підтвердження або спростування реалізації в об’єкті експертизи уточненого на етапі попереднього аналізу переліку функціональних послуг безпеки. При цьому можуть бути враховані такі фактори:

- результати випробувань, надані розробником об’єкта експертизи. Мають бути враховані: аргументи розробника про достатність тестового покриття для тестування певних функціональних послуг безпеки; повнота та коректність проведених розробником випробувань функціональних послуг безпеки;
- відомі вразливості, характерні для того типу систем, до яких відноситься оцінюваний об’єкт експертизи, у тому числі наведені у матеріалах передпроектних досліджень;
- важливість різних функціональних послуг безпеки, реалізованих в оцінюваному ОЕ, з погляду запобігання можливим загрозам інформації;
- складність (комплексність) засобів реалізації функціональних послуг безпеки в оцінюваному об’єкті експертизи;
- можливість неявної перевірки окремих функціональних послуг безпеки;
- наявність в оцінюваному об’єкті експертизи нових або нерегламентованих НД ТЗІ функцій захисту.

Розроблена програма випробувань функціональних послуг безпеки має бути узгоджена з Держкомзв'язку.

Розроблення методики випробувань функціональних послуг безпеки

Головною метою цього етапу є розроблення та узгодження методики випробувань функціональних послуг безпеки. У процесі підготовки методики випробувань мають бути виконані дії з вибору тестових процедур, методів випробувань і перевірок, розроблення або вибору програмних та/або апаратних засобів випробувань. Експерт має використовувати такі матеріали, залежно від варіанта подання на експертизу об'єкта експертизи:

- проектну документацію (за наявності) на об'єкт експертизи (наприклад, матеріали передпроектних досліджень, технічне завдання, технічні вимоги, матеріали ескізного, технічного та робочого проектів тощо), яка, зокрема, містить функціональні специфікації об'єкта у вигляді переліку реалізованих у ньому функціональних послуг безпеки згідно НД ТЗІ 2.5-004-99 і опису їхньої політики;
- документацію (за наявності), що містить результати проведених розробником випробувань об'єкт експертизи (програму випробувань, методику випробувань, протоколи випробувань тощо);
- підготовлений на етапі попереднього аналізу документ, який містить уточнений опис переліку та політики функціональних послуг безпеки, наприклад, у вигляді уточнених технічних вимог до об'єкта експертизи, на відповідність яким має здійснюватися перевірка об'єкта;
- підготовлену на попередньому етапі програму випробувань функціональних послуг безпеки.

У процесі розроблення методики випробувань, яка описує порядок і засоби проведення випробувань кожної функціональної послуги безпеки, зазначеної у програмі випробувань, експерт має, з урахуванням уточнених вимог до функціональних послуг безпеки, визначених на попередніх етапах, обрати найбільш прийнятний спосіб перевірки кожної послуги.

Під час розроблення методики випробувань мають бути враховані такі основні вимоги щодо загального підходу (стратегії) проведення випробувань:

- забезпечення достатності тестового покриття для перевірки кожної заявленої функціональної послуги безпеки з урахуванням її політики й особливостей реалізації;
- зниження кількості взаємозалежних методів випробувань (перевірок) різних функціональних послуг безпеки;
- забезпечення максимальної незалежності від стану оцінюваного ОЕ, тобто наявності засобів генерації всієї необхідної тестової та службової інформації для кожної перевірки;
- забезпечення максимального використання засобів автоматизації при проведенні випробувань, у тому числі для генерації тестової інформації, виконання підготовчих дій і безпосереднього виконання перевірок;
- забезпечення повторюваності процесу та результатів випробувань.

При виборі тестових процедур, методів випробувань і відповідних перевірок, залежно від виду оцінюваного об’єкта експертизи, можуть бути обрані такі підходи:

- підхід із використанням монолітного тестування (метод «чорної скриньки»), який передбачає використання у процесі проведення випробувань лише зовнішніх документованих інтерфейсів об’єкта експертизи, завдяки чому випробування можуть бути здійснені без використання додаткових спеціально розроблюваних засобів;
- підхід із використанням функціонально-синтетичного тестування (метод "білої скриньки"), який передбачає використання у процесі проведення випробувань як зовнішніх документованих інтерфейсів об’єкта, так і внутрішньосистемних інтерфейсів, але потребує спеціально розроблених засобів випробувань, що реалізують внутрішньо системні інтерфейси доступу до функціональних компонентів оцінюваного продукту (системи);
- змішаний підхід (метод "сірої скриньки"), при використанні якого намагаються максимальну кількість перевірок здійснювати з використанням зовнішніх документованих інтерфейсів, а внутрішньосистемні інтерфейси використовувати лише для тих перевірок, які не можна виконати в інший спосіб.

Оскільки, згідно НД ТЗІ, наявність, повнота та ступінь детальності опису внутрішньо системних інтерфейсів залежать від заявленого рівня гарантій коректності реалізації функціональних послуг безпеки, вибір підходу щодо проведення випробувань має здійснюватися з урахуванням цього рівня гарантій.

Розроблена методика випробування функціональних послуг безпеки має бути узгоджена з Держкомзв’язку України.

Проведення випробувань

Головною метою цього етапу є здійснення, згідно із затвердженою методикою, перевірки та фіксації (у відповідному журналі проведення випробувань) фактів реалізації в оцінюваному об’єкті експертизи заявленого й уточненого експертом переліку функціональних послуг безпеки, а також підтвердження їх політики, уточненої експертом на етапі попереднього аналізу. При цьому, якщо у процесі проведення випробувань здійснювалася перевірка будь-яких додаткових властивостей об’єкта (наприклад, продуктивності або стійкості до проникнення), відповідні результати також мають бути зафіксовані.

Аналіз і документування результатів випробувань

На цьому етапі має бути проведено аналіз отриманих у процесі проведення випробувань і зафіксованих відповідним чином результатів. На підставі результатів проведеного аналізу має бути складено протокол випробувань, в якому повинно бути наведено результати, отримані під час проведення випробувань за кожним пунктом методики випробувань, і зроблено висновок щодо відповідності або невідповідності наданого для випробувань об’єкта експертизи висунутим вимогам.

Питання для самоконтролю

1. Наведіть загальний опис моделі безпеки, що покладена в основу міжнародної Рекомендації X.800.
2. Подайте характеристику процедур захисту в архітектурі відкритих мереж.
3. Назвіть базові послуги (функції) захисту, що утворюються процедурами захисту в архітектурі відкритих систем.
4. Які основні механізми та засоби захисту використовуються в архітектурі відкритих систем?
5. Яким чином здійснюється адміністрування засобів захисту в архітектурі відкритих систем?
6. Наведіть загальний опис моделі безпеки, що покладена в основу НД ТЗІ 1.1-002-99.
7. Наведіть основні характеристики суб'єктів і об'єктів моделі безпеки, що покладена в основу НД ТЗІ 1.1-002-99.
8. Охарактеризуйте основні принципи керування доступом моделі безпеки, що покладена в основу НД ТЗІ 1.1-002-99.
9. Надайте стислу характеристику загальної структури функціональних критеріїв оцінки захищеності за НД ТЗІ 2.5-004-99.
10. Охарактеризуйте структуру послуг і вимог розділу «Критерії конфіденційності».
11. Охарактеризуйте структуру послуг і вимог розділу «Критерії цілісності».
12. Охарактеризуйте структуру послуг і вимог розділу «Критерії доступності».
13. Охарактеризуйте структуру послуг і вимог розділу «Критерії спостережності».
14. Поясніть зміст поняття профіль захищеності, наведіть 2 – 3 приклади профілів захищеності за НД ТЗІ 2.5-005-99, поясніть їх.
15. Наведіть і поясніть систему послуг за заданим профілем (наприклад, типовим відповідно до НД ТЗІ 2.5-005-99).
16. Наведіть загальний опис моделі безпеки, що покладена в основу Міжнародного стандарту ISO 15408.
17. Укажіть склад потенційних загроз безпеці та типові завдання захисту відповідно до Міжнародного стандарту ISO 15408.
18. Сформулюйте поняття "політика безпеки" відповідно до Міжнародного стандарту ISO 15408.
19. Охарактеризуйте поняття "продукт інформаційних технологій" відповідно до Міжнародного стандарту ISO 15408.
20. Наведіть структуру й охарактеризуйте зміст нормативного документа «Профіль захисту» відповідно до Міжнародного стандарту ISO 15408.
21. Наведіть структуру й охарактеризуйте зміст нормативного документа "проект захисту" відповідно до Міжнародного стандарту ISO 15408.

Розділ 2
ЕКСПЕРТНІ ОЦІНКИ У ДОСЛІДЖЕННІ СИСТЕМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Експертні оцінки сьогодні є найбільш розповсюдженим засобом отримання й аналізу якісної інформації стосовно рівня інформаційної безпеки системи. Успішне застосування методів експертних оцінок у багатьох випадках залежить від удосконалення математичних методів, за допомогою яких здійснюється аналіз і оброблення експертної інформації.

У тих випадках, коли об'єктивної інформації виявляється недостатньо для виявлення чисельного значення необхідного критерію при прийнятті рішення, повинні бути використані суб'єктивні оцінки, засновані на накопичувальному досвіді, знаннях, ідеях, поглядах і здогадках експертів, які залучаються до вироблення суб'єктивної оцінки.

Усі методи експертних оцінок можуть бути представлені двома класами, а саме: методи формування індивідуальних експертних оцінок і методи формування колективних експертних оцінок. Для обох методів для формалізації евристичної інформації використовують *різні типи шкал*: шкала класифікацій, шкала порядку, шкала інтервалів і шкала відношень. Отриману від експертів евристичну інформацію необхідно представляти в якісній формі, що є зручною для обробки та аналізу.

Задача оцінки об'єкта експертизи при системному проектуванні повинна ставитись таким чином, щоб максимізувати достовірність результатів за рахунок зближення суб'єктивних шкал і оцінок експертів. При цьому задача оцінки об'єкта буде зведена до задачі виявлення його корисності.

Окрім методу експертів широко відомі такі методи, як метод взаємного оцінювання, метод послідовного наближення (метод ітерацій), а також неформальні методи оцінювання результатів експертизи.

Кожен із методів має свої недоліки та переваги та дозволяє тою чи іншою мірою якості оцінити поточний або реалізований рівень захищеності системи інформаційної безпеки та бути засобом підтримки прийняття рішень щодо вдосконалення захисних заходів.

Найбільш відомі наступні методі експертних оцінок: методи парних і послідовних порівнянь; метод надання переваг; метод рангу; метод зважування експертних оцінок. Далі розглядаються підходи до оцінки суб'єктивної ймовірності, що лежить в основі проведення експертного оцінювання. Досліджуються методики експертного оцінювання ризиків. Пропонуються тести для оцінювання загроз і вражливостей.

2.1 Огляд експертних методів прийняття рішень

Неформальні методи експертів при прийнятті рішень. При оцінюванні рівня захищеності систем, доводиться оцінювати значення різних параметрів системи. Далеко не завжди значень параметрів систем вдається здобути

відомими математичними або статистичними методами. Така ситуація характерна для систем із високим рівнем невизначеності і таких, що не мають достатньої передісторії функціонування [17].

Наприклад, немає даних для визначення таких параметрів, як імовірність появи загроз інформаційним ресурсам за різних умов функціонування інформаційно-телекомунікаційних систем, імовірність використання зловмисниками вражливостей систем. У таких випадках доводиться користуватися неформальними методами оцінювання. Серед них найбільш відомими є *методи експертних оцінок*.

Послідовність і зміст вирішення завдань методами експертних оцінок у найзагальнішому вигляді можуть бути представлені таким чином:

- постановка завдання;
- обґрунтування переліку та змісту тих параметрів завдання, для визначення значення яких доцільно використовувати експертні оцінки;
- обґрунтування форм і способів експертних оцінок;
- розробка реквізитів (бланків, інструкцій), необхідних для проведення експертних оцінок;
- підбір і підготовка (навчання, інструктаж) експертів, що притягаються для вирішення завдання;
- організація та забезпечення роботи експертів;
- контроль і первинна обробка експертних оцінок;
- базова обробка експертних оцінок.

Принципово важливим для методів експертних оцінок є отримання такої вибірки оцінок експертів, на якій статистично стійко проявилася б їх загальна думка з вирішуваної проблеми.

Звідси одна з основних вимог і одна з труднощів полягає у підборі такої кількості компетентних експертів, яких вистачає для отримання статистично стійких вирішень. Проте при цьому виникає серйозне питання щодо порівняння компетентності різних експертів із вирішуваної проблеми.

Для вирішення цього питання у більшості існуючих методів експертних оцінок вводиться так званий коефіцієнт компетентності, що є числом в інтервалі 0 – 1, причому оцінці кожного експерта привласнюється вага, що дорівнює цьому коефіцієнту. Значення коефіцієнта компетентності визначається або самим експертом (самооцінка), або колегами з експертизи (взаємна оцінка). Іноді використовуються одночасно обидві оцінки.

Технологія використання методів експертних оцінок є послідовністю наступних операцій:

- формування досить представницької групи компетентних експертів;
- вибір способу організації роботи з експертами;
- вибір методу формування експертами оцінок із питань, що вирішуються при проведенні експертизи;
- вибір методу обробки оцінок групи експертів.

Метод експертів. У тих випадках, коли об’єктивної інформації виявляється недостатньо для визначення кількісних значень необхідного критерію при ухваленні рішення, повинні бути використані суб’єктивні оцінки, засновані на

накопиченому досвіді, знаннях, ідеях, думках і припущеннях фахівців, залучених до вироблення суб'єктивної оцінки [30].

Отримання об'єктивних оцінок базується на наступних загальних аксіомах:

- *аксіома не зміщення*, яка стверджує, що думка більшості компетентна;
- *аксіома транзитивності*, яка стверджує, що суб'єктивні оцінки транзитивні.

З цього виходить, що мірою якості суб'єктивних оцінок є їх *розсіяння*.

Для якісного ознайомлення з особливостями визначення людиною суб'єктивної оцінки та формування логічної моделі цього визначення доцільно розглянути низку прикладів.

Наприклад, нехай вимагається визначити суб'єктивну оцінку (вагові коефіцієнти) факторів *T* і *C* критерію у деякій випробувальній системі, що має вигляд

$$E = \lambda_1 T + \lambda_2 C, \qquad (2.1)$$

де *T* – час (тривалість випробувань); *C* – вартість випробувань; λ_1, λ_2 – вагові коефіцієнти, що визначають вплив *T* і *C* на ефективність випробувань.

Можна очікувати, що λ_1 *і* λ_2 змінюватимуться відповідно до обстановки, в якій проходять випробування та мірою впливу її на особу експерта. Так, якщо доля експерта залежить від успішності випробувань, то він вважатиме, що $\lambda_1 << \lambda_2$, тоді для забезпечення випробувань буде закуплено значну кількість обладнання, що різко збільшить їх вартість.

Якщо безпосередньої відповідальності за випробування експерт не несе, то результат оцінки «ваги» може бути іншим. Звідси випливає, що суб'єктивна оцінка схильна до впливу кон'юнктури. Якщо експерт у будь-чому особисто зацікавлений або нині вважається популярною певна думка, то експертна оцінка може впливати на цю кон'юнктуру. Крім того, у процесі визначення суб'єктивної оцінки можуть втручатися ті або інші авторитети так, що оцінка може бути деформована за рахунок їх впливу та з'являться помилки, якщо авторитет керується упередженою думкою.

Здатність експерта протистояти дії кон'юнктури, назвемо це об'єктивністю, яка є одним із найважливіших факторів, що визначають достовірність суб'єктивної оцінки [1]. У наступному прикладі припустимо, що визначення суб'єктивної оцінки *C* (рис. 2.1.) доручається одному експертові *E*, який базується при визначенні оцінки на інформації, отриманій з двох незалежних джерел *A* і *B*.

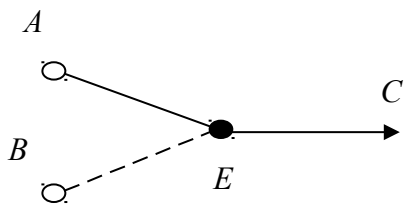

Рисунок 2.1. – Схема визначення суб'єктивної оцінки при двох незалежних джерелах інформації та одного експерта

Експерт видає оцінку *E* тільки у тому випадку, коли обидва джерела дають однакову інформацію.

Вважатимемо, що кожне джерело інформації забезпечує можливість правильної оцінки проблеми з ймовірністю, що дорівнює 0,7. Ця ймовірність обумовлена компетентністю експерта та його інформованістю про характер поставленого перед ним завдання.

Обмеженість компетентності й інформованості, властива будь-якій людині, обумовлює можливість помилки експерта. Припустимо, що він може помилитися один раз із двохсот. Тоді ймовірність правильного визначення ним суб'єктивної оцінки, обумовлена наведеними вище факторами, дорівнює 0,995. Звідси загальна ймовірність правильності суб'єктивної оцінки, даної експертом, дорівнює

$$P_1 = 0{,}7 \cdot 0{,}7 \cdot 0{,}995 = 0{,}487 ,$$

а ймовірність видачі ним помилкової оцінки

$$P_2 = 1 - 0{,}487 = 0{,}513.$$

Таким чином, наступними важливими факторами, що визначають правильність суб'єктивної оцінки, являються компетентність та інформованість експерта.

Наступний приклад відрізняється від попереднього тільки тим, що у ньому визначення оцінки доручається чотирьом експертам. У даному випадку для керівництва діями експертів призначається особа *a*, яка приймає рішення *C*, відповідне рішенням експертів у разі їх одноголосності (рис. 2.2).

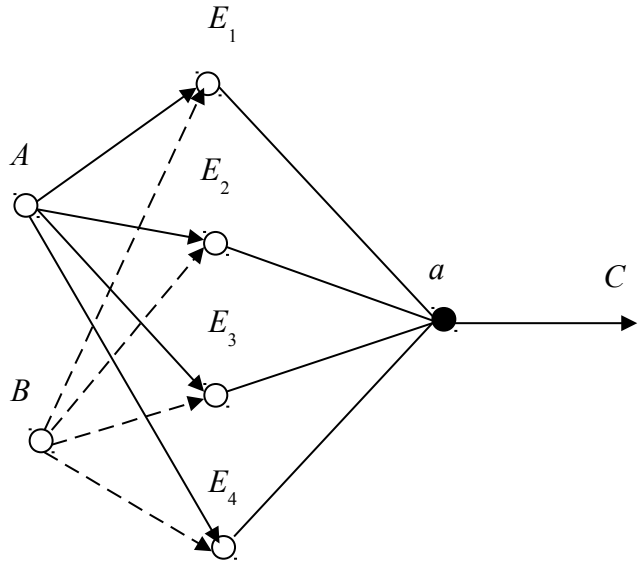

Рисунок 2.2 – Схема визначення суб'єктивної оцінки при двох незалежних джерелах інформації та чотирьох експертах

Простота функцій керівника дозволяє вважати, що ймовірність його помилки дорівнює нулю. У цьому випадку ймовірність отримання помилкової

оцінки (на основі одночасного прийняття помилкової оцінки усіма експертами) визначається як

$$[1 – (1 – 0{,}3)^2 \cdot 0{,}995]^4 \approx 0{,}000149.$$

Очевидно, що збільшення числа експертів і усереднення різко знижує ймовірність ухвалення помилкового рішення. Отже, збільшення числа експертів надає оцінці статичного характеру і є важливим фактором, який визначає правильність суб'єктивної оцінки.

Таким чином, лінгвістичну модель визначення суб'єктивних оцінок можна представити у вигляді

$$(A \wedge B \wedge C \wedge D) \rightarrow P, \qquad (2.2)$$

Де A – інформованість експерта – сукупність уявлень експерта про завдання експертизи, що ґрунтується на зовнішній інформації;

B – компетентність експерта – сукупність наукових гіпотез і конкретних ідей відносно характеру поведінки та розвитку оцінюваної альтернативи;

C – об'єктивність експерта – адекватність його уявлень про фактори, що визначають характер і поведінку об'єкта експертизи, а також умову його розвитку;

D – усередненість думок експерта, що передбачає усереднення як за множиною експертів, так і за множиною поставлених перед ним завдань або за часом;

P – суб'єктивна оцінка, що імплікується вказаними логічними передумовами.

З вищезгаданої моделі виходить, що *джерелами помилок* при суб'єктивній оцінці можуть бути:

– недостатня інформованість експерта, пов'язана з неточністю формулювання завдань експертизи, незрозумілістю та неоднозначністю використаної термінології, недостатньою ефективністю запропонованих шкал оцінок; погано складеною анкетою експерта;

– недостатня компетентність експерта, визначувана занадто високою мірою складності завдань, недостатністю сукупності його наукових гіпотез і конкретних ідей відносно характеру та поведінки об'єкта експертизи, малою науковою допитливістю;

– недостатня об'єктивність експерта внаслідок небажання брати участь в експертизі, наявність його прямої зацікавленості у деяких певних результатах експертизи, наявність морального тиску на експерта з боку деяких осіб, відсутності матеріального стимулювання, відсутності наукового інтересу та можливості підвищення наукової, технічної, або іншої кваліфікації експерта у результаті роботи, значна трудомісткість заповнення анкет і тому подібне;

– недостатня усередненість думок експертів, пов'язана з помилками анкетування, побудовою процесу експертизи; недостатньою кількістю експертів.

Таким чином, заходами для отримання достовірних оцінок є усунення вище перелічених джерел помилок. Методи реалізації цих заходів визначаються ресурсами, що знаходяться у розпорядженні особи, яка проводить експертизу

(часом і засобами, відведеними на експертизу, кількістю експертів і тому подібне).

Формально будь-яка експертиза може бути поділена на *три етапи: підготовка, проведення й оброблення результатів* [4].

Етап підготовки експертизи має на меті створення умов для отримання об'єктивних і точних оцінок альтернатив. Він звичайно включає:

– визначення завдання експертизи;

– складання анкети (опитальника), за якою опитуються експерти;

– визначення шкали оцінок, якою повинні користуватися експерти;

– визначення складу (списку) експертів, що залучаються до участі в експертизі;

– визначення порядку проведення експертизи, показників компетентності оцінок (характеристики їх точності) та методу обробки результатів.

Етап проведення експертизи має на меті отримання від експертів конкретних оцінок альтернатив, визначених анкетами опитування. Компетентність індивідуальних оцінок звичайно забезпечується використанням ітераційної процедури зі «зворотним зв'язком» до експертів. У цьому випадку проведення експертизи поділяється на декілька циклів опитування.

Отримана інформація, що повідомляється експертам («зворотний зв'язок» до експертів), служить підставою для коригування анкет опитування. Крім того, експерти можуть ознайомитися з думкою своїх колег (можлива відкрита дискусія). Опитування повторюється на новому, вищому інформаційному рівні. Об'єктивність ув'язувань досягається за рахунок незалежності експертів, їх незацікавленості у предметі експертизи та відсутності безпосереднього зв'язку між ними у ході експертизи. Опитування припиняються, як тільки будуть отримані задовільні значення показників компетентності оцінок.

Етап обробки результатів опитування має на меті підвищення компетентності оцінки альтернативи за рахунок обліку міри конкретної компетентності експертів, психологічних особливостей вироблення індивідуальних оцінок, а також соціального та статистичного характеру процесу експертизи. Облік компетентності експерта може здійснюватися методом "зважування" індивідуальних оцінок.

Облік психологічних особливостей вироблення людиною суб'єктивних оцінок альтернатив при їх розробленні може базуватися на загальних положеннях теорії корисності, обліку соціальних особливостей, на теоретичних положеннях групового вибору. Облік статистичного характеру оцінок виливається у використання при їх обробленні з метою підвищення компетентності методу усереднення.

Кожен із цих типів обробки суб'єктивних оцінок може бути реалізовано у відповідній конкретній ситуації оцінювання. Таких ситуацій може бути три:

1) коли оцінка має бути дана однією людиною; у цьому випадку обробка цієї оцінки проводиться з використанням загальних станів теорії корисності;

2) коли кількість притягнених експертів недостатня для забезпечення статистичної ефективності їх оцінок; у цьому випадку для отримання групової оцінки слід базуватися на теорії групових рішень;

3) коли для формування оцінки може бути притягнена така кількість експертів, яка забезпечує статистичну ефективність результатів експертизи; у цьому випадку засобом отримання об'єктивних оцінок є їх усереднення.

Необхідно зазначити, що використання усереднення оцінок вимагає попереднього аналізу причин, що викликають нівеляцію думки окремих експертів. Усереднення не має бути абсолютним, тобто не повинно призводити до згладжування індивідуальних оцінок, саме того, що у них є самостійного, заснованого на індивідуальному досвіді експерта.

2.2 Експертні оцінки з використанням непараметричних методів

2.2.1 Особливості використання експертних методів

Необхідність звернення до експертних методів оцінювання рівня захищеності систем, тобто до безпосереднього досвіду фахівців в області захисту інформації виникає у ситуаціях, що виявляються занадто складними для проведення кількісного аналізу.

Суттю експертного оцінювання є проведення експертами інтуїтивно-логічного аналізу проблем, отримання *кількісних* або *якісних експертних оцінок* й обробка отриманих результатів. Загальна класифікація методів отримання експертних оцінок показана на рис. 2.3.

Ефективне застосування методів експертних оцінок пов'язане, у першу чергу, з тим, які математико-статистичні моделі та методи використовуються при аналізі експертної інформації.

Сама специфіка даних експертного оцінювання говорить про те, що при аналізі інформації, отриманої від експертів, необхідно застосувати методи, що враховують наступні особливості отримуваних даних:

1) Оскільки необхідність у застосуванні методів експертних оцінок виникає у ситуаціях невизначеності, недоліку інформації, слабкого вивчення досліджуваних процесів і явищ, то невідомий є тип розподілу відповідей респондентів (оцінок експертів).

2) Експертна інформація частіше всього представлена у вигляді оцінок, отриманих за шкалою порядків (наприклад, ранжирування, парне порівняння і так далі).

3) В експертному опитуванні бере участь незначна кількість респондентів, отже дані є малими вибірками.

Найбільш ефективну обробку результатів експертного оцінювання дає застосування непараметричних методів статистики [31]. Особливо це відноситься до методів, призначених для аналізу суджень експертів, отриманих методом ранжирування.

В цілому *експертні методи* можна визначити як комплекс логічних і математико-статистичних процедур, спрямованих на отримання від фахівців інформації, її аналіз й узагальнення з метою підготовки та вибору раціональних рішень.

Експертна оцінка включає чотири компоненти:

- *суб'єкт* (окрема особа або група осіб (експертів), що приписує цінність деякому об'єкту шляхом вираження оцінки);

- *предмет* (об'єкти, цінності яких порівнюються);

- *характер* (оцінки поділяються на абсолютні – «задовільно», «незадовільно» та тому подібне, та порівняльні, коли об'єкти порівнюються між собою або певним чином – «краще», «гірше», «рівноцінно» та тому подібне);

- *основа* (позиції суб'єкта чи аргументи, що схиляють до певної переваги).

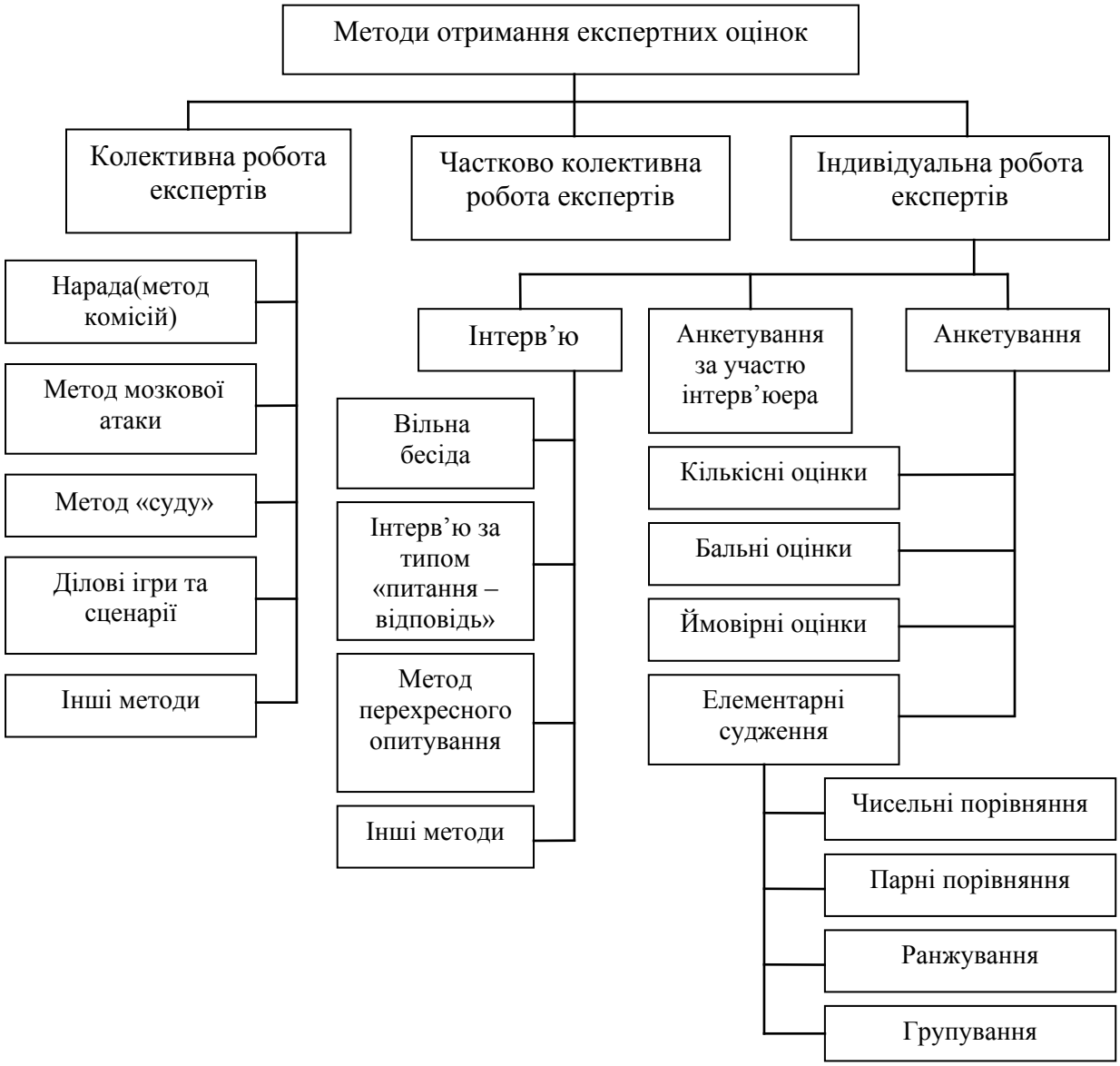

Рисунок 2.3 – Класифікація методів отримання експертних оцінок

Існує низка факторів (*внутрішніх і зовнішніх*), які можуть мати вплив на точність і надійність інформації, що отримується від експертів.

Внутрішні фактори можуть вплинути на інформацію та привести до відхилень як до ненавмисних, тобто до відхилень, пов'язаних із надмірно оптимістичним або песимістичним відношенням до проблеми, так і до тих, що мають намір, залежний від індивідуальної установки фахівця [32].

До *зовнішніх факторів* можна віднести різні впливи на інформацію, залежні передусім, від взаємодії експерта з довкіллям (наприклад, із колективом). Такі дії можуть бути викликані, наприклад, мірою відповідальності за результати експертизи.

Важливо підкреслити, що зведення методу експертних оцінок тільки до збирання й усереднення думок експертів є некоректним. Проте, застосовуючи статистичні методи аналізу цих експертних оцінок, необхідно пам'ятати і про перевірку *міри узгодженості думок експертів*.

Одним із основних методів отримання первинної інформації у дослідженні є *опитування*, яке спрямоване на отримання висловлювань респондентів про різного роду процеси й явища. Опитування можна поділити на *масові й експертні*. Масові опитування більше підходять для збирання соціологічної інформації. Однією з особливостей експертного опитування є те, що як джерела інформації (респондентів) у ньому виступають висококваліфіковані фахівці.

Відомі *два основні підходи* до аналізу експертних даних: «*алгебраїчний»* і «*статистичний*». Обидва ці підходи є досить напрацьованими та до певної міри такими, що відображають характер саме експертної інформації.

Алгебраїчний підхід припускає шукати компромісну точку зору – щось на зразок рівнодійної усіх висловлених думок. Це думка у певному значенні найближча до сукупності висловлених. Математичне оформлення цього задуму складає зміст першого підходу.

Другий підхід носить *статистичний характер*. За такого підходу кожного експерта пропонується розглядати як деякий вимірювальний «прилад», свідчення якого супроводжуються випадковою помилкою.

В цілому, алгебраїчний підхід застосовується у тому випадку, якщо думки усіх експертів розглядаються як рівноправні, а статистичний – якщо значущість думки експерта залежить від його компетентності.

Ретельна підготовка процедур експертного оцінювання є запорукою підвищення достовірності результатів експертизи. Велике значення за експертного оцінювання надається методам організації та проведення експертиз.

2.2.2 Процедури експертного оцінювання

Результатом експертного опитування повинне виступати таке надавання інформації, яке забезпечить її наступну обробку кількісними методами. Для цього використовуються наступні основні процедури: класифікація, шкалювання й оцінювання. Розглянемо детальніше процедуру оцінювання.

Оцінювання об'єктів буває пов'язано з низкою труднощів через відсутність для них точних одиниць виміру.

При використанні експертної інформації велике значення мають якісні оцінки об'єктів, для яких необхідно отримати кількісне вираження. Оскільки оцінки експертів можуть бути як кількісними, так і якісними, кожному типу оцінок ставиться у відповідність певний тип шкали (табл. 2.1).

Таблиця 2.1 – Типи шкал

Вимірювання (оцінки)	**Шкала**
Якісні	Номінальна/Порядкова
Кількісні	Інтервальна/Відношень

У багатьох випадках кількісні оцінки отримати неможливо, зокрема тому, що експерт утруднюється надати об’єкту точне кількісне значення, а виставлені приблизні оцінки можуть, у свою чергу, привести до невірних результатів.

Тобто для експерта не складає труднощів упорядкувати декілька об’єктів за мірою вираження у кожному з них певної ознаки, відобразивши тим самим свою систему переваг. Але сказати у скільки разів один об’єкт кращий за інший, швидше за все, він не зможе.

Використання порядкових шкал дозволяє розрізняти об’єкти також у тих випадках, коли дослідникові невідома ознака порівняння, але він може частково або повністю упорядкувати об’єкти на основі власної системи переваг. Оцінювання досліджуваних об’єктів можна здійснити декількома способами :

- імовірнісні характеристики;
- бальні оцінки;
- кількісні оцінки;
- елементарні судження.

Імовірнісні характеристики припускають вказівку експертами ймовірності переваги (імовірнісні оцінки) одного з варіантів (об’єктів) іншим. Труднощі, що виникають за використання цього методу, пов’язані з тим, що оцінити малоймовірні та надто ймовірні події досить просто, тоді як події зі ймовірністю переваги близько 0,5 оцінити складно.

У випадку з *бальними оцінками* експертам пропонується вказати міру цінностей або відмінності у цінності аналізованих альтернатив шляхом їх "зважування", наприклад, за 10-бальною шкалою, причому, найбільш важливому. З точки зору експерта, фактору дається повна оцінка – 10, а іншим – певна частка повної оцінки. Недоліком цього методу є, передусім, неоднозначність сприйняття експертами нав’язаної ним шкали.

Отримання від експертів безпосередньо кількісних оцінок складно, у першу чергу, через те, що навіть фахівцеві (експертові) іноді важко надати об’єкту кількісне значення, найбільш наближене до реальності.

Найбільш прийнятними для використання є методи опитування (анкетування), засновані на елементарних судженнях про перевагу об’єктів, що пред’являються експертам для оцінки.

При виконанні оцінних операцій *методами елементарних суджень* застосовують наступні процедури:

- безпосереднє оцінювання;
- парні порівняння;
- множинні порівняння;
- ранжирування.

Безпосереднє оцінювання полягає у призначенні досліджуваним об’єктам кількісних або якісних характеристик відповідно до вираження певної ознаки.

Парні порівняння полягають у порівнянні кожного об’єкта з кожним із інших відповідно до певної ознаки з метою їх ранжирування або оцінювання у міру вираження цієї ознаки.

Найбільш відомим методом *множинних порівнянь* є метод потрійних порівнянь, що дозволяє робити висновки на рівні елементарних суджень про міру близькості між собою трійок об’єктів. Основою *ранжирування* є впорядкування об’єктів у низку переваг у міру прояву певної ознаки. Ранжирування – привласнення кожному членові низки такого рангу, що фіксує місце об’єкта в ряду.

2.2.3 Проблема вибору методів обробки й аналізу суджень експертів

Дії експертів звичайно мають на увазі, що вони оцінюють об’єкти з деякими помилками, тобто відповіді усіх експертів містять помилку. Оцінки групи експертів розглядаються як сукупність незалежних однаково розподілених випадкових величин. У той самий час передбачається, що експерти частіше вказують на вірне (близьке до реальності), ніж «невірне», рішення (оцінку, ранжирування об’єктів).

Такі припущення відносно дій експертів обґрунтовують застосування математико-статистичних методів для аналізу суджень експертів.

Існує декілька причин, відповідно до яких застосування класичних методів статистики для аналізу цих експертних оцінок є сумнівним [див. 32]. Так, наприклад, відомо, що початковими даними для застосування статистичних методів є набір значень числових випадкових величин (кількісні оцінки досліджуваного об’єкта). Але практика застосування експертних опитувань привела до необхідності обробки «статистичних» даних іншої природи, це – виміри у номінальній, порядкових шкалах, ранжирування, парні та множинні порівняння. Аналіз такого типу даних можливий лише за допомогою *непараметричних методів статистики*.

Непараметричні методи статистики – комплекс методів обробки статистичних даних, що не вимагають, щоб розподіл ймовірності був описаний будь-яким параметричним законом розподілу.

Єдина умова застосування цих методів – вимога, щоб дані були обрані випадковим чином і незалежно один від одного з однієї та тієї ж генеральної сукупності.

Розглянемо *переваги та недоліки* непараметричних методів статистики.

До *переваг* цих методів відносяться:

1) Відносна простота у використанні (розрахунках). За цю якість вони дістали назву "швидких методів".

2) непараметричні методи застосовані до вибірок будь-якого обсягу, у тому числі й малого.

3) Для даних, виміряних на порядковому або номінальному рівнях, можуть бути застосовні тільки непараметричні критерії, тоді як для аналізу

інтервальних змінних підходять і параметричні, та непараметричні методи статистики.

У непараметричній статистиці використовуються у тому числі рангові методи, засновані не на самих спостереженнях, а на їх рангах. Ранги спостережень – це ті номери, які привласнюються спостереженням за їх розставляння у певному порядку (звичайно у порядку зростання).

Перехід від точних значень до рангів пов'язаний із втратою інформації, що є одним із *недоліків* непараметричних методів.

Іншим *недоліком* рангових методів є те, що вони можуть бути використані тільки для одновимірних спостережень, не існує природного способу порівняння та впорядкування.

Таким чином, можна виділити наступні *обґрунтування застосування непараметричних методів статистики* для аналізу цих експертних оцінок

1) Необхідність у застосуванні методів експертних оцінок виникає у ситуаціях невизначеності, недоліку інформації, слабко вивчених досліджуваних процесів і явищ. У цих випадках не можна зробити попередніх висновків про тип розподілу відповідей експертів, отже, саме непараметричні критерії виступають інструментами аналізу отриманих від експертів оцінок.

2) Найчастіше, через уже зазначені причини, експертна інформація представлена у вигляді оцінок, отриманих за шкалою порядків (наприклад, аранжирування). Із такими типами шкал «мають справу» непараметричні методи.

3) Як правило, в експертному опитуванні бере участь незначна кількість респондентів. Робота з малими вибірками також відноситься до зони дії непараметричної статистики.

2.2.4 Математико-статистичні моделі аналізу експертних оцінок, отриманих методом аранжирування

До *основних завдань* аналізу експертних оцінок можна віднести: перевірку узгодженості думок експертів, виділення однорідних груп експертів, отримання узагальненої думки у рамках однорідних груп експертів тощо.

При обробленні даних, отриманих від експертів, на перший план виходить перевірка узгодженості (близькості) думок експертів, оскільки увесь подальший аналіз будується виходячи з того – чи узгоджені думки експертів у цілому або ж сукупність експертних думок розбилася на декілька узгоджених груп суджень і так далі. Перевірка узгодженості також передує отриманню колективної думки та може, до певної міри, служити показником надійності проведеної експертизи.

Під узгодженістю думок експертів звичайно розуміють певний збіг оцінок, які дають незалежні експерти одним і тим же об'єктам за певними критеріями.

Залежно від цілей проведення експертизи одним із бажаних результатів експертного оцінювання може виступати отримання узагальненої думки експертів. Отримане у результаті обробки експертних оцінок узагальнене судження може бути основою для ухвалення правильного рішення, вибору оптимального варіанта із запропонованих альтернатив і так далі. Якщо стоїть

завдання вироблення результуючої думки, то необхідною процедурою аналізу цих експертних оцінок виступає перевірка узгодженості думок експертів.

У деяких випадках розсіювання експертних оцінок може вказувати не на міру некомпетентності опитуваних експертів, а на об'єктивну багатогранність явищ. Наприклад, це може відбуватися у невизначених ситуаціях, що допускають множину альтернатив. За таких обставин усі експертні судження (чи групи експертних думок) правомочні, а статистичний аналіз такого виду даних може визначати лише заходи узгодженості позицій експертів (груп експертів).

Розглядають два основні підходи до визначення міри узгодженості думок експертів.

Перший підхід полягає у виборі деякого показника розкиду балів, даних експертами (наприклад, таким показником може виступати дисперсія). Далі цей показник нормується, щоб він набував значень від 0 або від – 1 (у разі відсутності узгодженості) до 1 або до +1 відповідно (у разі узгодження думок).

Після цього обираються певні значення, причому таким чином, що якщо розрахований показник розкиду менше або більше цього значення, то узгодженість приймається або заперечується. Мінусом такого методу є труднощі за визначення порогового значення.

Другий підхід полягає у формулюванні поняття узгодженості для кожної певної ситуації. Далі відповідно до формулювання підбираються певні статистичні гіпотези. Далі перевірка зводиться до перевірки відповідних гіпотез.

Другий підхід теж має свої *недоліки*. Наприклад, розподіл багатьох статистик висуває умову незалежності отриманих ранжирувань, що не завжди можна виконати.

Як зазначалося раніше методи, що використані для отримання експертних оцінок досить різноманітні, але найбільш поширеними з них є *ранжирування*, *класифікація, парні та множинні порівняння*.

При вирішенні багатьох практичних завдань часто виявляється, що явища, які вивчаються, не піддаються безпосередньому виміру, наявні кількісні дані носять тою чи іншою мірою умовний характер (наприклад, тестові бали, експертні оцінки і так далі). У подібних випадках слід відмовитися від аналізу конкретних значень даних, а досліджувати тільки інформацію про їх взаємну впорядкованість. Для цього від початкових кількісних даних необхідно перейти до рангів.

Ранжирування – це процес впорядкування ряду об'єктів відповідно до вираження певної ознаки. Ранжирування може бути застосоване у ситуаціях:

- коли необхідно упорядкувати об'єкти відповідно до будь-якої якості, але при цьому не вимагається виробляти його точний вимір;
- коли якість, у принципі, вимірна, проте зараз не може бути виміряною через будь-які причини.

Розглянемо математико-статистичні моделі перевірки узгодженості думок експертів для даних, отриманих методом ранжирування.

Завдання узгодженості між двома групами експертних ранжирувань. Необхідність у перевірці узгодженості двох груп експертних ранжирувань зможе виникати, наприклад, за порівняння результатів роботи експертних груп, сформованих за різними ознаками.

При проведенні експертної оцінки двома групами експертів необхідно перевіряти узгодженість між цими групами за узгодженості ранжирувань усередині кожної з них. Внутрішньо групова узгодженість перевіряється за допомогою одного з методів, описаних вище.

На закінчення зазначимо, що непараметричні методи статистики мають недоліки, пов'язані у першу чергу, з деякою втратою інформації. Але у той самий час вони мають низку безперечних переваг порівняно з методами класичної статистики і є найбільш адекватними для аналізу експертної інформації.

2.3 Організація проведення експертних оцінок

2.3.1 Методи групових експертних оцінок

Група методів експертних оцінок найчастіше використовується у практиці оцінювання складних систем, на якісному рівні. За використання експертних оцінок звичайно передбачається, що думка групи експертів надійніша, ніж думка окремого експерта. У деяких теоретичних дослідженнях відзначається, що це припущення не є очевидним, але одночасно стверджується, що при дотриманні певних вимог у більшості випадків групові оцінки надійніші за індивідуальні. До таких вимог належать [30]:

- розподіл оцінок, отриманих від експертів, має бути «гладким»;
- дві групові оцінки, надані двома однаковими підгрупами, обраними випадковим чином, мають бути близькі.

Уся множина проблем, вирішуваних методами експертних оцінок, поділяються на *два класи*. До першого класу відносяться такі, відносно яких є достатнє забезпечення інформацією. При цьому методи опитування й обробки ґрунтуються на використанні принципу «хорошого вимірника», тобто експерт – це джерело достовірної інформації; групова думка експертів близька до істинного рішення.

До *другого класу* відносяться проблеми, відносно яких знань для впевненості та справедливості вказаних гіпотез недостатньо. У цьому випадку експертів не можна розглядати як «хороших вимірників» і необхідно обережно підходити до обробки результатів експертизи.

Експертні оцінки несуть у собі як вузько суб'єктивні риси, властиві кожному експертові, так і колективно-суб'єктивні, властиві колегії експертів. І якщо перші усуваються у процесі обробки індивідуальних експертних оцінок, то другі не зникають, які б способи обробки не застосовувалися.

Основними етапами експертизи є: формування мети, розробка процедури експертизи, формування групи експертів, опитування, аналіз і обробка

інформації. При формулюванні мети експертизи розробник повинен виробити чітке уявлення про те, ким і для яких цілей будуть використані результати.

При обробці матеріалів колективної експертної оцінки використовуються методи *теорії рангової кореляції*. Для кількісної оцінки міри узгодженості думок експертів застосовується *коефіцієнт конкордації W*, який дозволяє оцінити, наскільки узгоджені між собою ряди переваги, побудовані кожним експертом. Його значення знаходиться у межах $0 < W < 1$, де $W = 0$ означає повну протилежність, а $W = 1$ означає повний збіг ранжирувань. Практично достовірність вважається хорошою, якщо $W = 0{,}7 - 0{,}8$.

Невелике значення *коефіцієнта конкордації*, що свідчить про слабку узгодженість думок експертів, є наслідком того, що в даній сукупності експертів дійсно відсутня спільність думок або всередині даної сукупності експертів існують групи з високою узгодженістю думок, проте узагальнені думки таких груп протилежні.

Для наочності уявлення про міру узгодженості думок двох будь-яких експертів *А* і *Б* служить *коефіцієнт парної рангової кореляції p*, він набуває значень $-1 < p < +1$. Значення $p = +1$ відповідає повному збігу оцінок у рангах двох експертів (повна узгодженість думок двох експертів), а значення $p = -1$відповідає двом взаємно протилежним ранжируванням важливості властивостей (думка одного експерта протилежна до думки іншого).

Тип використаних процедур експертизи залежить від завдання оцінювання.

До найбільш застосованих процедур експертних вимірів відносяться [33]:

- ранжирування;
- парне порівняння;
- множинні порівняння;
- безпосередня оцінка;
- Черчмена-Акоффа;
- метод Терстоуна;
- метод фон Неймана-Моргенштерна.

Доцільність застосування того або іншого методу багато у чому визначається характером аналізованої інформації. Якщо виправдані лише якісні оцінки об'єктів за деякими якісними ознаками, то використовуються *методи ранжирування, парного та множинного порівняння*.

Якщо характер аналізованої інформації такий, що доцільно отримати кількісні оцінки об'єктів, то можна використати будь-який метод кількісної оцінки, починаючи від *безпосередніх кількісних оцінок* і закінчуючи тоншими *методами Терстоуна та фон Неймана-Моргенштерна*.

При описуванні кожного з перерахованих методів передбачається, що є кінцеве число вимірюваних або оцінюваних альтернатив (об'єктів) $A = \{a, .., a_n\}$ та сформульовано один або декілька ознак порівняння, за якими здійснюється порівняння властивостей об'єктів. Отже, методи виміру різнитимуться лише *процедурою порівняння об'єктів*. Ця процедура включає побудову відношень між об'єктами емпіричної системи, вибір перетворення c_p і визначення типу шкал вимірів. Із урахуванням викладених вище обставин розглянемо кожен метод виміру.

2.3.2 Характеристика методів вимірювання

Ранжирування. Метод є процедурою впорядкування об'єктів, що виконується експертом. На основі знань і досвіду експерт розташовує об'єкти у порядку переваги, керуючись одним або декількома обраними показниками порівняння. Залежно від виду відношень між об'єктами можливі різні варіанти впорядкування об'єктів.

Розглянемо можливі варіанти впорядкування об'єктів.

Нехай серед об'єктів немає однакових за порівнюваними показниками, тобто немає еквівалентних об'єктів. У цьому випадку між об'єктами існує тільки відношення суворого порядку. У результаті порівняння всіх об'єктів по відношенню суворого порядку складається впорядкована послідовність $a_1 > a_2 > ... > a_N$, де об'єкт із першим номером є найбільш прийнятним із усіх об'єктів, об'єкт із другим номером менш прийнятний, ніж перший об'єкт, але прийнятніший за усі інші об'єкти і так далі. Отримана система об'єктів із відношенням суворого порядку, за умови порівнянності усіх об'єктів за цим відношенням, утворює повний суворий порядок. Для цього відношення доведено існування числової системи, елементами якої є дійсні числа, пов'язані між собою відношенням нерівності >. Це означає, що впорядкуванню об'єктів відповідає впорядкування чисел $x_1 > ... > x_N$, *де* $x_i = \varphi(a_i)$. Можлива і зворотна послідовність $x_1 < ... < x_N$ в якій найбільш прийнятному об'єкту приписується найменше число та за мірою убування переваги об'єктам приписуються великі числа.

Відповідність перерахованих послідовностей можна здійснити, обираючи будь-які числові представлення. Єдиним обмеженням є монотонність перетворення. Отже, допустиме перетворення при переході від одного числового представлення до іншого повинне мати властивість монотонності. Таку властивість допустимого перетворення має шкала порядків, тому ранжирування об'єктів є вимір у порядковій шкалі.

У практиці ранжирування найчастіше застосовується числове представлення послідовності у вигляді натуральних чисел:

$$x_1 = \varphi(a_1) = 1,\ x_2 = \varphi(a_2) = 2,\ x_N = \varphi(a_N) = N,$$

тобто використовується числова послідовність. Числа $x_1, x_2, ..., x_N$ у цьому випадку називають *рангами* й, як правило, позначають літерами $r_1, r_2, ..., r_N$. Застосування суворих числових відношень «більше» (>), «менше» (<) або «рівне» (=) не завжди дозволяє встановити порядок між об'єктами. Тому разом із ними використовуються відношення для визначення більшої або меншої міри будь-якої якісної ознаки (відношення часткового порядку, наприклад корисності), відношення типу «прийнятніше» (>), «менш прийнятно» (<), «рівноцінно» (=) або «байдуже» (≈). Впорядкування об'єктів при цьому може мати, наприклад, наступний вигляд:

$$a_1 > a_2 > a_3 \approx a_4 \approx a_5 > a_6 > \ldots > a_{N-1} \approx a_N$$

Таке впорядкування утворює несуворий лінійний порядок.

Для відношення *несуворого лінійного порядку* доведено існування числової системи зі відношеннями нерівності та рівності між числами, що описують властивості об'єктів. Будь-які дві числові системи для несуворого лінійного порядку пов'язані між собою монотонним перетворенням. Отже, ранжируванням за умови наявності еквівалентних об'єктів є вимір також у порядковій шкалі.

У практиці ранжирування об'єктів, між якими допускаються відношення як *суворого порядку*, так і еквівалентності, числове представлення обирається таким чином. Найбільш прийнятному об'єкту привласнюється ранг, що дорівнює одиниці, другому за перевагою – ранг, що дорівнює двом, і так далі. Для еквівалентних об'єктів зручно з точки зору технології наступної обробки експертних оцінок призначати однакові ранги, що дорівнюють середньоарифметичному значенню рангів, що привласнюються однаковим об'єктам. Такі ранги називають *пов'язаними рангами*. Для наведеного прикладу впорядкування на основі несуворого лінійного порядку при N - *10* рангів об'єктів a_3, a_4, a_5 будуть дорівнювати

$$r_3 = r_4 = r_5 = (3 + 4 + 5)/3 = 4.$$

У цьому ж прикладі ранги об'єктів a_9, a_{10} також однакові та дорівнюють середньоарифметичному $r_9 = r_{10} = (9+10)/2 = 9{,}5$. Пов'язані ранги можуть виявитися дробовими числами. Зручність використання пов'язаних рангів полягає у тому, що сума рангів N об'єктів дорівнює сумі натуральних чисел від одиниці до N. При цьому будь-які комбінації пов'язаних рангів не змінюють цю суму. Ця обставина істотно спрощує обробку результатів ранжирування при груповій експертній оцінці.

При груповому ранжируванні кожен S-й експерт надає кожному об'єкту ранг r_{iS}. У результаті проведення експертизи виходить матриця рангів

$\| r_{iS} \|$ розмірності $N \cdot k$, де k – число експертів; N - число об'єктів; $\overline{S} = \overline{1,k}\,;\overline{1,N}$. Результати групового експертного ранжирування зручно представити у вигляді табл. 2.2.

Таблиця 2.2 – Результати групового ранжирування

Об'єкт	E_1	E_2	…	E_k
a_1	r_{11}	r_{12}	…	r_{1k}
a_2	r_{21}	r_{22}	…	r_{2k}
…	…	…	…	…
a_n	r_{n1}	r_{n2}	…	r_{nk}

Аналогічний вигляд має таблиця, якщо здійснюється ранжирування об'єктів одним експертом за декількома показниками порівняння. При цьому в таблиці замість експертів у відповідних графах вказуються показники. Нагадаємо, що ранги об'єктів визначають тільки порядок розташування об'єктів за

показниками порівняння. Ранги як числа не дають можливості зробити висновок про те, *на скільки* або у с*кільки разів* прийнятніше один об'єкт порівняно з іншим.

Позитивна якість ранжирування як методу експертного виміру – простота здійснення процедур, що не вимагає трудомісткого навчання експертів. Недоліком ранжирування є практична неможливість впорядкування значного числа об'єктів. Як показує досвід, при числі об'єктів, більшому за 10-15, експерти утруднюються в побудові ранжирування. Це пояснюється тим, що у процесі ранжирування експерт повинен встановити взаємозв'язок між усіма об'єктами, розглядаючи їх як єдину сукупність. При збільшенні числа об'єктів кількість зв'язків між ними зростає пропорційно квадрату числа об'єктів. Збереження у пам'яті й аналіз значної сукупності взаємозв'язків між об'єктами обмежуються психологічними можливостями людини. Психологія стверджує, що оперативна пам'ять людини дозволяє оперувати у середньому не більше ніж 7 ± 2 об'єктами одночасно. Тому при ранжируванні значного числа об'єктів експерти можуть допускати істотні помилки.

Парне порівняння. Цей метод є процедурою встановлення переваги об'єктів при порівнянні усіх можливих пар. На відміну від ранжирування, в якому здійснюється впорядкування усіх об'єктів, парне порівняння об'єктів є простішим завданням. При порівнянні пари об'єктів можливо або відношення суворого порядку, або відношення еквівалентності. Звідси витікає, що парне порівняння так само, як і ранжирування, є *вимір у порядковій шкалі*.

В результаті порівняння пари об'єктів a_i і a_j, експерт упорядковує її, висловлюючи або $a_i > a_j$, або $a_j > a_i$, або $a_i \approx a_j$. Вибір числового представлення $\varphi(a_i)$ можна зробити так:

– якщо $a_i > a_j$, то $\varphi(a_i) > \varphi(a_j)$*;*

– якщо перевага у парі зворотна, то знак нерівності замінюється на зворотний, тобто $\varphi(a_i) < \varphi(a_j)$*;*

– якщо об'єкти еквівалентні, то можна вважати, що $\varphi(a_i) = \varphi(a_j)$.

У практиці парного порівняння використовуються наступні числові представлення:

$$x_{ij} = \left\{ \begin{array}{l} 1, \textit{якщо } a_i \rangle a_j \ \textit{або } a_i \approx a_j \\ 0, \textit{якщо } a_i \langle a_j \ ; i, j = 1, N \end{array} \right\} \ ; \tag{2.3}$$

$$x_{ij} = \left\{ \begin{array}{c} 2, \textit{якщо } a_i \rangle a_j \ ; \\ 1, \textit{якщо } a_i \approx a_j \\ 0, \textit{якщо } a_i \langle a_j \ , i, j = 1, N \end{array} \right\} . \tag{2.4}$$

Результати порівняння усіх пар об'єктів зручно представляти у вигляді матриці. Нехай, наприклад, є п'ять об'єктів a_1, a_2, a_3, a_4, a_5 і проведено парне порівняння цих об'єктів за перевагою. Результати порівняння представлені у вигляді:

$$a_1 > a_2,\ a_1 > a_3,\ a_1 > a_4,\ a_1 < a_5;\ \ a_2 > a_3,\ a_2 > a_4,\ \ a_2 < a_5;$$

$$a_3 \approx a_4\ ,\ a_3 < a_5,\ a_4 < a_5.$$

Згідно формули (2.3), складемо матрицю вимірів результатів парних порівнянь (табл. 2.3). У табл. 2.3 на діагоналі завжди будуть розташовані одиниці, оскільки об'єкт еквівалентний собі. Представлення (2.4) характерне для відображення результатів, наприклад спортивних змагань. За виграш даються два очки, за нічию – одне і за програш – нуль очків.

Таблиця 2.3 – Матриця парних порівнянь

	a_1	a_2	a_3	a_4	a_5
a_1	1	1	1	1	0
a_2	0	1	1	1	0
a_3	0	0	1	1	0
a_4	0	0	1	1	0
a_5	1	1	1	1	1

Перевага одного об'єкта перед іншим трактується у даному випадку як виграш одного учасника турніру в іншого. Таблиця результатів виміру при використанні числового представлення не відрізняється від таблиць результатів спортивних турнірів за винятком діагональних елементів (звичайно у турнірних таблицях діагональні елементи заштриховані).

Як приклад у табл. 2.4 наведені результати виміру п'яти об'єктів із використанням представлення (2.4), відповідні табл. 2.2.

Таблиця 2.4 – Результати вимірювання п'яти об'єктів

	a_1	a_2	a_3	a_4	a_5
a_1	1	2	2	2	0
a_2	0	1	2	2	0
a_3	0	0	1	1	0
a_4	0	0	1	1	0
a_5	2	2	2	2	1

Замість представлення (2.4) часто використовують еквівалентне йому представлення, яке виходить із (2.4) заміною 2 на +1, 1 на 0 і 0 на 1.

$$x_{ij} = \left\{ \begin{array}{c} +1, \textit{якщо } a_i \rangle\ a_j\ ; \\ 0, \textit{якщо } a_i \approx a_j \\ -1, \textit{якщо } a_i \langle\ a_j\ , i, j = 1, N \end{array} \right\}\ . \qquad (2.5)$$

Якщо порівняння пар об’єктів виробляється окремо за різними показниками або порівняння здійснює група експертів, то за кожним показником або експертом складається своя таблиця результатів парних порівнянь. Порівняння усіх можливих пар не дає повного впорядкування об’єктів, тому виникає завдання ранжирування об’єктів за результатами їх парного порівняння.

Проте, як показує досвід, експерт далеко не завжди послідовний у своїх перевагах. У результаті використання методу парних порівнянь експерт може вказати, що об’єкт a_1, прийнятніше за об’єкт a_2, a_2 прийнятніше за об’єкт a_3, але у той самий час a_3 прийнятніше за об’єкт a_1. У разі поділу об’єкта на класи експерт може до одного класу віднести пари a_1 та a_2, a_2 та a_3, але у той самий час об’єкти a_1 і a_3 віднести до різних класів. Така непослідовність експерта може пояснюватися різними причинами: складністю завдання, неочевидністю переваги об’єктів або поділу їх на класи (інакше, коли усе очевидно, проведення експертизи необов’язкове), недостатньою компетентністю експерта, недостатньо чіткою постановкою завдання, багатокритеріальністю даних об’єктів тощо.

Непослідовність експерта призводить до того, що у результаті парних порівнянь при визначенні порівняльної переваги об’єктів ми не отримуємо ранжирування і навіть відношень часткового порядку, не виконана властивість транзитивності.

Якщо метою експертизи при визначенні порівняльної переваги об’єктів є отримання ранжирування або часткового впорядкування, потрібна їх додаткова ідентифікація. У цих випадках має сенс як результуюче відношення обирати відношення заданого типу, найближче до отриманого в експерименті.

Множинні порівняння. Множинні порівняння відрізняються від парних тим, що експертам послідовно пред’являються не пари, а трійки, четвірки,.., n -ки ($n < N$) об’єктів. Експерт їх упорядковує за важливістю або розбиває на класи залежно від цілей експертизи.

Множинні порівняння займають проміжне положення між парними порівняннями та ранжируванням. З одного боку, вони дозволяють використати більший, ніж при парних порівняннях, обсяг інформації для визначення експертного судження у результаті одночасного співвідношення об’єкта не з одним, а з великим числом об’єктів.

З іншого боку, при ранжируванні об’єктів їх може виявитися надто багато, що утруднює роботу експерта та позначається на якості результатів експертизи. У цьому випадку множинні порівняння дозволяють зменшити до розумних меж обсяг інформації, що надходить до експерта.

Безпосередня оцінка. Метод безпосередньої оцінки полягає у привласненні об’єктам числових значень у шкалі інтервалів. Експертові необхідно поставити у відповідність кожному об’єкту точку на певному відрізку числової осі. При цьому необхідно, щоб еквівалентним об’єктам приписувалися однакові числа. На рис. 2.4 як приклад наведено таке представлення для п’яти об’єктів на відрізок числової осі [0,1].

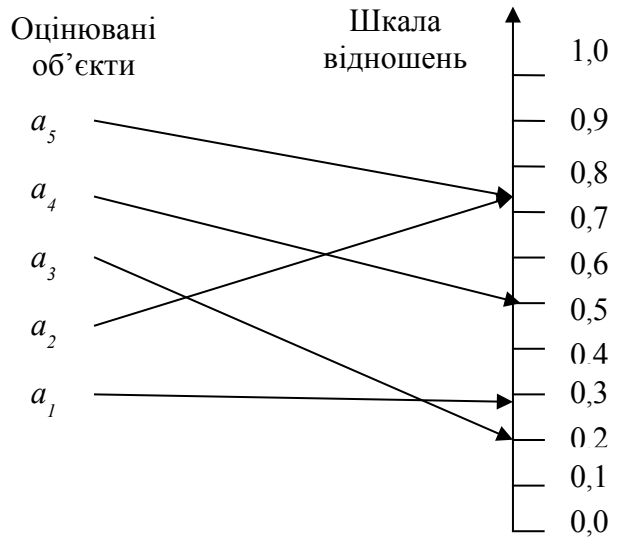

Рисунок 2.4 – Приклад порівняння п'яти об'єктів за шкалою

Оскільки за початок відліку обрана нульова точка, то у цьому прикладі вимір виробляється у шкалі відношень. Експерт поєднує кожен об'єкт лінією з точкою числової осі й отримує наступні числові представлення об'єктів

$$\varphi(a_1) = 0{,}28;\ \varphi(a_2) = \varphi(a_5) = 0{,}75;\ \varphi(a_3) = 0{,}2;\ \varphi(a_4) = 0{,}5.$$

Виміри у шкалі інтервалів можуть бути досить точними за повної інформованості експертів про властивості об'єктів. Ці умови на практиці зустрічаються рідко, тому для виміру застосовують бальну оцінку. При цьому замість безперервного відрізку числової осі розглядають ділянки, яким приписуються бали.

Експерт, приписуючи об'єкту бал, тим самим вимірює його з точністю до певного відрізку числової осі. Застосовуються 5-, 10 - і 100-бальні шкали.

Метод послідовного порівняння або метод Черчмена Акоффа. Цей метод належить до найбільш популярних при оцінці альтернатив. У ньому передбачається послідовне коригування оцінок, вказаних експертами.

Основні припущення, на яких засновано метод, полягають у наступному:

– кожній альтернативі $a_i (i = \overline{1, N})$ ставиться у відповідність дійсне ненегативне число $\varphi(a_i)$;

– якщо альтернатива a_i прийнятніше за альтернативу a_j, то $\varphi(a_i) > \varphi(a_j)$, якщо ж альтернативи a_i та a_j рівноцінні, то $\varphi(a_i) = \varphi(a_j)$;

– якщо $\varphi(a_i)$ *та* $\varphi(a_j)$ – оцінки альтернатив a_i та a_j, то $\varphi(a_i) + \varphi(a_j)$ відповідають сумісному здійсненню альтернатив a_i та a_j.

Найбільш сильним є останнє припущення щодо *адитивності оцінок альтернатив*.

Відповідно до методу Черчмена-Акоффа альтернативи a_1 , a_2, … a_N ранжируються за прийнятністю. Для зручності припустимо, що альтернатива a_1, найбільш прийнятна, за нею слідує a_2 тощо. Експерт вказує попередні числові оцінки $\varphi(a)$ для кожної з альтернатив. Іноді найбільш прийнятній альтернативі приписується оцінка 1, інші оцінки розташовуються між 0 і 1 відповідно до їх переваги. Потім експерт виробляє порівняння альтернативи a_1 та суми альтернатив a_2, .., a_N. Якщо a_1 прийнятніше, то експерт коригує оцінки так, щоб

$$\varphi(a_1) > \sum_{i=2}^{N} \varphi(a_i).$$

Інакше повинна виконуватися нерівність

$$\varphi(a_1) \le \sum_{i=2}^{N} \varphi(a_i).$$

Якщо альтернатива a_1, виявляється менш прийнятною, то для уточнення оцінок вона порівнюється за перевагою з сумою альтернатив $\{a_2,..., a_N\}$ тощо.

Після того, як альтернатива a_1, виявляється прийнятніше за суму альтернатив $a_2,.., a_k$ $(k \ge 2)$, вона виключається з розгляду, а замість оцінки альтернативи a_1 розглядається та коригується оцінка альтернативи a_2. Процес триває до тих пір, поки відкоригованими не виявляться оцінки усіх альтернатив.

За досить великого N застосування методу Черчмена-Акоффа стає занадто трудомістким. У цьому випадку доцільно розбити альтернативи на групи, а одну з альтернатив, наприклад максимальну, включити в усі групи. Це дозволяє отримати числові оцінки усіх альтернатив за допомогою оцінювання всередині кожної групи.

Метод Черчмена-Акоффа є одним найефективніших. Його можна успішно використати при вимірах у шкалі відношень. У цьому випадку визначається найбільш прийнятна альтернатива a_n. Їй надається максимальна оцінка. Для усіх інших альтернатив експерт вказує, у скільки разів вони менш прийнятні, ніж a_n. Для коригування числових оцінок альтернатив можна використати як стандартну процедуру методу Черчмена-Акоффа, так і попарне порівняння переваги альтернатив. Якщо числові оцінки альтернатив не збігаються з уявленням експерта про їх перевагу, виробляється коригування.

Метод фон Неймана-Моргенштерна. Метод фон Неймана-Моргенштерна полягає в отриманні числових оцінок альтернатив за допомогою так званих імовірнісних сумішей. В основі методу лежить припущення, згідно з яким експерт для будь-якої альтернативи, менш прийнятної, ніж a_i, але прийнятніше, ніж a_l, може вказати число p $(0 \le p \le l)$ таке, що альтернатива a_i еквівалентна змішаній альтернативі (імовірнісній суміші) $[pa_i, (1 - p)\ a_l]$. Змішана альтернатива полягає у тому, що альтернатива a_i обирається зі ймовірністю P, а альтернатива a_l – зі ймовірністю lP. Очевидно, що якщо P досить близько до 1, то альтернатива a_j менш прийнятна, ніж змішана альтернатива $[pa_i, (1 - p)\ a_l]$. У літературі крім згаданого вище припущення розглядається система припущень

(аксіом) про властивості змішаних і незмішаних альтернатив. До таких припущень належать припущення про зв'язність і транзитивність відношення переваги альтернатив, припущення про те, що змішана альтернатива й інші альтернативи $[pa_i, (1-p)\, a_l]$ прийнятніше, ніж $[p'a_i, (1-p')\, a_l]$, якщо $p > p'$.

Якщо вказана система переваг виконана, то для кожної з набору основних альтернатив $a_1, a_2, \ldots, a_N$ визначаються числа $x_1, x_2, \ldots, x_N$, що характеризують числову оцінку змішаних альтернатив.

Числова оцінка змішаної альтернативи $[p_1a_1, p_2a_2, \ldots, p_Na_N]$ дорівнює:

$$x_1p_1 + x_2p_2 + \ldots + x_Np_N .$$

Змішана альтернатива $[p_1a_1, p_2a_2, \ldots, p_Na_N]$ прийнятніше змішаної альтернативи $\left[p_1'a_1, p_2'a_2, \ldots, p_N'a_N\right]$, якщо

$$x_1p_1 + x_2p_2 + \ldots + x_Np_N > x_1p_1' + x_2p_2' + \ldots + x_Np_N' .$$

Таким чином, встановлюється існування функції корисності $x_1p_1 + x_2p_2 + \ldots + x_Np_N$, значення якої характеризує ступінь прийнятності будь-якої змішаної альтернативи, зокрема і незмішаної. Прийнятніше та змішана альтернатива, для якої значення функції корисності більше.

Методи типу «Делфі». Назва методів експертної оцінки *типу «Делфі»* пов'язана зі старогрецьким містом Делфі, де при храмі Аполлона з IX ст. до н.е. до IV ст. н.е. за переказами знаходився оракул Делфійский.

На відміну від традиційних методів експертної оцінки метод Делфі припускає повну відмову від колективних обговорень. Це робиться для того, щоб зменшити вплив таких психологічних факторів, як приєднання до думки найбільш авторитетного фахівця, небажання відмовитися від публічно висловленої думки, йде за думкою більшості. У методі Делфі прямі дебати замінені програмою послідовних індивідуальних опитувань, що проводяться у формі анкетування. Відповіді узагальнюються і разом із новою додатковою інформацією надходять у розпорядження експертів, після чого вони уточнюють свої первинні відповіді. Така процедура повторюється кілька разів до досягнення прийнятного збігу сукупності висловлених думок. Результати експерименту показали прийнятний збіг оцінок експертів після п'яти турів опитування.

Метод Делфі спочатку був запропонований О. Хелмером як ітеративна процедура «мозкової атаки», яка повинна допомогти знизити вплив психологічних факторів і підвищити об'єктивність результатів. Проте майже одночасно Делфі-процедури стали основним засобом підвищення об'єктивності експертних опитувань із використанням кількісних оцінок при оцінці «дерев мети» та при розробці сценаріїв за рахунок використання зворотного зв'язку, ознайомлення експертів із результатами попереднього туру опитування й обліку цих результатів при оцінці значущості думок експертів.

Процедура Делфі-методу полягає у наступному:

1) організовується послідовність циклів «мозкової атаки»;

2) розробляється програма послідовних індивідуальних опитувань за допомогою запитальників, що виключає контакти між експертами, але що передбачає ознайомлення їх із думками один одного між турами; запитальники від туру до туру можуть уточнюватися;

3) у найбільш розвинених методиках експертам привласнюються вагові коефіцієнти значущості їх думок, що обчислюються на основі попередніх опитувань, уточнюванні від туру до туру та що враховуються при отриманні узагальнених результатів оцінок.

Перше практичне застосування методу Делфі до вирішення деяких завдань міністерства оборони США, здійснене *RAND Corporation* у другій половині 40-х рр., показало його ефективність і доцільність поширення на широкий клас завдань, пов'язаний із оцінкою майбутніх подій.

Недоліки методу Делфі :

– значна витрата часу на проведення експертизи, що пов'язана зі значною кількістю послідовних повторень оцінок;

– необхідність неодноразового перегляду експертом своїх відповідей, що викликає у нього негативну реакцію, що позначається на результатах експертизи.

У 60-ті рр. сфера практичного застосування методу Дельфі значно розширилася, проте властиві йому обмеження привели до виникнення інших методів, що використовують експертні оцінки. Серед них на особливу увагу заслуговують методи QUEST, SEER, PATTERN.

Метод QUEST (*Qualitative Utility Estimates for Science and Technology*) – кількісні оцінки корисності науки та техніки був розроблений для цілей підвищення ефективності рішень з розподілу ресурсів, що виділяються на дослідження та розробки. В основу методу покладена ідея розподілу ресурсів на основі обліку можливого вкладу (визначуваного методу експертної оцінки) різних галузей і наукових напрямів у вирішення будь-якого кола завдань.

Метод SEER (*System for Event Evaluation and Review*) – система оцінок і огляду подій передбачає всього два тури оцінки. У кожному турі притягується різний склад експертів. Експерти першого туру – фахівці промисловості, експерти другого туру – найбільш кваліфіковані фахівці з органів, що приймають рішення, та фахівці в області природничих і технічних наук. Експерт кожного туру не повертається до розгляду своїх відповідей за винятком тих випадків, коли його відповідь випадає з деякого інтервалу, в якому знаходяться більшість оцінок (наприклад, інтервалу, в якому знаходиться 90 % усіх оцінок).

Підведемо *підсумок розгляду методів експертних оцінок*. Група методів експертних оцінок найчастіше використовується на практиці оцінювання складних систем на якісному рівні. Розглянуті вище методи експертних оцінок мають різні якості, але приводять у загальному випадку до близьких результатів. Практика застосування цих методів показала, що найбільш ефективне комплексне застосування різних методів для вирішення одного й

того ж завдання. Порівняльний аналіз результатів підвищує обґрунтованість висновків, що робляться. При цьому слід врахувати, що методом, який вимагає мінімальних витрат, є ранжирування, а найбільш трудомістким є метод послідовного порівняння (Черчмена Акоффа). Метод парного порівняння без додаткового оброблення не дає повного впорядкування об'єктів.

2.4 Оцінка ризиків експертними методами

2.4.1 Оцінка суб'єктивної ймовірності

Як правило, на практиці суб'єктивну ймовірність доводиться застосовувати у наступних випадках:

– коли об'єктивна ймовірність неякісна;

– якщо передбачається, що отримані закономірності й об'єктивна ймовірність не спостерігатимуться у майбутньому;

– коли немає об'єктивних даних про спостереження у минулому.

У таких ситуаціях суб'єктивну ймовірність можна розглядати як міру упевненості експерта про можливість настання події. Вона може бути представлена по-різному: ймовірнісним розподілом на множині подій, бінарним відношенням на множині подій, не повністю заданим імовірнісним розподілом або бінарним відношенням та іншими способами [31].

Покажемо, як визначити суб'єктивну ймовірність. Поділимо процес на три етапи:

- підготовчий етап;
- отримання оцінок;
- аналіз оцінок.

Перший етап (підготовчий) дозволяє виділити об'єкт дослідження – деяку множину подій. Далі проводиться попередній аналіз властивостей цієї значної кількості (встановлюється залежність або незалежність подій, дискретність або безперервність випадкової величини, що породжує цю множину подій). На основі такого аналізу обирається один із відповідних методів визначення суб'єктивної ймовірності. На цьому ж етапі проводиться підготовка експерта або групи експертів, ознайомлення його з методом і перевірка розуміння поставленого завдання експертами.

Другий етап (отримання оцінки) полягає у застосуванні методу, обраного на першому етапі. Результатом цього етапу є набір чисел, який відбиває суб'єктивний погляд експерта або групи експертів на ймовірність тієї або іншої події. Тут далеко не завжди вдається встановити остаточний розподіл, оскільки результати можуть бути суперечливими.

Третій етап (аналіз оцінки) полягає у дослідженні й узагальненні результатів опитування. Якщо ймовірність, представлена експертами, не узгоджується з аксіомами ймовірності, то доводиться до відома експертів і відповідь уточнюється так, щоб вони відповідали аксіомам.

Для деяких методів визначення суб'єктивної ймовірності третій етап виключається, оскільки сам метод полягає у виборі розподілу, що

підпорядковується аксіомам ймовірності, яке у тому або іншому сенсі найближче до оцінок експертів. Приклади таких методів – *метод головного значення для кінцевої множини незалежних подій* і *мінімаксний метод для залежних подій*. Особливу важливість третій етап набуває при *агрегації оцінок*, отриманих від групи експертів. Наприклад, у *методі Делфі*, після аналізу ймовірності, представленої окремими експертами, передбачається повторення другого етапу, тобто повторне опитування. Далі знову слідує третій етап, й, у разі потреби, процедура виконується ще раз.

2.4.2 Класифікація методів отримання суб'єктивної ймовірності

Методи визначення суб'єктивної ймовірності можна класифікувати залежно від форми поставлених перед експертами питань або від характеристик подій і випадкових величин, а також від числа експертів, що залучаються. У завданнях оцінки ризиків за умови невизначеності вимагається оцінювати ймовірність (можливість) станів зовнішнього середовища (невизначених факторів). Оскільки зовнішнє середовище може набувати лише одного значення із заданої множини, то при оцінці суб'єктивної ймовірності звичайно застосовують методи, призначені для множини неспільних подій. Серед методів, що служать для оцінки ймовірності у разі кінцевої множини несумісних подій, найбільш практичне значення мають три:

- *метод прямого приписування ймовірності;*
- *метод відношень;*
- *метод власного значення.*

У разі нескінченної множини несумісних подій:

- *метод мінливого інтервалу;*
- *метод фіксованого інтервалу*.

Для практичної реалізації вказаних методів потрібне їх детальне доопрацювання й адаптація до характеру вирішуваних завдань. Також знадобиться розробити та реалізувати конкретні алгоритми проведення опитування експертів за цими методами. Як доповнення до таких алгоритмів потрібні процедури графічного представлення даних, підготовлених експертом. Це дозволить експертові вносити необхідні коригування у свої колишні оцінки виходячи із загальної картини.

А для обробки ймовірності, представленої декількома експертами, слід створювати процедури агрегації ймовірності. До їх основи може бути покладено метод *зваженої суми*. Для кращої узгодженості оцінок експертів звичайно розробляють ітеративну процедуру проведення експертизи, засновану на методі Делфі.

Умовно методи знаходження суб'єктивної ймовірності можна поділити на наступні три групи (рис. 2.5).

Рисунок 2.5 – Методи отримання суб'єктивної ймовірності

Перша, найчисленніша група, – це прямі методи, що полягають у тому, що експерт відповідає на питання про ймовірність події. До них відносяться *метод мінливих інтервалів, метод фіксованих інтервалів, метод відношень, графічний метод, метод власного значення, методи оцінки параметрів розподілу* тощо. Незалежно від конкретного методу цієї групи експерт повинен оцінювати безпосередньо ймовірність подій.

Другу групу утворюють методи, в яких ймовірність подій виводиться з рішень експертів у гіпотетичній ситуації. Прикладом є *метод лотерей*, а також *метод рівноцінного кошику*. Формально кажучи, застосування методів другої групи вимагає від експерта порівняння не ймовірності як такої, а корисності альтернатив, за яких результат залежить від реалізації випадкової величини. Багато експертів зазначають зростаючу складність питань та найбільш істотні помилки при застосуванні цих методів порівняно з методами першої групи.

Третя група – це *гібридні методи*, що вимагають від експертів відповідей на питання як про ймовірність, так і про корисність. До гібридних методів відносяться деякі різновиди *методу лотерей*.

2.4.3 Методи отримання суб'єктивної ймовірності

Постановка завдання полягає у тому, що шляхом опитування експертів слід побудувати ймовірнісний розподіл на кінцевій множині несумісних (взаємовиключних) подій [34].

Пряма оцінка ймовірності подій. За цього методу експертові або групі експертів надається список усіх подій. Експерт повинен вказати послідовно ймовірність усіх подій. Можливі різні модифікації методу. В одній із

модифікацій пропонується спочатку обрати найбільш ймовірну подію зі запропонованого списку, а потім оцінити його ймовірність. Після цього подія із списку вилучається, а до списку, що залишився, застосовується вже описана процедура. Сума усієї отриманої ймовірності повинна дорівнювати одиниці.

Метод відношень. Експертові спочатку пропонується обрати найбільш ймовірну подію. Цій події приписується невідома ймовірність P_1. Потім експерт повинен оцінити відношення ймовірності усіх інших подій до ймовірності P_1 виділеної події (коефіцієнти $C_2,.., C_N$). З урахуванням того, що сума ймовірності дорівнює 1, складається рівняння:

$$P_1(1 + C_2 + C_3 + ... + C_N) = 1.$$

Вирішивши це рівняння та знайшовши величину P_1, можна обчислити шукану ймовірність.

Метод власного значення. Метод заснований на тому, що невідомий вектор ймовірності $(P_1,..., P_n)$ є власним вектором деякої спеціально побудованої матриці, що відповідає її найбільшому власному значенню. Спочатку експертові задається питання, яка з двох подій ймовірніше. Припустимо, що ймовірніше подія S_1. Потім експерта запитують, у скільки разів подія S_1 ймовірніша, ніж S_2. Отримане від експерта відношення записується на відповідне місце у матриці.

Метод рівноцінного кошика. Цей метод дозволяє отримати ймовірність виходячи з експертного порівняння корисності альтернатив. Припустимо, потрібно обчислити ймовірність деякої події S_1.

Визначимо будь-які два виграші, зокрема грошових, які істотно різні, наприклад: перший виграш – 1 млн. крб., а другий – 0 крб., та запропонуємо експертові на вибір участь у одній із двох лотерей. Перша лотерея полягає у тому, що виграш в 1 млн. крб. експерт отримує, якщо відбудеться подія S_1, а виграш у 0 крб. – якщо подія не відбувається.

Для організації другої лотереї уявимо собі гіпотетичний кошик, заповнений білими та чорними кулями, спочатку в рівній кількості, скажімо, по 50 куль кожного кольору.

Якщо вийнята куля біла, то учасникові дістається 1 млн. крб., якщо чорний – 0 крб. Експерта просять віддати перевагу однієї з двох лотерей. Якщо з точки зору експерта лотереї рівноцінні, робиться висновок про те, що ймовірність події S_1 дорівнює 0,5.

Якщо експерт обирає першу лотерею, то з кошика виймається частина чорних куль і замінюється тією ж кількістю білих.

Якщо перевага віддається другій лотереї, то частина білих куль замінюється чорними. В обох випадках експертові знову пропонується взяти участь в одній із двох лотерей. Змінюючи співвідношення куль у гіпотетичному кошику, домагаються рівноцінності двох лотерей. Тоді шукана ймовірність події S_1 дорівнює частці білих куль від загальної їх кількості.

2.4.4 Методи оцінок безперервних розподілів

Дані методи можна використати, наприклад, щоб знайти функцію розподілу (чи щільність розподілу) суб'єктивної ймовірності деякої безперервної випадкової величини [32]. Найчастіше для вирішення такого завдання застосовуються два методи, заснованих на опитуванні експертів: *метод мінливого інтервалу* та *метод фіксованого інтервалу*.

Метод мінливого інтервалу. Існує декілька модифікацій цього методу. Але для них загальною є вимога до експерта: вказати на множину значень випадкової величини такий інтервал, щоб ймовірність того, що випадкова величина набуває значення у вказаному інтервалі, дорівнювала заданій величині.

Наприклад, опитування експерта може будуватися за наступною схемою. Спочатку експерта просять вказати таке значення S_1 випадкової величини, за якого виявляються рівними дві ймовірності: того, що випадкова величина набуде значення менше S_1, і того, що вона набуде значення більше S_1. Набувши від експерта значення S_1, переходять до другого етапу. На цьому етапі в експерта запитують, за якого значення S_2 випадкової величини область значень більше S_1 поділиться на дві рівноймовірні частини. Так само поступають із областю значень менше S_1 і знаходять значення S_3.

Вслід за другим етапом проводиться третій етап, що полягає у знаходженні медіан кожного з ділянок, що утворилися. Цей процес не слід продовжувати занадто довго, оскільки за малих величин інтервалів зростає ймовірність помилки експерта. При використанні цього методу звичайно буває корисно повернутися до попередніх оцінок і проаналізувати їх несуперечність. У разі виявлення суперечностей експерт повинен змінити одну зі своїх колишніх оцінок.

У деяких варіантах методу мінливого інтервалу, перед експертом може бути поставлене завдання вказати дві точки на запропонованій множині значень випадкової величини, які розбивають цю множину на три рівноймовірні частини. За інших варіантів експерта можуть, наприклад, запитати, за якого значення випадкової величини S_1 ймовірність того, що випадкова величина набуде меншого значення, ніж S_1, дорівнює 0,1. Оцінки, отримані у такий спосіб, менше залежать одна від одної, тобто не відбувається накопичення помилки. У цьому й полягає їх перевага. Існують модифікації методу, засновані на припущенні, що для експерта простіше вказати точку, що ділить область на дві рівноймовірні частини, ніж точку, що відділяє область, відповідну ймовірності 0,1, від іншої множини. Таким чином, у разі застосування методу інтервалу, що змінюється, доводиться обирати між простотою порівняння та незалежністю отримуваних оцінок.

Метод фіксованого інтервалу. Відповідно до цього методу множина значень випадкової величини розбивається на інтервали й експерта просять оцінити ймовірність того, що випадкова величина набуде значення з цього інтервалу. Звичайно інтервали, за винятком крайніх зліва і справа, обираються

рівної довжини. Число інтервалів визначається з урахуванням необхідної точності та необхідного виду розподілу.

Після того, як експерт повідомив ймовірність усіх інтервалів, проводять перевірку отриманого розподілу.

Наприклад, якщо двом різним інтервалам приписана однакова ймовірність, можна запитати в експерта, чи дійсно вони рівноймовірні. Відносно інших інтервалів можна уточнити, чи дійсно один із них у стільки-то раз ймовірніший, ніж інший, як це випливає з приписаної цим інтервалам ймовірності. У результаті такого перегляду експерт може дещо підправити ймовірність.

Іноді метод фіксованого інтервалу застосовується спільно з методом інтервалу, що змінюється.

Так, можна спочатку запропонувати експертові визначити медіану, тобто таке значення випадкової величини, яке розбиває усю множину значень на дві рівноймовірні множини, а потім від знайденої медіани відкласти в обидві сторони рівні фіксовані інтервали.

Графічний метод. Метод дає надійні результати у тому випадку, коли експерт добре підготовлений до сприйняття графічної інформації про ймовірність. Полягає він у тому, що експерт повинен зображувати у графічній формі (у вигляді графіка функції розподілу або щільності ймовірності, у формі діаграми або графа) своє уявлення про ймовірність подій або про випадкову величину.

Часто загальний вигляд графіка відомий, а від експерта вимагається лише підібрати параметри розподілу. Графічний метод особливо корисний як допоміжний при аналізі ймовірності, знайденої будь-яким іншим способом.

Наприклад, функція розподілу може бути визначена методом фіксованого інтервалу, а потім її графік, а також графік функції щільності розподілу представляють експертові для остаточного доопрацювання.

Рекомендації для опитування експерта. Відомо, що суб’єктивна ймовірність, яка отримана експертним шляхом, істотно залежить від використаного методу. Зокрема, експерт нерідко схильний перебільшувати ймовірність найменш імовірної події, а також недооцінювати ймовірність найбільш імовірного або перебільшувати дисперсію оцінюваної випадкової величини. Розглянемо декілька рекомендацій, виконання яких дозволить коректно проводити опитування експерта за допомогою різних методів :

– необхідно навчити експерта процедурі проведення експертизи. Особливо це стосується експертів, що мають слабку підготовку з теорії ймовірності;

– потрібно усвідомлювати те, що сама процедура опитування експерта є лише однією ланкою в усьому процесі визначення ймовірності. Попередні кроки з вичленення подій і вибору відповідного методу такі ж важливі. Не можна нехтувати також і наступним аналізом отриманої ймовірності з метою можливого їх коригування;

– прагніть застосовувати об’єктивну інформацію щодо ймовірності подій, наприклад, дані про те, як такі події відбувалися у минулому. Ця інформація має бути доведена до експерта;

– для перевірки надійності представлених даних рекомендується звертатися до будь-яких інших методів знаходження суб'єктивної ймовірності або навіть до модифікації методів. Визначену різними методами ймовірність необхідно показати експерту для уточнення його оцінок;

– при виборі конкретного методу потрібно врахувати досвід роботи експерта з числовими показниками. І якщо такий досвід недостатній, то метод фіксованого інтервалу непридатний, оскільки припускає числові оцінки. Більш відповідним у цьому випадку буде метод мінливого інтервалу, оскільки у його рамках від експерта потрібно лише твердження про рівноймовірності двох інтервалів. У будь-якому випадку вживання знайомих експерту понять, фраз, питань і шкал полегшує можливості чисельного представлення ймовірності;

– завжди, коли це можливо, прагнуть отримувати суб'єктивну ймовірність від декількох експертів, а потім деяким чином агрегувати її в одну;

– складні методи, що вимагають значних зусиль від експерта, наприклад метод лотерей, краще не застосовувати, за винятком випадків, коли є серйозні аргументи на користь вибору цих методів.

Виконання цих рекомендацій дозволяє істотно поліпшити оцінки ймовірності.

Агрегація суб'єктивних ймовірностей. Проблема *агрегації* виникає у тому випадку, коли m експертів оцінює ймовірність на одній множині подій. Існують різні підходи до вирішення цієї задачі :

- індивідуальні оцінки розглядаються як випадкові величини на одному й тому ж імовірнісному просторі. Групова ймовірність є умовною ймовірністю події S_1 у припущенні, що індивідуальні оцінки дорівнюють $P_1,.., P_m$;

- у методі зваженої суми групова ймовірність знаходиться за формулою:

$$P = W_1 \times P_1 + ... + W_m \times P_m ,$$

де W_i – це ваги (коефіцієнти компетентності), приписані експерту i. Якщо оцінки P_i є незміщеними, то ваги можна приймати так, щоб мінімізувати дисперсію величини P. На практиці ваги слід обирати на основі аналізу оцінок експертів, отриманих під час попередніх експертиз;

- у підході, заснованому на методі Делфі, суб'єктивна ймовірність представлена експертами, доводиться до відомості усіх експертів, після чого експерти знову повідомляють свою ймовірність. Таким чином виконується ітеративна процедура, яка дозволяє кожному окремому експерту скоригувати свої оцінки після ознайомлення з оцінками інших.

2.4.5 Методи теорії корисності

Постановка задачі вибору за умов ризику. При вирішенні завдань вибору за умов невизначеності і, зокрема, *завдання оцінки ризиків* найбільш обґрунтований підхід, що базується на теорії корисності. Нині теорія корисності досягла високого рівня розвитку [32]. Питання практичного застосування цієї теорії добре висвітлені у літературі: введені поняття та

досліджені властивості, що дозволяють розбити процес побудови функції (одновимірною) корисності на етапи та зробити його максимально ефективним; розроблені методи побудови, що спираються на ці поняття та властивості. Теоретичні результати та методи практичної побудови функції одновимірної корисності досить апробовані при вирішенні різних завдань ухвалення рішень, і їх доцільно застосовувати у різних методиках оцінювання ризиків.

Розглянемо наступну постановку завдання.

Задано множина *S* можливих детермінованих результатів (наслідків). У ролі цієї множини найчастіше виступає множина значень скалярного або векторного критерію, за допомогою якого оцінюється ефективність (якість і тому подібне) варіантів рішень (стратегій, планів, альтернатив і так далі). Результат, що досягається, залежить не лише від варіанта рішення, що реалізується, але й від того, якого значення набудуть невизначені (випадкові) фактори, розподіли ймовірності яких відомі. Тому зручно вважати, що кожному варіанту рішення з допустимої множини ставиться у відповідність деяка ймовірнісна міра, задана на множині *S* (наприклад, розподіл імовірності або щільність імовірності). Той, хто приймає рішення повинен обрати найкращий варіант із *S* або, що еквівалентно, зробити вибір на множині відповідних елементів цієї підмножини ймовірнісних заходів.

Відомі *два основні підходи* до ухвалення рішень при ризику:

- підхід, що базується на застосуванні так званих об’єктивних критеріїв вибору (залучення різних моделей стохастичного програмування, застосування критеріїв типу математичного очікування, дисперсії і так далі);
- заснований на отриманні та використанні інформації суб’єктивного характеру, відомостей щодо структури переваг, особи, що приймає рішення (ОПР), у тому числі про її відношення до ризику.

Як показують численні дослідження, методи, що реалізують перший підхід, менш надійні, оскільки часто неадекватно описують ситуацію. Наприклад, дві дії, що характеризуються однаковим математичним очікуванням виграшу, для ОПР можуть не бути рівноцінними. Тому далі розглядатимемо суб’єктивний підхід до ухвалення рішень при ризику. Серед методів цього підходу найбільш поширені й обґрунтовані ті, які спираються на аксіоматичні побудови: переваги формалізуються за допомогою деякої моделі, та формулюються умови, що забезпечують її існування. Важливим напрямом у розвитку таких методів служить *теорія корисності*, заснована на представленні структури переваг ОПР за допомогою однієї або декількох дійсних функцій.

Деякі відомості з теорії корисності. Вперше умови, необхідні та достатні для представлення переваг ЛПР на множині ймовірнісних заходів за допомогою лінійної дійсної значущої функції, так званій *функції корисності*, були отримані Нейманом і Моргенштерном у 1947 р. Нині прийнято поділяти ці умови на дві групи.

Перша група умов торкається множини усіх даних імовірнісних заходів і у сучасній літературі просто включаються у визначення цієї значної кількості, званої множиною ймовірнісних сумішей.

Друга група умов торкається опису відношення переваги на множині сумішей. Саме вона відома нині як система аксіом Неймана-Моргенштерна, або аксіом класичного представлення корисності. Оцінюється лотерея *L*:

$$p(A) + (1 - p)(B),$$

де *A* – виграш з імовірністю *p*; *B* – виграш з імовірністю (1 – виграш з імовірністю *p).*

Щоб визначити величину корисності, що відображає відношення індивіда до будь-якого виграшу *X*, ми його запитуємо або спостерігаємо за його поведінкою; у цьому випадку ми встановлюємо, за якої ймовірності йому байдуже, що обрати - виграш з імовірністю стандартний лотерейний білет *L(p')* або *X*. Оцінка корисності *U* зводиться до визначення корисності *U(L(p'))* на основі вираження, сформульованого Нейманом і Моргенштерном. Крім того, Нейман і Моргенштерн постулювали п’ять аксіом, достатніх, щоб гарантувати існування такої функції корисності, за якої ранжирування лотерей за їх очікуваною корисністю повністю відповідає дійсним перевагам індивіда.

Розглянемо *застосування методів теорії корисності*. Вимога лінійності функції корисності у класичному представленні (забезпечуване також майже в усіх представленнях, розроблених пізніше) пов’язана з його застосуванням для вирішення практичних завдань. Річ у тому, що при виконанні низки додаткових припущень умова лінійності дає можливість виразити функцію корисності на множині ймовірнісних сумішей у вигляді математичного очікування її значень на множині детермінованих результатів. Це має велике практичне значення, оскільки дозволяє звести завдання побудови функції корисності на множині сумішей до завдання її побудови на множині результатів.

Класифікуємо *функції корисності* за їх схильністю до ризику.

Як правило, методи практичної побудови функції корисності спираються на порівняння простих лотерей. Розглядаються також вироджені лотереї, що ототожнюються з детермінованими результатами.

У зв’язку з цим усі методи *поділяються на два класи*: методи, засновані на порівнянні простої лотереї та детермінованого результату, та методи, що базуються на порівнянні двох невироджених простих лотерей. Кожен із цих класів, у свою чергу, розпадається на декілька груп. Наприклад, методи простої лотереї припускають порівняння лотереї *L*: $p(A) + (1 - p)(B)$ з детермінованим результатом *S*.

Методи порівняння за перевагою базуються на визначенні ризику для простої лотереї *L* і детермінованого результату *S*. Існують два підходи до реалізації подібних методів. Один із них включає попереднє дослідження відношення до ризику та перевірки узгодженості набутих значень функції корисності. При цьому кожне порівняння за перевагою задає лінійне обмеження на функцію корисності. Таким чином, можуть бути отримані скільки завгодно вузькі межі, в яких знаходиться шукана допустима функція корисності.

Другий підхід заснований на сходженні до точки байдужості.

Інші методи цього класу базуються на визначенні різного роду еквівалентів. Визначення еквівалента полягає у знаходженні точки байдужості між лотереєю

та детермінованим результатом. Є декілька підходів до оцінювання точки байдужості :

- пряма оцінка – ОПР вказує точне значення точки байдужості;
- метод границь – встановлення нижніх і верхніх границь для точки байдужості.
- сходження – послідовне коригування до отримання точки байдужості.

Багатовимірні функції корисності. У більшості завдань ухвалення рішень, у тому числі у завданнях аналізу ризиків, результати оцінюються не одним, а багатьма критеріями. За умов імовірнісної невизначеності порівняння варіантів багатокритерійних вирішень зводиться до порівняння за перевагою відповідних розподілів ймовірності на множині векторних оцінок (значень векторного критерію). На такі завдання повністю поширюються основні положення теорії корисності, що стосуються, зокрема, існування функції корисності. Проте при цьому функція корисності виявляється *багатовимірною*, тобто має векторний аргумент.

З формальної точки зору до багатокритеріальних завдань теж застосовні методи побудови (одновимірної) функції корисності, що описані вище. Проте безпосереднє використання таких методів звичайно неможливе внаслідок того, що особа, яка приймає рішення, не спроможна порівнювати лотереї з багатовимірними (багатокритерійними) результатами.

Основним шляхом побудови багатовимірної функції корисності є *декомпозиція багатовимірної структури переваг* на низку підструктур меншої розмірності (зокрема, одновимірних) і, відповідно, представлення багатовимірної функції корисності у вигляді складеної (складної) функції – «згортки» малорозмірних функцій корисності. Структура такої складної функції залежить від взаємозв’язків підструктур структури переваг.

За такого роду декомпозиції побудова багатовимірної функції корисності зводиться до побудови відповідних маловимірних (найпростіше, звичайно, одновимірних) умовних функцій корисності, а також оцінювання ряду числових параметрів, визначуваних конструкцією складеної функції згортки.

Декомпозиція багатовимірної структури переваг ЛПР на множині ймовірнісних розподілів випадкової векторної оцінки здійснюється за рахунок використання специфічних особливостей цієї структури. Звичайно ці особливості пов’язані з будь-якими видами незалежності одних (груп) критеріїв від інших. Оскільки умови незалежності не завжди виконуються у повному обсязі, вказаний підхід стали узагальнювати за рахунок «*розщеплювання» шкал* (точніше, носіїв шкал) критеріїв і відповідного розкладання структури переваг на підструктури, для кожної з яких справедливі певні види незалежності.

Існують і принципово інші підходи до моделювання багатовимірної корисності. Вони включають цілеспрямовану перебудову самої початкової математичної моделі ситуації на основі змістовного аналізу конкретної проблеми ухвалення рішень. Прикладом служить підхід, що припускає розщеплювання початкових критеріїв – представлення їх через такі, що

додатково вводяться так, щоб перетворена структура переваг мала деякі властивості незалежності.

Далі розглянемо основні результати декомпозиції структури переваг і методи отримання інформації про переваги, необхідні для побудови відповідних багатовимірних функцій корисності.

Методи та порядок побудови багатовимірних функцій корисності. Функція корисності виражає переваги особи, що приймає рішення (ОПР) на множині випадкових результатів і тому повинна будуватися на основі інформації про такі переваги. При цьому конкретний вид інформації визначається допущеннями, що висуваються відносно особливостей структури переваг (тобто конкретними видами незалежності для різних факторів), і відповідним функціональним представленням корисності.

Рекомендується структурувати систему переваг за допомогою функції багатовимірної корисності, дотримуючись послідовно п’яти стадій:

1) Введення термінології й основних допущень.
2) Перевірка необхідних умов допущень про незалежність.
3) Побудова умовних функцій корисності.
4) Знаходження значень констант, що задають масштаб шкали.
5) Перевірка узгодженості.

На першій стадії ОПР знайомиться з програмним забезпеченням, що реалізує аналітичну модель, критеріями та їх шкалами, а також необхідними поняттями з теорії корисності (лотерея, ймовірність, функція корисності, очікувана корисність і тому подібне), причому пояснення мають бути гранично простими, сформульованими зрозумілою ОПР мовою й одночасно досить чіткою та суворою.

Перевірка допущень щодо незалежності. Припущення щодо незалежності фактора (критерію) K_i від K_j за корисністю перевіряється, наприклад, оцінкою детермінованих еквівалентів для низки лотерей, значення яких покривають досить щільно простір результатів. Якщо переваги виявляються майже однаковими для різних фіксованих K_j (про справедливість висновку відносно постійності можна поцікавитися в особи, що приймає рішення), то допущення, що перевіряється, про незалежність можна прийняти. Пряма перевірка незалежності корисності K_i від K_j ускладнена тим, що фактично вона включає n факторів різної розмірності від їх доповнень, і перевірити справедливість їх усіх практично не можна вже при $n = 5$. Проте ця проблема різко спрощується при зменшенні розмірності незалежних змінних.

Обчислення значень констант шкал. Загальний підхід до вирішення цієї задачі полягає у складанні системи необхідного числа рівнянь, що містять ці константи як невідомі, шляхом розгляду лотерейних детермінованих еквівалентів, а також невипадкових результатів.

Перевірка узгодженості. Можливі три підходи до вирішення даної проблеми. Перший заснований на проведенні попарних порівнянь різних наслідків. Такого роду перевірка повторюється кілька разів, щоб з’явилася впевненість в її результатах. При цьому рекомендується починати з простих

порівнянь і поступово переходити до складніших. Другий підхід полягає у пред'явленні особі, що приймає рішення, графіків кривих умовно рівної переваги. Третій пов'язаний із з'ясуванням схильності особи, що приймає рішення, до ризику.

Якщо у процесі аналізу узгодженості виявляються суперечності, необхідно повторити відповідні стадії процедури побудови функції корисності до отримання деякої функції корисності обраного виду або ж перейти до побудови функції корисності загальнішого вигляду.

Рекомендації до побудови багатовимірних функцій корисності. Основним підходом до побудови функцій багатовимірної (багатокритерійної) корисності є *декомпозиційний.* Початкове завдання великої розмірності зводиться до низки завдань меншої розмірності, тобто встановлюються умовні (одновимірні) функції корисності та шкалювальні константи у функції багатовимірної корисності, вид якої залежить від допущень, що приймаються, про незалежність певних факторів (критеріїв) від усіх інших.

Складний (з великим числом тих, що підлягають відшукуванню параметрів – умовних функцій корисності та шкалювальних коефіцієнтів) вид функції багатовимірної корисності забезпечує достатню свободу та гнучкість для апроксимації структури переваг, проте робить надто трудомісткою процедуру побудови такої функції. Прикладом служить полілінійна функція корисності. Простий (що містить незначне число параметрів) вид функції корисності сильно спрощує процедуру її побудови, але він заснований на надто жорстких припущеннях про незалежність, які рідко виконуються на практиці, і тому такі функції звичайно погано апроксимують структури переваг. Приклад – адитивна функція корисності.

Найбільш перспективними є види функції корисності, що надають можливість підтримувати розумний компроміс між суперечливими вимогами до достатньої гнучкості функції та до простоти її побудови. Наприклад, до таких функцій відноситься мультиплікативна функція корисності.

2.5 Технологія оцінювання ризиків

2.5.1 Кількісні й якісні оцінки ризиків

Ризик – це ймовірна подія, яка може виникнути у процесі виконання робіт над проектом і яка негативно впливає на один або декілька з ключових факторів успішного проекту.

Система управління ризиками – комплекс засобів автоматизації, нормативної й організаційної документації, робочих процедур, штатних позицій і конкретних співробітників, тих, що їх займають, призначений для управління ризиками у рамках проектної діяльності організації.

У будь-якій методиці необхідно *ідентифікувати ризики*, як варіант, їх складові (загрози й уразливості). Природним при цьому є вимога повноти списку. Складність завдання складання списку та доказу його повноти залежить від того, які вимоги пред'являються до деталізації списку.

В даний час використовуються різні методи *оцінки інформаційних ризиків* і управління ними. Оцінка інформаційних ризиків може бути виконана відповідно до наступного плану [31]:

0001) Ідентифікація та кількісна оцінка інформаційних значимих ресурсів.

2) Оцінювання можливих загроз.

3) Оцінювання існуючих уразливостей.

4) Оцінювання ефективності засобів забезпечення інформаційної безпеки.

Передбачається, що значимі вразливі інформаційні ресурси піддаються ризику, якщо по відношенню до них існують будь-які загрози. Іншими словами, ризики характеризують небезпеку, яка може загрожувати компонентам корпоративної інформаційної системи. При цьому інформаційні ризики залежать від:

– показників цінності інформаційних ресурсів;

– ймовірності реалізації загроз для ресурсів;

– ефективності існуючих або планованих засобів забезпечення інформаційної безпеки.

Мета оцінювання ризиків полягає у визначенні характеристик ризиків корпоративної інформаційної системи та її ресурсів. Після оцінки ризиків можна обрати засоби, що забезпечують бажаний рівень інформаційної безпеки. При оцінюванні ризиків враховуються такі фактори, як цінність ресурсів, значущість загроз і вразливості, ефективність наявних і планованих засобів захисту. Самі показники ресурсів, значущості загроз і вразливості, ефективність засобів захисту можуть бути встановлені як кількісними методами (наприклад, при знаходженні вартісних характеристик), так і якісними, скажімо, з урахуванням штатних або надзвичайно небезпечних нештатних дій зовнішнього середовища.

Можливість реалізації загрози для деякого ресурсу оцінюється ймовірністю її реалізації протягом заданого відрізку часу. При цьому ймовірність того, що загроза реалізується, визначається наступними основними факторами:

- привабливістю ресурсу (враховується при розгляді загрози від умисної дії з боку людини);

- можливістю використання ресурсу для здобуття доходу (також у разі загрози від умисної дії з боку людини);

- технічними можливостями реалізації загрози за умисної дії з боку людини;

- мірою легкості, з якою вразливість може бути використана.

Раніше було розглянуто виконання оцінки ймовірностей (розд. 2.4).

Уточнимо визначення цього терміну.

Об'єктивна та суб'єктивна ймовірність. Термін «ймовірність» має декілька різних значень. Найчастіше зустрічаються два тлумачення, які позначаються поєднанням «*об'єктивна ймовірність*» і «*суб'єктивна ймовірність*». Під об'єктивною (інколи званою фізичною) ймовірністю розуміється відносна частота появи будь-якої події у загальному обсязі спостережень або відношення числа сприятливих результатів до загальної кількості спостережень. Це поняття застосовується при аналізі результатів

великого числа спостережень, що мало місце у минулому, а також отриманих як наслідок із моделей, що описують деякі процеси.

Під *суб'єктивною ймовірністю* мається на увазі міра впевненості деякої людини або групи людей у тому, що дана подія насправді матиме місце. Як міра упевненості у можливості настання події суб'єктивна ймовірність може бути формалізовано представлена різними способами: ймовірнісним розподілом на множині подій, бінарним відношенням на множині подій, не повністю заданим імовірнісним розподілом або бінарним відношенням та іншими способами. Найчастіше суб'єктивна ймовірність є ймовірнісною мірою, отриманою експертним шляхом. Саме у цьому сенсі ми й будемо розуміти суб'єктивну ймовірність.

Суб'єктивна ймовірність у сучасних роботах в області системного аналізу не просто дозволяє визначити міру впевненості на множині подій, а ув'язується з системою переваг особи, що приймає рішення (ОПР), і зрештою зі функцією корисності, що відображає його переваги з множини альтернатив. Тісний зв'язок між *суб'єктивною ймовірністю* та *корисністю* використовується при побудові деяких методів отримання суб'єктивної ймовірності.

2.5.2. Вимірювання ризиків

В даний час відома множина табличних методів оцінки інформаційних ризиків. Розглянемо декілька прикладів подібних методів, рекомендованих стандартами у галузі інформаційної безпеки [35]. Важливо, що за цих методів кількісні показники наявних або пропонованих фізичних ресурсів оцінюються з точки зору вартості їх заміни або відновлення працездатності ресурсу. А існуючі або передбачувані програмні ресурси оцінюються так само, як і фізичні, тобто шляхом визначення витрат на їх придбання або відновлення. Якщо виявиться, що до будь-якого прикладного програмного забезпечення пред'являються особливі вимоги до конфіденційності або цілісності, наприклад, вихідний текст програмного забезпечення має високу комерційну цінність, то оцінка цього ресурсу проводиться у вартісному вираженні за тією ж схемою, що й для інформаційних ресурсів.

Кількісні показники інформаційних ресурсів рекомендується оцінювати за результатами опитувань співробітників – власників інформації, тобто посадових осіб, які спроможні визначити цінність інформації, її характеристики та міру критичності виходячи з фактичного положення справ. На основі результатів опитувань оцінюються показники та міра критичності інформаційних ресурсів у разі несанкціонованого ознайомлення з конфіденційною інформацією, порушення її цілісності або доступності.

Оцінка ризиків. Вимірюється рівень ризиків порушення конфіденційності, цілісності та доступності інформаційних ресурсів. Рівень ризику залежить від рівнів загроз, уразливості та ціни можливих наслідків.

Існують різні методики виміру ризиків. Найчастіше використовуються табличні методи.

Ризики можуть бути оцінені за допомогою *кількісних шкал*. Це дасть можливість спростити аналіз за критерієм «вартість-ефективність» пропонованих контрзаходів. Проте у цьому випадку пред'являються вищі вимоги до шкал виміру вихідних даних і перевірки адекватності прийнятої моделі.

Якщо застосовуються *якісні методи*, можливі ризики порушення інформаційної безпеки мають бути ранжировані за мірою їх небезпеки з врахуванням таких факторів, як ціна можливих втрат, рівень загрози й уразливості.

Вибір шкали для оцінки параметрів ризиків. Під оцінкою параметрів ризиків розуміється визначення ймовірності реалізації потенційної вразливості, яка приведе до інциденту.

Типовою (найбільш поширеною) шкалою є *якісна* (бальна) шкала з декількома градаціями, наприклад: низький, середній і високий рівень. Оцінка проводиться експертом із урахуванням низки об'єктивних факторів. Рівні ризиків встановлюються, наприклад, як у табл. 2.5, або як у табл. 2.6.

Таблиця 2.5 – Приклад якісної шкали для оцінки ризику

Рівень ризиків	**Визначення**
Високий	Джерело загрози (порушник) має дуже високий рівень мотивації, існуючі методи зменшення вразливості малоефективні
Середній	Джерело загрози (порушник) має високий рівень мотивації, проте використовуються ефективні методи зменшення вразливості
Низький	Джерело загрози (порушник) має низький рівень мотивації, або існують надзвичайно ефективні методи зменшення вразливості

Приклад оцінки ризиків за двома факторами. У простому випадку проводиться оцінка двох факторів: ймовірність випадку та ступінь можливих наслідків. Звичайно вважається, що ризик тим більше, чим більше ймовірність випадку та ступінь наслідків. Загальна ідея може бути виражена формулою [31]:

$$R = P_в * C, \qquad (2.6)$$

де R – величина ризику; $P_в$ – ймовірність випадку; C – ступінь наслідків.

У таблиці можна наочно відобразити зв'язок факторів негативної дії (показників ресурсів) та ймовірності реалізації загрози з урахуванням показників уразливості. На першому кроці оцінюється негативна дія за заздалегідь визначеною шкалою, наприклад від 1 до 5, для кожного ресурсу, якому загрожує небезпека (II колонка у табл. 2.6).

Таблиця 2.6 – Оцінка ступеня наслідків порушення режиму інформаційної безпеки

Рівень ступеня наслідків порушення режиму ІБ	**Визначення**
Високий	Випадок надає сильну (катастрофічну) дію на діяльність організації, що виражається в одному або декількох проявах: - значна сума (має бути конкретизована) прямих фінансових втрат; - істотний збиток здоров'ю персоналу (загибель, інвалідність або необхідність тривалого лікування співробітника); - втрата репутації, що привела до істотного зниження ділової активності організації; - дезорганізація діяльності на тривалий (конкретизується) період часу
Середній	Випадок приводить до помітних негативних результатів, що виражаються в одному або декількох проявах: - помітна сума (має бути конкретизована) прямих фінансових втрат; - втрата репутації, яка може викликати зменшення потоку замовлень і негативну реакцію ділових партнерів; - неприємності з боку державних органів, внаслідок чого знизилася ділова активність
Низький	Випадок супроводиться незначними негативними наслідками, що виражаються в одному або декількох проявах: - незначна сума (має бути конкретизована) прямих фінансових втрат; - затримки у роботі деяких служб або дезорганізація діяльності на нетривалий період часу; - необхідність відновлення інформаційних ресурсів

На другому кроці за заданою шкалою, наприклад від 1 до 5, оцінюється ймовірність реалізації кожної загрози.

На третьому кроці обчислюється показник ризику. У простому варіанті методики це робиться шляхом множення (M x N). Необхідно пам'ятати, що операція множення визначена для кількісних шкал. Для рангових (якісних) шкал виміру показник ризику, відповідний ситуації $M = 1$, $N = 3$, зовсім не обов'язково еквівалентний випадку $M = 3$, $N = 1$. Відповідно, має бути розроблена методика оцінювання показників ризиків стосовно конкретної організації.

На четвертому кроці загрози ранжируються за значеннями їх фактора ризику. У даному прикладі для найменшої негативної дії та для найменшої можливості реалізації загрози обрано показник 1 (табл. 2.7).

Дана процедура дозволяє порівнювати та ранжирувати загрози з різними негативними діями та ймовірністю реалізації. У разі потреби додатково можуть братися до уваги вартісні показники.

Таблиця 2.7 – Ранжирування ризиків

Дескриптор загрози	**Ймовірність випадку (*M*)**	**Ціна втрати (*N*)**	**Показник ризику (суб'єктивна оцінка)**	**Ранг ризику**
Загроза A	5	2	10	2
Загроза B	2	4	8	3
Загроза C	3	5	15	1
Загроза D	1	3	3	5
Загроза E	4	1	4	4
Загроза F	2	4	8	3

Розподіл ризиків на прийнятні таі неприйнятні. Інший спосіб оцінювання ризиків полягає у розподілі їх лише на прийнятні та неприйнятні ризики. Підхід ґрунтується на тому, що кількісні показники ризиків служать лише для того, щоб їх упорядкувати та визначити, які дії необхідні у першу чергу. Але цього можна досягти з меншими витратами.

Матриця, використана у даному підході, містить не числа, а лише символи Д (ризик допустимий) і Н (ризик недопустимий). Наприклад, матриця може мати вигляд табл. 2.8.

Питання про те, як провести межу між прийнятними та неприйнятними ризиками, залишається на розсуд аналітика, що готує дану таблицю, та керівних фахівців у області інформаційної безпеки.

Приклад оцінки ризиків за трьома факторами. Ймовірність випадку, яка у даному підході може бути об'єктивною або суб'єктивною величиною, залежить від рівнів (ймовірності) загроз і вразливості:

$$P_B = P_З * P_У, \qquad (2.7)$$

де $P_з$ – ймовірність загрози, $P_у$ – ймовірність уразливості.

Таблиця 2.8 – Розділення ризиків на прийнятних і неприйнятних

Показник цінності ресурсу	**Показник можливості реалізації загрози**				
	0	1	2	3	4
0	Д	Д	Д	Д	Н
1	Д	Д	Д	Н	Н
2	Д	Д	Н	Н	Н
3	Д	Н	Н	Н	Н
4	Н	Н	Н	Н	Н

Відповідно, ризик розраховується таким чином:

$$R = P_З * P_У * C, \qquad (2.8)$$

де, R – величина ризику, C – ціна втрати.

Даний вираз можна розглядати як математичну формулу, якщо використовуються кількісні шкали, або як формулювання загальної ідеї, якщо хоча б одна зі шкал якісна. В останньому випадку застосовуються різного роду табличні методи для розрахунку ризику залежно від трьох факторів.

За кожною групою ресурсів, пов'язаною з даною загрозою, оцінюється рівень загрози (ймовірність реалізації) та рівень уразливості (міра легкості, з якою реалізована загроза, здатна привести до негативної дії). Оцінювання проводиться в якісних шкалах.

Спочатку визначимо рівні загроз, уразливості, ступені наслідків і ризиків. Рівні загроз:

– низький (Н) - реалізація даної загрози малоймовірна, за останні два роки подібних випадків не зафіксовано;

– середній (С) - загроза може реалізуватися протягом одного року з імовірністю близько 0,3;

– високий (В) - загроза, швидше за все, реалізується протягом року і, можливо, не один раз.

Рівні вразливості:

– низький (Н) - захищеність системи дуже висока, реалізація загроз майже ніколи не наводить до випадку порушення безпеки;

– середній (С) - захищеність системи середня, реалізація близько 30% загроз наводить до випадку порушення безпеки;

– високий (В) - захищеність системи низька, реалізація загрози практично завжди наводить до випадку порушення безпеки.

Показник негативної дії (ступінь наслідків). Використаємо наведену класифікацію наслідків:

1) Negligible (незначний – менше 800 грн).

2) Minor (низький – менше 8000 грн).

3) Moderate (середній – менше 80 000 грн).

4) Serious (високий – істотний негативний вплив на бізнес).

5) Critical (надвисокий – катастрофічна дія, можливе припинення функціонування системи).

Рівні ризиків. Показник ризику вимірюється за шкалою від 0 до 8, рівні ризику визначаються таким чином:

0 – відсутній ризик;

1 – ризик, яким можна знехтувати. Ситуації, за яких подія настає, практично виключені, а наслідки незначні, втрати менше 800 грн;

2 – ризик незначний. Подія настає рідко, наслідки (втрати) знаходяться у допустимих межах (не більше 8000 грн);

…

8 – ризик дуже високий. Подія, швидше за все, настане, і наслідки будуть катастрофічними (можливе повне припинення діяльності організації).

Прикладом таблиці, за допомогою якої задається значення рівня ризику залежно від рівнів загроз і вразливості за фіксованої вартості втрат (Moderate – виділено маркером), є табл. 2.9.

Таблиця 2.9 – Визначення рівня ризику залежно від рівнів загроз і вразливості

Міра серйозності випадку (ціна втрати)	**Рівень загрози**								
	Низький			Середній			Високий		
	Рівні вразливості			Рівні вразливості			Рівні вразливості		
	Н	С	В	Н	С	В	Н	С	В
Negligible	0	1	2	1	2	3	2	3	4
Minor	1	2	3	2	3	4	3	4	5
Moderate	2	3	4	3	4	5	4	5	6
Serious	3	4	5	4	5	6	5	6	7
Critical	4	5	6	5	6	7	6	7	8

Такі таблиці використовуються як у «паперових» варіантах методик оцінки ризиків, так й у різного роду інструментальних засобах, програмному забезпеченні аналізу ризиків.

2.5.3 Технологія оцінки загроз і вразливості

Як правило, для оцінки загроз і вразливості застосовуються різні методи, в основі яких можуть лежати:

– експертні оцінки;
– статистичні дані;
– облік факторів, що впливають на рівні загроз і вразливості.

Найбільш поширений у даний час підхід, заснований на обліку різних факторів, що впливають на рівні загроз і вразливості. Він дозволяє абстрагуватися від малоістотних технічних деталей, взяти до уваги не лише програмно - технічні, але й інші аспекти. Нижче показано приклад реалізації подібного підходу, використаного у методі CRAMM 4.0 для одного з класів ризиків. Структуру експертної оцінки наведено на рис. 2.6.

За непрямими факторами запропоновані питання та декілька фіксованих варіантів відповідей, які «коштують» певну кількість балів. Підсумкова оцінка загрози й уразливості даного класу визначається шляхом підсумування балів.

Тест для оцінки загрози

1. Скільки разів за останні три роки співробітники організації намагалися отримати несанкціонований доступ до інформації, що зберігається в інформаційній системі, з використанням прав інших користувачів? Варіанти відповідей:

а) жодного разу;
б) один або двічі;
в) у середньому один раз на рік;
г) у середньому частіше за один раз на рік;
д) невідомо.

2. Яка тенденція у статистиці такого роду спроб несанкціонованого проникнення в інформаційну систему? Варіанти відповідей:

а) до зростання;
б) залишатися постійно;
в) до зниження.

Рисунок 2.6 – Структура експертної оцінки загроз і вразливостей

3. Чи зберігається в інформаційній системі інформація (наприклад, особисті справи), яка може представляти інтерес для співробітників організації та спонукати до несанкціонованого доступу до неї? Варіанти відповідей:
а) так;
б) немає.
4. Чи відомі випадки нападу, загроз, шантажу, тиски на співробітників з боку сторонніх осіб? Варіанти відповідей:
а) так;
б) немає.
5. Чи є серед персоналу групи осіб або окремі особи з недостатньо високими моральними якостями? Варіанти відповідей:
а) ні, всі співробітники відрізняються високою чесністю та порядністю;
б) існують групи осіб й окремі особи з недостатньо високими моральними якостями, але це навряд чи може спровокувати їх на несанкціоноване використовування системи;

в) існують групи осіб й окремі особи з настільки низькими моральними якостями, що це підвищує ймовірність несанкціонованого використання системи співробітниками.

6. Чи зберігається у системі інформація, несанкціонована зміна якої може принести пряму вигоду співробітникам? Варіанти відповідей:

а) так;

б) немає.

7. Чи передбачена в інформаційній системі підтримка користувачів, що володіють технічними можливостями зробити подібні дії? Варіанти відповідей:

а) немає;

б) так.

8. Чи існують інші способи перегляду інформації, що дозволяють зловмисникові дістатися до неї простішими методами, ніж із використанням «маскараду»? Варіанти відповідей:

а) так;

б) немає.

9. Чи є інші способи несанкціонованої зміни інформації, що дозволяють зловмисникові досягти бажаного результату простішими методами, ніж із використанням «маскараду»? Варіанти відповідей:

а) так;

б) немає.

10. Скільки разів за останні три роки співробітники намагалися дістати несанкціонований доступ до інформації, що зберігається в інших подібних системах у вашій організації? Варіанти відповідей:

а) жодного разу;

б) один або двічі;

в) у середньому один раз на рік;

г) у середньому частіше за один раз на рік;

д) невідомо.

Підсумуємо кількість балів згідно з табл. 2.10 та зведемо результати даних у табл. 2.11:

Таблиця 2.10 – Кількість балів для оцінки міри загрози

Варіант відповіді	**Кількість балів**									
	1	2	3	4	5	6	7	8	9	10
а	0	10	5	10	0	5	0	10	10	0
б	10	0	0	0	5	0	5	0	0	5
в	20	10	-	-	10	-	-	-	-	10
г	30	-	-	-	-	-	-	-	-	15
д	10	-	-	-	-	-	-	-	-	10

Таблиця 2.11 – Міра загрози при кількості балів

Сума балів	Міра загрози
до 9	дуже низька
від 10 до 19	низька
від 20 до 29	середня
від 30 до 39	висока
від 40 і більше	дуже висока

Тест для оцінки вразливості

1. Скільки людей мають право користуватися інформаційною системою? Варіанти відповідей:

а) від 1 до 10;

б) від 11 до 50;

в) від 51 до 200;

г) від 200 до 1000;

д) понад 1000.

2. Чи буде керівництву відомо про те, що співробітники, які працюють під його керівництвом, поводяться незвичайним чином? Варіанти відповідей:

а) так;

б) немає.

3. Які пристрої та програми доступні користувачам? Варіанти відповідей:

а) лише термінали або мережні контролери, відповідальні за надання та маршрутизацію інформації, але не за передачу даних;

б) лише стандартні офісні пристрої та програми, а також керовані за допомогою меню службові прикладні програми;

в) користувачі можуть отримати доступ до операційної системи, але не до компіляторів;

d) користувачі можуть отримати доступ до компіляторів.

4. Чи можливі ситуації, коли співробітникам, попередженим про майбутнє скорочення або звільнення, вирішується логічний доступ до інформаційної системи? Варіанти відповідей:

а) так;

б) немає.

5. Які у середньому розміри робочих груп співробітників підрозділів, що призначені для обслуговування користувачів, які мають доступ до інформаційної системи? Варіанти відповідей:

а) менше 10 чоловік;

б) від 11 до 20 чоловік;

в) понад 20 чоловік.

6. Чи стане факт зміни даних, що зберігаються в інформаційній системі, очевидним відразу для декількох чоловік (внаслідок чого його буде важко приховати)? Варіанти відповідей:

а) так;

б) ні.

7. Наскільки великі офіційно надані користувачам можливості з перегляду тих даних, що зберігаються у системі? Варіанти відповідей:

а) офіційне право надане всім користувачам;

б) офіційне право надане лише деяким користувачам.

8. Наскільки необхідно користувачам знати всю інформацію, що зберігається у системі? Варіанти відповідей:

а) всім користувачам необхідно знати всю інформацію;

б) окремим користувачам необхідно знати інформацію, що лише відноситься до них.

Підсумуємо кількість балів згідно з табл. 2.12 та зведемо результати даних у табл. 2.13:

Таблиця 2.12 – Кількість балів для оцінки міри вразливості

Варіант відповіді	**Кількість балів**							
	1	2	3	4	5	6	7	8
а	0	0	5	10	0	0	2	4
б	4	10	0	0	5	10	0	0
в	10	-	5	-	10	-	-	-
г	14	-	10	-	-	-	-	-
д	20	-	-	-	-	-	-	-

Таблиця 2.13 – Міра вразливості при кількості балів

Сума балів	**Міра вразливості**
до 9	низька
від 10 до 19	середня
20 і більше	висока

Можливості й обмеження даного підходу. Безперечною перевагою даного підходу є можливість обліку багатьох непрямих факторів (не лише технічних). Методика проста та дає власникові інформаційних ресурсів можливість зрозуміти, яким чином виходить підсумкова оцінка і що потрібно змінити, щоб поліпшити оцінки.

До недоліків відноситься те, що непрямі фактори та їх вага залежать від сфери діяльності організації, а також від низки інших обставин. Таким чином, методика завжди вимагає налаштування під конкретний об’єкт. При цьому доказ повноти обраних непрямих факторів і правильності їх вагових коефіцієнтів є завданням формалізованим і складним, яке на практиці вирішується експертними методами (перевірка відповідності отриманих за методикою результатів, очікуваних для тестових ситуацій).

Подібні методики, як правило, розробляються для організацій певного профілю (відомств), випробовуються, а потім використовуються як відомчий стандарт. Таким шляхом пішли й творці CRAMM, випустивши близько десятка

версій методу для різних відомств (міністерство закордонних справ, збройні сили тощо).

Оцінки ризиків і вразливості у розглянутому прикладі є *якісними величинами*. Проте подібними методами можуть бути отримані й кількісні оцінки, необхідні при розрахунку залишкових ризиків і вирішенні оптимізаційних завдань. Для цього застосовується низка методів, що дозволяють встановити на впорядкованій множини оцінок систему відношень.

Здобуття об'єктивних кількісних оцінок ризиків має бути актуальне для страхових агентств інформаційних ризиків, що займаються страхуванням.

На практиці страхові агентства користуються у більшості випадків якісними оцінками. Прості методики, без тривалого та дорогого обстеження, дозволяють віднести інформаційну систему до тієї або іншої групи ризику (за класифікацією страхової компанії) на основі інтерв'ю з посадовими особами. За таких методик також фіксуються й аналізуються непрямі фактори.

Питання для самоконтролю

1. Які неформальні методи оцінювання застосовують при прийнятті експертних рішень?
2. У чому полягає метод експертів?
3. Дайте перелік експертних оцінок із використанням непараметричних методів.
4. Як проходить процедура експертного опитування?
5. Як проходить вибір методів обробки й аналізу суджень експертів?
6. Охарактеризуйте математико-статистичні моделі аналізу даних експертних оцінок, отриманих методом ранжирування.
7. Які є методи групових експертних оцінок?
8. Дайте характеристику методів вимірювання ранжируванням.
9. Дайте характеристику методів вимірювання парним порівнянням.
10. Дайте характеристику методів вимірювання числовим порівнянням.
11. Дайте характеристику методів вимірювання безпосередньою оцінкою.
12. Дайте характеристику вимірювання методом послідовного порівняння.
13. Дайте характеристику вимірювання методом фон Неймана-Моргенштерна.
14. Дайте характеристику вимірювання методами типу «Делфі».
15 Дайте перелік оцінки ризиків методів експертними методами.
16. Як проводять оцінку ризиків за допомогою оцінки суб'єктивної ймовірності?
17. Поясніть класифікацію методів отримання суб'єктивної ймовірності.
18. Поясніть методи оцінок безперервних розподілів.
19. Поясніть методи теорії корисності при оцінці ризиків.
20. У чому суть кількісних та якісних технологій оцінки ризиків?
21. Технологія вимірювання ризиків.
22. Технологія оцінки загроз і вразливостей.

Розділ 3

ОРГАНІЗАЦІЯ ДЕРЖАВНОЇ ЕКСПЕРТИЗИ СИСТЕМ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОКОМУНІКАЦІЯХ

Система оцінювання відповідності реалізованих засобів і заходів захисту встановленим вимогам і нормам в Україні функціонує на підставі «Положення про державну експертизу у сфері технічного захисту інформації» (далі – «Положення…») й упорядковується новими нормативними документами НД ТЗІ 2.6-001-11 [37], НД ТЗІ 2.7-009-09 і НД ТЗІ 2.7-010-09 [див. 23, 24]. Терміни та визначення, що стосуються оцінки інформаційної захищеності телекомунікацій, наведені у Додатку 1.

3.1 Положення щодо порядку проведення державної експертизи комплексних систем захисту інформації

У НД ТЗІ 1.1-002-99 зазначається, що у проблемі захисту від несанкціонованого доступу (НСД) інформації, оброблюваної в ІТС, виокремлюються дві частини:

- забезпечення захищеності інформації у функціонуючих та/або створюваних ІТС;
- створення засобів ТЗІ від НСД або захищених від НСД компонентів обчислювальної системи поза конкретним середовищем експлуатації.

У телекомунікаційних системах це твердження означає, що комплексна система захисту інформації (КСЗІ) в них складається зі спеціалізованих (штатних) засобів захисту інформації (ЗЗІ) та загальних засобів ТЗІ, створюваних поза системою.

Спеціалізовані ЗЗІ включають у себе засоби забезпечення: конфіденційності, керування доступом, цілісності даних, автентифікації, керування маршрутизацією, невідмовності. Вони закладаються розробником як штатні можливості телекомунікаційних систем, поряд із їх функціональними можливостями надання телекомунікаційних послуг.

Без загальних засобів ТЗІ, створюваних поза системою та застосовуються в усіх системах, неможливі інсталяція, випробування й експлуатація спеціальних ЗЗІ. До загальних засобів ТЗІ відносять: довірчу функціональність, категоріювання об’єктів безпеки, виявлення небезпечних подій, аудит безпеки, відновлювання безпеки.

В усіх випадках має бути незалежне підтвердження (оцінювання) відповідності реалізованих засобів та заходів захисту встановленим вимогам та нормам. Умовою обов’язковості такого підтвердження є оброблення в ІТС інформації, порядок захисту якої регламентується законами України або іншими нормативно-правовими актами (наприклад, інформації, яка становить державну таємницю або вимоги щодо захисту якої встановлено законодавством).

Результатами проведеного оцінювання має бути відповідний висновок, на підставі якого власники ІТС та оброблюваних у них інформаційних ресурсів можуть приймати рішення щодо прийнятності та достатності вжитих заходів і реалізованих засобів.

Система оцінювання відповідності реалізованих засобів і заходів захисту встановленим вимогам і нормам в Україні функціонує на підставі Положення про державну експертизу у сфері технічного захисту інформації (далі – «Положення…») [див. 3]. Згідно вимог цього документа оцінювання відповідності реалізованих засобів і заходів захисту встановленим вимогам і нормам здійснюється шляхом проведення експертизи.

Суб'єктами експертизи є: юридичні та фізичні особи, які є Замовниками експертизи; уповноважений державний орган; підрозділи уповноваженого державного органу, підприємства, установи й організації, які проводять експертизу (Організатори експертизи); державні органи, які проводять експертизу у сфері свого управління; фізичні особи – виконавці експертних робіт із ТЗІ (Експерти).

Об'єктами експертизи (ОЕ) можуть бути як КСЗІ, які є невід'ємною складовою частиною ІТС, так і окремі засоби ТЗІ від НСД. Останні у цьому навчальному посібнику не розглядаються.

Мета експертизи КСЗІ, яка є невід'ємною складовою частиною ІТС, має передбачати оцінювання відповідності КСЗІ технічному завданню, вимогам чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу (НД ТЗІ 2.5-007-2007, НД ТЗІ 2.5-008-02, НД ТЗІ 2.5-010-03 тощо), вимогам інших чинних нормативних документів і визначення можливості введення КСЗІ у складі ІТС в експлуатацію та забезпечення захисту інформації відповідно до встановлених вимог.

Згідно вимог «Положення…» експертиза може бути первинною, додатковою та контрольною. *Первинна експертиза* є основним видом експертизи та передбачає виконання Організатором експертизи усіх необхідних заходів, визначених у «Положенні…» та необхідних для підготовки та прийняття рішення щодо відповідності ОЕ висунутим вимогам. *Додаткова експертиза* проводиться стосовно ОЕ, щодо яких відкрилися нові наукові та науково-технічні обставини або у зв'язку із закінченням терміну дії документів, що засвідчують результати експертизи. *Контрольна експертиза* проводиться іншим Організатором експертизи з ініціативи Замовника за наявності у нього обґрунтованих претензій до висновку первинної чи додаткової експертизи або з ініціативи уповноваженого державного органу для перевірки висновку первинної чи додаткової експертизи.

Загальний порядок організації та проведення робіт із експертизи передбачає збирання Експертами та подальше оцінювання необхідних свідоцтв (сукупності свідоцтв), які характеризують ступінь відповідності об'єкта експертизи висунутим вимогам, із подальшим формулюванням результатів оцінювання у вигляді відповідного Експертного висновку.

З метою забезпечення максимальної достовірності та повноти результатів при організації та проведенні експертизи мають бути дотримані такі основні принципи її проведення:

– незалежність Організаторів експертизи й Експертів. Організатори експертизи й Експерти мають бути незалежні у своїй діяльності та невідповідальні за створення (розроблення) об'єкта експертизи. Незалежність є підставою для неупередженості при проведенні експертизи й об'єктивності при формулюванні висновків за результатами експертизи. Дотримання принципу незалежності означає, що Організаторами експертизи (Експертами) не можуть бути організації (особи), для яких може бути документально підтверджено причетність до будь-яких етапів робіт зі створення об'єкта експертизи, на будь-якому етапі життєвого циклу об'єкта експертизи, обґрунтування та вибору певних проектних рішень;

– повнота оцінювання. Експертні роботи повинні охоплювати всі аспекти, які стосуються виконання вимог, що висуваються до об'єкта експертизи. Крім того, повнота оцінювання визначається достатністю наданих Замовником експертизи матеріалів і документів, а також рівнем їх відповідності висунутим вимогам. Повнота оцінювання є необхідною умовою для формування об'єктивних висновків за результатами експертизи;

– оцінювання на підставі отриманої сукупності свідоцтв. Проведення оцінювання на підставі свідоцтв є єдиним способом, який дозволяє отримати повторювані висновки за результатами експертизи, що підвищує довіру до таких висновків. Для цього повинна забезпечуватися можливість повторної перевірки сукупності свідоцтв оцінювання. Джерелами свідоцтв оцінювання можуть бути: отримані від Замовника експертизи документи та матеріали; усні висловлювання та письмові відповіді співробітників Замовника експертизи, отримані у процесі проведених опитувань; результати спостереження за діяльністю співробітників Замовника експертизи; результати самостійного виконання Експертами експертних робіт;

– достовірність свідоцтв оцінювання. Експерти повинні бути впевнені у достовірності наявних свідоцтв оцінювання. Довіра до документальних свідоцтв підвищується при підтвердженні їх достовірності третьою стороною або керівництвом Замовника експертизи. Довіра до фактів, отриманих при опитуванні співробітників Замовника експертизи, підвищується при підтвердженні цих фактів із різних джерел. Довіра до фактів, отриманих при спостереженні за діяльністю співробітників Замовника експертизи, підвищується, якщо вони отримані безпосередньо при функціонуванні процедур або процесів, які перевіряються;

– компетентність Експертів. Компетентність базується на наявності в Експерта необхідних знань і навиків у галузі технічного захисту інформації та на здатності застосувати їх під час виконання експертних робіт. На вимогу Замовника Експерт зобов'язаний надати йому документи, які підтверджують його досвід і рівень кваліфікації;

– етичність поведінки Експертів. Етичність поведінки передбачає відповідальність, непідкупність, неупередженість.

З метою виконання зазначених принципів Експерти повинні дотримуватися таких основних принципів виконання оцінювання:

– об’єктивність – результати оцінювання повинні ґрунтуватися на використаних свідоцтвах і містити мінімум суб’єктивної думки Експерта;

– неупередженість – результати оцінювання повинні бути неупередженими навіть у тих випадках, коли потрібне суб’єктивне судження;

– повторюваність – дії того самого Експерта, виконувані з використанням однієї й тієї самої сукупності свідоцтв, повинні привести до одних і тих же результатів;

– відтворюваність – дії іншого Експерта, виконувані з використанням однієї й тієї самої сукупності свідоцтв, повинні привести до одних і тих самих результатів;

– коректність – повинні виконуватися лише ті дії Експерта, які потрібні, і вони повинні виконуватися належним чином, щоб забезпечити правильні результати оцінювання;

– достатність – кожен вид дій Експерта повинен здійснюватися до рівня, необхідного для задоволення всіх висунутих вимог;

– прийнятність – кожна дія Експерта повинна сприяти підвищенню довіри до результатів оцінювання.

Якщо об’єкт експертизи являє собою КСЗІ, яка є невід’ємною складовою частиною ІТС, проведення первинної експертизи має передбачати виконання таких етапів експертних робіт:

- попереднє ознайомлення з ОЕ;
- поглиблене обстеження ОЕ;
- розроблення програми проведення експертизи КСЗІ;
- розроблення методики проведення експертизи КСЗІ;
- проведення експертних випробувань і досліджень ОЕ за розробленими програмою та методикою;
- документування та затвердження результатів експертизи.

Проведення додаткової або контрольної експертизи КСЗІ може передбачати як виконання усіх робіт, передбачених для випадку первинної експертизи, так і (за узгодженням із уповноваженим державним органом) лише тих робіт, які обумовлені причинами проведення відповідної експертизи.

3.2 Порядок проведення робіт із експертизи комплексних систем захисту інформації

Первинна експертиза КСЗІ у загальному випадку передбачає виконання таких етапів експертних робіт:

1) попереднє ознайомлення з об’єктом експертизи;
2) поглиблене обстеження об’єкта експертизи;
3) розроблення програми експертизи;
4) розроблення методики експертизи;
5) проведення експертних випробувань і досліджень об’єкта експертизи за розробленими програмою та методикою;
6) документування та затвердження результатів експертизи.

1 Метою етапу попереднього ознайомлення з об’єктом експертизи є прийняття рішення щодо можливості проведення робіт із експертизи, визначення обсягів і плану подальших робіт.

1.1 На етапі попереднього ознайомлення з об’єктом експертизи Експертами повинні бути виконані такі дії:

- попередній аналіз наданих Замовником вхідних даних щодо об’єкта експертизи з метою отримання й усвідомлення первинної інформації про основні вимоги із захисту інформації, які висуваються чинними нормативними документами та задоволення яких має забезпечуватися, а також основні характеристики, які повинні бути підтверджені у ході проведення експертизи;
- ознайомлення з об’єктом експертизи за реальних умов функціонування ІТС з метою визначення ступеня його готовності до виконання робіт із експертизи;
- попередній аналіз наданої Замовником проектної, експлуатаційної та нормативно-розпорядчої документації щодо відповідності її складу вимогам чинних нормативних документів;
- документування отриманих результатів і прийняття рішення щодо проведення подальших етапів робіт або щодо їх припинення.

1.2 При виконанні попереднього аналізу вхідних даних щодо ОЕ Експерту слід користуватися відомостями, наведеними у матеріалах, наданих Замовником експертизи (технічне завдання на створення КСЗІ в ІТС і формуляр ІТС, наявність яких на цьому етапі є необхідною відповідно до вимог Положення про державну експертизу у сфері технічного захисту інформації), а також, за необхідності, поясненнями Замовника експертизи. За результатами проведеного аналізу зазначених матеріалів Експерт повинен сформувати попередню думку про:

- архітектуру та функціональний склад ІТС;
- клас і підклас ІТС як ІТС (АС) згідно вимог НД ТЗІ 2.5-005-99;
- інформаційні ресурси, оброблювані в ІТС, які відповідно до вимог чинного законодавства підлягають захисту, а також про технологію їх оброблення;
- характеристику інформації відповідно до встановленого Законом України «Про інформацію» та іншими законодавчими актами правового режиму та режиму доступу (відкрита інформація (ВІ); відкрита інформація, що є власністю держави (ВІВД); конфіденційна інформація (КІ); конфіденційна інформація, що є власністю держави (КІВД); інформація, що становить державну таємницю (ІДТ)), яка міститься у певних інформаційних ресурсах і відповідно до вимог чинного законодавства потребує захисту;
- вимоги чинних нормативних документів щодо захисту певних властивостей (конфіденційності, цілісності, доступності) інформації, оброблюваної в ІТС, задоволення яких має забезпечуватися КСЗІ;
- функціональний склад об’єкта експертизи та його основні характеристики, які мають бути підтверджені у ході проведення експертизи (реалізований функціональний профіль захищеності; рівень гарантій коректності реалізації функціональних послуг безпеки; певний перелік організаційних, фізичних й інших заходів захисту тощо);

- місце розташування, категорію й інші загальні характеристики ІТС, у складі якої створено та функціонує об’єкт експертизи.

1.3 При ознайомленні з об’єктом експертизи за реальних умов функціонування ІТС зусилля Експерта мають бути спрямовані, у першу чергу, на збирання доказів, які підтверджують сам факт існування об’єкта експертизи у тому складі та з тими характеристиками, які були виявлені під час попереднього аналізу вхідних даних щодо об’єкта експертизи.

1.4 При проведенні попереднього аналізу наданої документації на об’єкт експертизи щодо відповідності її вимогам чинних нормативних документів Експерту слід із урахуванням результатів попереднього аналізу вхідних даних перевірити склад наданої Замовником проектної, експлуатаційної та нормативно-розпорядчої документації й визначити, чи відповідає він із урахуванням зазначених рекомендацій вимогам чинних нормативних документів, задоволення яких має забезпечуватися КСЗІ.

1.5 Результатом виконання робіт із попереднього ознайомлення з об’єктом експертизи повинен бути звіт, в якому Експерти, що здійснювали аналіз відповідних матеріалів та ознайомлення з об’єктом експертизи, повинні викласти свою думку щодо ступеня відповідності об’єкта експертизи наданим відомостям, повноти складу наданої проектної, експлуатаційної та нормативно-розпорядчої документації, обґрунтувати рішення щодо можливості та доцільності проведення подальших робіт із експертизи або щодо їх припинення, а у випадку позитивного рішення – пропозиції щодо плану та послідовності проведення подальших робіт. У звіті можуть бути наведені рекомендації щодо необхідності доопрацювання наданих документів, розроблення додаткових документів або надання додаткових матеріалів, які повинні бути використані на подальших етапах експертизи.

2 Метою етапу поглибленого обстеження об’єкта експертизи є збирання та ретельний аналіз всіх відомостей про об’єкт експертизи, які визначають або можуть визначати перелік та обсяг експертних робіт із розроблення програми та методики проведення експертизи КСЗІ, а також проведення експертних випробувань і досліджень об’єкта експертизи за розробленими програмою та методикою й отримання необхідних вхідних даних для проведення подальших етапів експертних робіт.

2.1 На етапі поглибленого обстеження об’єкта експертизи Експертами повинні бути виконані такі дії:

- поглиблений аналіз об’єкта експертизи та наданої проектної, експлуатаційної та нормативно-розпорядчої документації щодо її повноти та відповідності її змісту реальній ІТС й умовам її функціонування;
- перевірка складу КЗЗ, створеного у складі об’єкта експертизи, та визначення необхідності проведення експертизи складових частин КЗЗ, які не мають Експертних висновків щодо відповідності вимогам чинних нормативних документів системи ТЗІ.

2.2 При проведенні поглибленого аналізу ОЕ та наданої проектної, експлуатаційної та нормативно-розпорядчої документації Експерту слід крім використання матеріалів, що аналізуються, врахувати результати, отримані на

етапі попереднього ознайомлення з ОЕ, а також, за необхідності, пояснення Замовника експертизи та/або Розробника ОЕ. Крім цього, при виконанні такого аналізу Експерту слід використати вимоги чинних нормативних документів щодо забезпечення захисту інформації. За результатами проведеного аналізу зазначених матеріалів Експерт повинен:

– розширити та деталізувати уявлення про об’єкт експертизи та його особливості (архітектура та функціональний склад ІТС; клас і підклас ІТС як автоматизованої системи (АС) згідно вимог НД ТЗІ 2.5-005-99; інформаційні ресурси, оброблювані в ІТС, які підлягають захисту, і технологія їх оброблення; характеристика інформації, що міститься у певних інформаційних ресурсах і потребує захисту, відповідно до встановленого законодавством правового режиму та режиму доступу; вимоги чинних нормативних документів щодо захисту певних властивостей інформації, оброблюваної в ІТС; функціональний склад КСЗІ та її основні характеристики, які мають бути підтверджені у ході проведення експертизи; структурний склад підсистем);

– надати (за наявності) Замовнику зауваження щодо змісту окремих документів і рекомендації щодо усунення наданих зауважень;

– провести повторний аналіз доопрацьованих документів і прийняти рішення щодо повноти наданої документації та відповідності її змісту реальній ІТС й умовам її функціонування, а також щодо можливості та доцільності проведення подальших робіт із експертизи. Якщо надані Замовнику зауваження щодо змісту окремих документів не усунуто, Експерт може прийняти рішення щодо припинення подальших робіт або щодо їх призупинення до усунення всіх наданих зауважень.

2.3 При виконанні перевірки складу КЗЗ, створеного у складі ОЕ, Експертом повинні бути визначені (за наявності) складові частини КЗЗ, які не мають Експертних висновків щодо відповідності вимогам чинних нормативних документів системи ТЗІ, та прийнято рішення щодо оцінювання функціональних послуг безпеки (ФПБ) і рівня гарантій коректності реалізації ФПБ в окремих компонентах КЗЗ КСЗІ у ході робіт із експертизи КСЗІ. При цьому обов’язково мають бути оцінені ті ФПБ, наявність яких згідно вимог НД ТЗІ 2.5-004-99 є необхідною умовою для реалізації ФПБ.

2.4 Результатом виконання робіт щодо поглибленого обстеження об’єкта експертизи має бути уточнений перелік відомостей про об’єкт експертизи й інших вхідних даних, необхідних для розроблення програми та методики проведення експертизи.

2.5 Допускається об’єднання етапів попереднього ознайомлення та поглибленого обстеження об’єкта експертизи. У цьому випадку допускається не виконувати роботи, передбачені у п. 1.5.

3 Метою етапу розроблення програми експертизи є розроблення та узгодження в установленому порядку програми проведення експертизи КСЗІ.

3.1 Як вхідні дані на цьому етапі Експертом повинні бути використані всі матеріали, які були зібрані, проаналізовані та, за необхідності, доопрацьовані на попередніх етапах робіт.

3.2 У розробленій програмі експертизи КСЗІ повинен бути наведений опис того, відповідність об’єкта експертизи яким саме вимогам і в якій послідовності має бути перевірена з метою підтвердження або спростування його відповідності вимогам Технічного завдання на створення КСЗІ в ІТС і вимогам чинних нормативних документів системи ТЗІ.

3.3 При розробленні змістовної частини програми проведення експертизи КСЗІ Експертам слід керуватися вимогами щодо змісту програми проведення експертизи КСЗІ в ІТС, викладеними далі у розд. 4.3 – 4.6.

3.4 При документуванні програми проведення експертизи КСЗІ Експертам слід керуватися вимогами «Положення…», ГОСТ 19.301-79, ДСТУ 2853-94, інших чинних стандартів і нормативних документів у галузі інформаційних технологій і захисту інформації, що стосуються підготовки та проведення випробувань.

3.5 Результатом етапу повинна бути розроблена та згідно вимог «Положення…» узгоджена із Замовником експертизи й уповноваженим державним органом програма проведення експертизи КСЗІ.

4 Метою етапу розроблення методики експертизи є розроблення та узгодження в установленому порядку методики проведення експертизи КСЗІ.

4.1 Як вхідні дані на цьому етапі Експертом мають бути використані всі матеріали, які були зібрані, проаналізовані та, за необхідності, доопрацьовані на етапах попереднього ознайомлення з об’єктом експертизи та поглибленого обстеження об’єкта експертизи, а також розроблена на попередньому етапі програма проведення експертизи КСЗІ.

4.2 У розробленій методиці проведення експертизи КСЗІ повинен бути наведений опис того, з використанням яких документів (матеріалів), засобів і в якій послідовності мають бути виконані експертні роботи з метою підтвердження або спростування відповідності об’єкта експертизи вимогам Технічного завдання на створення КСЗІ в ІТС і вимогам чинних нормативних документів системи ТЗІ.

4.3 При розробленні змістовної частини методики експертизи КСЗІ Експертам слід керуватися вимогами щодо змісту методики проведення експертизи КСЗІ в ІТС.

4.4 При документуванні методики проведення експертизи КСЗІ Експертам слід керуватися вимогами «Положення…», ГОСТ 19.301-79, ДСТУ 2853-94, інших чинних стандартів і нормативних документів у галузі інформаційних технологій і захисту інформації, що стосуються підготовки та проведення випробувань.

4.5 Результатом етапу повинна бути розроблена та згідно вимог «Положення…» узгоджена з уповноваженим державним органом методика проведення експертизи КСЗІ.

5 Метою етапу проведення експертних випробувань і досліджень об’єкта експертизи є виконання повного обсягу експертних робіт, передбаченого затвердженою програмою проведення експертизи, шляхом здійснення визначених у затвердженій методиці проведення експертизи дій і перевірок із

фіксацією висновків Експерта щодо результатів виконання певних пунктів методики.

5.1 Проведення експертних випробувань і досліджень об'єкта експертизи за розробленими програмою та методикою проведення експертизи передбачає виконання таких експертних робіт:

- аналіз документації, розробленої на етапі виконання передпроектних робіт зі створення КСЗІ;
- аналіз Технічного завдання на створення КСЗІ в ІТС;
- оцінювання (за необхідності) функціональних послуг безпеки (ФПБ), що реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ;
- оцінювання (за необхідності) рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ;
- аналіз проектної документації КСЗІ та матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів КЗЗ КСЗІ;
- аналіз експлуатаційної документації компонентів КЗЗ КСЗІ;
- аналіз нормативно-розпорядчої документації КСЗІ;
- аналіз документації щодо проведених випробувань КСЗІ;
- аналіз організаційно-розпорядчої документації КСЗІ;
- перевірка фактичного використання внесених до складу КЗЗ КСЗІ засобів захисту інформації;
- перевірка порядку використання внесених до складу КЗЗ КСЗІ засобів захисту інформації;
- перевірка впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших нетехнічних заходів захисту;
- перевірка підготовленості співробітників служби захисту інформації (СЗІ), персоналу та користувачів ІТС;
- перевірка (за необхідності) результатів створення й атестації комплексу ТЗІ.

5.2 Роботи з оцінювання ФПБ, що реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ, а також із оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ повинні проводитися у порядку, наведеному у НД ТЗІ 2.6-001-11.

5.3 Роботи з аналізу документації, що стосується створення КСЗІ (документації, розробленої на етапі виконання передпроектних робіт; Технічного завдання на створення КСЗІ в ІТС; проектної документації КСЗІ та матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів КЗЗ КСЗІ; експлуатаційної документації компонентів КЗЗ КСЗІ; нормативно-розпорядчої документації КСЗІ; документації щодо проведених випробувань КСЗІ; організаційно-розпорядчої документації КСЗІ) можуть виконуватися як за умов випробувальної лабораторії, так і безпосередньо за умов ІТС, у складі якої функціонує об'єкт експертизи.

5.4 Роботи з перевірки фактичного використання внесених до складу КЗЗ КСЗІ засобів захисту інформації, з перевірки порядку використання внесених до складу КЗЗ КСЗІ засобів захисту інформації, з перевірки впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших нетехнічних

заходів захисту, з перевірки підготовленості співробітників СЗІ, персоналу та користувачів ІТС, із перевірки результатів створення й атестації комплексу ТЗІ повинні виконуватися безпосередньо за умов ІТС, у складі якої функціонує об'єкт експертизи.

5.5 Виконання зазначених у методиці проведення експертизи перевірок матеріалів (документів) або перевірок певних фактів передбачає просте порівняння змісту матеріалів (документів) з висунутими вимогами без залучення спеціальних знань і досвіду Експерта або фіксацію (за наявності або відсутності відповідних ознак, визначених у методиці експертизи як мета перевірки) підтвердження або спростування відповідних фактів. Висновки, які формулюються за результатами виконаної перевірки, повинні містити лише результати виконаної перевірки без їх обґрунтування.

5.6 Виконання зазначених у методиці проведення експертизи досліджень матеріалів (документів) із метою формулювання обґрунтованого висновку про відповідність висунутим вимогам передбачає виконання поглибленого аналізу вмісту матеріалів на предмет відповідності висунутим вимогам із використанням спеціальних знань і досвіду Експерта. Висновки, які формулюються за результатами виконаних досліджень, повинні містити як результати проведеного аналізу, так і їх обґрунтування, що містить аргументацію на користь цих висновків.

5.7 При виконанні окремих пунктів методики експертизи, які стосуються перевірки фактичного використання внесених до складу КЗЗ КСЗІ засобів захисту інформації та порядку їх використання, перевірки впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших нетехнічних заходів захисту, а також перевірки підготовленості співробітників СЗІ, персоналу та користувачів ІТС, Експерти можуть використати (у частині, що стосується виконання аналогічних робіт) рекомендації щодо відвідування підприємств, викладені у додатку Г до НД ТЗІ 2.7-010-09.

5.8 Сформульовані Експертом висновки за результатами виконання перевірок згідно з певними пунктами методики проведення експертизи повинні фіксуватися у журналі результатів проведення експертних робіт. У цьому журналі повинні фіксуватися як висновки Експерта, так і (безпосередньо або шляхом посилання на проаналізовані матеріали та документи) аргументи, на підставі яких були зроблені відповідні висновки.

6 Документування та затвердження результатів експертизи передбачають виконання таких робіт:

- оформлення та затвердження протоколу виконання робіт із експертизи КСЗІ (далі – протокол експертизи КСЗІ);
- оформлення, затвердження та надання Замовнику експертизи Експертного висновку за результатами експертизи КСЗІ.

6.1 При оформленні протоколу експертизи КСЗІ слід керуватися вимогами «Положення…» щодо форми протоколу.

6.2 При оформленні Експертного висновку за результатами експертизи КСЗІ слід керуватися вимогами «Положення…» щодо форми Експертного висновку.

6.3 Затверджені Організатором експертизи протокол та Експертний висновок у порядку, визначеному «Положенням…», повинні бути зареєстровані уповноваженим державним органом і надані Замовнику експертизи. На підставі позитивного Експертного висновку уповноважений державний орган надає Замовнику експертизи Атестат відповідності КСЗІ в ІТС вимогам нормативних документів із технічного захисту інформації.

3.3 Документація замовника, що надається при проведенні державної експертизи

Розглянемо склад і зміст документів і матеріалів, які повинні бути розроблені у процесі створення комплексної системи захисту інформації (КСЗІ) та надаються Замовником Організатору експертизи для використання Експертами у процесі проведення експертизи КСЗІ.

3.3.1 Склад документів замовника, що надаються для проведення державної експертизи

Документація щодо створення КСЗІ

Документація, розроблювана на етапі виконання передпроектних робіт:

– перелік інформації, що підлягає обробленню в інформаційно-телекомунікаційній системі (ІТС) і потребує захисту;

– акт категоріювання ІТС (лише для інформації з обмеженим доступом, що належить державі);

– положення про службу захисту інформації в ІТС;

– результати обстеження середовищ функціонування ІТС;

– опис політики безпеки інформації в ІТС;

– опис моделі порушника безпеки інформації в ІТС;

– опис моделі загроз для інформації, оброблюваної в ІТС;

– звіт за результатами проведення аналізу ризиків і формування завдань на створення КСЗІ;

– план захисту інформації в ІТС;

– технічне завдання на створення КСЗІ в ІТС.

Проектна документація КСЗІ:

– документація ескізного проекту КСЗІ в ІТС;

– документація технічного проекту КСЗІ в ІТС;

– документація робочого проекту КСЗІ в ІТС.

Матеріали, що містять результати державної експертизи окремих компонентів (складових частин) комплексу засобів захисту (КЗЗ) КСЗІ:

– експертні висновки щодо відповідності вимогам чинних нормативних документів системи ТЗІ, використаних у складі КЗЗ КСЗІ засобів захисту інформації;

– експертні висновки, сертифікати, інші документи, що підтверджують відповідність вимогам чинних нормативних документів системи

криптографічного захисту інформації (КЗІ), використаних у складі КЗЗ КСЗІ засобів КЗІ;

– матеріали (документи), необхідні для оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ, створення й експертиза яких здійснюється у ході створення й експертизи КСЗІ;

– експлуатаційна документація компонентів (складових частин) КЗЗ КСЗІ.

Нормативно-розпорядча документація КСЗІ:

– інструкції щодо забезпечення правил оброблення інформації з обмеженим доступом (ІзОД) в ІТС (лише для інформації з обмеженим доступом, що належить державі);

– посадові (функціональні) інструкції співробітників СЗІ, персоналу та користувачів ІТС;

– технологічні (операційні) інструкції (настанови) щодо виконання завдань із адміністрування й обслуговування КСЗІ;

– інструкції про порядок використання засобів КЗІ;

– документація щодо проведених випробувань КСЗІ;

– організаційно-розпорядча документація КСЗІ;

– супровідна документація КСЗІ в ІТС;

– журнали обліку та реєстрації сховищ і матеріальних носіїв ІзОД (лише для інформації з обмеженим доступом, що належить державі).

Документація щодо створення комплексу ТЗІ:

– документація, що розробляється на етапі виконання передпроектних робіт;

– документація, що розробляється на етапі розроблення та впровадження заходів із захисту інформації;

– документація, що розробляється на етапі випробувань й атестації комплексу ТЗІ.

3.3.2 Зміст документів замовника, що надаються для проведення державної експертизи (Рекомендації до змісту документації щодо створення КСЗІ)

Документація, що розробляється на етапі виконання передпроектних робіт

Перелік інформації, що підлягає обробленню в ІТС і потребує захисту.

У переліку інформації, що підлягає обробленню в ІТС і потребує захисту, має бути наведено перелік інформаційних ресурсів (видів інформації), що підлягають обробленню в ІТС, класифікований за такими ознаками:

– семантичний вміст відповідного інформаційного ресурсу, який визначається цільовим призначенням відповідної інформації;

– характеристики інформації відповідно до встановленого законодавством правового режиму та режиму доступу (інформація, що становить державну таємницю – ІДТ, конфіденційна інформація, що є власністю держави – КІВД, конфіденційна інформація – КІ, відкрита інформація, що є власністю держави – ВІВД, відкрита інформація – ВІ;

– вищий ступінь обмеження доступу (для ІДТ) до інформації (ступінь секретності) відповідно до вимог Зводу відомостей, що становлять державну таємницю;

– критичні властивості інформації з погляду забезпечення її захищеності, визначені з урахуванням вимог Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах [39] і вимог власника (розпорядника) інформації;

– вимоги (за наявності) щодо обмеження доступу до інформації користувачів ІТС різних категорій.

Окрім зазначених вище, можуть бути використані додаткові класифікаційні ознаки, корисні з погляду подальшого формулювання політики безпеки інформації, оброблюваної в ІТС, наприклад, вид подання відповідних інформаційних ресурсів тощо.

Перелік інформації, що підлягає обробленню в ІТС та потребує захисту, може бути оформлений у вигляді окремого документа, затвердженого керівником організації (установи), яка є власником (розпорядником) відповідної інформації або його заступником, відповідальним за забезпечення ТЗІ, або внесений у вигляді розділу до інших документів (Опису політики безпеки інформації в ІТС, Плану захисту інформації в ІТС, Технічного завдання на створення КСЗІ в ІТС тощо).

Акт категоріювання ІТС. В акті категоріювання ІТС повинні бути викладені результати відповідного категоріювання, проведеного у порядку, визначеному ТПКО-95 [38]. Структура та зміст акта категоріювання мають відповідати вимогам ТПКО-95. Зокрема, в акті категоріювання повинні бути обов’язково наведені такі відомості:

- підстава для категоріювання (первинне, планове, у зв’язку зі змінами);
- вищий ступінь обмеження доступу (ступінь секретності) інформації, що підлягає обробленню в ІТС;
- категорія, призначена ІТС.

Положення про службу захисту інформації в ІТС. Положення про службу захисту інформації (СЗІ) в ІТС має визначати завдання, функції, повноваження та відповідальність, штатний розклад і структуру СЗІ, порядок організації її робіт і взаємодії з іншими підрозділами організації (установи), яка є власником (розпорядником) ІТС, а також порядок її фінансування.

Відповідно до вимог Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах [39], якщо обсяг робіт, пов’язаних із захистом інформації в ІТС, є незначним, забезпечення захисту інформації у такій ІТС може бути покладено на одну особу, а СЗІ у такій ІТС може не створюватися. У цьому випадку завдання, функції, повноваження та відповідальність особи, на яку покладено забезпечення захисту інформації в ІТС (в обсязі, що відповідає наведеним вище вимогам), повинні бути визначені у відповідному наказі керівника організації (установи), яка є власником (розпорядником) ІТС, або його заступника, відповідального за забезпечення ТЗІ.

Структура та зміст Положення про СЗІ в ІТС повинні відповідати рекомендаціям НД ТЗІ 1.4-001-2000 [36] і врахувати особливості функціонування конкретної ІТС (зокрема у частині, що стосується реалізованої інформаційної технології, переліку інформаційних ресурсів, що потребують захисту, встановленого розподілу обов'язків персоналу та користувачів ІТС).

Завдання та функції співробітників (посадових осіб) СЗІ, визначені у Положенні про СЗІ в ІТС, мають бути сформульовані з урахуванням вимог Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [39], НД ТЗІ 1.1-002-99 [16], НД ТЗІ 2.5-007-2007 [40], НД ТЗІ 2.5-008-02 [20], НД ТЗІ 2.5-010-03 [21] та інших чинних нормативних документів, які визначають вимоги щодо порядку створення, введення в експлуатацію й експлуатації КСЗІ в ІТС, і формулюють завдання, які повинен вирішувати персонал ІТС на різних стадіях створення КСЗІ.

Положення про СЗІ в ІТС має бути оформлено у вигляді окремого документа відповідно до рекомендації НД ТЗІ 1.4-001-2000 [36].

Результати обстеження середовищ функціонування ІТС

Результати обстеження середовищ функціонування ІТС повинні містити результати проведеного обстеження обчислювальної системи ІТС, інформаційного середовища, фізичного середовища, середовища користувачів. Загальні вимоги щодо порядку проведення такого обстеження та змісту його результатів визначено у ДСТУ 3396.1-96 [42] та НД ТЗІ 3.7-003-05 [41].

У частині, що стосується результатів обстеження обчислювальної системи ІТС, повинні бути наведені:

– загальна структурна схема та склад обчислювальної системи ІТС;

– види та характеристики каналів мережі передачі даних;

– особливості взаємодії окремих компонентів ІТС, їх взаємний вплив один на одного;

– можливі обмеження щодо використання певних засобів тощо.

Повинні бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів щодо забезпечення захисту інформації, відповідні їхні властивості та характеристики тощо.

Наведені результати обстеження обчислювальної системи ІТС повинні надавати вичерпні відомості щодо можливостей обчислювальної системи ІТС як із погляду забезпечення функціонування загальносистемного та прикладного програмного забезпечення ІТС, так і з погляду забезпечення функціонування засобів захисту, які можуть бути реалізовані та впроваджені у процесі створення КСЗІ.

У частині, що стосується результатів обстеження інформаційного середовища, мають бути наведені:

– уточнений перелік і класифікація (на підставі та з урахуванням відомостей, наведених у Переліку інформації, що підлягає обробленню в ІТС і потребує захисту) інформаційних ресурсів ІТС (даних і програмного

забезпечення), які потребують захисту. Як додаткові класифікаційні ознаки можуть бути використані, наприклад, вид подання відповідної інформації у різних компонентах обчислювальної системи, стан відповідних інформаційних об'єктів (зберігання, оброблення, передавання тощо), характеристики (атрибути) відповідних об'єктів у різному стані тощо;

– опис технології оброблення інформації, що потребує захисту, в усіх загальносистемних і прикладних програмних засобах ІТС із наведенням компонентів обчислювальної системи ІТС, на базі яких функціонують відповідні програмні засоби, інформаційних потоків, що створюються у процесі оброблення, середовищ, через які вони передаються, джерел утворення інформаційних потоків і місць їх призначення. Як частина опису має бути наведена структурна схема інформаційних потоків, в якій для кожного елемента схеми повинен бути визначений склад, вид подання, критичні з погляду захищеності властивості інформації й інші необхідні характеристики відповідних інформаційних об'єктів;

– припущення (за наявності) щодо можливого впливу (з погляду збереження критичних властивостей інформації) на інформаційні об'єкти, що містять інформацію, яка потребує захисту, елементів середовища користувачів і фізичного середовища.

У частині, що стосується результатів обстеження фізичного середовища, повинні бути наведені такі характеристики:

– територіальне розміщення компонентів ІТС;

– наявність охорони території та перепускний режим;

– наявність категорійованих приміщень, в яких повинні розміщуватися компоненти ІТС (з урахуванням результатів категоріювання);

– режим доступу до компонентів фізичного середовища ІТС;

– вплив факторів навколишнього середовища, захищеність від засобів технічної розвідки (наводиться у випадку, якщо передбачається створення комплексу ТЗІ);

– наявність елементів комунікацій, систем життєзабезпечення та зв'язку, що мають вихід за межі контрольованої зони (наводиться у випадку, якщо передбачається створення комплексу ТЗІ);

– наявність і технічні характеристики систем заземлення (наводиться у випадку, якщо передбачається створення комплексу ТЗІ);

– умови зберігання магнітних, оптико-магнітних, паперових й інших носіїв інформації;

– наявність проектної й експлуатаційної документації на компоненти фізичного середовища.

У частині, що стосується результатів обстеження середовища користувачів, повинні бути наведені такі характеристики:

– функціональний і кількісний склад персоналу та користувачів ІТС, їх класифікація за функціональними обов'язками та рівнем кваліфікації;

– повноваження користувачів ІТС різних категорій щодо доступу до інформаційних ресурсів, які обробляються в ІТС, доступу до ІТС та її окремих

компонентів, визначені з урахуванням відповідних вимог, наведених у Переліку інформації, що підлягає обробленню в ІТС і потребує захисту;

– рівня можливостей різних категорій користувачів, що надаються (можуть бути наданими) їм засобами ІТС;

– повноваження персоналу щодо керування засобами захисту КСЗІ, визначені з урахуванням відповідних вимог щодо завдань і функцій співробітників (посадових осіб) СЗІ, наведених у Положенні про СЗІ в ІТС.

Згідно вимог Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [39], НД ТЗІ 3.7-003-05 [41], НД ТЗІ 1.4-001-2000 [36] та НД ТЗІ 3.7-001-99 [42], результати обстеження середовищ функціонування ІТС повинні бути оформлені у вигляді відповідного акта, затвердженого керівником організації (установи), яка є власником (розпорядником) ІТС, і внесені, за необхідності, до відповідних розділів Плану захисту інформації в ІТС і Технічного завдання на створення КСЗІ в ІТС.

Опис політики безпеки інформації в ІТС

Опис політики безпеки інформації в ІТС повинен містити набір вимог, правил, обмежень, рекомендацій тощо, які регламентують порядок оброблення в ІТС інформації, зазначеної у Переліку інформації, що підлягає обробленню в ІТС і потребує захисту, та спрямовані на захист її критичних властивостей від загроз, притаманних умовам функціонування конкретної ІТС.

Відповідно до рекомендацій НД ТЗІ 1.1-002-99 [16] та НД ТЗІ 1.4-001-2000 [36] в Описі політики безпеки інформації в ІТС повинні бути (з урахуванням результатів обстеження середовищ функціонування ІТС) визначені інформаційні ресурси ІТС, що потребують захисту. Мають бути сформульовані основні загрози для інформації з різними характеристиками відповідно до встановленого законодавством правового режиму та режиму доступу, компонентів обчислювальної системи, персоналу та вимоги щодо захисту від цих загроз. Як складові частини загальної політики безпеки інформації в ІТС повинні бути наведені політики забезпечення конфіденційності, цілісності та доступності оброблюваної інформації, а також політика забезпечення спостережності ІТС.

З урахуванням визначених повноважень користувачів ІТС різних категорій щодо доступу до інформаційних ресурсів, які обробляються в ІТС, як частина політики безпеки мають бути сформульовані правила розмежування доступу (ПРД) користувачів і процесів до інформаційних ресурсів ІТС, що потребують захисту. Як атрибути користувачів, процесів й інформаційних об’єктів у сформульованих ПРД мають бути використані атрибути, що відповідають вимогам Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [39], НД ТЗІ 2.5-007-2007 [40], НД ТЗІ 2.5-008-02 [20], НД ТЗІ 2.5-010-03 [21] та інших чинних нормативних документів, які визначають вимоги щодо порядку створення, введення в експлуатацію й експлуатації КСЗІ в ІТС (у частині, що стосується розмежування доступу до захищених інформаційних ресурсів), а

також забезпечують підтримку повноважень користувачів ІТС різних категорій щодо доступу до інформаційних ресурсів й керування засобами захисту КСЗІ, визначених за результатами обстеження середовища користувачів.

З урахуванням відповідних вимог щодо завдань і функцій співробітників (посадових осіб) СЗІ, наведених у Положенні про СЗІ в ІТС в Описі політики безпеки інформації в ІТС має бути визначена відповідальність персоналу за виконання положень політики безпеки.

Опис моделі порушника безпеки інформації в ІТС

Опис моделі порушника безпеки інформації в ІТС має містити абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час і місце дії тощо. В Описі моделі порушника (з урахуванням результатів обстеження середовищ функціонування ІТС) мають бути визначені:

– можливі цілі порушника та їх градація за ступенями небезпечності для ІТС та інформації, що потребує захисту;

– категорії персоналу, користувачів ІТС і сторонніх осіб, із числа яких може бути порушник;

– припущення щодо кваліфікації порушника;

– припущення щодо характеру його дій.

Відповідно до рекомендацій НД ТЗІ 1.1-002-99 [16] доцільно класифікувати порушників за рівнем можливостей, які надаються їм засобами ІТС.

Опис моделі порушника безпеки інформації в ІТС (у частині, що стосується припущень щодо кваліфікації порушника та характеру його дій) має бути викладений настільки детально, щоб дозволяти однозначне визначення можливості або неможливості реалізації порушником певних загроз інформації (певних атак) із використанням уразливостей певних компонентів обчислювальної системи ІТС або використаних програмних засобів.

Опис моделі загроз для інформації, оброблюваної в ІТС

Опис моделі загроз для інформації, що обробляється в ІТС, має містити абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз для інформації, яка потребує захисту. В Описі моделі загроз для інформації (з урахуванням результатів обстеження середовищ функціонування ІТС, а також прийнятої моделі потенційного порушника політики безпеки інформації в ІТС) мають бути визначені:

– перелік можливих типів загроз, класифікований за результатом впливу на інформацію, тобто на порушення яких її властивостей вони спрямовані (конфіденційності, цілісності або доступності інформації);

– перелік можливих способів реалізації загроз певного типу (способів атак) відносно різних інформаційних об’єктів ІТС у різному стані класифікований, наприклад, за такими ознаками, як компонент обчислювальної системи ІТС або програмний засіб, уразливості яких експлуатуються порушником, причини виникнення відповідної уразливості тощо.

Опис моделі загроз для інформації, що обробляється в ІТС (у частині, що стосується переліку можливих способів реалізації загроз та їх класифікації), має бути викладений настільки детально, щоб дозволяти (на етапі аналізу ризиків, пов'язаних із реалізацією загроз для інформації в ІТС) однозначне визначення як збитків, що завдаються у випадку успішної реалізації загрози, так і ймовірності реалізації загрози (здійснення атаки) у певний спосіб.

Звіт за результатами проведення аналізу ризиків і формування завдань на створення КСЗІ

Звіт за результатами проведення аналізу ризиків і формування завдання на створення КСЗІ повинен містити:

– формалізований або неформалізований опис результатів аналізу ризиків, пов'язаних із реалізацією загроз для інформації в ІТС;

– формулювання, з урахуванням результатів виконаного аналізу ризиків, завдань на створення КСЗІ в ІТС.

В Описі результатів аналізу ризиків, проведеного з урахуванням рекомендацій НД ТЗІ 1.1-002-99 [16] і ДСТУ ISO/IEC TR 13335-2:2003 [44], для кожного зі способів реалізації загроз інформації, наведених в Описі моделі загроз для інформації, оброблюваної в ІТС, мають бути надані результати оцінювання ризику, пов'язаного з реалізацією певної загрози у певний спосіб, як функції ймовірності реалізації відповідної загрози у відповідний спосіб, виду та величини збитків, що завдаються у випадку успішної реалізації загрози. Повинні бути визначені неприйнятні ризики та загрози для інформації та способи їх реалізації, з якими ці ризики пов'язані.

Завдання на створення КСЗІ повинні бути сформульовані з урахуванням вимог НД ТЗІ 3.7-003-05 [41] і необхідності забезпечення (в результаті створення КСЗІ) запобігання тим загрозам для інформації та способів їх реалізації, з якими пов'язані неприйнятні ризики. Зокрема, у завданнях на створення КСЗІ мають бути визначені завдання захисту інформації в ІТС і можливі варіанти їх вирішення, загальна структура та склад КСЗІ, вимоги до можливих заходів, методів і засобів захисту інформації, допустимі обмеження щодо застосування певних заходів і засобів захисту, інші обмеження щодо середовищ функціонування ІТС, обмеження щодо використання ресурсів ІТС для реалізації завдань захисту, припустимі витрати на створення КСЗІ, умови створення, введення у дію та функціонування КСЗІ (окремих її підсистем, компонентів), загальні вимоги до співвідношення та меж застосування в ІТС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних й інших заходів захисту інформації, що ввійдуть до складу КСЗІ.

При формулюванні завдань на створення КСЗІ мають бути враховані вимоги Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [39], НД ТЗІ 1.1-002-99 [16], НД ТЗІ 2.5-007-2007 [40], НД ТЗІ 2.5-008-02 [20], НД ТЗІ 2.5-010-03 [21] та інших чинних нормативних документів щодо забезпечення захисту інформації в ІТС.

План захисту інформації в ІТС

План захисту інформації в ІТС має містити: класифікацію інформації, що обробляється в ІТС; опис технології оброблення інформації в ІТС; Опис моделі загроз для інформації в ІТС; Опис політики безпеки інформації в ІТС; визначення завдань захисту інформації в ІТС; визначення переліку документів, згідно з якими має здійснюватися захист інформації в ІТС; перелік і терміни виконання робіт СЗІ в ІТС.

Структура та зміст Плану захисту інформації в ІТС повинні відповідати рекомендаціям НД ТЗІ 1.4-001-2000 [36], врахувати особливості функціонування конкретної ІТС, а також завдання захисту, що мають вирішуватися створюваною КСЗІ, викладені у: Переліку інформації, що підлягає обробленню в ІТС і потребує захисту; Положенні про СЗІ в ІТС; результатах обстеження середовищ функціонування ІТС; Описі політики безпеки інформації в ІТС; Описі моделі порушника безпеки інформації в ІТС; Описі моделі загроз для інформації, оброблюваної в ІТС; Звіті за результатами проведення аналізу ризиків і формування завдань на створення КСЗІ.

При формулюванні Плану захисту інформації в ІТС мають бути враховані вимоги Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [39], НД ТЗІ 1.1-002-99 [16], НД ТЗІ 2.5-007-2007 [40], НД ТЗІ 2.5-008-02 [20], НД ТЗІ 2.5-010-03 [21] та інших чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу.

План захисту інформації в ІТС повинен бути оформлений у вигляді окремого документа відповідно до рекомендації НД ТЗІ 1.4-001-2000 [36]. Згідно вимог Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [39] і НД ТЗІ 1.4-001-2000 [36], План захисту інформації в ІТС має бути затверджений керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

Технічне завдання на створення КСЗІ в ІТС

Технічне завдання на створення КСЗІ в ІТС є засадничим організаційно-технічним документом для виконання робіт щодо забезпечення захисту інформації в ІТС. У Технічному завданні на створення КСЗІ в ІТС, відповідно до положень НД ТЗІ 3.7-003-05 [41] і НД ТЗІ 3.7-001-99 [42], повинні бути викладені вимоги щодо функціонального складу, порядку розроблення та впровадження технічних, організаційних, фізичних та інших заходів захисту, які у сукупності складають КСЗІ.

Структура та зміст Технічного завдання на створення КСЗІ в ІТС повинні відповідати вимогам НД ТЗІ 3.7-003-05 [41], НД ТЗІ 3.7-001-99 [42] та рекомендаціям НД ТЗІ 2.7-010-09 [24] (у частині, що стосується визначення функціональних специфікації КЗЗ КСЗІ для відповідного рівня гарантій коректності реалізації ФПБ), враховувати особливості функціонування конкретної ІТС, а також завдання захисту, що мають вирішуватися створюваною КСЗІ, викладені у: Переліку інформації, що підлягає обробленню

в ІТС і потребує захисту; Положенні про СЗІ в ІТС; результатах обстеження середовищ функціонування ІТС; Описі політики безпеки інформації в ІТС; Описі моделі порушника безпеки інформації в ІТС; Описі моделі загроз для інформації, що обробляється в ІТС; Звіті за результатами проведення аналізу ризиків і формування завдання на створення КСЗІ; Плані захисту інформації.

При розробленні Технічного завдання на створення КСЗІ в ІТС мають бути враховані вимоги Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [39], НД ТЗІ 1.1-002-99 [16], НД ТЗІ 2.5-007-2007 [40], НД ТЗІ 2.5-008-02 [20], НД ТЗІ 2.5-010-03 [21] та інших чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу.

Відповідно до НД ТЗІ 3.7-003-05 [41] і НД ТЗІ 3.7-001-99 [42], Технічне завдання на створення КСЗІ в ІТС може бути оформлено:

– у вигляді окремого розділу технічного завдання на створення ІТС;

– у вигляді окремого (часткового) технічного завдання;

– у вигляді доповнення до технічного завдання на створення ІТС.

Згідно вимог Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [39] і НД ТЗІ 3.7-001-99 [42], Технічне завдання на створення КСЗІ в ІТС має бути узгоджено з Розробником ІТС, затверджено виконавцем робіт зі створення КСЗІ в ІТС і керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС. У випадках, передбачених Положенням про технічний захист інформації в Україні [45] і НД ТЗІ 3.6-001-2000 [19], Технічне завдання на створення КСЗІ в ІТС має бути узгоджено з уповноваженим державним органом.

Документація ескізного проекту КСЗІ в ІТС

У документації ескізного проекту КСЗІ, відповідно до положень НД ТЗІ 3.7-003-05 [41], мають бути наведені відомості щодо попередніх проектних рішень, які визначають порядок реалізації вимог Технічного завдання на створення КСЗІ в ІТС, щодо КСЗІ у цілому та, за необхідності, щодо її окремих складових частин. Якщо відповідно до положень НД ТЗІ 3.7-003-05 [41] етап ескізного проектування КСЗІ вилучається, документація ескізного проекту КСЗІ не розробляється.

Зміст і склад документації ескізного проекту повинні бути достатніми для повного опису проектних рішень рівня ескізного проекту. Конкретний перелік документації ескізного проекту має визначатися на підставі ГОСТ 34.201-89 [46] і РД 50-34.698-90 [47] з урахуванням особливостей відповідної КСЗІ. Обов’язковою є наявність пояснювальної записки до ескізного проекту КСЗІ, структура та зміст якої повинні відповідати вимогам РД 50-34.698-90.

Документація ескізного проекту КСЗІ в ІТС має бути узгоджена з Розробником ІТС, затверджена виконавцем робіт зі створення КСЗІ в ІТС і керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

Документація технічного проекту КСЗІ в ІТС

У документації технічного проекту КСЗІ, відповідно до положень НД ТЗІ 3.7-003-05 [41], мають бути наведені відомості щодо загальних проектних рішень, достатніх (з урахуванням результатів ескізного проектування) для забезпечення реалізації вимог Технічного завдання на створення КСЗІ в ІТС; рішень щодо структури КСЗІ (організаційної структури, структури технічних і програмних засобів); рішень щодо архітектури та складу КЗЗ КСЗІ (у тому числі щодо використаних засобів антивірусного захисту, засобів виявлення та попередження про мережеві вторгнення тощо); рішень щодо механізмів реалізації ФПБ, визначених у наведеному в Технічному завданні функціональному профілі захищеності; рішень щодо алгоритмів, порядку й умов функціонування засобів захисту інформації, які використовуються у складі КЗЗ КСЗІ для реалізації певних ФПБ (функціональних послуг захисту).

Зміст і склад документації технічного проекту повинні бути достатніми для повного опису проектних рішень КСЗІ в обсязі, достатньому для виконання етапу робочого (технороботочого) проектування (реалізації) КСЗІ. Конкретний перелік документації технічного проекту має визначатися на підставі ГОСТ 34.201-89 [46] і РД 50-34.698-90 [47] з урахуванням особливостей відповідної КСЗІ. Обов’язковою є наявність пояснювальної записки до технічного проекту КСЗІ, структура та зміст якої повинні відповідати вимогам РД 50-34.698-90 та рекомендаціям НД ТЗІ 2.7-010-09 [23] (у частині, що стосується проекту архітектури та детального проекту компонентів КЗЗ КСЗІ, створення яких здійснюється у ході створення КСЗІ, для визначеного у Технічному завданні на створення КСЗІ в ІТС рівня гарантій коректності реалізації ФПБ).

Документація технічного проекту КСЗІ в ІТС має бути узгоджена з Розробником ІТС, затверджена виконавцем робіт зі створення КСЗІ в ІТС і керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

Документація робочого проекту КСЗІ в ІТС

У документації робочого проекту КСЗІ, відповідно до положень НД ТЗІ 3.7-003-05 [41], мають бути наведені детальні рішення щодо реалізації технічного проекту КСЗІ, щодо забезпечення керування КСЗІ та взаємодії її компонентів, а також відомості, необхідні для проведення пусконалагоджувальних робіт і тестування підсистем і засобів КСЗІ.

Зміст і склад документації робочого проекту повинні бути достатніми для повного виконання етапу робочого (технороботочого) проектування (реалізації) КСЗІ. Конкретний перелік документації робочого проекту має визначатися на підставі ГОСТ 34.201-89 [46] і РД 50-34.698-90 [47] з урахуванням особливостей відповідної КСЗІ. Якщо у ході створення КСЗІ здійснюються роботи зі створення певних компонентів КЗЗ КСЗІ, обов’язковою є наявність матеріалів робочого проекту (реалізації) відповідних компонентів КЗЗ, зміст яких відповідає рекомендаціям НД ТЗІ 2.7-010-09 [24] для визначеного у Технічному завданні на створення КСЗІ в ІТС, рівня гарантій коректності реалізації ФПБ.

Документація робочого проекту КСЗІ в ІТС має бути узгоджена з Розробником ІТС, затверджена виконавцем робіт зі створення КСЗІ в ІТС і керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

Експлуатаційна документація компонентів КЗЗ КСЗІ

До складу експлуатаційної документації мають входити документи, що визначають порядок інсталяції, ініціалізації, налаштування й експлуатації всіх без винятку компонентів (складових частин) КЗЗ КСЗІ, визначених у документації технічного проекту КСЗІ в ІТС.

Відповідно до вимог НД ТЗІ 2.5-004-99 [17], для кожного компонента (складової частини) КЗЗ КСЗІ у вигляді окремих документів або розділів інших документів повинні бути надані:

– опис процедур безпечної інсталяції, генерації та запуску;

– опис послуг безпеки, що реалізуються відповідним компонентом;

– настанови адміністратору з послуг безпеки;

– настанови користувачу з послуг безпеки.

Зміст відповідних документів повинен відповідати вимогам НД ТЗІ 2.5-004-99 і рекомендаціям НД ТЗІ 2.7-010-09 [24].

3.3.3 Нормативно-розпорядча документація КСЗІ

Інструкції щодо забезпечення правил оброблення ІзОД в ІТС

Інструкції щодо забезпечення правил оброблення ІзОД в ІТС (Інструкція про забезпечення режиму секретності під час оброблення в ІТС інформації, що становить державну таємницю, або Інструкція про порядок оброблення в ІТС конфіденційної інформації, що є власністю держави) мають розроблятися у випадку, якщо в ІТС передбачається оброблення ІзОД, що становить ІДТ, або КІВД. У відповідних інструкціях має бути окреслено перелік заходів, спрямованих на дотримання визначеного вимогами чинної нормативно-правової бази режиму доступу до ІзОД, визначено порядок дій персоналу та користувачів ІТС із метою реалізації зазначених заходів, а також встановлено їх відповідальність у випадку порушення зазначених вимог. Зокрема, в інструкціях щодо забезпечення правил оброблення ІзОД в ІТС рекомендується у вигляді, наприклад, окремих розділів викласти:

– загальні відомості щодо організації захисту ІзОД в ІТС;

– опис порядку доступу до приміщень, в яких розташовані засоби обчислювальної системи ІТС;

– опис порядку захисту інформації від витоку технічними каналами;

– опис порядку захисту інформації від НСД;

– опис порядку здійснення антивірусного захисту;

– опис порядку впровадження та використання програмного забезпечення;

– опис порядку створення захищених інформаційних ресурсів, реєстрації користувачів і надання прав доступу до інформації користувачам ІТС;

– опис порядку контролю за дотриманням користувачами правил роботи із засобами ІТС;

– опис порядку обліку, зберігання, обігу, резервування, ротації та знищення матеріальних носіїв, що використовуються для зберігання ІзОД;

– опис порядку проведення ремонтних робіт і відновлення працездатності ІТС;

– опис порядку контролю за забезпеченням захисту ІзОД в ІТС;

– обов'язки користувачів і персоналу ІТС стосовно дотримання встановленого порядку оброблення ІзОД;

– відповідальність користувачів і персоналу ІТС за порушення встановленого порядку оброблення ІзОД.

В інструкціях щодо забезпечення правил оброблення ІзОД в ІТС мають бути враховані положення посадових (функціональних) інструкцій співробітників СЗІ, персоналу та користувачів ІТС, а також технологічних (операційних) інструкцій (настанов) щодо виконання завдань адміністрування й обслуговування КСЗІ.

Посадові інструкції співробітників СЗІ, персоналу та користувачів ІТС

Посадові інструкції співробітників СЗІ, персоналу та користувачів ІТС мають визначати обов'язки, відповідальність і порядок дій співробітників (посадових осіб) СЗІ, персоналу та користувачів ІТС у процесі виконання ними завдань щодо керування засобами ІТС і КСЗІ, а також оброблення в ІТС інформаційних ресурсів, що потребують захисту. Перелік і зміст цих інструкцій повинні визначатися з урахуванням:

– структури та штатного розкладу СЗІ, визначених у Положенні про СЗІ в ІТС;

– завдань, функцій і повноважень співробітників (посадових осіб) СЗІ, наведених у Положенні про СЗІ в ІТС;

– категорій персоналу та користувачів ІТС, визначених в Описі політики безпеки інформації в ІТС, і вимог Технічного завдання на створення КСЗІ в ІТС, щодо розподілу обов'язків користувачів та їх функціональних завдань;

– порядку дій співробітників (посадових осіб) СЗІ, персоналу та користувачів ІТС, який випливає з положень Опису політики безпеки інформації в ІТС, документації технічного проекту КСЗІ в ІТС, документації робочого проекту КСЗІ в ІТС та експлуатаційної документації компонентів (складових частин) КЗЗ КСЗІ, щодо забезпечення визначеного порядку функціонування ІТС і КСЗІ.

Як приклади зазначених інструкцій можна розглядати такі:

– Інструкція системного адміністратора ІТС;

– Інструкція адміністратора безпеки ІТС;

– Інструкція користувача ІТС.

У посадових (функціональних) інструкціях необхідно у вигляді, наприклад, окремих розділів викласти:

– загальні положення, в яких визначено категорії співробітників СЗІ, персоналу або користувачів ІТС, на яких поширюються вимоги відповідних інструкцій;

– основні завдання та функції (функціональні завдання), що мають виконуватися співробітниками СЗІ, персоналом або користувачами ІТС, на яких поширюються вимоги відповідних інструкцій;

– опис правил і порядку дій співробітників СЗІ, персоналу або користувачів ІТС у процесі виконання функціональних завдань;

– повноваження, обов'язки та відповідальність осіб, на яких поширюються вимоги відповідних інструкцій.

У посадових інструкціях співробітників СЗІ, персоналу та користувачів ІТС повинні бути враховані положення технологічних (операційних) інструкцій (настанов) щодо виконання завдань адміністрування й обслуговування КСЗІ.

Посадові інструкції співробітників СЗІ, персоналу та користувачів ІТС можуть бути оформлені як у вигляді окремих документів, так і у вигляді структурних частин інших документів, наприклад, Інструкції щодо забезпечення правил оброблення ІзОД в ІТС.

Посадові інструкції співробітників СЗІ, персоналу та користувачів ІТС мають бути узгоджені з Розробником ІТС, виконавцем робіт зі створення КСЗІ в ІТС і затверджені керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

Технологічні (операційні) інструкції щодо виконання завдань адміністрування й обслуговування КСЗІ

Технологічні (операційні) інструкції (настанови) щодо виконання завдань адміністрування й обслуговування КСЗІ повинні детально визначати послідовність дій співробітників (посадових осіб) СЗІ та персоналу ІТС у процесі виконання відповідних завдань. Перелік і зміст відповідних інструкцій повинні визначатися з урахуванням:

– структури та штатного розкладу СЗІ, визначених у Положенні про СЗІ в ІТС;

– завдань, функцій і повноважень співробітників (посадових осіб) СЗІ, наведених у Положенні про СЗІ в ІТС;

– категорій персоналу та користувачів ІТС, визначених в Описі політики безпеки інформації в ІТС, і вимог Технічного завдання на створення КСЗІ в ІТС щодо розподілу обов'язків користувачів та їх функціональних завдань;

– порядку дій співробітників (посадових осіб) СЗІ, персоналу та користувачів ІТС, який випливає з положень Опису політики безпеки інформації в ІТС, документації технічного проекту КСЗІ в ІТС, документації робочого проекту КСЗІ в ІТС та експлуатаційної документації компонентів КЗЗ КСЗІ, щодо забезпечення визначеного порядку функціонування ІТС і КСЗІ.

Як приклади зазначених інструкцій можна розглядати такі:

- Інструкція про порядок введення в експлуатацію КСЗІ;
- Інструкція про порядок модернізації КСЗІ;
- Інструкція про порядок резервування та відновлення інформації в ІТС;
- Інструкція про порядок оперативного відновлення функціонування ІТС;
- Інструкція про порядок проведення ремонтних робіт;
- Інструкція про організацію контролю за функціонуванням КСЗІ;

- Інструкція про порядок розроблення, впровадження та модернізації програмного забезпечення ІТС;

- Інструкція про порядок реєстрації користувачів ІТС;

- Інструкція про порядок створення захищених інформаційних ресурсів в ІТС;

- Інструкція про порядок надання доступу до захищених інформаційних ресурсів в ІТС;

- Інструкція про порядок забезпечення антивірусного захисту в ІТС.

У технологічних (операційних) інструкціях (настановах) необхідно у вигляді, наприклад, окремих розділів викласти:

- загальні положення, в яких визначено завдання з адміністрування й обслуговування КСЗІ, порядок виконання яких встановлюється інструкцією (настановою), категорії співробітників СЗІ або персоналу ІТС, на яких поширюються вимоги відповідних інструкцій (настанов) та які є відповідальними за виконання відповідних завдань;

- опис послідовності, правил і порядку здійснення технологічних операцій в ході виконання відповідальними особами певних завдань адміністрування й обслуговування КСЗІ;

- опис порядку реєстрації фактів і результатів виконання певних завдань у відповідних реєстраційних журналах.

Повинні бути визначені (наприклад, у додатках до інструкцій) форми використаних реєстраційних журналів.

У технологічних (операційних) інструкціях мають бути враховані положення посадових інструкцій співробітників СЗІ та персоналу ІТС.

Технологічні (операційні) інструкції (настанови) щодо виконання завдань адміністрування й обслуговування КСЗІ можуть бути оформлені як у вигляді окремих документів, так і у вигляді структурних частин інших документів, наприклад, Інструкції щодо забезпечення правил оброблення ІзОД в ІТС.

Технологічні (операційні) інструкції (настанови) щодо виконання завдань адміністрування й обслуговування КСЗІ мають бути узгоджені з Розробником ІТС, виконавцем робіт зі створення КСЗІ в ІТС і затверджені керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

Інструкції про порядок використання засобів КЗІ

Інструкції про порядок використання засобів криптографічного захисту інформації (КЗІ) повинні визначати порядок забезпечення безпеки, порядок керування ключовими даними використаними у складі КЗЗ КСЗІ засобів КЗІ та, за необхідності, порядок користування засобами КЗІ. Перелік і зміст відповідних інструкцій визначаються вимогами чинної нормативно-правової бази у сфері КЗІ, зокрема Положенням про порядок розроблення, виробництва й експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису та Положенням про порядок розроблення, виробництва й уведення в експлуатацію засобів криптографічного захисту конфіденційної інформації, що є власністю держави.

Так, відповідно до вимог Положення про порядок розроблення, виробництва й експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису повинні бути розроблені:

- Інструкція із забезпечення безпеки експлуатації засобів КЗІ;
- Інструкція щодо порядку генерації ключових даних і поводження з ключовими документами.

Інструкції про порядок використання засобів КЗІ повинні бути розроблені на основі типових інструкцій, узгоджених відповідним чином із уповноваженим державним органом і затверджені керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

Документація щодо проведених випробувань КСЗІ

До складу документації щодо проведених випробувань КСЗІ, відповідно до положень НД ТЗІ 3.7-003-05 [41], повинні входити:

- Програма та методика випробувань КСЗІ в ІТС;
- Протокол (протоколи) попередніх випробувань КСЗІ в ІТС.

Програма та методика випробувань КСЗІ в ІТС має містити перелік перевірок й опис методів (методик) виконання окремих перевірок, успішне проведення яких дозволяє дійти однозначного висновку щодо відповідності створеної КСЗІ вимогам Технічного завдання на створення КСЗІ в ІТС. Зміст Програми та методики випробувань КСЗІ в ІТС має відповідати вимогам РД 50-34.698-90 [47].

Програма та методика випробувань КСЗІ в ІТС має бути узгоджена з Розробником ІТС, керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС, і затверджена виконавцем робіт зі створення КСЗІ в ІТС.

Протокол (протоколи) попередніх випробувань КСЗІ в ІТС повинен містити:

– задокументовані результати випробувань, передбачених Програмою та методикою випробувань КСЗІ в ІТС;

– перелік виявлених недоліків, необхідних заходів щодо їх усунення та рекомендовані терміни виконання цих робіт;

– висновки щодо можливості прийняття КСЗІ у дослідну експлуатацію.

Зміст Протоколу (протоколів) попередніх випробувань КСЗІ в ІТС має відповідати вимогам РД 50-34.698-90 [47] і рекомендаціям НД ТЗІ 2.7-010-09 [24] для визначеного у Технічному завданні на створення КСЗІ в ІТС рівня гарантій коректності реалізації функціональних послуг безпеки (ФПБ).

Протокол (протоколи) попередніх випробувань має бути підписаний членами комісії з проведення випробувань і затверджений керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

Організаційно-розпорядча документація КСЗІ

До складу організаційно-розпорядчої документації КСЗІ, відповідно до положень НД ТЗІ 3.7-003-05 [41] та інших чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу, повинні входити:

- Акт про приймання КСЗІ в ІТС у дослідну експлуатацію;

- Акт завершення дослідної експлуатації КСЗІ в ІТС;

- Акт завершення робіт зі створення КСЗІ в ІТС.

Зміст Акта про приймання КСЗІ в ІТС у дослідну експлуатацію має відповідати вимогам РД 50-34.698-90 [47]. В Акті про приймання КСЗІ в ІТС у дослідну експлуатацію мають бути відображені задокументовані у Протоколі (протоколах) попередніх випробувань КСЗІ в ІТС, відомості щодо результатів випробувань, виявлених недоліків і необхідних заходів з їх усунення, а також наведені висновки щодо можливості прийняття КСЗІ у дослідну експлуатацію.

Акт про приймання КСЗІ в ІТС у дослідну експлуатацію має бути підписаний членами комісії з проведення випробувань (представниками виконавця робіт зі створення КСЗІ в ІТС, представниками організації (установи), яка є власником (розпорядником) ІТС), і затверджений керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

Акт завершення дослідної експлуатації КСЗІ в ІТС має бути складений у довільній формі. В Акті завершення дослідної експлуатації КСЗІ в ІТС мають бути відображені результати дослідної експлуатації, а також наведені висновки щодо можливості (неможливості) надання КСЗІ на державну експертизу.

Акт завершення дослідної експлуатації КСЗІ в ІТС має бути підписаний представниками виконавця робіт зі створення КСЗІ в ІТС, представниками організації (установи), яка є власником (розпорядником) ІТС, і затверджений керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

Зміст Акта завершення робіт зі створення КСЗІ в ІТС має відповідати вимогам РД 50-34.698-90 [47] й у випадках створення КСЗІ в ІТС, яка являє собою АС класу 1, рекомендаціям НД ТЗІ 2.5-007-2007 [40].

Акт завершення робіт зі створення КСЗІ в ІТС має бути підписаний представниками виконавця робіт зі створення КСЗІ в ІТС, представниками організації (установи), яка є власником (розпорядником) ІТС, і затверджений керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

Супровідна документація КСЗІ

До складу супровідної документації КСЗІ, відповідно до положень НД ТЗІ 3.7-003-05 [41] й інших чинних нормативних документів щодо забезпечення захисту інформації в ІТС певного типу, повинні входити:

– Формуляр ІТС;

– реєстраційні журнали, використані для реєстрації фактів і результатів виконання певних завдань адміністрування й обслуговування КСЗІ.

Форма та зміст Формуляра ІТС мають відповідати вимогам РД 50-34.698-90 [47] та у випадках створення КСЗІ в ІТС, яка являє собою АС класу 1, рекомендаціям НД ТЗІ 2.5-007-2007 [40]. У частині, що стосується відомостей про стан ІТС, Формуляр ІТС може містити посилання на відповідні реєстраційні журнали.

Перелік і форми реєстраційних журналів повинні відповідати визначеним у технологічних (операційних) інструкціях (настановах) щодо виконання завдань адміністрування й обслуговування КСЗІ.

Як приклади зазначених реєстраційних журналів можна розглядати такі:

- Журнал обліку користувачів ІТС;
- Журнал обліку роботи користувачів ІТС;
- Журнал обліку захищених інформаційних ресурсів ІТС;
- Журнал реєстрації проведених робіт із технічного обслуговування, ремонту, модернізації;
- Журнал реєстрації перевірок складу програмних засобів ІТС;
- Журнал реєстрації нештатних ситуацій у роботі ІТС.

Експерт використовує всю документацію під час проведення експертизи об’єкта експертизи.

3.4 Перелік й етапність експертних робіт при проведенні експертизи комплексної системи захисту інформації в інформаційно-телекомунікаційній системі

Програма проведення експертизи КСЗІ в ІТС має передбачати послідовно проведення таких експертних робіт:

– аналіз документації, розробленої на етапі виконання передпроектних робіт;

– аналіз Технічного завдання на створення КСЗІ в ІТС;

– оцінювання (за необхідності) ФПБ, що реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ;

– оцінювання (за необхідності) рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ;

– аналіз проектної документації КСЗІ та матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів КЗЗ КСЗІ;

– аналіз експлуатаційної документації компонентів КЗЗ КСЗІ;

– аналіз нормативно-розпорядчої документації КСЗІ;

– аналіз документації щодо проведених випробувань КСЗІ;

– аналіз організаційно-розпорядчої документації КСЗІ;

– перевірка фактичного використання введених до складу КЗЗ КСЗІ засобів захисту інформації;

– перевірка порядку використання введених до складу КЗЗ КСЗІ засобів захисту інформації;

– перевірка впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших нетехнічних заходів захисту;

– перевірка підготовленості співробітників СЗІ, персоналу та користувачів ІТС;

– перевірка (за необхідності) результатів створення й атестації комплексу ТЗІ.

В усіх випадках, на завершення кожного етапу проведення експертних робіт перевіряється, що відповідна даному етапу документація, технічні завдання,

проектна документація тощо, узгоджена та затверджена у порядку, передбаченому положенням чинної нормативно-правової бази у сфері ТЗІ.

Аналіз документації, розробленої на етапі виконання передпроектних робіт, повинен передбачати виконання Експертом необхідних дій із метою підтвердження того, що:

Склад і зміст документації, розробленої на етапі виконання передпроектних робіт, відповідає положенням чинної нормативно-правової бази у сфері ТЗІ, які стосуються забезпечення захисту інформації, оброблюваної в ІТС.

Вміст документації відповідає особливостям конкретної ІТС й умовам її функціонування, визначеним на етапах попереднього ознайомлення з об'єктом експертизи та поглибленого обстеження об'єкта експертизи.

Аналіз Технічного завдання на створення КСЗІ в ІТС, повинен передбачати виконання Експертом дій із метою підтвердження того, що:

У Технічному завданні на створення КСЗІ в ІТС у повному обсязі та коректно враховані:

- положення чинної нормативно-правової бази у сфері ТЗІ, які стосуються забезпечення захисту інформації, оброблюваної в ІТС;
- особливості конкретної ІТС й умови її функціонування, визначені на етапах попереднього ознайомлення з об'єктом експертизи та поглибленого його обстеження, а також наведені у документації, розробленій на етапі виконання передпроектних робіт.

Реалізація визначеного у Технічного завданні на створення КСЗІ в ІТС переліку вимог є достатньою для задоволення вимог чинних нормативних документів щодо забезпечення захисту інформації, оброблюваної в ІТС.

Оцінювання ФПБ, які реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ, має врахувати склад і зміст матеріалів (документів), наданих для оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ, створення й експертиза яких здійснюється у ході створення та проведення експертизи КСЗІ та відповідати вимогам НД ТЗІ 2.7-009-09 [23] для визначеного у Технічному завданні на створення КСЗІ в ІТС рівня гарантій коректності реалізації ФПБ.

Оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ, має врахувати склад і зміст матеріалів (документів), наданих для оцінювання рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ, створення й експертиза яких здійснюється у ході створення та проведення експертизи КСЗІ та відповідати вимогам НД ТЗІ 2.7-010-09 [24] для визначеного у Технічному завданні на створення КСЗІ в ІТС рівня гарантій коректності реалізації ФПБ.

Аналіз проектної документації КСЗІ та матеріалів, які містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ, має передбачати виконання Експертом необхідних дій із метою підтвердження того, що:

Склад і зміст проектної документації КСЗІ відповідає положенням чинної нормативно-правової бази у сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС.

У проектній документації належним чином відображено порядок реалізації усіх вимог, висунутих у Технічному завданні на створення КСЗІ в ІТС.

У проектній документації належним чином враховано особливості конкретної ІТС й умови її функціонування, визначені на етапах попереднього ознайомлення з об'єктом експертизи та його поглибленого обстеження, а також зазначені у документації, розробленій на етапі передпроектних робіт.

У складі матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ для всіх окремих компонентів (складових частин) КЗЗ КСЗІ, зазначених у проектній документації, наявні Експертні висновки (сертифікати) щодо відповідності вимогам чинних нормативних документів системи ТЗІ та/або КЗІ.

Зміст матеріалів, що містять результати державної експертизи (сертифікації) всіх окремих компонентів (складових частин) КЗЗ КСЗІ, зазначених у проектній документації, підтверджує можливість використання відповідних засобів.

Визначений у проектній документації КСЗІ перелік заходів захисту, засобів їх реалізації, а також порядок функціонування відповідних засобів є дієвим і достатнім для задоволення вимог Технічного завдання на створення КСЗІ.

Аналіз експлуатаційної документації компонентів КЗЗ КСЗІ, має передбачати виконання Експертом дій із метою підтвердження того, що:

Склад і зміст експлуатаційної документації компонентів КЗЗ КСЗІ відповідає визначеному у проектній документації КСЗІ складу КЗЗ КСЗІ та відповідає положенням чинної нормативно-правової бази у сфері ТЗІ.

В експлуатаційній документації компонентів КЗЗ КСЗІ наявні відомості щодо порядку застосування відповідних компонентів КЗЗ КСЗІ при реалізації (з урахуванням положень проектної документації КСЗІ) всіх ФПБ (функцій захисту), визначених у Технічному завданні на створення КСЗІ в ІТС.

Аналіз нормативно-розпорядчої документації КСЗ, має передбачати виконання Експертом необхідних дій із метою підтвердження того, що:

Склад нормативно-розпорядчої документації КСЗІ відповідає визначеному у проектній документації КСЗІ складу КСЗІ та відповідає положенням чинної нормативно-правової бази у сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС.

У нормативно-розпорядчій документації КСЗІ належним чином враховано:

– положення чинної нормативно-правової бази у сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС;

– особливості функціонування компонентів КЗЗ КСЗІ, наведені у проектній та експлуатаційній документації у процесі функціонування КСЗІ;

– особливості реалізації організаційних, фізичних й інших заходів захисту, зазначені у проектній документації КСЗІ.

Дотримання положень нормативно-розпорядчої документації забезпечує можливість задоволення вимог Технічного завдання на створення КСЗІ в ІТС із

урахуванням особливостей реалізації організаційних, фізичних та інших заходів захисту, наведених у проектній документації КСЗІ.

Аналіз документації щодо проведених випробувань КСЗІ, має передбачати виконання Експертом необхідних дій із метою підтвердження того, що:

Склад і зміст документації щодо проведених випробувань КСЗІ відповідає положенням чинної нормативно-правової бази у сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється ІТС.

У документації щодо проведених випробувань КСЗІ:

– належним чином враховано особливості функціонування компонентів КЗЗ КСЗІ, наведені у проектній та експлуатаційній документації;

– належним чином враховано особливості реалізації організаційних, фізичних та інших заходів захисту, наведені у проектній і нормативно-розпорядчій документації КСЗІ.

– наявні відомості стосовно результатів випробувань, які підтверджують задоволення засобами КСЗІ всіх вимог Технічного завдання на створення КСЗІ.

Аналіз організаційно-розпорядчої документації КСЗІ, має передбачати виконання Експертом необхідних дій із метою підтвердження того, що:

Склад і зміст організаційно-розпорядчої документації КСЗІ відповідає положенням чинної нормативно-правової бази у сфері ТЗІ, які стосуються забезпечення захисту інформації, що обробляється в ІТС відповідного типу.

В організаційно-розпорядчій документації КСЗІ належним чином враховані результати випробувань КСЗІ, наведені у документації щодо проведених випробувань КСЗІ.

Перевірка фактичного використання введених до складу КЗЗ КСЗІ засобів захисту інформації має передбачати виконання Експертом необхідних дій із метою підтвердження того, що:

Серед компонентів КЗЗ КСЗІ, розгорнутих на базі відповідних компонентів обчислювальної системи ІТС, наявні всі компоненти КЗЗ, визначені у проектній документації КСЗІ.

Усі компоненти КЗЗ належним чином відображені у супровідній документації КСЗІ. Усі компоненти КЗЗ КСЗІ інстальовані й ініціалізовані відповідно до положень експлуатаційної документації та нормативно-розпорядчої документації КСЗІ.

Фактичні параметри налаштування всіх наявних компонентів КЗЗ КСЗІ відповідають визначеному в експлуатаційній документації та нормативно-розпорядчої документації КСЗІ порядку застосування відповідних компонентів КЗЗ при реалізації (з урахуванням положень проектної документації КСЗІ) всіх ФПБ (функцій захисту), визначених у Технічному завданні на створення КСЗІ.

Усі компоненти (складові частини) КЗЗ КСЗІ знаходяться у працездатному стані та функціонують належним чином.

Перевірка порядку використання введених до складу КЗЗ КСЗІ засобів захисту інформації має передбачати виконання Експертом необхідних дій із метою підтвердження того, що:

Фактично використаний порядок створення захищених інформаційних ресурсів, реєстрації користувачів, надання прав доступу до інформації

користувачам ІТС і виконання інших завдань адміністрування й обслуговування КСЗІ відповідає положенням експлуатаційної документації та нормативно-розпорядчої документації КСЗІ.

Фактично використаний порядок реєстрації фактів і результатів виконання певних завдань адміністрування й обслуговування КСЗІ відповідає положенням нормативно-розпорядчої документації КСЗІ.

Вміст наданих у складі супровідної документації КСЗІ в ІТС реєстраційних журналів підтверджує факти належного застосування визначеного положеннями нормативно-розпорядчої документації КСЗІ порядку створення захищених інформаційних ресурсів, реєстрації користувачів, надання прав доступу до інформації користувачам ІТС і виконання інших завдань адміністрування й обслуговування КСЗІ.

Фактичні атрибути доступу користувачів, процесів і захищених інформаційних ресурсів, які містяться у відповідних сховищах компонентів КЗЗ КСЗІ, відповідають наведеним у реєстраційних журналах відомостям.

Перевірка впровадження реалізованих у складі КСЗІ організаційних, фізичних й інших заходів захисту має передбачати виконання Експертом необхідних дій із метою підтвердження того, що:

У складі КСЗІ впроваджено всі організаційні, фізичні й інші нетехнічні заходи захисту, визначені у проектній документації КСЗІ та нормативно-розпорядчій документації КСЗІ.

Зміст наданої супровідної документації КСЗІ, а також журналів обліку та реєстрації сховищ і матеріальних носіїв інформації з обмеженим доступом (ІзОД) підтверджує факти належного застосування всіх впроваджених організаційних, фізичних й інших нетехнічних заходів захисту.

Перевірка підготовленості співробітників служби захисту інформації (СЗІ), персоналу та користувачів ІТС повинна передбачати виконання Експертом необхідних дій із метою підтвердження того, що: співробітники СЗІ, персонал і користувачі ІТС мають достатній для виконання своїх посадових та/або функціональних обов’язків рівень знань положень експлуатаційної та нормативно-розпорядчої документації КСЗІ та практичних навиків щодо використання засобів ІТС і КСЗІ.

Перевірка результатів створення й атестації комплексу ТЗІ має передбачати виконання Експертом дій з метою підтвердження того, що:

Склад і характеристики створеного комплексу ТЗІ, наведені у документації щодо створення комплексу ТЗІ, розробленій на етапі виконання передпроектних робіт і на етапі розроблення та впровадження заходів із захисту інформації відповідають особливостям конкретної ІТС й умовам її функціонування, визначеним на етапах попереднього ознайомлення з об’єктом експертизи та його поглибленого обстеження, а також зазначеним у документації, розробленій на етапі передпроектних робіт зі створення КСЗІ.

Відомості, наведені у документації, розробленій на етапі випробувань й атестації комплексу ТЗІ підтверджують відповідність створеного комплексу ТЗІ вимогам технічного завдання та положенням чинної нормативно-правової бази

у сфері ТЗІ, які стосуються забезпечення захисту інформації від витоку технічними каналами.

Питання для самоконтролю

1. Якими нормативними документами впорядковується проведення державної експертизи засобів технічного захисту інформації?
2. Які дві частини виокремлюються у проблемі захисту від НСД інформації, оброблюваної в ІТС.
3. Назвіть складові КСЗІ у рамках спеціалізованих (штатних) ЗЗІ та загальних засобів ТЗІ, створюваних поза системою.
4. Хто є суб'єктами й об'єктами державної експертизи?
5. Сформулюйте мету державної експертизи.
6. Сформулюйте основні принципи проведення державної експертизи, що забезпечують максимальну достовірність і повноту результатів при організації та проведенні експертизи.
7. Які етапи експертних робіт передбачаються при проведенні первинної експертизи?
8. Яка мета, які повинні бути виконані дії, та що повинні проаналізувати Експерти на етапі попереднього ознайомлення з об'єктом експертизи?
9. Яка мета, які повинні бути виконані дії, та що повинні проаналізувати Експерти на етапі поглибленого обстеження об'єкта експертизи?
10. Яка мета, які повинні бути виконані дії, та що повинні проаналізувати Експерти на етапі розроблення програми експертизи?
11. Яка мета, які повинні бути виконані дії, та що повинні проаналізувати Експерти на етапі розроблення методики експертизи?
12. Яка мета, які повинні бути виконані дії, та що повинні проаналізувати Експерти на етапі проведення експертних випробувань і досліджень об'єкта експертизи за розробленими програмою та методикою?
13. Яка мета, які повинні бути виконані дії, та що повинні проаналізувати Експерти на етапі документування та затвердження результатів експертизи?
14. Яка документація замовника, надається при проведенні державної експертизи на етапі виконання передпроектних робіт?
15. Зміст переліку інформації, що підлягає обробленню в ІТС і потребує захисту.
16. Зміст Положення про службу захисту інформації (СЗІ) в ІТС.
17. Зміст опису політики безпеки інформації в ІТС.
18. Зміст опису моделі порушника безпеки інформації в ІТС.
19. Зміст опису моделі загроз для інформації, що обробляється в ІТС.
20. Зміст плану захисту інформації в ІТС.
21. Зміст технічного завдання на створення КСЗІ в ІТС.
22. Зміст документації технічного проекту КСЗІ.

Розділ 4

ПРОГРАМА ТА МЕТОДИКА ПРОВЕДЕННЯ ДЕРЖАВНОЇ ЕКСПЕРТИЗИ КОМПЛЕКСНИХ СИСТЕМ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОКОМУНІКАЦІЯХ

Зміст програми та методики проведення експертизи комплексної системи захисту інформації (КСЗІ) в інформаційно-телекомунікаційній системі (ІТС) визначається положеннями чинної нормативно-правової бази у сфері технічного захисту інформації (ТЗІ)), що регламентує порядок проведення робіт зі створення та експертизи КСЗІ в ІТС: «Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [22]», НД ТЗІ 2.6-001-11 [37], НД ТЗІ 2.7-009-09 [23], НД ТЗІ 2.7-010-09 [24]. При цьому, враховуються рекомендації щодо складу та змісту проектної, експлуатаційної та нормативно-розпорядчої документації, яка надається Замовником при проведенні експертизи КСЗІ. Терміни та визначення, що стосуються оцінки інформаційної захищеності телекомунікацій, наведені у додатку 1.

Цілі й основні положення державної експертизи комплексної системи захисту інформації в інформаційно-телекомунікаційних системах детально викладені у пункті 3.1 цього навчального посібника. Тут розглянемо загальний зміст програми проведення експертизи.

4.1 Загальний зміст програми проведення експертизи та спеціальні запитання на етапах експертних робіт

Об’єктом експертизи на відповідність НД ТЗІ в Україні у частині, що стосується оцінювання функціональних послуг безпеки, можуть бути комплекси засобів захисту (КЗЗ) комплексних систем захисту інформації (КСЗІ), засоби технічного захисту інформації (ЗТЗІ) від несанкціонованого доступу (НСД), а також захищені від НСД компоненти інформаційно-телекомунікаційної системи (ІТС). В усіх трьох випадках об’єкт експертизи (ОЕ) складається, як правило, зі множини компонентів, деякі з яких спеціально призначені для реалізації функціональних послуг безпеки (ФПЗ), інші можуть впливати на забезпечення захисту опосередковано, наприклад, забезпечувати функціонування компонентів першого типу.

Програма проведення експертизи КСЗІ в ІТС за своїм змістом має передбачати послідовне проведення таких експертних робіт:

- аналіз документації, розробленої на етапі виконання передпроектних робіт;
- аналіз Технічного завдання на створення КСЗІ в ІТС;
- оцінювання (за необхідності) ФПБ, що реалізуються окремими компонентами (складовими частинами) КЗЗ КСЗІ;
- оцінювання (за необхідності) рівня гарантій коректності реалізації ФПБ в окремих компонентах (складових частинах) КЗЗ КСЗІ;

- аналіз проектної документації КСЗІ та матеріалів, що містять результати державної експертизи (сертифікації) окремих компонентів КЗЗ КСЗІ;
- аналіз експлуатаційної документації компонентів КЗЗ КСЗІ;
- аналіз нормативно-розпорядчої документації КСЗІ;
- аналіз документації щодо проведених випробувань КСЗІ;
- аналіз організаційно-розпорядчої документації КСЗІ;
- перевірка фактичного використання та порядку використання введених до складу КЗЗ КСЗІ засобів захисту інформації;
- перевірка впровадження реалізованих у складі КСЗІ організаційних, фізичних та інших нетехнічних заходів захисту;
- перевірка підготовленості співробітників СЗІ, персоналу та користувачів;
- перевірка (за необхідності) результатів створення й атестації комплексу ТЗІ.

Специфічні вимоги щодо змісту програми випробувань функціональних послуг безпеки різних типів і різних рівнів складені з урахуванням вимог НД ТЗІ 2.5-004-99 [17] до політики функціональних послуг, а також із урахуванням результатів ідентифікації функціональних послуг безпеки, уточнення їх рівнів і політики, отриманих експертом із використанням переліку спеціальних питань.

Відповіді на спеціальні питання повинні допомогти експерту усвідомити склад і архітектуру об’єкта експертизи, а також склад, архітектуру й основні особливості реалізації його КЗЗ. Відповіді повинні бути сформульовані на початковому етапі попереднього аналізу об’єкта експертизи та, за необхідності, можуть бути уточнені у процесі поглибленого аналізу особливостей реалізації різних функціональних послуг безпеки.

Спеціальні питання щодо складу й архітектури об’єкта експертизи.

Питання 1. Наведіть перелік компонентів ІТС, на базі якої функціонує ОЕ, їх основні характеристики (тип, версія тощо) та стислий опис архітектури ІТС.

Під компонентами ІТС слід розуміти як апаратні компоненти (сервери, робочі станції, активне мережеве обладнання, канали локальних обчислювальних мереж, канали мереж передачі даних тощо), так і програмні засоби (операційні системи, системи управління базами даних (СУБД), сервери застосувань тощо).

Питання 2. Наведіть перелік основних функціональних модулів об’єкта експертизи, стислий опис кожного функціонального модуля з наведенням його призначення (з погляду функцій оброблення інформації, які реалізуються об’єктом експертизи), характеру та вигляду подання оброблюваної інформації, основних зв’язків (потоків команд і даних) з іншими функціональними модулями об’єкта експертизи та використаних при цьому інтерфейсів, характеру та вигляду подання інформації, що передається між функціональними модулями об’єкта у процесі його функціонування.

Під функціональними модулями слід розуміти компоненти, що реалізують чітко визначену функціональність. Наприклад, для операційної системи такими є: ядро; програми оброблення переривань; менеджер процесів; оброблювачі запитів введення-виведення інформації; менеджер введення-виведення інформації; інтерфейси користувач/процес; інтерфейси прикладного

програмування; програми діагностики апаратури; програми тестування апаратури; командні мови/інтерфейси (використані для генерації системи операторами, адміністраторами, користувачами тощо).

Питання 3. Для кожного з функціональних модулів вкажіть, на базі або з використанням яких компонентів ІТС він функціонує.

Спеціальні питання щодо складу й архітектури КЗЗ об'єкта експертизи.

Питання 4. Наведіть перелік основних функціональних модулів об'єкта експертизи, що входять до складу КЗЗ, тобто спеціально призначені або для реалізації функціональних послуг безпеки, або для реалізації функцій, які впливають на реалізацію функцій захисту опосередковано.

Питання 5. Наведіть опис архітектури КЗЗ на рівні функціональних модулів КЗЗ, реалізованих у різних функціональних модулях об'єкта експертизи, виділивши в описі ядро КЗЗ й інші його компоненти. Наведіть стислий опис кожного функціонального модуля КЗЗ із наведенням його призначення, реалізованих функціональних послуг безпеки, характеру та вигляду подання оброблюваної інформації, основних зв'язків (потоків команд і даних) із іншими функціональними модулями КЗЗ і використаних при цьому інтерфейсів, а також основних зв'язків (потоків команд і даних) із функціональними модулями ОЕ, що не входять до складу КЗЗ, і використаних при цьому інтерфейсів.

Під ядром КЗЗ слід розуміти апаратні засоби, вбудоване програмне забезпечення (програми постійних запам'ятовуючих пристроїв (ПЗП)) і програмні засоби, що безпосередньо реалізують концепцію диспетчера доступу, тобто, є посередником при всіх спробах (запитах) доступу активних об'єктів (користувачів, процесів) до пасивних об'єктів.

Спеціальні питання щодо об'єктів, що мають відношення до політики функціональних послуг безпеки. Відповідно до підходу, визначеного у діючих НД ТЗІ, КЗЗ розглядає ресурси ОЕ як об'єкти та керує взаємодією цих об'єктів згідно з реалізованою політикою функціональних послуг безпеки. Як об'єкти ресурси характеризуються двома аспектами: логічне подання (вміст, семантика, значення) та фізичне (форма, синтаксис). Об'єкт характеризується своїм станом, який, у свою чергу, характеризується атрибутами та поведінкою, що визначає способи зміни стану. При розгляді взаємодії двох об'єктів ОЕ, які виступають як приймачі або джерела інформації, слід виділяти пасивний об'єкт, над яким виконується операція, й активний об'єкт, який виконує або ініціює цю операцію. При визначенні політики функціональних послуг безпеки повинні виділятися та розглядатися такі типи об'єктів: об'єкти-користувачі, об'єкти-процеси та пасивні об'єкти.

Об'єкти-користувачі й об'єкти-процеси є такими лише всередині конкретного домену – ізольованої логічної області, всередині якої об'єкти мають певні властивості, повноваження та зберігають певні відносини. В інших доменах об'єкти залишаються у пасивному стані. Це дозволяє одному об'єкту-процесу керувати іншим процесом або навіть об'єктом-користувачем, оскільки останній залишається «пасивним» із погляду керуючого об'єкта. Іншими

словами, об’єкти можуть знаходитися в одному з трьох різних станів: об’єкт-користувач, об’єкт-процес і пасивний об’єкт. Перехід між станами означає, що об’єкт просто розглядається в іншому контексті. Взаємодія двох об’єктів (звернення активного об’єкта до пасивного з метою отримання певного виду доступу) призводить до появи потоку інформації між об’єктами та/або зміни стану ОЕ. Як потік інформації розглядається будь-яка порція інформації, передана між об’єктами.

Відповіді на питання повинні допомогти експерту усвідомити перелік об’єктів і набір їх основних атрибутів, використаних функціональними модулями КЗЗ при реалізації різних функціональних послуг безпеки.

Спеціальні питання щодо об’єктів-користувачів та атрибутів доступу.

Питання 6. Наведіть перелік різних ролей (типів) користувачів (що характеризуються чітко визначеною сукупністю доступних користувачам функцій із керування об’єктом експертизи, КЗЗ й оброблення інформації), які підтримуються в об’єкті експертизи.

Під користувачем слід розуміти фізичну особу, яка може взаємодіяти з об’єктом експертизи за допомогою наданого їй інтерфейсу. Як приклади ролей користувачів, підтримуваних, наприклад, операційною системою, можуть розглядатися такі ролі: системний оператор; адміністратор системи; оператор резервного копіювання; досвідчений користувач; користувач тощо.

Питання 7. Для кожної з ролей наведіть опис порядку створення та знищення об’єктів-користувачів відповідного типу, а також вигляду їх представлення в усіх функціональних модулях, що входять до складу КЗЗ.

В описах, що наводяться, для кожного функціонального модуля, що входить до складу КЗЗ, повинно бути зазначено, в який момент та яким чином створюються об’єкти-користувачі певного типу, що є представленням фізичних користувачів в об’єкті експертизи (наприклад, вони можуть створюватися при вході користувача у систему, при породженні процесу, встановленні з’єднання тощо), яким чином (у вигляді спеціальних структур даних або будь-яким іншим способом) представляються об’єкти-користувачі у функціональному модулі ОЕ, з яким об’єктом системи зв’язуються структури даних (маркери), що представляють користувачів у функціональному модулі (наприклад, із породженим процесом, активним мережевим з’єднанням, підключеним до сервера віддаленим терміналом або робочою станцією тощо), яким чином (наприклад, при завершенні процесу, закритті мережевого з’єднання, відключенні від сервера віддаленого термінала або робочої станції) знищуються об’єкти-користувачі та структури даних (маркери), що представляють їх у функціональному модулі.

Питання 8. Для кожного з типів об’єктів-користувачів і кожного вигляду їх представлення у різних функціональних модулях, що входять до складу КЗЗ, наведіть опис складу структур даних (маркерів), що представляють користувачів у функціональних модулях, у вигляді опису переліку та можливих значень атрибутів доступу об’єктів-користувачів, що входять або не входять до складу цих структур, але однозначно пов’язані з ними.

Як можливі атрибути доступу об’єктів-користувачів, що входять до складу структур даних (маркерів), які представляють користувачів у функціональних модулях, що входять до складу КЗЗ, або однозначно пов’язані з ними, можуть, наприклад, бути використані: псевдонім користувача; ідентифікатор користувача; ідентифікатори груп, членом яких є користувач; ідентифікатор ролі користувача; рівень допуску користувача; ознаки наявності/відсутності у користувача різних адміністративних повноважень; список повноважень користувача, що визначає права доступу до різних пасивних об’єктів тощо.

Спеціальні питання щодо об’єктів-процесів та їх атрибутів доступу.

Питання 9. Наведіть перелік різних типів процесів (процесів, які породжуються з програм із різним виглядом подання виконуваного коду), що підтримуються в об’єкті експертизи.

Як приклади різних типів процесів, залежно від призначення, архітектури та прикладної функціональності об’єкта експертизи, можуть розглядатися, наприклад, такі: прикладні та системні програми у вигляді виконуваних модулів; динамічні бібліотеки; системні драйвери; скриптові модулі; процедури та методи, що реалізують різні прикладні функції у межах об’єкта тощо.

Питання 10. Для кожного з типів процесів наведіть опис порядку створення та знищення об’єктів-процесів відповідного типу, а також вигляду їх представлення в усіх функціональних модулях, що входять до складу КЗЗ.

В описах, що наводяться, для кожного функціонального модуля, що входить до складу КЗЗ, повинно бути зазначено, яким чином при запуску програм створюються об’єкти-процеси певного типу, яким чином (у вигляді спеціальних структур даних або інакше) представляються об’єкти-процеси у функціональному модулі, яким чином (наприклад, при завершенні процесу, завершенні батьківського процесу тощо) знищуються об’єкти-процеси та структури даних (маркери), що представляють їх у функціональному модулі.

Питання 11. Для кожного з типів об’єктів-процесів і кожного вигляду їх представлення у різних функціональних модулях, що входять до складу КЗЗ, наведіть опис складу структур даних (маркерів), які представляють процеси у функціональних модулях, у вигляді опису переліку та можливих значень атрибутів доступу об’єктів-процесів, що входять або не входять до складу цих структур, але однозначно пов’язані з ними.

Як можливі атрибути доступу об’єктів-процесів, що входять до складу структур даних (маркерів), які представляють процеси у функціональних модулях, що входять до складу КЗЗ, або однозначно пов’язані з ними, можуть, наприклад, бути використані: найменування програми (процесу); ідентифікатор процесу; ідентифікатори груп, до яких входить процес; рівень допуску процесу; ознаки наявності/відсутності у процесі різних адміністративних повноважень; список повноважень процесу, що визначає права доступу до різних пасивних об’єктів тощо.

Питання 12. Для кожного з типів об’єктів-процесів, кожного вигляду їх представлення у різних функціональних модулях, що входять до складу КЗЗ і різного складу структур даних (маркерів), що представляють процеси у функціональних модулях, наведіть опис порядку та правил ініціалізації й

успадкування атрибутів доступу дочірніх процесів від об’єктів-користувачів або об’єктів-процесів, що їх породжують.

Спеціальні питання щодо пасивних об’єктів та їх атрибутів доступу.

Питання 13. Наведіть перелік різних типів пасивних об’єктів, у вигляді яких можуть бути представлені у процесі функціонування об’єкта експертизи інформаційні ресурси, що зберігаються, обробляються та передаються у процесі функціонування об’єкта експертизи та над якими виконуються певні дії.

Як приклади різних типів пасивних об’єктів, залежно від призначення, архітектури та прикладної функціональності об’єкта експертизи, можуть розглядатися, наприклад, такі: каталоги; файли; сегменти оперативної пам’яті; процеси; зовнішні пристрої; таблиці СУБД; записи таблиць СУБД; джерела та/або приймачі даних для мережевих комунікацій тощо.

Питання 14. Для кожного з типів пасивних об’єктів наведіть опис порядку створення (ініціалізації) та знищення пасивних об’єктів і пов’язаних із ними наборів атрибутів доступу у процесі оброблення в усіх функціональних модулях об’єкта експертизи, що входять до складу КЗЗ.

В описах, які наводяться, для кожного функціонального модуля, що входить до складу КЗЗ, повинно бути зазначено, в якому вигляді створюються (ініціалізуються) нові пасивні об’єкти, яким чином (у вигляді спеціальних структур даних або в інший спосіб) надаються пов’язані з ними набори атрибутів доступу у цьому функціональному модулі, яким чином виконується знищення пасивних об’єктів і пов’язаних із ними наборів атрибутів доступу.

Питання 15. Для кожного з типів пасивних об’єктів наведіть опис складу наборів атрибутів доступу у вигляді опису переліку та можливих значень атрибутів доступу пасивних об’єктів, що входять до складу цих наборів.

Як можливі атрибути доступу пасивних об’єктів, що входять до складу наборів атрибутів доступу, можуть, наприклад, бути використані: найменування пасивного об’єкта; ідентифікатор пасивного об’єкта; ідентифікатор власника пасивного об’єкта; ідентифікатор групи власника пасивного об’єкта; рівень доступу; мітка доступу; список керування доступом, що визначає права доступу різних об’єктів-користувачів, об’єктів-процесів та/або їх груп до пасивного об’єкта тощо.

4.2 Програма випробування функціональних послуг безпеки критеріїв конфіденційності

Комплекс заходів захисту (КЗЗ), оцінюваної на предмет відповідності критеріям конфіденційності інформаційно-телекомунікаційної системи, має надавати послуги із захисту об’єктів від несанкціонованого ознайомлення з їх змістом, тобто компрометації. До функціональних послуг безпеки критеріїв конфіденційності відносяться:

КД – довірча конфіденційність;

КА – адміністративна конфіденційність;

КО – повторне використання об’єктів;

КК – аналіз прихованих каналів;
КВ – конфіденційність при обміні.

4.2.1 Спеціальні питання щодо послуги довірчої/адміністративної конфіденційності

Послуги довірчої/адміністративної конфіденційності забезпечують можливість керування потоками інформації від захищених пасивних об'єктів до об'єктів-користувачів із метою захисту пасивних об'єктів від несанкціонованого ознайомлення з їх вмістом (компрометації). Відповіді на питання повинні допомогти експерту з'ясувати факт реалізації в об'єкті експертизи послуг довірчої/адміністративної конфіденційності, перелік об'єктів різного типу, стосовно яких визначено політику та реалізовані ці функціональні послуги безпеки, атрибутів доступу, використаних функціональними модулями КЗЗ при реалізації відповідних послуг. Сформульовані відповіді дозволять експерту визначити рівні, політику, засоби, механізми й особливості реалізації послуг довірчої/адміністративної конфіденційності, а також отримати вхідні дані для розроблення програм і методик випробувань цих послуг.

Послуги довірчої/адміністративної конфіденційності ранжируються за рівнями 1 … 4 на підставі повноти захисту та вибірковості керування потоками інформації:

КД-1 – мінімальна довірча/адміністративна конфіденційність;
КД-2 – базова довірча/адміністративна конфіденційність;
КД-3 – повна довірча/адміністративна конфіденційність;
КД-4 – абсолютна довірча/адміністративна конфіденційність.

Питання 16. Чи існує для будь-якого з типів пасивних об'єктів можливість розмежування доступу з боку користувачів, що відносяться до будь-яких з ролей, або процесів різного типу до пасивних об'єктів цього типу з метою отримання інформації, що міститься у пасивному об'єкті.

Якщо такої можливості не існує, тобто, всі користувачі у межах певної ролі або всі процеси певного типу завжди мають однакові можливості доступу з метою отримання інформації (читання) до всієї множини пасивних об'єктів усіх типів, то це означає, що послуги довірчої та/або адміністративної конфіденційності засобами КЗЗ ОЕ не реалізуються. Якщо ж така можливість існує, то це означає, що засобами КЗЗ реалізуються послуги довірчої та/або адміністративної конфіденційності, їх політики та рівні можуть бути уточнені при відповіді на наступні питання.

Питання 17. Чи існують у складі будь-яких функціональних модулів, що входять до складу КЗЗ, засоби та відповідні механізми керування доступом з боку об'єктів-користувачів або об'єктів-процесів одного чи декількох типів, до пасивних об'єктів одного чи декількох типів, шляхом аналізу запитів на доступ із боку користувачів або об'єктів-процесів із метою отримання інформації, що міститься у пасивному об'єкті, та прийняття рішення на підставі інформації, що міститься у наборах атрибутів доступу ініціатора запиту та пасивного об'єкта. Чи існують у складі будь-яких функціональних модулів, що входять до складу

КЗЗ засоби, які дозволяють користувачам, що відносяться до будь-яких із ролей, змінювати набори атрибутів доступу об’єктів-користувачів та/або об’єктів-процесів і пасивних об’єктів.

Механізмами, що забезпечують реалізацію послуг довірчої й адміністративної конфіденційності, є механізми керування доступом, тобто надання можливості доступу до ресурсу згідно зі спеціально визначеними правилами. Як основні схеми, на підставі яких може здійснюватися керування доступом, можуть бути використані такі:

– на підставі списків керування доступом (під списком керування доступом слід розуміти пов’язаний із запитуваним ресурсом набір атрибутів доступу у вигляді сукупностей ідентифікаторів ініціаторів запиту й атрибутів, що визначають дозволені види доступу або операції над запитуваним ресурсом);

– на підставі списків повноважень (під списком повноважень слід розуміти пов’язаний із ініціатором запиту набір атрибутів доступу у вигляді сукупності операцій, дозволених над заданою множиною запитуваних ресурсів);

– на підставі міток безпеки (під мітками слід розуміти атрибути доступу, пов’язані як із ініціатором запиту, так зі запитуваним ресурсом, рішення про надання доступу приймається на підставі оброблення міток ініціатора та ресурсу за заданими правилами). Для прийняття рішення про можливість надання доступу ці механізми можуть бути використані, наприклад:

– ідентифікатори відповідних об’єктів;

– ідентифікатори груп відповідних об’єктів;

– інформацію про права доступу до пасивних об’єктів у вигляді міток доступу, списків керування доступом або списків повноважень;

– інформацію про права володіння пасивним об’єктом;

– інформацію про час спроби доступу;

– інформацію про маршрут запиту доступу у розподілених системах;

– інформацію про тривалість сеансу доступу до ресурсу.

Засоби керування доступом, що приймають рішення про можливість задоволення або відхилення запиту, повинні бути реалізовані у тих компонентах КЗЗ, що входять до складу ядра КЗЗ і реалізують концепцію диспетчера доступу. Засоби, що дозволяють змінювати атрибути доступу, можуть бути реалізовані у довільних компонентах КЗЗ.

Питання 18. Чи дозволяють реалізовані у складі функціональних модулів, що входять до складу КЗЗ, засоби змінювати атрибути доступу об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів, на підставі яких реалізується керування доступом:

– будь-яким користувачам, що відносяться до кожної з ролей, але лише для частини пасивних об’єктів певних типів, що належать їх домену, тобто з урахуванням атрибутів, що визначають їх права володіння цими об’єктами;

– будь-яким користувачам, що відносяться лише до певних ролей, для всіх пасивних об’єктів певних типів, без урахування атрибутів, що визначають їх права володіння цими пасивними об’єктами.

У випадку позитивної відповіді не можна стверджувати, що засобами КЗЗ реалізуються послуги довірчої чи адміністративної конфіденційності. Політики

та рівні відповідних послуг для пасивних об’єктів різного типу можуть бути уточнені при відповіді на наступні питання.

Питання 19. Чи відноситься політика послуг довірчої або адміністративної конфіденційності, реалізована КЗЗ (чи забезпечується можливість керування доступом користувачів або об’єктів-процесів до пасивних об’єктів:

– до всіх типів об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів;

– лише до певних (укажіть, до яких) типів об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів.

У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ можуть бути реалізовані послуги довірчої конфіденційності рівнів КД-3 чи КД-4 або адміністративної конфіденційності рівнів КА-3 чи КА-4. У випадку негативної відповіді можна стверджувати, що засобами КЗЗ можуть бути реалізовані послуги довірчої конфіденційності рівнів КД-1 чи КД-2 або адміністративної конфіденційності рівнів КА-1 чи КА-2.

Питання 20. На підставі яких атрибутів доступу: об’єктів-процесів і пасивних об’єктів різних типів або об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів і згідно з якими правилами реалізується розмежування доступу для об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів різного типу, до яких відноситься політика послуг довірчої або адміністративної конфіденційності.

Питання 21. В яких функціональних модулях, що входять до складу КЗЗ із використанням механізмів керування доступом, здійснюється оброблення запитів на надання доступу (розмежування доступу) згідно правил для об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів різного типу.

Питання 22. На підставі яких атрибутів пасивних об’єктів та атрибутів доступу об’єктів-користувачів, що визначають права володіння для послуги довірчої конфіденційності або адміністративні повноваження для послуги адміністративної конфіденційності, та згідно з якими правилами здійснюється оброблення запитів на зміну прав доступу до захищених об’єктів для об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів різного типу.

Питання 23. В яких функціональних модулях, що входять до складу КЗЗ, здійснюється оброблення запитів на зміну прав доступу до захищених об’єктів згідно правил для об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів різного типу.

Питання 24. Чи існує у функціональних компонентах, що входять до складу КЗЗ, із використанням атрибутів доступу для об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів різного типу:

– можливість визначення конкретних процесів та/або груп процесів, що мають право отримувати інформацію від об’єкта (чи можна реалізувати послугу довірчої конфіденційності рівня КД-1 або адміністративної конфіденційності рівня КА-1);

– можливість визначення конкретних користувачів та/або груп користувачів, що мають право отримувати інформацію від об’єкта (чи можна реалізувати послугу довірчої конфіденційності рівня КД-2 або адміністративної конфіденційності рівня КА-2);

– можливість визначення конкретних користувачів (і груп користувачів), що мають, а також тих, що не мають права отримувати інформацію від об’єкта (чи можна реалізувати послугу довірчої конфіденційності рівня КД-3 або адміністративної конфіденційності рівня КА-3);

– можливість визначення конкретних користувачів і процесів (і груп користувачів і процесів), що мають, а також тих, що не мають права отримувати інформацію від об’єкта (чи можна реалізувати послугу довірчої конфіденційності рівня КД-3 або адміністративної конфіденційності КА-3).

Питання 25. Чи існує у функціональних компонентах, що входять до складу КЗЗ, із використанням атрибутів доступу для об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів різного типу:

– можливість визначення конкретних користувачів та/або груп користувачів, що мають право ініціювати процес (чи можна реалізувати послугу довірчої конфіденційності рівня КД-2 або адміністративної конфіденційності КА-2);

– можливість визначення конкретних користувачів (і груп користувачів), що мають, а також тих, що не мають права ініціювати процес (чи можна реалізувати послугу довірчої конфіденційності рівня КД-3 чи КД-4 або адміністративної конфіденційності КА-4 чи КА-4).

Питання 26. Які атрибути доступу, що характеризують права доступу до захищених пасивних об’єктів різного типу установлюються: у момент створення пасивного об’єкта чи у момент ініціалізації об’єкта. Укажіть, яке значення призначається кожному атрибуту, обґрунтуйте його безпечність.

Питання 27. Чи зберігаються, якщо так, то які, атрибути доступу пасивних об’єктів, що характеризують права користувачів на отримання інформації з цих об’єктів (укажіть для пасивних об’єктів кожного типу, при експорті об’єкта за межу об’єкта експертизи. Яким чином здійснюється зв’язування переданих наборів атрибутів доступу з експортованими пасивними об’єктами.

Питання 28. Чи зберігаються, якщо так, то які, атрибути доступу пасивних об’єктів, що характеризують права користувачів на отримання інформації з цих об’єктів (укажіть для пасивних об’єктів кожного типу) при імпорті об’єкта із-за межі об’єкта експертизи. Яким чином здійснюється зв’язування прийнятих наборів атрибутів доступу з імпортованими пасивними об’єктами різного типу.

4.2.2 Програми випробувань функціональної послуги безпеки «Довірча конфіденційність»

Спільними для всіх рівнів функціональної послуги безпеки «Довірча конфіденційність» є перевірки таких вимог:

– запити на зміну прав доступу до об’єкта обробляються КЗЗ ОЕ на підставі атрибутів доступу користувачів, які ініціюють запит, й об’єктів за правилами та з використанням засобів, наведених при відповіді на питання 22, 23;

– права доступу до кожного захищеного об’єкта встановлюються у момент його створення або ініціалізації за правилами, наведеними при відповіді на питання 26 для об’єктів різного типу;

– як частина політики послуги представлені правила збереження атрибутів доступу об’єктів різного типу при їх експорті й імпорті, наведені при відповіді на питання 26, 27.

Програма випробувань функціональної послуги безпеки «Мінімальна довірча конфіденційність» рівня КД-1 має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ об’єкта експертизи (ОЕ), та наведена при відповіді на питання 19, відноситься до об’єктів ОЕ всіх типів;

– КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу процесів і захищених об’єктів різного типу, за правилами, з використанням засобів, наведених при відповіді на питання 20, 21;

– КЗЗ ОЕ надає користувачу можливість для захищеного об’єкта кожного типу, що належить його домену, з використанням атрибутів доступу користувачів, процесів й об’єктів різного типу, а також засобів, наведених у вищезгаданих відповідях, визначити конкретні процеси та/або групи процесів, що мають право отримувати інформацію від об’єкта.

Атрибути користувачів різного типу, які ініціюють запити з метою зміни прав доступу до об’єкта, автентифіковані з використанням засобів реалізації послуги «Ідентифікація й автентифікація» рівня НИ-1 або вище згідно політики цієї послуги, наведеної при відповіді на питання 125.

Програма випробувань функціональної послуги безпеки «Базова довірча конфіденційність» рівня КД-2 має передбачати перевірку таких вимог:

– Політика послуги, що реалізується КЗЗ об’єкта експертизи (ОЕ), відноситься до об’єктів ОЕ всіх типів, наведених при відповіді на питання 19;

– КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу користувачів і захищених об’єктів різного типу, за правилами, з використанням засобів, наведених при відповіді на питання 20, 21;

– КЗЗ ОЕ надає користувачу можливість для захищеного об’єкта кожного типу, що належить його домену, з використанням атрибутів доступу користувачів й об’єктів різного типу, а також засобів, наведених при відповіді на питання 22, 23, визначити конкретних користувачів та/або групи користувачів, що мають право отримувати інформацію від об’єкта.

– КЗЗ ОЕ надає користувачу можливість для процесу кожного типу, що належить його домену, з використанням атрибутів доступу користувачів і процесів різного типу, а також засобів, наведених при відповіді на питання 22, 23, визначити конкретних користувачів та/або групи користувачів, що мають право ініціювати процес.

Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об’єкта, запуску процесу або зміни прав доступу до об’єкта, автентифіковані з використанням засобів реалізації послуги «Ідентифікація й автентифікація» рівня НИ-1 або вище згідно політики цієї послуги.

Програма випробувань функціональної послуги безпеки «Повна довірча конфіденційність» рівня КД-3 має передбачати перевірку таких вимог:

– Політика послуги, що реалізується КЗЗ об’єкта експертизи (ОЕ), відноситься до об’єктів ОЕ всіх типів, наведених при відповіді на питання 19;

– КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу користувачів і захищених об’єктів різного типу, за правилами, з використанням засобів, наведених при відповіді на питання 20, 21;

– КЗЗ ОЕ надає користувачу можливість для процесу кожного типу, що належить його домену, з використанням атрибутів доступу користувачів і процесів різного типу, а також засобів, наведених при відповіді на питання 22, 23, визначити конкретних користувачів та/або групи користувачів, що мають, а також тих, що не мають права ініціювати процес.

Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об’єкта, запуску об’єкта, запуску процесу або зміни прав доступу до об’єкта, автентифіковані з використанням засобів реалізації послуги «Ідентифікація й автентифікація» рівня НИ-1 або вище згідно політики цієї послуги.

Згідно політики та правил стосовно поділюваних ресурсів, використаних для збереження захищених пасивних об’єктів усіх типів, реалізується послуга «Повторне використання об’єктів» рівня КО-1.

Програма випробувань функціональної послуги безпеки «Абсолютна довірча конфіденційність» рівня КД-4 має передбачати перевірку таких вимог:

– Політика послуги, що реалізується КЗЗ об’єкта експертизи (ОЕ), відноситься до об’єктів ОЕ всіх типів, наведених при відповіді на питання 19;

– КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу користувачів, процесів і захищених об’єктів різного типу, за правилами, з використанням засобів, наведених при відповіді на питання 20, 21;

КЗЗ ОЕ надає користувачу можливість для захищеного об’єкта кожного типу, що належить його домену, з використанням атрибутів доступу користувачів, процесів й об’єктів різного типу, а також засобів, наведених при відповіді на питання 22, 23, визначити конкретних користувачів та/або групи користувачів, що мають, а також тих, що не мають права отримувати інформацію від об’єкта;

– КЗЗ ОЕ надає користувачу можливість для процесу кожного типу, що належить його домену, з використанням атрибутів доступу користувачів і процесів різного типу, а також засобів, наведених при відповіді на питання 22, 23, визначити конкретних користувачів (групи користувачів), що мають, а також тих, що не мають права ініціювати процес.

Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об’єкта, запуску об’єкта, запуску процесу або зміни прав доступу до об’єкта, автентифіковані з використанням засобів реалізації послуги «Ідентифікація й автентифікація» рівня НИ-1 або вище згідно політики цієї послуги.

Згідно політики та правил стосовно поділюваних ресурсів, використаних для збереження захищених пасивних об’єктів усіх типів, реалізується послуга «Повторне використання об’єктів» рівня КО-1.

4.2.3 Програми випробувань функціональної послуги безпеки «Адміністративна конфіденційність»

Спільними для всіх рівнів функціональної послуги безпеки «Адміністративна конфіденційність» є перевірки таких вимог:

– запити на зміну прав доступу обробляються КЗЗ ОЕ за правилами та з використанням засобів, наведених при відповіді питання 22, 23, лише у тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження та які відносяться до їх ролей згідно політики реалізованої КЗЗ послуги «Розмежування обов'язків» рівня НО-1 або вище;

– права доступу до кожного захищеного об'єкта встановлюються у момент його створення або ініціалізації за правилами, наведеними при відповіді на питання 26 для об'єктів різного типу;

– як частина політики послуги представлені правила збереження атрибутів доступу об'єктів різного типу при їх експорті й імпорті, наведені при відповіді на питання 26, 27.

***Програма випробувань функціональної послуги безпеки «Мінімальна адміністративна конфіденційність» рівня КА*-1** має передбачати перевірку:

– політика послуги, що реалізується КЗЗ об'єкта експертизи (ОЕ), та наведена при відповіді на питання 19, відноситься до об'єктів ОЕ всіх типів;

– КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу процесів і захищених об'єктів різного типу, за правилами, з використанням засобів, наведених при відповіді на питання 20, 21;

– запити на зміну прав доступу обробляються КЗЗ ОЕ за правилами та з використанням засобів, наведених при відповіді питання 22, 23, лише у тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження та які відносяться до їх ролей згідно політики реалізованої КЗЗ послуги «Розмежування обов'язків» рівня НО-1 або вище;

– КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для захищеного об'єкта кожного типу, з використанням атрибутів доступу користувачів, процесів й об'єктів різного типу, а також засобів, наведених при відповіді на питання 22, 23, шляхом керування приналежністю процесів й об'єктів до відповідних доменів визначити конкретні процеси та/або групи процесів, що мають право отримувати інформацію від об'єкта.

Атрибути користувачів різного типу, які ініціюють запити з метою зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги «Ідентифікація й автентифікація» рівня НИ-1 або вище згідно політики цієї послуги, наведеної при відповіді на питання 125.

***Програма випробувань функціональної послуги безпеки «Базова адміністративна конфіденційність» рівня КА*-2** має передбачати перевірку:

– політика послуги, що реалізується КЗЗ об'єкта експертизи (ОЕ), відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на питання 19;

– КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу користувачів і захищених об'єктів різного типу, за правилами, з використанням засобів, наведених при відповіді на питання 20, 21;

– КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для захищеного об'єкта кожного типу, з використанням атрибутів доступу користувачів й об'єктів різного типу, а також

засобів, наведених при відповіді на питання 22, 23, шляхом керування приналежністю користувачів, процесів й об'єктів до відповідних доменів визначити конкретних користувачів та/або групи користувачів, що мають право отримувати інформацію від об'єкта;

– КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для процесу кожного типу, з використанням атрибутів доступу користувачів і процесів різного типу а також засобів, наведених при відповіді на питання 22, 23, шляхом керування приналежністю користувачів і процесів до відповідних доменів визначити конкретних користувачів та/або групи користувачів, що мають право ініціювати процес.

Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги «Ідентифікація й автентифікація» рівня НИ-1 або вище згідно політики цієї послуги.

Програма випробувань функціональної послуги безпеки «Повна адміністративна конфіденційність» рівня КА-3 має передбачати перевірку:

– політика послуги, що реалізується КЗЗ об'єкта експертизи (ОЕ), відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на питання 19;

– КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу користувачів і захищених об'єктів різного типу, за правилами, з використанням засобів, наведених при відповіді на питання 20, 21;

– КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для захищеного об'єкта кожного типу, з використанням атрибутів доступу користувачів й об'єктів різного типу, а також засобів, наведених при відповіді на питання 22, 23, шляхом керування приналежністю користувачів, процесів й об'єктів до відповідних доменів визначити конкретних користувачів (групи користувачів), що мають, а також тих, що не мають права отримувати інформацію від об'єкта;

– КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для процесу кожного типу, з використанням атрибутів доступу користувачів і процесів різного типу, а також засобів, наведених при відповіді на питання 22, 23, шляхом керування приналежністю користувачів і процесів до відповідних доменів визначити конкретних користувачів (групи користувачів), що мають, а також тих, що не мають права ініціювати процес.

Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги «Ідентифікація й автентифікація» рівня НИ-1 або вище згідно політики цієї послуги.

Згідно політики та правил стосовно поділюваних ресурсів, використаних для збереження захищених пасивних об'єктів усіх типів, реалізується послуга «Повторне використання об'єктів» рівня КО-1.

Програма випробувань функціональної послуги безпеки «Абсолютна адміністративна конфіденційність» рівня КА-4 має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ об’єкта експертизи (ОЕ), відноситься до об’єктів ОЕ всіх типів, наведених при відповіді на питання 19;

– КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу користувачів, процесів і захищених об’єктів різного типу, за правилами, з використанням засобів, наведених при відповіді на питання 20, 21;

– КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для захищеного об’єкта кожного типу, з використанням атрибутів доступу користувачів, процесів й об’єктів, а також засобів, наведених при відповіді на питання 22, 23, шляхом керування приналежністю користувачів, процесів й об’єктів до відповідних доменів визначити конкретних користувачів і процеси (групи користувачів і процесів), що мають, а також тих, що не мають права отримувати інформацію від об’єкта;

– КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для процесу кожного типу, з використанням атрибутів доступу користувачів, процесів й об’єктів різного типу, а також засобів наведених при відповіді на питання 22, 23, шляхом керування приналежністю користувачів і процесів до відповідних доменів визначити конкретних користувачів (групи користувачів), що мають, а також тих, що не мають права ініціювати процес.

Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об’єкта, запуску об’єкта, запуску процесу або зміни прав доступу до об’єкта, автентифіковані з використанням засобів реалізації послуги «Ідентифікація й автентифікація» рівня НИ-1 або вище згідно політики цієї послуги.

Згідно політики та правил стосовно поділюваних ресурсів, використаних для збереження захищених пасивних об’єктів усіх типів, реалізується послуга «Повторне використання об’єктів» рівня КО-1.

4.2.4 Програми випробувань функціональної послуги безпеки «Повторне використання об’єктів»

Послуга дозволяє забезпечити коректність повторного використання поділюваних ресурсів, гарантуючи, що у випадку, якщо поділюваний ресурс виділяється новому користувачу або процесу, він не містить інформації, що залишилася від попереднього користувача або процесу.

Спеціальні питання щодо послуги «Повторне використання об’єктів».

Питання 29. Чи існують у складі будь-яких функціональних модулів об’єкта експертизи (ОЕ), що входять до складу КЗЗ засоби та відповідні механізми звільнення (очищення) вмісту поділюваних ресурсів, використаних для збереження пасивних об’єктів, а також їх атрибутів доступу.

Механізмами, що забезпечують реалізацію послуги «Повторне використання об’єктів», є механізми:

– видалення атрибутів доступу пасивних об’єктів, що видаляються;

– ініціалізації (заповнення наперед заданими або випадковими даними) вмісту поділюваних ресурсів, використаних для збереження пасивних об’єктів.

Ці механізми можуть бути реалізовані або у компонентах КЗЗ, що входять до складу ядра КЗЗ і в яких здійснюється оброблення запитів на видалення пасивних об’єктів і звільнення займаних об’єктами поділюваних ресурсів, або у компонентах КЗЗ, в яких здійснюється оброблення запитів на створення нових пасивних об’єктів і виділення необхідних для їх збереження поділюваних ресурсів. Якщо зазначених засобів у складі КЗЗ немає, то це означає, що послуга «Повторне використання об’єктів» засобами КЗЗ ОЕ не реалізується та відповідати на подальші питання не потрібно.

Питання 30. Чи забезпечується засобами КЗЗ можливість звільнення (очищення) вмісту поділюваних ресурсів, використаних для збереження пасивних об’єктів усіх типів, стосовно яких визначені політики послуг довірчої й адміністративної конфіденційності, а також їх атрибутів доступу.

У випадку позитивної відповіді на питання 30 можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Повторне використання об’єктів» рівня КО-1.

Питання 31. З використанням яких механізмів і в яких функціональних модулях, що входять до складу КЗЗ, реалізується послуга «Повторне використання об’єктів» стосовно атрибутів доступу пасивних об’єктів. Укажіть значення, що призначаються атрибутам видалених пасивних об’єктів.

Питання 32. З використанням яких механізмів і в яких функціональних модулях, що входять до складу КЗЗ, реалізується послуга «Повторне використання об’єктів» стосовно ресурсів, використаних для збереження захищених пасивних об’єктів кожного з типів.

Програма випробувань функціональної послуги безпеки «Повторне використання об’єктів» рівня КО-1 має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ об’єкта експертизи, відноситися до всіх поділюваних ресурсів, використаних для збереження захищених пасивних об’єктів усіх типів, зазначених при відповіді на питання 30;

– перш ніж користувач або процес зможе отримати у своє розпорядження звільнений іншим користувачем або процесом об’єкт певного тип, встановлені для попереднього користувача або процесу права доступу до цього об’єкта скасовуються з використанням механізмів, наведених при відповіді на питання 31;

Перш ніж користувач або процес зможе отримати у своє розпорядження звільнений іншим користувачем або процесом об’єкт певного типу, вся інформація, що міститься у цьому об’єкті, з використанням механізмів, наведених при відповіді на питання 32, стає недоступною.

4.2.5 Програми випробувань функціональної послуги безпеки «Аналіз прихованих каналів»

Реалізація послуги «Аналіз прихованих каналів» дозволяє виявити та виключити потоки інформації, що існують, але не контролюються іншими функціональними послугами безпеки.

Функціональні послуги «Аналіз прихованих каналів» ранжируються за рівнями 1 … 4 на підставі того, чи виконуються тільки виявлення, контроль і перекриття прихованих каналів:

КК-1 – виявлення прихованих каналів;

КК-2 – контроль прихованих каналів;

КК-3 – перекриття прихованих каналів.

Спеціальні питання щодо послуги «Аналіз прихованих каналів».

Питання 33. Чи наведені у проектній або експлуатаційній документації на об'єкт експертизи (ОЕ) результати аналізу прихованих каналів, проведеного з метою виявлення та виключення потоків інформації, що існують, але не контролюються іншими послугами безпеки. Яку множину прихованих каналів виявлено у процесі аналізу. Використання цих каналів може призвести до порушення конфіденційності інформації, що міститься у пасивних об'єктах.

Питання 34. Чи документовані (описані з погляду механізму реалізації) усі виявлені в апаратному та програмному забезпеченні, а також у програмах постійних запам'ятовуючих пристроїв (ПЗП) приховані канали. Які особливості та можливості яких функціональних компонентів ОЕ, що входять до складу КЗЗ, при цьому використовуються. Наведіть перелік документованих прихованих каналів із їх характеристиками.

У випадку позитивної відповіді на питання 33, 34 можна стверджувати, що в ОЕ може бути реалізована послуга «Аналіз прихованих каналів» рівня КК-1, КК-2 чи КК-3. У цьому випадку політика послуги може бути уточнена при відповіді на наступні питання. У випадку негативної відповіді на питання 33 можна стверджувати, що ця послуга в ОЕ не реалізується.

Питання 35. Чи усунуті всі виявлені на етапі аналізу та наведені при відповіді на питання 34 приховані канали. Якщо так, то вкажіть, із використанням яких механізмів і в яких функціональних компонентах ОЕ, що входять до складу КЗЗ, здійснюється усунення (запобігання можливості використання) кожного виявленого на етапі аналізу прихованого каналу.

У випадку позитивної відповіді на питання 35 можна стверджувати, що в ОЕ може бути реалізована послуга «Аналіз прихованих каналів» рівня КК-3. У випадку негативної відповіді – можна стверджувати, що в ОЕ може бути реалізована послуга «Аналіз прихованих каналів» рівня КК-1 чи КК-2.

Питання 36. Чи документована (на підставі теоретичної оцінки або вимірів) максимальна пропускна здатність кожного з виявлених і наведених при відповіді на питання 33 прихованих каналів. Чи документована сукупна пропускна здатність для груп прихованих каналів, що можуть бути використані спільно (якщо такі існують). Наведіть відповідні дані для всіх виявлених груп прихованих каналів. У випадку позитивної відповіді на питання 36 можна стверджувати, що в ОЕ може бути реалізована послуга «Аналіз прихованих каналів» рівня КК-1 чи КК-2. У цьому випадку політика послуги може бути уточнена при відповіді на питання 37.

Питання 37. Чи здійснюється у будь-яких функціональних компонентах ОЕ, що входять до складу КЗЗ, контроль використання будь-якої затвердженої

підмножини множини виявлених, документованих прихованих каналів. Якщо так, то з використанням яких механізмів і в яких функціональних компонентах ОЕ, що входять до складу КЗЗ, здійснюється контроль використання цієї підмножини множини документованих прихованих каналів. Наведіть опис для кожного з каналів, внесених до затвердженої підмножини.

У випадку позитивної відповіді на питання 37 можна стверджувати, що в ОЕ може бути реалізована послуга «Аналіз прихованих каналів» рівня КК-2.

Спільною для всіх рівнів послуги «Аналіз прихованих каналів» є перевірка такої вимоги: виконано аналіз прихованих каналів, відповідні результати наведені при відповіді на питання 33.

Програма випробувань функціональної послуги безпеки «Аналіз прихованих каналів» рівня КК-1 має передбачати перевірку таких вимог:

– усі приховані канали, що існують в апаратному та програмному забезпеченні, а також у програмах ПЗП, документовані, відповідні результати наведені при відповіді на питання 34;

– документовано максимальну пропускну здатність кожного виявленого прихованого каналу, отриману на підставі теоретичної оцінки або вимірів, відповідні результати наведені при відповіді на питання 36;

– для прихованих каналів, що можуть бути використані спільно, документовано сукупну пропускну здатність, відповідні результати наведені при відповіді на питання 36;

– згідно політики та правил, наведених при відповіді на питання 30 – 32, послуга «Повторне використання об’єктів» рівня КО-1 реалізується стосовно поділюваних ресурсів, використаних для збереження захищених пасивних об’єктів усіх типів, для яких визначені політики послуг довірчої та/або адміністративної конфіденційності

– проектування та реалізація ОЕ виконувалися з дотриманням вимог НД ТЗІ 2.5-004-99 [17] до рівня гарантій коректності реалізації функціональних послуг безпеки не нижче, ніж Г-3. (Тобто, діє необхідна умова КО-1 і Г-3).

Програма випробувань функціональної послуги безпеки «Аналіз прихованих каналів» рівня КК-2 має передбачати перевірку таких вимог:

– вимоги, що передбачені для рівня КК-1, додатково така вимога:

– КЗЗ ОЕ, згідно з переліком реєстраційних подій, забезпечує реєстрацію фактів використання затвердженої підмножини виявлених прихованих каналів за допомогою засобів реалізації послуги «Реєстрація» рівня НР-1 або вище з використанням засобів і механізмів, наведених при відповіді на питання 37.

Програма випробувань функціональної послуги безпеки «Аналіз прихованих каналів» рівня КК-3 має передбачати перевірку таких вимог:

– вимоги, що передбачені для рівня КК-1, додатково така вимога:

– затверджену підмножину виявлених при аналізі прихованих каналів, наведену при відповіді на питання 34, усунуто з використанням засобів і механізмів, наведених при відповіді на питання 35.

А також діє необхідна умова КО-1 і Г-3.

4.2.6 Програми випробувань функціональної послуги безпеки «Конфіденційність при обміні»

Послуга «Конфіденційність при обміні» дозволяє забезпечити захист об’єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, при їх передачі (експорті/імпорті) через незахищене середовище.

Послуги «Конфіденційність при обміні» ранжируються за рівнями 1 … 4 на підставі повноти захисту та вибірковості керування потоками інформації:

КВ-1 – мінімальна конфіденційність при обміні;

КВ-2 – базова конфіденційність при обміні;

КВ-3 – повна конфіденційність при обміні;

КВ-4 – абсолютна конфіденційність при обміні;

Спеціальні питання щодо послуги «Конфіденційність при обміні»

Питання 38. Чи існує в об’єкті експертизи (ОЕ) можливість обміну (з використанням відповідних інтерфейсних процесів) між різними компонентами ОЕ через незахищене середовище пасивними об’єктами. Якщо така можливість існує, то наведіть цю підмножину типів пасивних об’єктів.

Питання 39. Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ, засоби та відповідні механізми, що забезпечують захист пасивних об’єктів будь-яких типів від безпосереднього ознайомлення з інформацією, що міститься у цих об’єктах, при їх передачі між різними компонентами ОЕ через незахищене середовище.

Функціонування механізмів, що забезпечують реалізацію послуги «Конфіденційність при обміні», може ґрунтуватися на таких принципах:

– забезпечення конфіденційності шляхом керування маршрутом передачі пасивних об’єктів із метою унеможливлення несанкціонованого ознайомлення з їх умістом;

– забезпечення конфіденційності шляхом приховування семантики (вмісту) переданих пасивних об’єктів з використанням шифрування;

– забезпечення конфіденційності шляхом заповнення трафіка методом доповнення хибних даних;

– забезпечення конфіденційності шляхом заповнення трафіка методом генерації хибних повідомлень;

– забезпечення конфіденційності шляхом використання змінного надання даних;

– забезпечення конфіденційності шляхом розподілу каналів для передачі різних частин повідомлення (розподілу спектра);

– забезпечення конфіденційності шляхом організації прихованого каналу передачі усередині іншого відкритого каналу (стеганографія).

Питання 40. Чи відноситься політика послуги «Конфіденційність при обміні», реалізована КЗЗ (чи забезпечується можливість захисту від безпосереднього ознайомлення з інформацією):

1) до пасивних об’єктів усіх типів, а також до використаних для їх приймання/передачі функціональних модулів, що входять до складу КЗЗ

(інтерфейсних процесів). Тоді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Конфіденційність при обміні» рівня КВ-3 чи КВ-4;

2) лише до пасивних об’єктів певних (укажіть яких) типів, а також до використаних для їх приймання/передачі функціональних модулів ОЕ, що входять до складу КЗЗ (інтерфейсних процесів). Тоді може бути реалізована послуга «Конфіденційність при обміні» рівня КВ-1 чи КВ-2.

Питання 41. В яких функціональних модулях ОЕ, що входять до складу КЗЗ, із використанням яких саме механізмів захисту реалізується захист від безпосереднього ознайомлення з інформацією, що міститься у переданих об’єктах. Який рівень захищеності забезпечується використаними механізмами. Якими параметрами (якими атрибутами доступу пасивних об’єктів або властивостями використаних механізмів) визначається рівень захищеності, що забезпечується для пасивних об’єктів. Чи існує можливість у користувачів та/або процесів (укажіть яких) із використанням відповідних функціональних модулів ОЕ, що входять до складу КЗЗ (укажіть яких), керувати (шляхом зміни відповідних параметрів) рівнем захищеності, що забезпечується для пасивних об’єктів різного типу.

Питання 42. Чи існує можливість у наведених при відповіді на питання 41 засобах керування рівнем захищеності, що забезпечується для пасивних об’єктів різного типу, оброблення запитів на присвоєння або зміну рівня захищеності лише у випадку, якщо вони надходять від користувачів, які відносяться лише до певних ролей (від адміністраторів або користувачів, яким надані відповідні повноваження). На підставі яких атрибутів об’єктів-користувачів, що визначають їх повноваження, та за якими правилами виконується оброблення цих запитів.

У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Конфіденційність при обміні» рівня КВ-2, КВ-3 чи КВ-4, інакше рівня КВ-1.

Питання 43. Чи обробляються запити на експорт (передачу) захищеного пасивного об’єкта передавальним компонентом (функціональним модулем ОЕ, що входить до складу КЗЗ) на підставі:

1) атрибутів доступу інтерфейсного процесу, що здійснює передачу, і КЗЗ, що є приймачем об’єкта (вкажіть яких). Тоді може бути реалізована послуга «Конфіденційність при обміні» рівня КВ-3 чи КВ-4 інакше – рівня КВ-2;

2) лише атрибутів доступу інтерфейсного процесу, що здійснює передачу (вкажіть яких).

У випадку негативних відповідей на п. 1) і 2) можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Конфіденційність при обміні» рівня КВ-1, відповідати на наступні питання не потрібно.

Питання 44. Чи обробляються запити на імпорт (приймання) захищеного пасивного об’єкта приймаючим компонентом (функціональним модулем ОЕ, що входить до складу КЗЗ) на підставі:

1) атрибутів доступу інтерфейсного процесу, що здійснює приймання, і КЗЗ (компонента КЗЗ), що є джерелом об’єкта (вкажіть яких);

2) лише атрибутів доступу інтерфейсного процесу, що здійснює приймання (укажіть яких).

У випадку позитивної відповіді на п. 1) можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Конфіденційність при обміні» рівня КВ-3 чи КВ-4. У випадку негативної відповіді на п. 1) і позитивної відповіді на п. 2) – рівня КВ-2. У випадку негативних відповідей на п. 1) і 2) – рівня КВ-1.

Питання 45. Чи є представлення захищеного переданого пасивного об'єкта функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела та приймача. Якщо так, то опишіть відповідну функціональну залежність.

У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Конфіденційність при обміні» рівня КВ-3 чи КВ-4, інакше – може бути реалізована послуга «Конфіденційність при обміні» рівня КВ-2.

Питання 46. Чи наведені у проектній або експлуатаційній документації на ОЕ результати аналізу прихованих каналів обміну. Яку множину прихованих каналів обміну, що дозволяють порушити конфіденційність інформації шляхом спільного аналізу низки отриманих об'єктів, виявлено у процесі аналізу. До порушення конфіденційності інформації, що міститься у пасивних об'єктах будь-якого з типів, наведених при відповіді на питання 40.1, може призвести використання цих каналів. Наведіть опис інформації, яку можна отримати шляхом спільного аналізу низки отриманих об'єктів.

У випадку позитивної відповіді на питання 46 можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Конфіденційність при обміні» рівня КВ-4, інакше – може бути реалізована послуга «Конфіденційність при обміні» рівня КВ-3.

Питання 47. Чи документовані (описані з погляду механізму реалізації) у наведених при відповіді на питання 46 результатах усі виявлені у процесі аналізу приховані канали обміну. Які особливості та можливості яких функціональних компонентів ОЕ, що входять до складу КЗЗ, при цьому використовуються. Наведіть перелік документованих прихованих каналів обміну з їх характеристиками.

У випадку позитивної відповіді на питання 47 можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Конфіденційність при обміні» рівня КВ-4, інакше – може бути реалізована ця послуга рівня КВ-3.

Питання 48. Чи документована (на підставі теоретичної оцінки або вимірів) максимальна пропускна здатність кожного виявленого прихованого каналу обміну. Наведіть відповідні дані для кожного виявленого прихованого каналу обміну.

У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Конфіденційність при обміні» рівня КВ-4, інакше – рівня КВ-3.

Питання 49. Чи здійснюється у будь-яких функціональних компонентах ОЕ, що входять до складу КЗЗ, реєстрація використання будь-якої затвердженої підмножини множини виявлених і документованих прихованих каналів обміну.

Якщо так, то з використанням яких механізмів і в яких функціональних компонентах ОЕ, що входять до складу КЗЗ, здійснюється реєстрація використання цієї підмножини множини документованих прихованих каналів обміну. Наведіть опис для кожного з каналів, внесених до затвердженої підмножини.

У випадку позитивної відповіді не можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Конфіденційність при обміні» рівня КВ-4, інакше – рівня КВ-3.

Питання 50. Чи забезпечується у функціональних компонентах ОЕ, що входять до складу КЗЗ усунення всіх виявлених на етапі аналізу та наведених при відповіді на питання 46 прихованих каналів обміну. Якщо так, то з використанням яких механізмів і в яких функціональних компонентах ОЕ, що входять до складу КЗЗ, здійснюється усунення (запобігання можливості використання) або часткове перекриття кожного виявленого прихованого каналу обміну.

У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Конфіденційність при обміні» рівня КВ-4.

Спільними для всіх рівнів функціональної послуги безпеки «Конфіденційність при обміні» є перевірки таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, визначає рівень захищеності, наведений при відповіді на питання 41, який забезпечується використаними механізмами, і (для КВ-2 – КВ-4) здатність користувачів та/або процесів керувати рівнем захищеності згідно правил, наведених при відповіді на питання 41;

– КЗЗ ОЕ забезпечує захист від безпосереднього ознайомлення з інформацією, що міститься у переданих об’єктах різного типу, з використанням засобів і механізмів, наведених при відповіді на питання 41.

***Програма випробувань функціональної послуги безпеки «Мінімальна конфіденційність при обміні» рівня КВ*-1** має передбачати перевірку вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до об’єктів й існуючих інтерфейсних процесів усіх типів.

***Програма випробувань функціональної послуги безпеки «Базова конфіденційність при обміні» рівня КВ*-2** має передбачати перевірку вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до об’єктів й існуючих інтерфейсних процесів усіх типів;

– запити на присвоєння або зміну рівня захищеності обробляються КЗЗ ОЕ у засобах, наведених при відповіді на питання 41, за правилами, наведеними при відповіді на питання 42, лише у тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження та які відносяться до певних ролей згідно політики реалізованої КЗЗ ОЕ послуги «Розмежування обов’язків» рівня НО-1 або вище;

– запити на експорт захищеного об’єкта певного типу обробляються передавальним КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на

питання 41, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на питання 43.2;

– запити на імпорт захищеного об’єкта певного типу обробляються приймаючим КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на питання 41, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на питання 44.2.

Програма випробувань функціональної послуги безпеки «Повна конфіденційність при обміні» рівня КВ-3 має передбачати перевірку вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до об’єктів й існуючих інтерфейсних процесів усіх типів;

– запити на присвоєння або зміну рівня захищеності обробляються КЗЗ ОЕ у засобах, наведених при відповіді на питання 41, за правилами, наведеними при відповіді на питання 42, лише у тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження та які відносяться до певних ролей згідно політики реалізованої КЗЗ ОЕ послуги «Розмежування обов’язків» рівня НО-1 або вище;

– запити на експорт захищеного об’єкта певного типу обробляються передавальним КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на питання 41, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на питання 43.1, й атрибутів приймача об’єкта, наведених при відповіді на питання 43.1 й автентифікованих із використанням засобів реалізації послуги «Ідентифікація й автентифікація при обміні» рівня НВ-1 або вище згідно політики та правил цієї послуги;

– запити на імпорт захищеного об’єкта певного типу обробляються приймаючим КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на питання 41, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на питання 44.1, й атрибутів джерела об’єкта, наведених при відповіді на питання 44.1 й автентифікованих із використанням засобів реалізації послуги «Ідентифікація й автентифікація при обміні» рівня НВ-1 або вище згідно політики та правил цієї послуги;

– подання захищеного об’єкта певного типу є функцією атрибутів доступу інтерфейсного процесу відповідного типу, самого об’єкта, а також його джерела та приймача згідно з описом, наведеним при відповіді на питання 45.

Програма випробувань функціональної послуги безпеки «Абсолютна конфіденційність при обміні» рівня КВ-4 має передбачати перевірку вимог:

– вимоги, що застосовані для рівня КВ-3, та додатково наступні вимоги;

– політика послуги містить опис інформації, яку можна отримати шляхом спільного аналізу низки отриманих об’єктів певного типу, результати, наведені при відповіді на питання 46, містять цей опис;

– виконано аналіз прихованих каналів обміну, всі виявлені приховані канали обміну та максимальна пропускна здатність кожного з них документовані, дані, наведені при відповіді на питання 46, 47, 48, містять результати виконаного аналізу;

– КЗЗ ОЕ, згідно з переліком реєстраційних подій, забезпечує реєстрацію фактів використання затвердженої підмножини виявлених прихованих каналів, наведеної при відповіді на питання 49, за допомогою засобів реалізації послуги «Реєстрація» рівня НР-1 або вище з використанням засобів і механізмів, наведених при відповіді на питання 49;

– забезпечено часткове перекриття або виключення множини виявлених прихованих каналів обміну, наведеної при відповіді на питання 46, з використанням засобів і механізмів, наведених при відповіді на питання 50;

– проектування та реалізація ОЕ виконувалися з дотриманням вимог НД ТЗІ 2.5-004-99 [17] до рівня гарантій коректності реалізації функціональних послуг безпеки не нижче, ніж Г-3.

4.3 Програма випробування функціональних послуг безпеки критеріїв цілісності

Комплекс заходів захисту (КЗЗ), оцінюваної на предмет відповідності критеріям цілісності інформаційно-телекомунікаційної системи, має надавати послуги із захисту оброблюваної інформації від несанкціонованої модифікації.

Цілісність забезпечується такими послугами:

ЦД – довірча цілісність;

ЦА – адміністративна цілісність;

ЦО – відкіт;

ЦВ – цілісність при обміні.

4.3.1 Спеціальні питання щодо послуг довірчої/адміністративної цілісності

Послуги довірчої/адміністративної цілісності забезпечують можливість керування потоками інформації від об’єктів-користувачів до захищених пасивних об’єктів із метою захисту пасивних об’єктів від несанкціонованого створення, модифікації або видалення.

Послуги довірчої/адміністративної цілісності ранжируються за рівнями 1 … 4 на підставі повноти захисту та вибірковості керування:

ЦД-1 – мінімальна довірча цілісність;

ЦД-2 – базова довірча цілісність;

ЦД-3 – повна довірча цілісність;

ЦД-4 – абсолютна адміністративна цілісність;

ЦА-1 – мінімальна адміністративна цілісність;

ЦА-2 – базова адміністративна цілісність;

ЦА-3 – повна адміністративна цілісність;

ЦА-4 – абсолютна адміністративна цілісність.

Питання 51. Чи існує в об’єкті експертизи (ОЕ) для будь-якого з типів пасивних об’єктів, можливість розмежування доступу з боку користувачів, що відносяться до будь-якої з ролей, або процесів різного типу до пасивних

об’єктів цього типу з метою створення/модифікації/видалення об’єктів (створення потоків інформації від користувачів до об’єктів).

Якщо такої можливості не існує, тобто, всі користувачі у межах певної ролі або всі процеси певного типу завжди мають однакові можливості доступу з метою створення/модифікації/видалення до всієї множини пасивних об’єктів усіх типів, то це означає, що послуги довірчої та/або адміністративної цілісності засобами КЗЗ ОЕ не реалізуються. Інакше, якщо така можливість існує, то це означає, що засобами КЗЗ реалізуються послуги довірчої та/або адміністративної цілісності, їх політики та рівні повинні бути уточнені.

Питання 52. Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ, засоби та відповідні механізми керування доступом із боку об’єктів-користувачів одного чи декількох типів, або об’єктів-процесів одного чи декількох типів, до пасивних об’єктів одного чи декількох типів, шляхом аналізу запитів на доступ із боку користувачів або об’єктів-процесів із метою створення/модифікації/видалення пасивного об’єкта (зміни об’єкта) та прийняття рішення на підставі інформації, що міститься у наборах атрибутів доступу ініціатора запиту (користувача або об’єкта-процесу) та пасивного об’єкта). Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ засоби, які дозволяють користувачам, що відносяться до будь-якої з ролей, змінювати відповідні набори атрибутів доступу об’єктів-користувачів та/або об’єктів-процесів і пасивних об’єктів.

Механізмами, що забезпечують реалізацію послуг довірчої й адміністративної цілісності, є механізми керування доступом, тобто, надання можливості доступу до ресурсу згідно зі спеціально визначеними правилами. Як основні схеми, на підставі яких може здійснюватися керування доступом, можуть бути використані схеми:

– на підставі списків керування доступом (під списком керування доступом слід розуміти пов’язаний із запитуваним ресурсом набір атрибутів доступу у вигляді сукупностей ідентифікаторів ініціаторів запиту й атрибутів, що визначають дозволені види доступу або операції над запитуваним ресурсом);

– на підставі списків повноважень (під списком повноважень слід розуміти пов’язаний із ініціатором запиту набір атрибутів доступу у вигляді сукупності операцій, дозволених над заданою множиною запитуваних ресурсів);

– на підставі міток безпеки (під мітками слід розуміти атрибути доступу, пов’язані як із ініціатором запиту, так і з запитуваним ресурсом, рішення про надання доступу приймається на підставі оброблення міток ініціатора та ресурсу за заданими правилами).

Для прийняття рішення про можливість надання доступу ці механізми можуть використовувати:

– ідентифікатори відповідних об’єктів;

– ідентифікатори груп відповідних об’єктів;

– інформацію про права доступу до пасивних об’єктів у вигляді міток доступу, списків керування доступом або списків повноважень;

– інформацію про права володіння пасивним об’єктом;

– інформацію про час спроби доступу;

– інформацію про маршрут запиту доступу у розподілених системах;

– інформацію про тривалість доступу до ресурсу.

Засоби керування доступом, що приймають рішення про можливість задоволення або відхилення запиту, повинні бути реалізовані у тих компонентах КЗЗ, що входять до складу ядра КЗЗ і реалізують концепцію диспетчера доступу. Засоби, що дозволяють змінювати атрибути доступу, можуть бути реалізовані у довільних компонентах КЗЗ. Якщо зазначених засобів у складі КЗЗ немає, то це означає, що послуги довірчої та/або адміністративної цілісності засобами КЗЗ ОЕ не реалізуються. Інакше, засобами КЗЗ реалізуються послуги довірчої та/або адміністративної цілісності, їх політики та рівні мають бути уточнені.

Питання 53. Чи дозволяють реалізовані у складі функціональних модулів ОЕ, що входять до складу КЗЗ, засоби змінювати атрибути доступу об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів, на підставі яких реалізується керування доступом:

1) будь-яким користувачам, що відносяться до кожної з ролей, але лише для частини пасивних об’єктів певних типів, що належать їх домену, тобто з урахуванням атрибутів, що визначають їх права володіння цими пасивними об’єктами;

2) будь-яким користувачам, що відносяться лише до певних ролей, для всіх пасивних об’єктів певних типів, без урахування атрибутів, що визначають їх права володіння цими пасивними об’єктами.

У випадку позитивної відповіді на п. 1) можна стверджувати, що засобами КЗЗ реалізуються послуги довірчої цілісності. У випадку позитивної відповіді на п. 2) можна стверджувати, що засобами КЗЗ реалізуються послуги адміністративної цілісності. Політики та рівні відповідних послуг для пасивних об’єктів різного типу можуть бути уточнені при відповіді на наступні питання.

Питання 54. Чи відноситься політика послуг довірчої або адміністративної цілісності, реалізована КЗЗ (чи забезпечується можливість керування доступом об’єктів-користувачів або об’єктів-процесів до пасивних об’єктів):

1) до всіх типів об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів;

2) лише до певних (укажіть до яких) типів об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів.

У випадку позитивної відповіді на п. 1) можна стверджувати, що засобами КЗЗ можуть бути реалізовані послуги довірчої цілісності рівнів ЦД-3 чи ЦД-4 або адміністративної цілісності рівнів ЦА-3 чи ЦА-4. У цьому випадку політика та рівні відповідних послуг можуть бути уточнені при відповіді на наступні питання. Інакше, у випадку негативної відповіді на п. 1) можна стверджувати, що засобами КЗЗ можуть бути реалізовані послуги довірчої цілісності рівнів ЦД-1 чи ЦД-2 або адміністративної цілісності рівнів ЦА-1 чи ЦА-2 стосовно об’єктів, наведених при відповіді на питання 2).

Питання 55. На підставі яких атрибутів доступу:

1) об’єктів-користувачів і пасивних об’єктів різних типів або

2) об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів різних типів і згідно з якими правилами реалізується розмежування доступу для об’єктів-

користувачів, об’єктів-процесів і пасивних об’єктів різного типу, наведених при відповіді на питання 54, до яких відноситься політика послуг довірчої або адміністративної цілісності.

Питання 56. В яких функціональних модулях ОЕ, що входять до складу КЗЗ, з використанням механізмів керування доступом, здійснюється оброблення запитів на надання доступу (розмежування доступу) згідно із зазначеними при відповіді на питання 55 правилами для об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів різного типу.

Питання 57. На підставі яких атрибутів пасивних об’єктів й атрибутів доступу об’єктів-користувачів, що визначають права володіння для послуги довірчої цілісності або адміністративні повноваження для послуги адміністративної цілісності, та згідно з якими правилами здійснюється оброблення запитів на зміну прав доступу до захищених об’єктів для об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів різного типу.

Питання 58. В яких функціональних модулях ОЕ, що входять до складу КЗЗ, здійснюється оброблення запитів на зміну прав доступу до захищених об’єктів згідно із зазначеними при відповіді на питання 57 правилами для об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів.

Питання 59. Чи існує у функціональних компонентах ОЕ, що входять до складу КЗЗ і наведені при відповіді на питання 58, з використанням атрибутів доступу, наведених при відповіді на питання 55, 57, для об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів різного типу:

1) можливість визначення конкретних користувачів та/або груп користувачів, що мають право створювати/видаляти/модифікувати об’єкт. У цьому випадку засобами КЗЗ може бути реалізована послуга довірчої цілісності рівня ЦД-1 або адміністративної цілісності рівня ЦА-1;

2) можливість визначення конкретних процесів та/або груп процесів, що мають право створювати/видаляти/модифікувати об’єкт. У цьому випадку можна стверджувати, що засобами КЗЗ може бути реалізована послуга довірчої цілісності рівня ЦД-2 або адміністративної цілісності рівні ЦА-2;

3) можливість визначення конкретних процесів (і груп процесів), що мають, а також тих, що не мають права створювати/видаляти/модифікувати об’єкт. У цьому випадку засобами КЗЗ може бути реалізована послуга довірчої цілісності рівня ЦД-3 або адміністративної цілісності рівні ЦА-3;

4) можливість визначення конкретних користувачів і процесів (і груп користувачів і процесів), що мають, а також тих, що не мають права модифікувати об’єкт. У цьому випадку можна стверджувати, що засобами КЗЗ може бути реалізована послуга довірчої цілісності рівня ЦД-4 або адміністративної цілісності рівні ЦА-4.

Питання 60. Чи існує у функціональних компонентах ОЕ, що входять до складу КЗЗ і наведені при відповіді на питання 58, з використанням атрибутів доступу, наведених при відповіді на питання 55, 57 для об’єктів-користувачів, об’єктів-процесів і пасивних об’єктів різного типу:

1) можливість визначення конкретних користувачів та/або груп користувачів, що мають право ініціювати процес У цьому випадку можна

стверджувати, що засобами КЗЗ може бути реалізована послуга довірчої цілісності рівня ЦД-2 або адміністративної цілісності рівня ЦА-2;

2) можливість визначення конкретних користувачів (і груп користувачів), що мають, а також тих, що не мають права ініціювати процес. У цьому випадку засобами КЗЗ можуть бути реалізовані послуги довірчої цілісності рівня ЦД-3 чи ЦД-4 або адміністративної цілісності рівня ЦА-3 чи ЦА-4.

Питання 61. Які атрибути доступу, наведені при відповіді на питання 55, 57, що характеризують права доступу до захищених пасивних об'єктів, наведених при відповіді на питання 54, установлюються:

1) у момент створення пасивного об'єкта;

2) у момент ініціалізації об'єкта.

Укажіть, яке значення призначається кожному атрибуту, обґрунтуйте його безпечність.

Питання 62. Чи зберігаються, якщо так, то які, атрибути доступу пасивних об'єктів, наведені при відповіді на питання 55, 57, що характеризують права користувачів за модифікацією цих об'єктів (укажіть для пасивних об'єктів кожного з типів) при експорті об'єкта за межі ОЕ. Яким чином здійснюється зв'язування переданих наборів атрибутів доступу з експортованими пасивними об'єктами різного типу.

Питання 63. Чи зберігаються, якщо так, то які, атрибути доступу пасивних об'єктів, наведені при відповіді на питання 55, 57, що характеризують права користувачів за модифікацією цих об'єктів (укажіть для пасивних об'єктів, наведених при відповіді на питання 54) при імпорті пасивного об'єкта із-зі межі ОЕ. Яким чином здійснюється зв'язування прийнятих наборів атрибутів доступу з імпортованими пасивними об'єктами.

4.3.2 Програми випробувань функціональної послуги безпеки «Довірча цілісність»

Спільними для всіх рівнів функціональної послуги безпеки «Довірча цілісність» є перевірки таких вимог:

– запити на зміну прав доступу до об'єкта обробляються КЗЗ ОЕ на підставі атрибутів доступу користувачів, які ініціюють запит, й об'єктів різного типу за правилами, наведеними при відповіді на питання 57, з використанням засобів, наведених при відповіді на питання 58;

– права доступу до кожного захищеного об'єкта встановлюються у момент його створення або ініціалізації за правилами, наведеними при відповіді на питання 61 для об'єктів різного типу;

– як частина політики послуги подані правила збереження атрибутів доступу об'єктів різного типу при їх експорті й імпорті, наведені при відповіді на питання 62, 63;

– атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги «Ідентифікація й автентифікація» рівня НИ-1 або вище згідно політики цієї послуги.

Програма випробувань функціональної послуги безпеки «Мінімальна довірча цілісність» рівня ЦД-1 має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів експертизи (ОЕ) всіх типів, наведених при відповіді на питання 54.2;

– КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу користувачів і захищених об'єктів різного типу, наведених при відповіді на питання 55.1, за правилами, наведеними при відповіді на питання 55, з використанням засобів, наведених при відповіді на питання 56;

– КЗЗ ОЕ надає користувачу можливість для захищеного об'єкта кожного типу, що належить його домену, з використанням атрибутів доступу користувачів й об'єктів, наведених при відповіді на питання 55.1, 57, а також засобів, наведених при відповіді на питання 58, визначити конкретних користувачів та/або групи користувачів, що мають право модифікувати об'єкт.

Програма випробувань функціональної послуги безпеки «Базова довірча цілісність» рівня ЦД-2 має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на питання 54.2;

– КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу процесів і захищених об'єктів різного типу, наведених при відповіді на питання 55.2, за правилами, наведеними при відповіді на питання 55, з використанням засобів, наведених при відповіді на питання 56;

– КЗЗ ОЕ надає користувачу можливість для захищеного об'єкта кожного типу, що належить його домену, з використанням атрибутів доступу процесів й об'єктів, наведених при відповіді на питання 55.2, 57, а також засобів, наведених при відповіді на питання 58, визначити конкретні процеси та/або групи процесів, що мають право модифікувати об'єкт;

– КЗЗ ОЕ надає користувачу можливість для процесу кожного типу, що належить його домену, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на питання 55.2, 57, а також засобів, наведених при відповіді на питання 58, визначити конкретних користувачів та/або групи користувачів, що мають право ініціювати процес.

Програма випробувань функціональної послуги безпеки «Повна довірча цілісність» рівня ЦД-3 має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на питання 54.1;

– КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу процесів і захищених об'єктів різного типу, наведених при відповіді на питання 55.2, за правилами, наведеними при відповіді на питання 55, з використанням засобів, наведених при відповіді на питання 56;

– КЗЗ ОЕ надає користувачу можливість для захищеного об'єкта кожного типу, що належить його домену, з використанням атрибутів доступу процесів й об'єктів, наведених при відповіді на питання 55.2, 57, а також засобів,

наведених при відповіді на питання 58, визначити конкретні процеси (групи процесів), що мають, а також тих, що не мають права модифікувати об’єкт;

КЗЗ ОЕ надає користувачу можливість для процесу кожного типу, що належить його домену, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на питання 55.2, 57, а також засобів, наведених при відповіді на питання 58, визначити конкретних користувачів (групи користувачів), що мають, а також тих, що не мають права ініціювати процес.

Згідно політики та правил, наведених при відповіді на питання 30 - 32, стосовно поділюваних ресурсів, використаних для збереження захищених пасивних об’єктів усіх типів, наведених при відповіді на питання 54.1, реалізується послуга «Повторне використання об’єктів» рівня КО-1.

Програма випробувань функціональної послуги безпеки «Абсолютна довірча цілісність» рівня ЦД-4 має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до об’єктів ОЕ всіх типів, наведених при відповіді на питання 54.1;

– КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу процесів, користувачів і захищених об’єктів, наведених при відповіді на питання 55.2, за правилами, наведеними при відповіді на питання 55, з використанням засобів, наведених при відповіді на питання 56;

– КЗЗ ОЕ надає користувачу можливість для захищеного об’єкта кожного типу, що належить його домену, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на питання 55.2, 57, а також засобів, наведених при відповіді на питання 58, визначити конкретних користувачів і процеси (групи користувачів і процесів), що мають, а також тих, що не мають права модифікувати об’єкт;

– КЗЗ ОЕ надає користувачу можливість для процесу кожного типу, що належить його домену, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на питання 55.2, 57, а також засобів, наведених при відповіді на питання 58, визначити конкретних користувачів (групи користувачів), що мають, а також тих, що не мають права ініціювати процес.

Згідно політики та правил, наведених при відповіді на питання 30 – 32, стосовно поділюваних ресурсів, використаних для збереження захищених пасивних об’єктів усіх типів, наведених при відповіді на питання 54.1, реалізується послуга «Повторне використання об’єктів» рівня КО-1.

4.3.2 Програми випробувань функціональної послуги безпеки «Адміністративна цілісність»

Спільними для всіх рівнів функціональної послуги безпеки «Адміністративна цілісність» є перевірки таких вимог:

– запити на зміну прав доступу обробляються КЗЗ ОЕ за правилами, наведеними при відповіді на питання 57, з використанням засобів, наведених

при відповіді на питання 58, лише у тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження та які відносяться до певних ролей згідно політики реалізованої КЗЗ послуги «Розмежування обов'язків» рівня НО-1 або вище;

– права доступу до кожного захищеного об'єкта встановлюються у момент його створення або ініціалізації за правилами, наведеними при відповіді на питання 61 для об'єктів різного типу;

– як частина політики послуги подані правила збереження атрибутів доступу об'єктів різного типу при їх експорті й імпорті, наведені при відповіді на питання 62, 63;

– атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги «Ідентифікація й автентифікація» рівня НИ-1 або вище згідно політики цієї послуги.

Програма випробувань функціональної послуги безпеки «Мінімальна адміністративна цілісність» рівня ЦА-1 має передбачати перевірку вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на питання 54.2;

– КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу користувачів і захищених об'єктів різного типу, наведених при відповіді на питання 55.1, за правилами, наведеними при відповіді на питання 55, з використанням засобів, наведених при відповіді на питання 56;

– КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для захищеного об'єкта кожного типу, з використанням атрибутів доступу користувачів й об'єктів різного типу, наведених при відповіді на питання 55.1, 57, а також засобів, наведених при відповіді на питання 58, визначити конкретних користувачів та/або групи користувачів, що мають право модифікувати об'єкт;

– права доступу до кожного захищеного об'єкта встановлюються у момент його створення або ініціалізації за правилами, наведеними при відповіді на питання 61 для об'єктів різного типу.

Програма випробувань функціональної послуги безпеки «Базова адміністративна цілісність» рівня ЦА-2 має передбачати перевірку вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на питання 54.2;

– КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу процесів і захищених об'єктів різного типу, наведених при відповіді на питання 55.2, за правилами, наведеними при відповіді на питання 55, з використанням засобів, наведених при відповіді на питання 56;

– КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для захищеного об'єкта кожного типу, з використанням атрибутів доступу процесів й об'єктів різного типу, наведених при відповіді на питання 55.2, 57, а також засобів, наведених при відповіді на

питання 58, визначити конкретні процеси та/або групи процесів, що мають право модифікувати об’єкт;

– КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для процесу кожного типу, що належить його домену, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на питання 55.2, 57, а також засобів, наведених при відповіді на питання 58, визначити конкретних користувачів та/або групи користувачів, що мають право ініціювати процес.

Програма випробувань функціональної послуги безпеки «Повна адміністративна цілісність» рівня ЦА-3 має передбачати перевірку вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до об’єктів ОЕ всіх типів, наведених при відповіді на питання 54.1;

– КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу процесів і захищених об’єктів різного типу, наведених при відповіді на питання 55.2, за правилами, наведеними при відповіді на питання 55, з використанням засобів, наведених при відповіді на питання 56;

– КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для захищеного об’єкта кожного типу, з використанням атрибутів доступу процесів й об’єктів різного типу, наведених при відповіді на питання 55.2, 57, а також засобів, наведених при відповіді на питання 58, визначити конкретні процеси та/або групи процесів, що мають право модифікувати об’єкт;

– КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для процесу кожного типу, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на питання 55.2, 57, а також засобів, наведених при відповіді на питання 58, визначити конкретних користувачів (групи користувачів), що мають, а також тих, що не мають права ініціювати процес.

Згідно політики та правил, наведених при відповіді на питання 30 - 32, стосовно поділюваних ресурсів, використаних для збереження захищених пасивних об’єктів усіх типів, наведених при відповіді на питання 54.1, реалізується послуга «Повторне використання об’єктів» рівня КО-1.

Програма випробувань функціональної послуги безпеки «Абсолютна адміністративна цілісність» рівня ЦА-4 має передбачати перевірку вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до об’єктів ОЕ всіх типів, наведених при відповіді на питання 54.1;

– КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу процесів, користувачів і захищених об’єктів, наведених при відповіді на питання 55.2, за правилами, наведеними при відповіді на питання 55, з використанням засобів, наведених при відповіді на питання 56;

– КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для захищеного об’єкта кожного типу, з використанням атрибутів доступу користувачів, процесів й об’єктів різного

типу, наведених при відповіді на питання 55.2, 57, а також засобів, наведених при відповіді на питання 58, визначити конкретних користувачів і процеси (групи користувачів і процесів), що мають право модифікувати об’єкт;

– КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для процесу кожного типу, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на питання 55.2, 57, а також засобів, наведених при відповіді на питання 58, визначити конкретних користувачів (групи користувачів), що мають, а також тих, що не мають права ініціювати процес.

Згідно політики та правил, наведених при відповіді на питання 30 - 32, стосовно поділюваних ресурсів, використаних для збереження захищених пасивних об’єктів усіх типів, наведених при відповіді на питання 54.1, реалізується послуга «Повторне використання об’єктів» рівня КО-1.

4.3.3 Програми випробувань функціональної послуги безпеки «Відкіт»

Послуга «Відкіт» забезпечує можливість скасування операції або послідовності операцій, виконаних над захищеним пасивним об’єктом, із поверненням захищеного об’єкта у попередній стан.

Функціональні послуги «Відкіт» ранжируються за рівнями 1, 2 множиною операцій, для яких забезпечується відкіт:

ЦО-1 – обмежений відкіт;

ЦО-2 – повний відкіт.

Спеціальні питання щодо послуги «Відкіт».

Питання 64. Чи існує в об’єкті експертизи (ОЕ) для будь-якого з типів пасивних об’єктів можливість автоматизованого виконання скасування окремих операцій або послідовності операцій, пов’язаних зі зміною самих об’єктів або їх атрибутів, із поверненням пасивного об’єкта у стан, що передував виконанню операції або набору операцій.

Якщо така можливість існує, то це означає, що засобами КЗЗ реалізується послуга «Відкіт», її політика та рівні можуть бути уточнені при відповіді на питання 65 – 67. Інакше, послуга «Відкіт» засобами КЗЗ ОЕ не реалізується.

Питання 65. Наведіть перелік типів пасивних об’єктів, для яких існує зазначена при відповіді на питання 64 можливість автоматизованого виконання скасування окремих операцій або послідовності операцій, пов’язаних зі зміною самих об’єктів або їх атрибутів, із поверненням пасивного об’єкта у стан, що передував виконанню операції або набору операцій, а також множину відповідних операцій для пасивних об’єктів кожного типу.

Питання 66. В яких функціональних модулях ОЕ, що входять до складу КЗЗ, із використанням яких механізмів реалізується можливість скасування наведеної при відповіді на питання 65 множини операцій, виконаних над захищеними пасивними об’єктами різного типу.

Питання 67. Чи забезпечується наведеними при відповіді на питання 66 механізмами, реалізованими у функціональних модулях ОЕ, що входять до складу КЗЗ, можливість:

1) скасування всіх операцій, проведених над захищеними об'єктами за певний (укажіть який) проміжок часу (вкажіть для кожного з типів об'єктів, наведених при відповіді на питання 65). Тоді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Відкіт» рівня ЦО-2;

2) скасування лише певного набору (множини) операцій, проведених над захищеними об'єктами за певний (укажіть який) проміжок часу (вкажіть для кожного з типів об'єктів). Тоді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Відкіт» рівня ЦО-1.

***Програма випробувань функціональної послуги безпеки «Обмежений відкіт» рівня ЦО-*1** має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на питання 65;

– існують автоматизовані засоби, що дозволяють авторизованому користувачу, атрибути якого автентифіковані з використанням засобів реалізації послуги «Ідентифікація й автентифікація» рівня НИ-1 або вище згідно політики цієї послуги, або процесу «відкотити» чи скасувати певний набір (множину) операцій, виконаних над захищеним об'єктом певного типу за певний проміжок часу, з використанням засобів, механізмів і правил, наведених при відповіді на питання 66, 67.2.

***Програма випробувань функціональної послуги безпеки «Повний відкіт» рівня ЦО-*2** має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на питання 65.

Існують автоматизовані засоби, що дозволяють авторизованому користувачу, атрибути якого автентифіковані з використанням засобів реалізації послуги «Ідентифікація й автентифікація» рівня НИ-1 або вище згідно політики цієї послуги або процесу «відкотити» чи скасувати всі операції, виконані над захищеним об'єктом певного типу за певний проміжок часу, з використанням засобів, механізмів і правил, наведених при відповіді на питання 66, 67.1.

4.3.4 Програми випробувань функціональної послуги безпеки «Цілісність при обміні»

Послуга «Цілісність при обміні» дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься у них, при їх передачі (експорті/імпорті) через незахищене середовище. Функціональна послуга «Цілісність при обміні» ранжирується на підставі повноти захисту та вибірковості керування:

ЦВ-1 – мінімальна цілісність при обміні;

ЦВ-2 – базова цілісність при обміні;
ЦВ-3 – повна цілісність при обміні;

Спеціальні питання щодо послуги «Цілісність при обміні».

Питання 68. Чи існує в об’єкті експертизи (ОЕ) можливість обміну (з використанням відповідних інтерфейсних процесів) між різними компонентами ОЕ через незахищене середовище пасивними об’єктами будь-якого з типів. Якщо така можливість існує, то наведіть цю підмножину типів пасивних об’єктів.

У випадку позитивної відповіді можна стверджувати, що в ОЕ може бути реалізована послуга «Цілісність при обміні» рівня ЦВ-1, ЦВ-2 чи ЦВ-3. Інакше, ці послуги не реалізується та відповідати на наступні питання не потрібно.

Питання 69. Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ, засоби та відповідні механізми, які забезпечують:

1) виявлення фактів несанкціонованої модифікації інформації, що міститься у переданих пасивних об’єктах, наведених при відповіді на питання 68, при їх передачі між різними компонентами ОЕ через незахищене середовище;

2) виявлення фактів несанкціонованого видалення або дублювання переданих пасивних об’єктів, наведених при відповіді на питання 68, при їх передачі між різними компонентами ОЕ через незахищене середовище.

Функціонування механізмів, що забезпечують реалізацію послуги «Цілісність при обміні», у частині, що стосується виявлення фактів несанкціонованої модифікації, може ґрунтуватися на одному з таких принципів:

– виявлення порушень цілісності шляхом вироблення/перевірки криптографічних (таких, що обчислюються з використанням ключових даних) кодів контролю цілісності (кодів автентифікації повідомлень);

– виявлення порушень цілісності шляхом вироблення/перевірки не криптографічних кодів контролю цілісності з їх подальшим зашифруванням/розшифруванням;

– виявлення порушень цілісності шляхом вироблення/перевірки електронного цифрового підпису;

– виявлення порушень цілісності шляхом зашифрування/розшифрування повідомлень, що містять надмірні дані (наприклад, текст оригінальною мовою), з подальшим контролем збереження надмірності.

Функціонування механізмів, що забезпечують реалізацію послуги «Цілісність при обміні», у частині, що стосується виявлення фактів несанкціонованого видалення або дублювання переданих пасивних об’єктів, може ґрунтуватися на принципі використання узгодженого контексту повідомлення (наприклад, порядкового номера або часової мітки) у комбінації з механізмами, що забезпечують виявлення фактів несанкціонованої модифікації.

Якщо у складі КЗЗ є засоби, що реалізують механізми, наведені при відповіді на питання 69.1, то це означає, що засобами КЗЗ може бути реалізована послуга «Конфіденційність при обміні». Інакше, ця послуга не реалізується та відповідати на наступні питання не потрібно.

Питання 70. Наведіть перелік типів пасивних об’єктів (з урахуванням відповіді на питання 68), а також використаних для їх приймання/передачі функціональних модулів ОЕ, що входять до складу КЗЗ (інтерфейсних процесів), стосовно яких визначена політика функціональної послуги «Цілісність при обміні», тобто, забезпечується можливість виявлення фактів несанкціонованої модифікації інформації, що міститься у переданих пасивних об’єктах, при їх передачі через незахищене середовище.

Питання 71. В яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на питання 69.1), з використанням яких саме механізмів захисту реалізується виявлення фактів несанкціонованої модифікації інформації, що міститься у переданих пасивних об’єктах кожного з типів. Який рівень захищеності забезпечується використаними механізмами. Якими параметрами (якими атрибутами доступу пасивних об’єктів або властивостями використаних механізмів) визначається рівень захищеності, забезпечуваний для пасивних об’єктів різного типу, наведених при відповіді на питання 70. Чи існує можливість у користувачів та/або процесів (укажіть яких), з використанням відповідних функціональних модулів ОЕ, що входять до складу КЗЗ (вкажіть яких), керувати (шляхом зміни відповідних параметрів) рівнем захищеності, що забезпечується для пасивних об’єктів різного типу.

У випадку позитивної відповіді на питання 71 (в частині можливості керування рівнем захищеності) можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Цілісність при обміні» рівня ЦВ-2 чи ЦВ-3. Інакше – може бути реалізована послуга «Цілісність при обміні» рівня ЦВ-1.

Питання 72. В яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на питання 69.2), з використанням яких саме механізмів захисту реалізується виявлення фактів видалення чи дублювання переданих пасивних об’єктів, наведених при відповіді на питання 70. Який рівень захищеності забезпечується використаними механізмами. Якими параметрами (якими атрибутами доступу пасивних об’єктів або властивостями використаних механізмів) визначається рівень захищеності, забезпечуваний для пасивних об’єктів, наведених при відповіді на питання 70. Чи існує можливість у користувачів та/або процесів (укажіть яких), з використанням відповідних функціональних модулів ОЕ, що входять до складу КЗЗ (укажіть яких), керувати (шляхом зміни відповідних параметрів) рівнем захищеності, що забезпечується для пасивних об’єктів різного типу.

У випадку позитивної відповіді на питання 72 можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Цілісність при обміні» рівня ЦВ-2 чи ЦВ-3. Інакше – може бути реалізована ця послуга рівня ЦВ-1.

Питання 73. Чи існує можливість у наведених при відповіді на питання 71, 72 засобах керування рівнем захищеності, що забезпечується для пасивних об’єктів різного типу, оброблення запитів на присвоєння або зміну рівня захищеності лише у випадку, якщо вони надходять від користувачів, що відносяться лише до певних ролей (від адміністраторів або користувачів, яким надані відповідні повноваження). На підставі яких атрибутів об’єктів-

користувачів, що визначають їх повноваження, та за якими правилами виконується оброблення цих запитів.

У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Цілісність при обміні» рівня ЦВ-2 чи ЦВ-3. Інакше – може бути реалізована ця послуга «Цілісність при обміні» рівня ЦВ-1.

Питання 74. Чи обробляються запити на експорт (передачу) захищеного пасивного об’єкта передавальним компонентом (функціональним модулем ОЕ, що входить до складу КЗЗ) на підставі:

1) атрибутів доступу інтерфейсного процесу, що здійснює передачу, і КЗЗ (компонента КЗЗ), що є приймачем об’єкта (вкажіть яких). У цьому випадку можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Цілісність при обміні» рівня ЦВ-3;

2) лише атрибутів доступу інтерфейсного процесу, що здійснює передачу (вкажіть яких). У цьому випадку може бути реалізована послуга «Цілісність при обміні» рівня ЦВ-2.

У випадку негативної відповіді на питання 74.1 і 74.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Цілісність при обміні» рівня ЦВ-1, відповідати на питання 75, 76 не потрібно.

Питання 75. Чи обробляються запити на імпорт (приймання) захищеного пасивного об’єкта приймаючим компонентом (функціональним модулем ОЕ, що входить до складу КЗЗ) на підставі:

1) атрибутів доступу інтерфейсного процесу, що здійснює приймання, і КЗЗ (компонента КЗЗ), що є джерелом об’єкта (вкажіть яких). Тоді, засобами КЗЗ може бути реалізована послуга «Цілісність при обміні» рівня ЦВ-3;

2) лише атрибутів доступу інтерфейсного процесу, що здійснює приймання (вкажіть яких). У цьому випадку засобами КЗЗ може бути реалізована послуга «Цілісність при обміні» рівня ЦВ-2. Інакше – може бути реалізована послуга "Цілісність при обміні" рівня ЦВ-1.

Питання 76. Чи є представлення захищеного переданого пасивного об’єкта функцією атрибутів доступу інтерфейсного процесу (з урахуванням відповідей на питання 74.1, 75.1), самого об’єкта, а також його джерела та приймача. Якщо так, то опишіть відповідну функціональну залежність.

У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Цілісність при обміні» рівня ЦВ-3.

Спільною для всіх рівнів функціональної послуги безпеки «Цілісність при обміні» є перевірка вимоги: політика послуги, що реалізується КЗЗ ОЕ, відноситься до об’єктів й існуючих інтерфейсних процесів усіх типів.

***Програма випробувань функціональної послуги безпеки «Мінімальна цілісність при обміні» рівня ЦВ*-1** має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, визначає рівень захищеності, наведений при відповіді на питання 71, який забезпечується використаними механізмами;

КЗЗ ОЕ забезпечує можливість виявлення порушення цілісності інформації, що міститься у переданих об’єктах різного типу, з використанням засобів і механізмів, наведених при відповіді на питання 69.1, 71.

Програма випробувань функціональної послуги безпеки «Базова цілісність при обміні» рівня ЦВ-2 має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, визначає рівень захищеності, який забезпечується використаними механізмами, і здатність користувачів та/або процесів керувати рівнем захищеності згідно правил, наведених при відповіді на питання 71,72;

– КЗЗ ОЕ забезпечує можливість виявлення порушення цілісності інформації, що міститься у переданих об’єктах різного типу, а також фактів їх видалення або дублювання, з використанням засобів і механізмів, наведених при відповіді на питання 69.1, 69.2, 71, 72;

– запити на експорт захищеного об’єкта певного типу обробляються передавальним КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на питання 71, 72, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на питання 74.2;

– запити на імпорт захищеного об’єкта певного типу обробляються приймаючим КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на питання 71, 72, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на питання 75.2;

– запити на присвоєння або зміну рівня захищеності обробляються КЗЗ ОЕ у засобах, наведених при відповіді на питання 71, 72, за правилами, наведеними при відповіді на питання 73, лише у тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно політики реалізованої КЗЗ послуги «Розмежування обов’язків» рівня НО-1 або вище.

Програма випробувань функціональної послуги безпеки «Повна цілісність при обміні» рівня ЦВ-3 має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, визначає рівень захищеності, який забезпечується використаними механізмами, і здатність користувачів та/або процесів керувати рівнем захищеності згідно правил, наведених при відповіді на питання 71, 72;

– КЗЗ ОЕ забезпечує можливість виявлення порушення цілісності інформації, що міститься у переданих об’єктах різного типу, а також фактів їх видалення або дублювання, з використанням засобів і механізмів, наведених при відповіді на питання 69.1, 69.2, 71, 72;

– запити на експорт захищеного об’єкта певного типу обробляються передавальним КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на питання 71, 72, на підставі атрибутів доступу інтерфейсного процесу відповідного типу й атрибутів приймача об’єкта, наведених при відповіді на питання 74.1 й автентифікованих з використанням засобів реалізації послуги «Ідентифікація й автентифікація при обміні» рівня НВ-1 або вище згідно політики та правил цієї послуги;

– запити на імпорт захищеного об’єкта певного типу обробляються приймаючим КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на питання 71, 72, на підставі атрибутів доступу інтерфейсного процесу відповідного типу й атрибутів джерела об’єкта, наведених при відповіді на питання 75.1 й автентифікованих з використанням засобів реалізації послуги «Ідентифікація й автентифікація при обміні» рівня НВ-1 або вище згідно політики та правил цієї послуги;

– запити на присвоєння або зміну рівня захищеності обробляються КЗЗ ОЕ у засобах, наведених при відповіді на питання 71, 72, за правилами, наведеними при відповіді на питання 73, лише у тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження та які відносяться до певних ролей згідно політики реалізованої КЗЗ послуги «Розмежування обов’язків» рівня НО-1 або вище.

Подання захищеного об’єкта певного типу є функцією атрибутів доступу інтерфейсного процесу відповідного типу, самого об’єкта, а також його джерела та приймача згідно з описом, наведеним при відповіді на питання 76.

4.4 Програма випробування функціональних послуг безпеки критеріїв доступності

Комплекс заходів захисту (КЗЗ), оцінюваної на предмет відповідності критеріям доступності інформаційно-телекомунікаційної системи (ІТС), має надавати послуги щодо забезпечення можливості використання ІТС у цілому, окремих функцій або оброблюваної інформації на певному проміжку часу та гарантувати здатність ІТС функціонувати у випадку відмови її компонентів. Доступність може забезпечуватись в інформаційно-телекомунікаційній системі наступними послугами:

ДР – використання ресурсів;

ДС – стійкість до відмов;

ДЗ – гаряча заміна;

ДВ – відновлення після збоїв.

4.4.1 Програма випробування функціональної послуги «Використання ресурсів»

Послуга «Використання ресурсів» дозволяє забезпечити доступність послуг і ресурсів ОЕ шляхом керування обсягом ресурсів, що виділяються користувачам. Функціональна послуга «Використання ресурсів» ранжирується на підставі повноти захисту та вибірковості керування доступністю послуг:

ДР-1 – квоти;

ДР-2 – недопущення захоплення ресурсів;

ДР-3 – пріоритетність використання ресурсів.

Спеціальні питання щодо послуги «Використання ресурсів»

Питання 77. Чи існує в ОЕ можливість керування обсягом поділюваних ресурсів, що надаються користувачу та використовуються у процесі оброблення, збереження або передачі пасивних об’єктів будь-якого з типів.

Як приклади поділюваних ресурсів, використаних для збереження, оброблення або передачі пасивних об’єктів різних типів, можна навести:

– дисковий простір (для збереження об’єктів у вигляді файлів);

– табличний простір систем управління базами даних (СУБД) (для збереження об’єктів у вигляді записів таблиць СУБД);

– мережеві з’єднання (для передачі пасивних об’єктів);

– процесорний час, що виділяється певному користувачу для виконання ініційованих ним процесів, тощо.

Питання 78. Чи відноситься політика послуги (можливість керування обсягом ресурсів, що виділяються користувачу) до поділюваних ресурсів, використаних для оброблення, збереження та передачі:

1) пасивних об’єктів усіх типів. У цьому випадку засобами КЗЗ може бути реалізована послуга «Використання ресурсів» рівня ДР-2 чи ДР-3;

2) пасивних об’єктів лише деяких (укажіть яких) типів. У цьому випадку засобами КЗЗ може бути реалізована ця послуга рівня ДР-1.

Питання 79. Наведіть перелік обмежень (з урахуванням відповіді на питання 78.2) на обсяг поділюваних ресурсів, що виділяються користувачу та використовуються для оброблення, збереження та передачі пасивних об’єктів.

Питання 80. Чи існує можливість у функціональних модулях ОЕ, що входять до складу КЗЗ, установлювати наведені при відповіді на питання 79 обмеження для:

1) окремих користувачів і довільних груп користувачів різного типу. У цьому випадку можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Використання ресурсів» рівня ДР-3;

2) лише окремих користувачів різного типу. У цьому випадку засобами КЗЗ може бути реалізована послуга «Використання ресурсів» рівня ДР-1 чи ДР-2.

Питання 81. В яких функціональних модулях ОЕ, що входять до складу КЗЗ, з використанням яких саме механізмів реалізується контроль за дотриманням встановлених обмежень, наведених при відповіді на питання 79, на обсяг поділюваних ресурсів, що виділяються користувачам різного типу (з урахуванням відповіді на питання 80) і використовуються для оброблення, збереження та передачі пасивних об’єктів різного типу. На підставі яких атрибутів користувачів і груп користувачів, пасивних об’єктів і за якими правилами виконується прийняття рішення про виділення або не виділення користувачу (групі) необхідного обсягу ресурсу.

Питання 82. В яких функціональних модулях ОЕ, що входять до складу КЗЗ, здійснюється оброблення запитів на зміну встановлених обмежень, наведених при відповіді на питання 79, на обсяг поділюваних ресурсів, що виділяються користувачам різного типу та використовуються для оброблення, збереження та передачі пасивних об’єктів різного типу.

Питання 83. Чи існує можливість у засобах, наведених при відповіді на питання 82, оброблення запитів на зміну встановлених обмежень лише у випадку, якщо вони надходять від користувачів, що відносяться лише до певних ролей (від адміністраторів або користувачів, яким надані відповідні

повноваження). На підставі яких атрибутів повноважень об’єктів-користувачів, і за якими правилами виконується оброблення цих запитів.

У випадку позитивної відповіді можна стверджувати, що може бути реалізована послуга «Використання ресурсів» рівня ДР-1, ДР-2 чи ДР-3.

Питання 84. Чи існує можливість у вказаних у питанні 83 засобах установлювати зазначені у питанні 79 обмеження таким чином, щоб засоби КЗЗ мали можливість запобігти діям, які можуть призвести до недоступності функцій (послуг) ОЕ для інших користувачів:

1) з боку окремого користувача та довільних груп користувачів. У цьому випадку може бути реалізована послуга «Використання ресурсів» рівня ДР-3;

2) лише з боку окремого користувача. У цьому випадку засобами КЗЗ може бути реалізована послуга «Використання ресурсів» рівня ДР-2.

Питання 85. Наведіть правила, згідно з якими, на підставі атрибутів пасивних об’єктів і використаних для їх оброблення, збереження та передачі поділюваних ресурсів, наведених при відповіді на питання 78, 79, атрибутів користувачів або груп користувачів, наведених при відповіді на питання 80, у функціональних компонентах ОЕ, що входять до складу КЗЗ і задіяні у реалізації послуги (з урахуванням відповіді на питання 81), реалізуються можливості встановлення обмежень, наведених при відповіді на питання 84.

Спільною для всіх рівнів функціональної послуги безпеки «Використання ресурсів» є перевірка вимоги: запити на зміну встановлених обмежень обробляються КЗЗ ОЕ у засобах, наведених при відповіді на питання 82, за правилами, наведеними при відповіді на питання 83, лише у тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження та які відносяться до певних ролей згідно політики реалізованої КЗЗ послуги «Розмежування обов’язків» рівня НО-1 або вище.

Програма випробувань функціональної послуги безпеки «Використання ресурсів» рівня ДР-1 «Квоти» має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до об’єктів ОЕ всіх типів, наведених при відповіді на питання 78.2;

– політика послуги визначає обмеження, наведені при відповіді на питання 79, 80.2, які можна накладати на кількість об’єктів (обсяг ресурсів) певного типу, що виділяються окремому користувачу;

– КЗЗ ОЕ забезпечує можливість контролю за дотриманням встановлених обмежень із боку окремого користувача з використанням засобів, механізмів і правил, наведених при відповіді на питання 81.

Програма випробувань функціональної послуги безпеки «Використання ресурсів» рівня ДР-2 «Недопущення захоплення ресурсів» має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до об’єктів ОЕ всіх типів, наведених при відповіді на питання 78.1;

– політика послуги визначає обмеження, наведені при відповіді на питання 79, 80.2, які можна накладати на кількість об’єктів (обсяг ресурсів) певного типу, що виділяються окремому користувачу;

– існує можливість у засобах, наведених при відповіді на питання 82, за правилами, наведеними при відповіді на питання 85, встановлювати обмеження таким чином, щоб КЗЗ ОЕ мав можливість запобігти діям, які можуть призвести до неможливості доступу інших користувачів до функцій КЗЗ ОЕ або захищених об’єктів;

– КЗЗ ОЕ забезпечує можливість контролю за дотриманням встановлених обмежень із боку окремого користувача з використанням засобів, механізмів і правил, наведених при відповіді на питання 81.

Програма випробувань функціональної послуги безпеки «Використання ресурсів» рівня ДР-3 «Пріоритетність використання ресурсів» має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до об’єктів ОЕ всіх типів, наведених при відповіді на питання 78.1;

– політика послуги визначає обмеження, наведені при відповіді на питання 79, 80.1, які можна накладати на кількість об’єктів (обсяг ресурсів) певного типу, що виділяються окремому користувачу та довільним групам користувачів;

– існує можливість у засобах, наведених при відповіді на питання 82, за правилами, наведеними при відповіді на питання 85, встановлювати обмеження таким чином, щоб КЗЗ ОЕ мав можливість запобігти діям, що можуть призвести до неможливості доступу інших користувачів до функцій КЗЗ ОЕ або захищених об’єктів;

– КЗЗ ОЕ забезпечує можливість контролю за дотриманням встановлених обмежень із боку окремого користувача та довільних груп користувачів із використанням засобів, механізмів і правил, наведених при відповіді на питання 81.

4.4.2 Програма випробування функціональної послуги «Стійкість до відмов»

Послуга «Стійкість до відмов» дозволяє забезпечити доступність послуг і ресурсів об’єкта експертизи (ОЕ) шляхом забезпечення використання окремих функцій ОЕ чи ОЕ у цілому після відмови його компонента. Послуги «Стійкість до відмов» ранжируються за рівням 1 … 3 на підставі здатності КЗЗ забезпечити можливість функціонування інформаційно-комунікаційної системи залежно від кількості відмов і послуг, доступних після відмови:

ДС-1 – стійкість при обмежених відмовах;

ДС-2 – стійкість при погіршенні характеристик обслуговування;

ДС-3 – стійкість без погіршення характеристик обслуговування.

Спеціальні питання щодо послуги «Стійкість до відмов»

Питання 86. Чи існує в ОЕ можливість збереження часткової або повної працездатності та продовження виконання функцій з оброблення інформації при відмові (виході з ладу) будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ, або компонентів ІТС, на базі яких функціонують відповідні функціональні модулі. Якщо така можливість існує, то це означає, що засобами КЗЗ може бути реалізована послуга «Стійкість до відмов».

Питання 87. Наведіть результати аналізу відмов функціональних модулів ОЕ, що входять до складу КЗЗ, і компонентів ІТС, на базі яких функціонують відповідні функціональні модулі, з наведенням модулів (компонентів) і типів відмов, після яких ОЕ у стані продовжувати функціонування, нехай і зі зниженням характеристик обслуговування (вкажіть яких), а також компонентів і типів відмов, що призводять до недоступності певних функцій (послуг) ОЕ (вкажіть яких). У наведених результатах аналізу повинні бути чітко вказані (для всіх проаналізованих функціональних модулів ОЕ, що входять до складу КЗЗ, і компонентів ІТС) рівні відмов, які призводять до зниження характеристик обслуговування або до недоступності певних послуг ОЕ.

Питання 88. Чи відносяться результати аналізу, наведені при відповіді на питання 87:

1) до всіх функціональних модулів ОЕ, що входять до складу КЗЗ. У цьому випадку можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Стійкість до відмов» рівня ДС-2 чи ДС-3;

2) лише до частини функціональних модулів ОЕ (вкажіть яких), що входять до складу КЗЗ. У цьому випадку може бути реалізована ця послуга рівня ДС-1.

Питання 89. Чи забезпечується умова збереження доступності (працездатності) при відмові будь-якого функціонального модуля ОЕ, введеного до складу КЗЗ, або компонента ІТС, на базі якого функціонує відповідний модуль, з наведених при відповіді на питання 87, 88, для всіх інших функціональних модулів ОЕ, внесених до складу КЗЗ:

1) без зниження характеристик обслуговування. У цьому випадку засобами КЗЗ може бути реалізована послуга «Стійкість до відмов» рівня ДС-3.

2) зі зниженням характеристик обслуговування (вкажіть яких). Тоді може бути реалізована послуга «Стійкість до відмов» рівня ДС-1 чи ДС-2.

Питання 90. В яких функціональних модулях ОЕ, що входять до складу КЗЗ, із використанням яких саме механізмів реалізується можливість оповіщення користувачів, що відносяться до певних ролей (адміністраторів), про відмову будь-якого захищеного компонента з наведених при відповіді на питання 88. У випадку відсутності таких механізмів можна стверджувати, що послуга «Стійкість до відмов» засобами КЗЗ ОЕ не реалізується.

Спільними для всіх рівнів функціональної послуги безпеки «Стійкість до відмов» є перевірки таких вимог:

– розробником проведено аналіз відмов компонентів об’єкта експертизи (ОЕ), відповідні результати наведені при відповіді на питання 87;

– у результатах аналізу, наведеного при відповіді на питання 87, чітко вказані рівні відмов різних компонентів ОЕ, наведених при відповіді на питання 88, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги.

– КЗЗ ОЕ здатний, із використанням засобів і механізмів, наведених при відповіді на питання 90, повідомляти про відмову будь-якого захищеного компонента адміністратора, який відноситься до певної ролі згідно політики реалізованої КЗЗ послуги «Розмежування обов’язків» рівня НО-1 або вище.

Програма випробувань функціональної послуги безпеки «Стійкість до відмов» рівня ДС-1 «Стійкість при обмежених відмовах» має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, визначає множину компонентів ОЕ, до яких вона відноситься, наведену при відповіді на питання 88.2, і типи їх відмов, наведені при відповіді на питання 87, після яких ОЕ у стані продовжувати функціонування;

– відмова одного захищеного компонента з наведених при відповіді на питання 88.2 не призводить до недоступності всіх послуг, а у гіршому випадку проявляється у зниженні характеристик обслуговування, наведених при відповіді на питання 89.2.

Програма випробувань функціональної послуги безпеки «Стійкість до відмов» рівня ДС-2 «Стійкість із погіршенням характеристик обслуговування» має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до всіх компонентів ОЕ, наведених при відповіді на питання 88.1, і визначає типи їх відмов, наведені при відповіді на питання 87, після яких ОЕ у стані продовжувати функціонування;

– відмова одного захищеного компонента з наведених при відповіді на питання 88.1 не призводить до недоступності всіх послуг, а у гіршому випадку проявляється у зниженні характеристик обслуговування, наведених при відповіді на питання 89.2.

Програма випробувань функціональної послуги безпеки «Стійкість до відмов» рівня ДС-3 «Стійкість без погіршення характеристик обслуговування» має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, відноситься до всіх компонентів ОЕ, наведених при відповіді на питання 88.1, і визначає типи їх відмов, наведені при відповіді на питання 87, після яких ОЕ у стані продовжувати функціонування;

– відмова одного захищеного компонента не призводить до недоступності всіх послуг або до зниження характеристик обслуговування.

4.4.3 Програма випробування функціональної послуги «Гаряча заміна»

Послуга «Гаряча заміна» дозволяє забезпечити доступність послуг і ресурсів ОЕ у процесі заміни окремих його компонентів. Функціональні послуги «Гаряча заміна» ранжирується за рівнями 1 … 3 у залежності від повноти реалізації:

ДЗ-1 – модернізація;

ДЗ-2 – обмежена гаряча заміна;

ДЗ-3 – гаряча заміна будь-якої компоненти.

Спеціальні питання щодо послуги «Гаряча заміна»

Питання 91. Чи існує в ОЕ можливість проведення заміни (модернізації) будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ, без

необхідності заново проводити інсталяцію ОЕ або настроювання відповідних функціональних модулів.

Якщо існує можливість проведення заміни (модернізації) будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ, без необхідності заново проводити інсталяцію ОЕ або настроювання відповідних функціональних модулів, то це означає, що засобами КЗЗ може бути реалізована послуга «Гаряча заміна».

Питання 92. Наведіть перелік функціональних модулів ОЕ, що входять до складу КЗЗ, які можуть бути замінені (модернізовані) без необхідності заново проводити інсталяцію ОЕ або настроювання відповідних функціональних модулів. Чи складає зазначений перелік:

1) всю множину функціональних модулів ОЕ, що входять до складу КЗЗ. При цьому може бути реалізована послуга «Гаряча заміна» рівня ДЗ-3 чи ДЗ-2;

2) лише частину множини функціональних модулів ОЕ, що входять до складу КЗЗ. Тоді може бути реалізована послуга «Гаряча заміна» рівня ДЗ-1.

Питання 93. Чи існує можливість проведення, з використанням засобів, реалізованих у відповідних функціональних модулях ОЕ, що входять до складу КЗЗ, заміни (модернізації) усіх функціональних модулів ОЕ, що входять до складу КЗЗ, лише користувачами, що відносяться до певних ролей (адміністраторами або користувачами, яким надані відповідні повноваження).

Питання 94. Чи існує можливість проведення користувачами, що відносяться до певних ролей (адміністраторами або користувачами, яким надані відповідні повноваження), з використанням засобів, реалізованих у відповідних функціональних модулях ОЕ, що входять до складу КЗЗ заміни (модернізації) без переривання обслуговування (без зупинки та наступного запуску ОЕ):

1) кожного з функціональних модулів ОЕ, що входять до складу КЗЗ і наведені при відповіді на питання 92. У цьому випадку можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Гаряча заміна» рівня ДЗ-3;

2) лише деяких функціональних модулів ОЕ, що входять до складу КЗЗ і наведені при відповіді на питання 9.2 (вкажіть яких). У цьому випадку, засобами КЗЗ може бути реалізована послуга «Гаряча заміна» рівня ДЗ-2.

Питання 95. На підставі яких атрибутів доступу об’єктів-користувачів, що визначають їх приналежність до певних ролей (адміністраторів або користувачів, яким надані відповідні повноваження), в яких функціональних модулях ОЕ, що входять до складу КЗЗ, і згідно з якими правилами здійснюється оброблення запитів на виконання заміни (модернізації) різних функціональних модулів ОЕ, що входять до складу.

Програма випробувань функціональної послуги безпеки «Гаряча заміна» рівня ДЗ-1 – «Модернізація» має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, визначає політику проведення модернізації певної множини компонентів ОЕ, що входять до складу КЗЗ ОЕ, наведену при відповіді на питання 92.2, 93;

– адміністратор або користувачі, яким надані відповідні повноваження та які відносяться до певних ролей згідно політики реалізованої КЗЗ послуги

«Розмежування обов’язків» рівня НО-1 або вище, мають можливість провести модернізацію (*upgrade*) відповідних компонентів ОЕ, що входять до складу КЗЗ ОЕ, з використанням засобів і за правилами, що не призводить до необхідності переінсталяції ОЕ або до переривання виконання КЗЗ ОЕ функцій захисту.

Програма випробувань функціональної послуги безпеки «Гаряча заміна» рівня ДЗ-2 – «Обмежена гаряча заміна» має передбачати перевірку вимог:

– політика послуги, що реалізується КЗЗ ОЕ, визначає множину компонентів ОЕ, що входять до складу КЗЗ ОЕ, які можуть бути замінені без переривання обслуговування, наведену при відповіді на питання 94.2.

Стосовно компонентів ОЕ, що входять до складу КЗЗ ОЕ та можуть бути замінені без переривання обслуговування, наведених при відповіді на питання 94.2, згідно політики, наведеної при відповіді на питання 87, 88, реалізовано послугу «Стійкість до відмов» рівня ДС-1 або вище.

Адміністратор або користувачі, яким надані відповідні повноваження та які відносяться до певних ролей згідно політики реалізованої КЗЗ послуги «Розмежування обов’язків» рівня НО-1 або вище, мають можливість замінити будь-який захищений компонент ОЕ, що входить до складу КЗЗ ОЕ, з використанням засобів і за правилами, наведеними при відповіді на питання 92, 93, 95.

Програма випробувань функціональної послуги безпеки «Гаряча заміна» рівня ДЗ-3 – «Гаряча заміна будь-якого компонента» має передбачати перевірку таких вимог:

Політика послуги, що реалізується КЗЗ ОЕ, забезпечує можливість заміни будь-якого компонента ОЕ, що входить до складу КЗЗ ОЕ, наведеного при відповіді на питання 94.1, без переривання обслуговування.

Стосовно компонентів ОЕ, що входять до складу КЗЗ ОЕ та можуть бути замінені без переривання обслуговування, наведених при відповіді на питання 94.1, згідно політики, наведеної при відповіді на питання 87, 88, реалізовано послугу «Стійкість до відмов» рівня ДС-1 або вище.

Адміністратор або користувачі, яким надані відповідні повноваження та які відносяться до певних ролей згідно політики реалізованої КЗЗ послуги «Розмежування обов’язків» рівня НО-1 або вище, мають можливість замінити будь-який захищений компонент ОЕ, що входить до складу КЗЗ ОЕ, з використанням засобів і за правилами, наведеними при відповіді на питання 92, 93, 95.

4.4.4 Програма випробування функціональної послуги «Відновлення після збоїв»

Послуга «Відновлення після збоїв» дозволяє забезпечити доступність послуг і ресурсів об’єкта експертизи (ОЕ) шляхом переведення ОЕ у відомий захищений стан після відмови або переривання обслуговування. Функціональні послуги «Відновлення після збоїв» ранжируються за рівнями 1 … 3 за мірою автоматизації процесу відновлення:

ДВ-1 – ручне відновлення;
ДВ-2 – автоматизоване відновлення;
ДВ-3 – вибіркове відновлення.

Спеціальні питання щодо послуги «Відновлення після збоїв»

Питання 96. Чи існує в ОЕ можливість повернення у визначений захищений стан у випадку відмови або збою будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ.

Питання 97. Наведіть результати аналізу відмов функціональних модулів ОЕ, що входять до складу КЗЗ, із наведенням функціональних модулів, типів відмов і переривань обслуговування, після яких можливе повернення у визначений захищений стан без порушення політики безпеки. У наведених результатах аналізу повинні бути чітко вказані (для всіх проаналізованих функціональних модулів ОЕ, що входять до складу КЗЗ) рівні відмов, при перевищенні яких необхідна повторна інсталяція ОЕ.

Питання 98. Чи існує можливість при відмові різних функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на питання. 97), з використанням засобів, реалізованих у відповідних функціональних модулях ОЕ, що входять до складу КЗЗ (вкажіть яких), переведення ОЕ у стан із припиненням обслуговування, з якого повернути його до нормального функціонування можуть лише користувачі, що відносяться до певних ролей. За якими правилами приймається рішення про необхідність переведення ОЕ у такий стан при відмові різних функціональних модулів ОЕ, що входять до складу КЗЗ, які характеристики цього стану.

У цьому випадку можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Відновлення після збоїв» рівня ДВ-1, ДВ-2 чи ДВ-3.

Питання 99. Чи існує можливість при відмові різних функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на питання 97), з використанням засобів, реалізованих у відповідних функціональних модулях ОЕ, що входять до складу КЗЗ, визначення можливості використання автоматизованих процедур для повернення безпечним чином ОЕ до нормального функціонування. За якими правилами приймається рішення про можливість використання автоматизованих процедур для повернення ОЕ до нормального функціонування для різних типів відмов різних функціональних модулів ОЕ, що входять до складу.

У цьому випадку можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Відновлення після збоїв» рівня ДВ-2 чи ДВ-3.

Питання 100. Чи існує можливість при відмові різних функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на питання 97), з використанням засобів, реалізованих у відповідних функціональних модулях ОЕ, що входять до складу КЗЗ, визначення можливості використання автоматизованих процедур для повернення безпечним чином ОЕ до функціонування у режимі з погіршеними характеристиками обслуговування. За якими правилами приймається рішення про можливість використання автоматизованих процедур для повернення ОЕ до функціонування у режимі з

погіршеними характеристиками обслуговування для різних типів відмов різних функціональних модулів ОЕ.

У цьому випадку можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Відновлення після збоїв» рівня ДВ-3.

Питання 101. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ, реалізовані автоматизовані процедури для повернення безпечним чином функціональних модулів ОЕ, що входять до складу КЗЗ, після відмови або переривання обслуговування (з урахуванням відповідей на питання 99, 100) до нормального функціонування або функціонування у режимі з погіршеними характеристиками обслуговування. Яким чином (за якими правилами та у якій послідовності) виконується повернення після відмови або переривання обслуговування до нормального функціонування або функціонування у режимі з погіршеними характеристиками обслуговування при різних типах відмов різних функціональних модулів ОЕ.

Питання 102. Чи існує можливість із використанням засобів, реалізованих у відповідних функціональних модулях ОЕ, що входять до складу КЗЗ (укажіть яких, для різних типів відмов), у випадку, якщо автоматизовані процедури, наведені при відповіді на питання 99, 100, не можуть бути використані, переведення ОЕ у стан із припиненням обслуговування, з якого повернути його до нормального функціонування можуть лише користувачі, що відносяться до певних ролей (адміністратори або користувачі).

У цьому випадку можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Відновлення після збоїв» рівня ДВ-2 чи ДВ-3.

Питання 103. Чи існує можливість із використанням засобів, реалізованих у відповідних функціональних модулях ОЕ, що входять до складу КЗЗ (укажіть яких, для різних типів відмов), повернення користувачами, що відносяться до певних ролей (адміністраторами або користувачами, яким надані відповідні повноваження), ОЕ зі стану з припиненням обслуговування (з урахуванням відповідей на питання 98, 102) до нормального функціонування.

Питання 104. Чи існує можливість із використанням засобів, реалізованих у відповідних функціональних модулях ОЕ, що входять до складу КЗЗ (укажіть яких, для різних типів відмов), повернення користувачами, що відносяться до певних ролей (адміністраторами або користувачами, яким надані відповідні повноваження), ОЕ з режиму з погіршеними характеристиками обслуговування до нормального функціонування.

У цьому випадку можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Відновлення після збоїв» рівня ДВ-3.

Питання 105. На підставі яких атрибутів доступу об’єктів-користувачів, що визначають їх приналежність до певних ролей (адміністраторів або користувачів, яким надані відповідні повноваження), в яких функціональних модулях ОЕ, що входять до складу КЗЗ, і згідно з якими правилами здійснюється оброблення запитів на повернення ОЕ зі стану з припиненням обслуговування до нормального функціонування.

Питання 106. На підставі яких атрибутів доступу об’єктів-користувачів, що визначають їх приналежність до певних ролей (адміністраторів або

користувачів, яким надані відповідні повноваження), в яких функціональних модулях ОЕ, що входять до складу КЗЗ, і згідно з якими правилами здійснюється оброблення запитів на повернення ОЕ зі стану з погіршеними характеристиками обслуговування (з урахуванням відповідей на питання 100, 104) до нормального функціонування.

Спільною для всіх рівнів функціональної послуги безпеки «Відновлення після збоїв» є перевірка вимоги:

– політика послуги, що реалізується КЗЗ ОЕ, визначає множину типів відмов ОЕ та переривань обслуговування, наведену при відповіді на питання 97, після яких можливе повернення у відомий захищений стан без порушення політики безпеки, чітко вказані рівні відмов різних компонентів ОЕ, що входять до складу КЗЗ ОЕ, при перевищенні яких необхідна повторна інсталяція ОЕ.

Програма випробувань функціональної послуги безпеки «Відновлення після збоїв» рівня ДВ*-1 – *«Ручне відновлення» передбачає перевірку вимог:

– після відмови ОЕ або переривання обслуговування КЗЗ ОЕ здатний, з використанням засобів і за правилами, наведеними при відповіді на питання 98, 105, перевести ОЕ у стан, із якого повернути його до нормального функціонування може лише адміністратор або користувачі, яким надані відповідні повноваження та які відносяться до певних ролей згідно політики реалізованої КЗЗ послуги «Розмежування обов’язків» рівня НО-1 або вище;

– існують ручні процедури, що дозволяють із використанням засобів, наведених при відповіді на питання 103, з використанням атрибутів і за правилами, наведеними при відповіді на питання 105, безпечним чином повернути ОЕ зі стану з припиненням обслуговування до нормального функціонування.

Програма випробувань функціональної послуги безпеки «Відновлення після збоїв» рівня ДВ*-2 – *«Автоматизоване відновлення» має передбачати перевірку таких вимог:

– після відмови ОЕ або переривання обслуговування певного типу КЗЗ ОЕ здатний, з використанням засобів і за правилами, наведеними при відповіді на питання 99, визначити, чи можуть бути використані автоматизовані процедури для повернення ОЕ до нормального функціонування безпечним чином. Якщо такі процедури можуть бути використані, то КЗЗ ОЕ здатний виконати їх та з використанням засобів і за правилами, наведеними при відповіді на питання 101, повернути ОЕ до нормального функціонування;

– якщо автоматизовані процедури не можуть бути використані, КЗЗ ОЕ здатний із використанням засобів і за правилами, наведеними при відповіді на питання 102, перевести ОЕ у стан, з якого повернути його до нормального функціонування може лише адміністратор або користувачі, яким надані відповідні повноваження та які відносяться до певних ролей згідно політики реалізованої КЗЗ послуги «Розмежування обов’язків» рівня НО-1 або вище.

Існують ручні процедури, що дозволяють із використанням засобів, наведених при відповіді на питання 103, атрибутів і за правилами, наведеними при відповіді на питання 105, безпечним чином повернути ОЕ зі стану з припиненням обслуговування до нормального функціонування.

Програма випробувань функціональної послуги безпеки «Відновлення після збоїв» рівня ДВ-3 – «Вибіркове відновлення» має передбачати перевірку таких вимог:

– після будь-якої відмови ОЕ або переривання обслуговування, що не призводять до необхідності заново інсталювати ОЕ, КЗЗ ОЕ здатний, з використанням засобів і за правилами, наведеними при відповіді на питання 99, 100, 101, виконати необхідні процедури та безпечним чином повернути ОЕ до нормального функціонування або, у гіршому випадку, до функціонування у режимі з погіршеними характеристиками обслуговування, з якого повернути його до нормального функціонування може лише адміністратор або користувачі, яким надані відповідні повноваження та які відносяться до певних ролей згідно політики реалізованої КЗЗ послуги «Розмежування обов'язків» рівня НО-1 або вище, наведеною при відповіді на питання 140, 141;

– якщо автоматизовані процедури не можуть бути використані, КЗЗ ОЕ здатний із використанням засобів і за правилами, наведеними при відповіді на питання 102, перевести ОЕ у стан, із якого повернути його до нормального функціонування може лише адміністратор або користувачі, яким надані відповідні повноваження та які відносяться до певних ролей згідно політики реалізованої КЗЗ послуги «Розмежування обов'язків» рівня НО-1 або вище.

Існують ручні процедури, що дозволяють із використанням засобів, наведених при відповіді на питання 103, 104, атрибутів і за правилами, наведеними при відповіді на питання 105, 106, безпечним чином повернути ОЕ з режиму з погіршеними характеристиками обслуговування або стану з припиненням обслуговування до нормального функціонування.

4.5 Програма випробування функціональних послуг безпеки критеріїв спостережності

Для того, щоб інформаційно-телекомунікаційна система (ІТС) могла бути оцінена на відповідність критеріям спостережності, комплекс заходів захисту (КЗЗ) має надавати послуги щодо забезпечення відповідальності користувачів за свої дії із підтримки здатності КЗЗ виконувати свої функції. Спостережність забезпечується в інформаційно-телекомунікаційній системі такими послугами:

НР – реєстрація (аудит);

НИ – ідентифікація й автентифікація;

НК – достовірний канал;

НО – розмежування обов'язків;

НЦ – цілісність комплексу засобів захисту;

НТ – самотестування;

НВ – ідентифікація й автентифікація при обміні;
НА – автентифікація відправника;
НП – автентиікація отримувача.

4.5.1 Програма випробування функціональної послуги «Реєстрація»

Послуга «Реєстрація» дозволяє контролювати небезпечні для об’єкта експертизи (ОЕ) дії. Функціональні послуги «Реєстрація» ранжируються за рівнями 1 … 5 залежно від повноти та вибірковості контролю, складності засобів аналізу даних журналів реєстрації та здатності вияву потенційних порушень:

НР-1 – зовнішній аналіз;
НР-2 – захищений журнал;
НР-3 – сигналізація про небезпеку;
НР-4 – детальна реєстрація;
НР-5 – аналіз у реальному часі.

Спеціальні питання щодо послуги «Реєстрація»

Питання 107. Чи існує в ОЕ можливість реєстрації подій, пов’язаних зі спробами або фактами виконання певних дій, що мають безпосереднє або непряме відношення до безпеки оброблюваної інформації.

Під можливістю реєстрації подій слід розуміти наявність засобів, що дозволяють, як мінімум, виконувати такі дії:

– виявляти (реєструвати) факти виникнення подій;

– генерувати записи у журналі реєстрації;

– накопичувати та зберігати дані журналів реєстрації або передавати їх в інші системи.

Під подіями, що мають відношення до безпеки, слід розуміти події, пов’язані зі спробами або фактами певних дій, які стосуються виконання функціональними модулями ОЕ, що входять до складу КЗЗ, операцій згідно вимог політики різних функціональних послуг безпеки.

Питання 108. Наведіть перелік подій, пов’язаних зі спробами або фактами виконання певних дій, що мають безпосереднє або непряме відношення до безпеки оброблюваної інформації, реєстрація яких можлива засобами, реалізованими у складі ОЕ.

Чіткого визначення поняття події, що має безпосереднє відношення до безпеки, не існує, проте звичайно під такою подією слід розуміти подію, пов’язану зі звертанням до засобів КЗЗ, які реалізують будь-яку функціональну послугу безпеки, наприклад: надання доступу; відмова у доступі; виконання автентифікації; зміна атрибутів доступу; створення об’єкта; модифікація об’єкта; видалення об’єкта; використання привілеїв тощо.

Під подіями, що мають непряме відношення до безпеки, слід розуміти події, які, хоча прямо й не пов’язані з функціонуванням засобів КЗЗ, що реалізують будь-яку функціональну послугу безпеки, але можуть призвести до порушення безпеки оброблюваної інформації.

Питання 109. Наведіть перелік реєстраційних подій (як частину всього переліку реєстраційних подій), що мають безпосереднє відношення до безпеки.

Питання 110. Наведіть перелік реєстраційних подій (як частину всього переліку реєстраційних подій), що мають непряме відношення до безпеки.

У випадку, якщо до переліку подій, що мають непряме відношення до безпеки, внесено хоча б одну подію, можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Реєстрація» рівня НР-4 чи НР-5, у протилежному випадку можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Реєстрація» рівнів НР-1, НР-2 чи НР-3.

Питання 111. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ, реалізовані засоби реєстрації фактів виникнення подій різного типу, наведених при відповіді на питання 108. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ, реалізовані засоби запису (занесення) у журнал реєстрації інформації про події різного типу, наведені при відповіді на питання 107. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ реалізовані засоби зберігання журналів реєстрації, в якому вигляді та в якому сховищі зберігаються журнали.

Питання 112. Наведіть структуру запису журналу реєстрації. Чи дозволяє структура запису журналу реєстрації зберегти інформацію про дату, час, місце, тип й успішність або неуспішність кожної зареєстрованої події. Чи дозволяє структура запису журналу реєстрації зберегти інформацію, достатню для встановлення користувача, процесу та/або об’єкта, що мали відношення до кожної зареєстрованої події.

У випадку негативної відповіді на це питання можна стверджувати, що послуга «Реєстрація» засобами КЗЗ ОЕ не реалізується.

Питання 113. Чи існує можливість із використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ, передачі збереженого журналу реєстрації (з урахуванням відповіді на питання 111) в інші системи з використанням певних механізмів захисту переданого журналу від несанкціонованого доступу з метою модифікації або руйнування.

У випадку позитивної відповіді на це питання можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга «Реєстрація» рівня НР-1.

Питання 114. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на питання 113), реалізовані засоби передачі збереженого журналу реєстрації (з урахуванням відповіді на питання 111) в інші системи. З використанням яких саме механізмів реалізується захист переданого журналу від несанкціонованого доступу з метою модифікації або руйнування. Який порядок функціонування цих механізмів.

Питання 115. Чи існує можливість забезпечення з використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ, захисту збереженого журналу реєстрації (з урахуванням відповіді на питання 111) від несанкціонованого доступу з метою модифікації або руйнування.

У цьому випадку можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга «Реєстрація» рівнів НР-2 – НР-5. Інакше, можна

стверджувати, що, за умови позитивної відповіді на питання 111, засобами КЗЗ ОЕ може бути реалізована послуга «Реєстрація» рівня НР-1.

Питання 116. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на питання 115), реалізовані засоби захисту збереженого журналу реєстрації (з урахуванням відповіді на питання 111) від несанкціонованого доступу з метою модифікації або руйнування. З використанням яких саме механізмів реалізується захист збереженого журналу від несанкціонованого доступу з метою модифікації або руйнування. Який порядок функціонування цих механізмів.

Питання 117. Чи існує можливість забезпечення з використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ, перегляду й аналізу збереженого (з урахуванням відповіді на питання 111) журналу реєстрації.

У випадку позитивної відповіді на це питання можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга «Реєстрація» рівнів НР-2 – НР-5. Інакше, можна стверджувати, що, за умови позитивної відповіді на питання 113, може бути реалізована послуга «Реєстрація» рівня НР-1.

Питання 118. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на питання 117), реалізовані засоби перегляду й аналізу збережених (з урахуванням відповіді на питання 111) журналів реєстрації. Які саме функції перегляду й аналізу журналів реєстрації вони реалізують.

Питання 119. Чи існує можливість забезпечення з використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ, контролю одиничних або повторюваних реєстраційних подій, що можуть свідчити про прямі (істотні) порушення політики безпеки.

Як підходи до забезпечення контролю реєстраційних подій можуть бути використані, наприклад, такі:

– порівняння результатів дій деякого користувача або об’єкта-процесу із заздалегідь заданим набором правил (профілем);

– виявлення факту виникнення подій одного або декількох типів протягом заданого періоду часу;

– виявлення факту відсутності подій одного або декількох типів протягом заданого періоду часу.

У цьому випадку можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга «Реєстрація» рівнів НР-3, НР-4 чи НР-5.

Питання 120. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на питання 119), реалізовані засоби контролю одиничних або повторюваних реєстраційних подій, що можуть свідчити про прямі (істотні) порушення політики безпеки. Виникнення яких подій, наведених при відповіді на питання 109, 110, вони дозволяють контролювати. Який порядок функціонування цих засобів.

Питання 121. Чи існує можливість забезпечення з використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ, негайного інформування адміністратора про події, які свідчать про

перевищення порогів безпеки, та здійснення неруйнівних дій щодо припинення повторення цих подій. У випадку позитивної відповіді на питання 121 можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга «Реєстрація» рівнів НР-3, НР-4 чи НР-5.

Питання 122. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на питання 121, реалізовані засоби негайного інформування адміністратора про події, які свідчать про перевищення порогів безпеки, та здійснення неруйнівних дії щодо припинення повторення цих подій. Про виникнення яких подій, наведених при відповіді на питання 109, 110, вони дозволяють негайно інформувати адміністратора. Який порядок функціонування цих засобів, які механізми використовуються для негайного інформування адміністратора та для здійснення неруйнівних дії щодо припинення повторення критичних подій.

Питання 123. Чи забезпечується функціонування реалізованих у складі функціональних модулів ОЕ, що входять до складу КЗЗ, засобів, які реалізують реєстрацію подій різного типу, запис (занесення) інформації у журнал реєстрації (з урахуванням відповіді на питання 111), контроль одиничних або повторюваних реєстраційних подій, що можуть свідчити про прямі (істотні) порушення політики безпеки (з урахуванням відповіді на питання 120), негайне інформування адміністратора про події, які свідчать про перевищення порогів безпеки, та здійснення неруйнівних дії щодо припинення повторення цих подій (з урахуванням відповіді на питання 122) у режимі реального часу. У цьому випадку можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга «Реєстрація» рівня НР-5.

Програма випробувань функціональної послуги безпеки «Реєстрація» рівня НР-1 – «Зовнішній аналіз» має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, визначає перелік реєстраційних подій, наведений при відповіді на питання 108;

– КЗЗ ОЕ здатний здійснювати реєстрацію подій, наведених при відповіді на питання 109, що мають безпосереднє відношення до безпеки, з використанням засобів, наведених при відповіді на питання 111;

– журнал реєстрації, згідно з описом структури його записів, наведеним при відповіді на питання 112, містить інформацію про дату, час, місце, тип і успішність або неуспішність кожної зареєстрованої події;

– журнал реєстрації, згідно з описом структури його записів, наведеним при відповіді на питання 112, містить інформацію, достатню для встановлення користувача, процесу та/або об’єкта, що мали відношення до кожної зареєстрованої події;

– атрибути користувачів різного типу, що зберігаються у журналі реєстрації та на підставі яких приймається рішення про відношення користувача до зареєстрованої події, автентифіковані з використанням засобів реалізації послуги «Ідентифікація й автентифікація» рівня НИ-1 або вище згідно політики цієї послуги, наведеної при відповіді на питання 125;

– КЗЗ ОЕ здатний передавати журнал реєстрації в інші системи з використанням засобів і механізмів захисту, наведених при відповіді на питання 114.

Програма випробувань функціональної послуги безпеки «Реєстрація» рівня НР-2 – «Захищений журнал» має передбачати перевірку таких вимог:

– програма випробувань має містити ті ж вимоги, що містить програма випробувань функціональної послуги «Зовнішній аналіз» за винятком вимоги щодо здатності передавати журнал реєстрації в інші системи.

Додатково мають передбачатись перевірка таких вимог:

– КЗЗ ОЕ забезпечує захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування з використанням засобів і механізмів, наведених при відповіді на питання 116;

– адміністратори та користувачі, яким надані відповідні повноваження та які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги «Розмежування обов'язків» рівня НО-1 або вище, наведеною при відповіді на питання 140, 141, мають у своєму розпорядженні засоби перегляду й аналізу журналу реєстрації, наведені при відповіді на питання 118.

Програма випробувань функціональної послуги безпеки "Реєстрація" рівня НР-3 – «Сигналізація про небезпеку» має передбачати перевірку вимог:

– програма має містити ті ж вимоги, що містить програма випробувань функціональної послуги «Захищений журнал».

Додатково мають передбачатись перевірка таких вимог:

– КЗЗ ОЕ здатний, із використанням засобів, наведених при відповіді на питання 120, контролювати одиничні або повторювані реєстраційні події, що можуть свідчити про прямі (істотні) порушення політики безпеки ОЕ, наведені при відповіді на питання 120;

– КЗЗ ОЕ здатний, із використанням засобів, наведених при відповіді на питання 122, негайно інформувати адміністратора про перевищення порогів безпеки та за умови, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій.

Програма випробувань функціональної послуги безпеки «Реєстрація» рівня НР-4 – «Детальна реєстрація» має передбачати перевірку таких вимог:

– програма має містити ті ж вимоги, що містить програма випробувань функціональної послуги «Сигналізація про небезпеку».

Додатково мають передбачатись перевірка такої вимоги:

– КЗЗ ОЕ здатний здійснювати реєстрацію подій, наведених при відповіді на питання 110, що мають непряме відношення до безпеки, з використанням засобів, наведених при відповіді на питання 111.

Програма випробувань функціональної послуги безпеки «Реєстрація» рівня НР-5 – «Аналіз у реальному часі» має передбачати перевірку вимог:

– програма має містити ті ж вимоги, що містить програма випробувань функціональної послуги «Детальна реєстрація»;

– додатково мають передбачатись перевірка такої вимоги: КЗЗ ОЕ здатний, із використанням засобів, наведених при відповіді на питання 120, 122, виявляти й аналізувати несанкціоновані дії у реальному часі.

4.5.2 Програма випробування функціональної послуги «Ідентифікація й автентифікація»

Послуга «Ідентифікація й автентифікація» дозволяє КЗЗ визначити та перевірити особистість користувача, що намагається отримати доступ до ОЕ. Функціональні послуги «Ідентифікація й автентифікація» ранжируються за рівнями 1 … 3 залежно від числа задіяних механізмів автентифікації:

– НИ-1 – зовнішня ідентифікація й автентифікація;

– НИ-2 – одиночна ідентифікація й автентифікація;

– НИ-3 – множинна ідентифікація й автентифікація.

Спеціальні питання щодо послуги «Ідентифікація й автентифікація»

Питання 124. Чи існує в ОЕ можливість однозначної ідентифікації користувачів, що відносяться до різних ролей, і виконують операції, на підставі призначених їм унікальних (у межах ОЕ) ідентифікаторів або інших атрибутів.

Питання 125. Наведіть перелік функціональних послуг безпеки, реалізованих функціональними модулями ОЕ, введеними до складу КЗЗ для реалізації яких необхідні атрибути користувачів.

Питання 126. Чи існує можливість із використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ, отримання (перш ніж дозволити будь-якому користувачу виконувати будь-які інші контрольовані КЗЗ дії) від деякого зовнішнього джерела з використанням захищеного механізму автентифікованого ідентифікатора цього користувача.

У цьому випадку можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга «Ідентифікація й автентифікація» рівня НИ-1, її політика може бути уточнена при відповіді на наступне питання.

Питання 127. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на питання 126), реалізовані засоби отримання від зовнішнього джерела (вкажіть якого) автентифікованого ідентифікатора користувача. Який порядок функціонування цих засобів, які механізми використовуються для захисту переданих ідентифікаторів.

Питання 128. Чи існує можливість із використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ, установлення, за результатами виконання перевірки дійсності з використанням відповідних механізмів (автентифікації), однозначної відповідності між користувачем й унікальним ідентифікатором, яким користувач представляється в ОЕ.

Функціонування механізмів, що забезпечують виконання автентифікації користувачів, може ґрунтуватися на одному з таких принципів:

– принцип «знання чогось» (наприклад, паролів або криптографічних ключів);

– принцип «володіння чимось» (карткою з магнітною смугою, смарт-карткою, переносним ідентифікатором тощо);

– принцип «притаманність невід'ємних характеристик» (рукописний підпис, відбиток пальця, голосові характеристики, характеристики сітківки ока, динамічні характеристики при роботі з клавіатурою тощо).

Якщо існують засоби, що реалізують механізми, які функціонують на підставі зазначених принципів, то це означає, що засобами КЗЗ може бути реалізована послуга «Ідентифікація й автентифікація» рівня НИ-2 чи НИ-3.

Питання 129. Чи використовуються у наведених при відповіді на питання 128 засобах автентифікації, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ, у процесі виконання перевірки дійсності (автентифікації) користувача:

1) механізми різного типу (вкажіть якого), тобто такі, що функціонують на підставі різних принципів. У цьому випадку засобами КЗЗ може бути реалізована послуга «Ідентифікація й автентифікація» рівня НИ-3;

2) механізми лише одного типу (вкажіть якого), тобто такі, що функціонують на підставі однакових принципів. У цьому випадку засобами КЗЗ може бути реалізована послуга «Ідентифікація й автентифікація» рівня НИ-2.

Питання 130. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на питання 128), реалізовані засоби перевірки дійсності (автентифікації) користувачів із використанням кожного з механізмів автентифікації, наведених при відповіді на питання 129. Які атрибути користувачів при цьому використовуються. Наведіть опис протоколу виконання автентифікації та структуру наборів даних автентифікації, використаних при цьому, для кожного з механізмів автентифікації, наведених при відповіді на питання 128.

Питання 131. Чи існує можливість забезпечення з використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ, захисту даних автентифікації, наведених при відповіді на питання 130, від несанкціонованого доступу з метою перегляду, модифікації, руйнування для кожного з використаних механізмів автентифікації.

У цьому випадку можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга «Ідентифікація й автентифікація» рівня НИ-2 чи НИ-3.

Питання 132. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ, реалізовані засоби захисту даних автентифікації, наведених при відповіді на питання 131, від несанкціонованого доступу з метою перегляду, модифікації, руйнування для кожного з використаних механізмів автентифікації. З використанням яких саме механізмів реалізується захист даних автентифікації від несанкціонованого доступу з метою перегляду, модифікації, руйнування. Який порядок функціонування цих механізмів.

Спільними для всіх рівнів функціональної послуги безпеки «Ідентифікація й автентифікація» є перевірки таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, визначає атрибути, якими характеризуються користувачі різного типу, наведені при відповіді на питання 124, і послуги, для використання яких необхідні ці атрибути, наведені при відповіді на питання 125;

– кожен користувач кожного типу однозначно ідентифікується КЗЗ ОЕ на підставі атрибутів, наведених при відповіді на питання 124.

Програма випробувань функціональної послуги безпеки «Ідентифікація й автентифікація» рівня НИ-1 – «Зовнішня ідентифікація й автентифікація» має передбачати перевірку таких вимог:

Перш ніж дозволити будь-якому користувачу будь-якого типу виконувати будь-які інші, контрольовані КЗЗ ОЕ дії, КЗЗ ОЕ здатний із використанням засобів і захищених механізмів, наведених при відповіді на питання 127, отримати від зовнішнього джерела, наведеного при відповіді на питання 127, автентифікований ідентифікатор цього користувача.

Програма випробувань функціональної послуги безпеки «Ідентифікація й автентифікація» рівня НИ-2 – «Одиночна ідентифікація й автентифікація» має передбачати перевірку таких вимог:

– перш ніж дозволити будь-якому користувачу будь-якого типу виконувати будь-які інші, контрольовані КЗЗ ОЕ дії, КЗЗ ОЕ здатний автентифікувати цього користувача з використанням механізму та засобів, наведених при відповіді на питання 129.2, 130;

– КЗЗ ОЕ забезпечує захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування з використанням засобів і механізмів, наведених при відповіді на питання 132;

– взаємодія користувача будь-якого типу з КЗЗ ОЕ у процесі виконання автентифікації здійснюється з використанням засобів реалізації послуги «Достовірний канал» рівня НК-1 або вище, які функціонують згідно політики та правил цієї послуги.

Програма випробувань функціональної послуги безпеки «Ідентифікація й автентифікація» рівня НИ-3 – «Множинна ідентифікація й автентифікація» має передбачати перевірку таких вимог:

– перш ніж дозволити будь-якому користувачу будь-якого типу виконувати будь-які інші, контрольовані КЗЗ ОЕ дії, КЗЗ ОЕ здатний автентифікувати цього користувача з використанням механізму та засобів, наведених при відповіді на питання 129.1, 130;

– КЗЗ ОЕ забезпечує захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування з використанням засобів і механізмів, наведених при відповіді на питання 132;

– взаємодія користувача будь-якого типу з КЗЗ ОЕ у процесі виконання автентифікації за допомогою кожного з механізмів здійснюється з використанням засобів реалізації послуги «Достовірний канал» рівня НК-1 або

вище, які функціонують згідно політики цієї послуги та правил, наведених при відповіді на питання 134 – 136.

4.5.3 Програма випробування функціональної послуги «Достовірний канал»

Послуга «Достовірний канал» дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Функціональні послуги «Достовірний канал» ранжируються за рівнями 1, 2 залежно від гнучкості надавання можливості КЗЗ або користувачу ініціювати захищений обмін:

– НК-1 – однонаправлений достовірний канал;

– НК-2 – двонаправлений достовірний канал.

Спеціальні питання щодо послуги «Достовірний канал»

Питання 133. Чи існує в об’єкті експертизи (ОЕ) можливість створення захищеного шляху передачі інформації між користувачем і функціональними компонентами ОЕ, що входять до складу КЗЗ, який не може бути імітований, а інформація, що передається через нього, не може бути отримана або модифікована стороннім користувачем або процесом (достовірного каналу). Зазначена можливість, ініційована користувачем, повинна забезпечувати захист від шкідливих програмних засобів типу «троянський кінь». Якщо в ОЕ існує зазначена можливість, то це означає, що засобами КЗЗ може бути реалізована послуга «Достовірний канал».

Питання 134. Чи використовується створюваний засобами ОЕ, що входять до складу КЗЗ, достовірний канал:

1) лише при виконанні початкової ідентифікації й автентифікації користувачів різних типів (укажіть яких). У цьому випадку засобами КЗЗ може бути реалізована послуга «Достовірний канал» рівня НК-1;

2) при виконанні початкової ідентифікації й автентифікації користувачів різних типів (укажіть яких) та в інших випадках (укажіть в яких), коли необхідна безпосередня взаємодія користувача із засобами КЗЗ. Тоді засобами КЗЗ може бути реалізована послуга «Достовірний канал» рівня НК-2.

Питання 135. Чи ініціюється зв’язок із використанням достовірного каналу при виконанні операцій, наведених при відповіді на питання 134:

1) лише користувачем. У цьому випадку можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Достовірний канал» рівня НК-1;

2) як користувачем, так і засобами КЗЗ. У випадку позитивної відповіді на питання 135.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Достовірний канал» рівня НК-2.

Питання 136. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ, реалізовані засоби створення достовірного каналу, використаного для початкової ідентифікації й автентифікації користувача (з урахуванням відповідей на питання 134.1, 135.1). З використанням яких саме механізмів реалізується створення достовірного каналу, використаного для початкової ідентифікації й автентифікації користувача, які атрибути користувачів і властивості компонентів КЗЗ при цьому використовуються. Наведіть протокол установлення достовірного каналу, використаного для початкової ідентифікації

й автентифікації користувача, й опис порядку передачі інформації з використанням цього каналу.

Питання 137. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ, реалізовані засоби створення достовірного каналу, використаного з метою, відмінною від початкової ідентифікації й автентифікації користувача (з урахуванням відповідей на питання 134.1, 135.1). З використанням яких саме механізмів реалізується створення достовірного каналу, використаного з метою, відмінною від початкової ідентифікації й автентифікації користувача, які атрибути користувачів і властивості компонентів КЗЗ при цьому використовуються. Наведіть протокол установлення достовірного каналу, використаного з метою, відмінною від початкової ідентифікації й автентифікації користувача, й опис порядку обміну інформації з використанням цього каналу (для всіх випадків його використання).

Питання 138. Чи забезпечує наведений при відповіді на питання 137 протокол можливість однозначної ідентифікації факту обміну з використанням достовірного каналу, ініційованого засобами КЗЗ, а також можливість початку обміну лише після позитивного підтвердження користувачем готовності до обміну. Яким чином забезпечується ця можливість.

У випадку позитивної відповіді на це питання можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Достовірний канал» рівня НК-2.

Програма випробувань функціональної послуги безпеки «Достовірний канал» рівня НК-1 – «Однонаправлений достовірний канал» має передбачати перевірку таких вимог:

– політика послуги, реалізована КЗЗ ОЕ та наведена при відповіді на питання 134, 135, визначає механізми встановлення достовірного зв’язку між користувачем і КЗЗ ОЕ, наведені при відповіді на питання 136;

– достовірний канал використовується для початкової ідентифікації й автентифікації, зв’язок із використанням цього каналу ініціюється винятково користувачем із використанням засобів і протоколу, наведених при відповіді на питання 136.

Програма випробувань функціональної послуги безпеки «Достовірний канал» рівня НК-2 – «Двонаправлений достовірний канал» має передбачати перевірку таких вимог:

– політика послуги, реалізована КЗЗ ОЕ та наведена при відповіді на питання 134, 135, визначає механізми встановлення достовірного зв’язку між користувачем і КЗЗ ОЕ, наведені при відповіді на питання 136, 137;

– достовірний канал певного типу використовується для початкової ідентифікації й автентифікації, а також в інших випадках, коли необхідний прямий зв’язок користувач/КЗЗ або КЗЗ/користувач, зв’язок із використанням цього каналу ініціюється користувачем, із використанням засобів і протоколу, наведених при відповіді на питання 136, або КЗЗ ОЕ, з використанням засобів і протоколу, наведених при відповіді на питання 137;

– обмін із використанням достовірного каналу, ініційований КЗЗ ОЕ, однозначно ідентифікований як такий, і може відбуватися лише після

позитивного підтвердження готовності до обміну з боку користувача за правилами, наведеними при відповіді на питання 138.

4.5.4 Програма випробування функціональної послуги «Розмежування обов'язків»

Послуга «Розмежування обов'язків» дозволяє зменшити потенційний збиток від навмисних або помилкових дій користувачів і обмежити авторитарність керування. Функціональні послуги «Розмежування обов'язків» ранжируються за рівнями 1 … 3 залежно від вибірковості керування можливостями користувачів й адміністраторів:

– НО-1 – виділення адміністратора;
– НО-2 – розподіл обов'язків адміністратора;
– НО-3 – розподіл обов'язків на підставі привілеїв.

Спеціальні питання щодо послуги«Розмежування обов'язків»

Питання 139. Чи існує серед переліку ролей користувачів, підтримуваних в ОЕ, хоча б одна роль, яка передбачає можливість виконання користувачем операцій адміністрування та керування будь-якими засобами, що входять до складу КЗЗ. Якщо так, то це означає, що засобами КЗЗ може бути реалізована послуга «Розмежування обов'язків» рівнів НО-1, НО-2 чи НО-3.

Питання 140. Наведіть перелік адміністративних ролей (ролей користувачів, які мають можливість виконання операцій адміністрування та керування будь-якими засобами, що входять до складу КЗЗ) і ролей звичайних користувачів (ролей користувачів, які не мають можливості виконання операцій керування будь-якими засобами, що входять до складу КЗЗ).

Питання 141. Чи існує серед переліку адміністративних ролей користувачів, підтримуваних в ОЕ, одна чи декілька ролей. Наведіть перелік функцій, притаманних різним адміністративним ролям.

У випадку, якщо серед переліку ролей, підтримуваних в ОЕ, є декілька адміністративних ролей, то це означає, що засобами КЗЗ може бути реалізована послуга «Розмежування обов'язків» рівня НО-2 чи НО-3. У протилежному випадку, якщо серед переліку ролей, підтримуваних в ОЕ, є лише одна адміністративна роль, то це означає, що засобами КЗЗ може бути реалізована послуга «Розмежування обов'язків» рівня НО-1.

Питання 142. Чи існує серед переліку ролей звичайних користувачів, підтримуваних в ОЕ, одна чи декілька ролей. Наведіть перелік функцій, притаманних різним ролям звичайних користувачів.

У випадку, якщо серед переліку ролей, підтримуваних в ОЕ, є декілька ролей звичайних користувачів, то це означає, що засобами КЗЗ може бути реалізована послуга «Розмежування обов'язків» рівня НО-3. У протилежному випадку, якщо серед переліку ролей, підтримуваних в ОЕ, є лише одна роль користувача, то це означає, що засобами КЗЗ може бути реалізована послуга «Розмежування обов'язків» рівня НО-1 чи НО-2.

Питання 143. На підставі яких атрибутів доступу об'єктів-користувачів і згідно з якими правилами здійснюється призначення користувачів на ролі, наведені при відповіді на питання 141, 142.

Питання 144. В яких функціональних модулях ОЕ, що входять до складу КЗЗ, підтримується призначення користувачів на ролі, наведені при відповіді на питання 141, 142, на підставі атрибутів, наведених при відповіді на питання 144.

Питання 145. Які дії при роботі з різними функціональними модулями ОЕ, що входять до складу КЗЗ, повинен виконати користувач для підтвердження прийняття ним певної ролі (для всіх ролей, наведених при відповіді на питання 141, 142).

Програма випробувань функціональної послуги безпеки «Розмежування обов'язків» рівня НО-1 – «Виділення адміністратора» має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, визначає ролі адміністратора та звичайного користувача, наведені при відповіді на питання 140 і притаманні їм функції, наведені при відповіді на питання 141, 142;

– засоби КЗЗ ОЕ, наведені при відповіді на питання 144, підтримують призначення користувачів на відповідні ролі згідно з атрибутами, наведеними при відповіді на питання 143;

– користувачі при роботі із засобами КЗЗ ОЕ, наведеними при відповіді на питання 144, мають можливість виступати у певній ролі лише після того, як вони виконають певні дії, наведені при відповіді на питання 145, що підтверджують прийняття ними цієї ролі;

– перед виконанням призначення на роль атрибути користувачів автентифіковані з використанням засобів реалізації послуги «Ідентифікація й автентифікація» рівня НИ-1 або вище згідно політики цієї послуги, наведеної при відповіді на питання 125.

Програма випробувань функціональної послуги безпеки «Розмежування обов'язків» рівня НО-2 – «Розмежування обов'язків адміністраторів» має передбачати перевірку таких вимог:

– програма має містити ті ж вимоги, що містить програма випробувань функціональної послуги «Виділення адміністратора».

Додатково програма має передбачити перевірку такої вимоги:

– політика послуги визначає мінімум дві різні адміністративні ролі: адміністратора безпеки й іншого адміністратора. Функції, притаманні кожній із ролей і наведені при відповіді на питання 141, мінімізовані так, щоб включати лише ті функції, що необхідні для виконання цієї ролі.

Програма випробувань функціональної послуги безпеки «Розмежування обов'язків» рівня НО-3 – «Розмежування обов'язків на підставі привілеїв» має передбачати перевірку таких вимог:

– програма має містити ті ж вимоги, що містить програма випробувань функціональної послуги «Розмежування обов'язків адміністраторів».

Додатково програма має передбачити перевірку такої вимоги:

– політика послуги визначає множину різних ролей користувачів, наведену при відповіді на питання 140, 142.

4.5.5 Програма випробування функціональної послуги «Цілісність комплексу засобів захисту»

Послуга «Цілісність комплексу засобів захисту» визначає міру здатності КЗЗ захищати себе та гарантувати свою здатність керувати захищеними об’єктами. Функціональні послуги «Цілісність комплексу засобів захисту» ранжируються за рівнями 1 … 3 залежно від рівня гарантування цілісності:

– НЦ-1 – КЗЗ із контролем цілісності;

– НЦ-2 – КЗЗ із гарантованою цілісністю;

– НЦ-3 – КЗЗ із функціями диспетчера доступу.

Спеціальні питання щодо послуги «Цілісність комплексу засобів захисту»

Питання 146. Чи існують в ОЕ можливість і відповідні засоби захисту всіх функціональних модулів, що входять до складу КЗЗ, від несприятливих зовнішніх впливів, метою яких є порушення цілісності компонентів КЗЗ.

Під захистом цілісності компонентів КЗЗ слід розуміти або виявлення фактів порушення цілісності компонентів із подальшим її відновленням, або запобігання самій можливості порушення цілісності компонентів КЗЗ. Функціонування механізмів, що забезпечують реалізацію послуги «Цілісність комплексу засобів захисту», у частині, яка стосується виявлення фактів порушення цілісності компонентів КЗЗ, може ґрунтуватися на принципах:

– виявлення порушень цілісності шляхом порівняння із заздалегідь створеною еталонною копією;

– виявлення порушень цілісності шляхом вироблення/перевірки криптографічних (таких, що обчислюються з використанням ключових даних) кодів контролю цілісності (кодів автентифікації повідомлень);

– виявлення порушень цілісності шляхом вироблення/перевірки некриптографічних кодів контролю цілісності з їх подальшим зашифруванням/розшифруваннням;

– виявлення порушень цілісності шляхом вироблення/перевірки електронного цифрового підпису.

Функціонування механізмів, що забезпечують реалізацію послуги «Цілісність комплексу засобів захисту», у частині, яка стосується запобігання самій можливості порушення цілісності компонентів КЗЗ, може ґрунтуватися на одному з таких принципів:

– з використанням механізму керування доступом для захисту компонентів КЗЗ, що знаходяться у стані зберігання;

– на підставі апаратно реалізованих засобів обмеження доступної різним процесам оперативної пам’яті (кільця захисту, захищені сегменти пам’яті,

захищені комірки пам’яті) для захисту компонентів КЗЗ, що знаходяться у стані виконання.

Питання 147. Чи існує можливість забезпечення з використанням засобів, наведених при відповіді на питання 146, контролю цілісності (виявлення фактів порушення цілісності) всіх функціональних модулів ОЕ, що входять до складу КЗЗ.

У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Цілісність комплексу засобів захисту» рівня НЦ-1. Якщо такі засоби відсутні, то можна переходити до відповіді на питання 152.

Питання 148. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ, наведених при відповіді на питання 146, реалізовані засоби контролю цілісності (виявлення фактів порушення цілісності) всіх функціональних модулів ОЕ, що входять до складу КЗЗ. Який порядок функціонування цих засобів, які механізми використовуються для виявлення фактів порушення цілісності різних функціональних модулів ОЕ.

Питання 149. Чи існує можливість забезпечення з використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ, оповіщення адміністратора про виявлені факти порушення цілісності компонентів КЗЗ. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ, реалізовані ці засоби. Який порядок функціонування цих засобів, які механізми використовуються для оповіщення адміністратора про виявлені факти порушення цілісності компонентів КЗЗ. У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Цілісність комплексу засобів захисту» рівня НЦ-1.

Питання 150. Чи існує можливість забезпечення з використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ, автоматичного відновлення відповідності компонентів КЗЗ із порушеною цілісністю еталону або переведення ОЕ у випадку виявлення порушення цілісності будь-якого з компонентів КЗЗ у стан із припиненням обслуговування, з якого повернути його до нормального функціонування зможуть лише користувачі, що відносяться до певних ролей (адміністратори або користувачі, яким надані відповідні повноваження). У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ реалізовані ці засоби. Який порядок функціонування цих засобів. У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Цілісність комплексу засобів захисту» рівня НЦ-1.

Питання 151. На підставі яких атрибутів доступу об’єктів-користувачів, що визначають їх приналежність до певних ролей (адміністраторів або користувачів, яким надані відповідні повноваження), в яких функціональних модулях ОЕ, що входять до складу КЗЗ, і згідно з якими правилами здійснюється оброблення запитів на повернення ОЕ зі стану з припиненням обслуговування, в який він був переведений після виявлення порушення цілісності компонентів КЗЗ, до нормального функціонування (з урахуванням відповіді на питання 150).

Питання 152. Чи існує можливість забезпечення з використанням засобів, наведених при відповіді на питання 146, розподілу домену КЗЗ й інших доменів шляхом виділення для збереження та виконання функціональних модулів ОЕ, що входять до складу КЗЗ, ізольованої логічної області всередині ОЕ з метою захисту від зовнішніх впливів і несанкціонованої модифікації та/або втрати керування. У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Цілісність комплексу засобів захисту» рівня НЦ-2 чи НЦ-3.

Питання 153. На підставі яких атрибутів компонентів КЗЗ і відповідних процесів (як пасивних об'єктів у стані зберігання й об'єктів-процесів у стані виконання) реалізується виділення домену КЗЗ із метою захисту від зовнішніх впливів і несанкціонованої модифікації та/або втрати керування.

Питання 154. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ, наведених при відповіді на питання 146, реалізовані засоби виділення домену КЗЗ із метою захисту від зовнішніх впливів і несанкціонованої модифікації та/або втрати керування на підставі атрибутів, наведених при відповіді на питання 153. Який порядок функціонування цих засобів, які механізми використовуються для виділення домену КЗЗ із метою захисту від зовнішніх впливів і несанкціонованої модифікації та/або втрати керування.

Питання 155. Наведіть опис обмежень, дотримання яких дозволяє гарантувати, що послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Питання 156. Чи забезпечують реалізовані у складі КЗЗ засоби та механізми виділення домену КЗЗ із метою захисту від зовнішніх впливів і несанкціонованої модифікації та/або втрати керування, наведені при відповіді на питання 154, гарантію того, що всі послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ. Наведіть обґрунтування цього твердження. У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Цілісність комплексу засобів захисту» рівня НЦ-3.

Програма випробувань функціональної послуги безпеки «Цілісність комплексу засобів захисту» рівня НЦ-1 – «Цілісність комплексу засобів захисту» має передбачати перевірку таких вимог:

– політика послуги визначає склад КЗЗ ОЕ та механізми контролю цілісності всіх компонентів, що входять до складу КЗЗ ОЕ, наведені при відповіді на питання 147, 148;

– у випадку виявлення засобами контролю цілісності, наведеними при відповіді на питання 148, порушення цілісності будь-якого зі своїх компонентів, КЗЗ ОЕ, з використанням засобів, наведених при відповіді на питання 149, здатний зареєструвати факт порушення, за допомогою засобів реалізації послуги «Реєстрація» рівня НР-1 або вище повідомити адміністратора та з використанням засобів, наведених при відповіді на питання 150, або автоматично відновити відповідність компонента еталону, або перевести ОЕ у стан, з якого повернути його до нормального функціонування може лише

адміністратор або користувачі, яким надані відповідні повноваження та які відносяться до певних ролей згідно політики реалізованої КЗЗ послуги «Розмежування обов'язків» рівня НО-1 або вище, наведеної при відповіді на питання 140, 141;

– описані обмеження, наведені при відповіді на питання 155, дотримання яких дозволяє гарантувати, що послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Програма випробувань функціональної послуги безпеки «Цілісність комплексу засобів захисту» рівня НЦ-2 – «КЗЗ із гарантованою цілісністю» має передбачати перевірку таких вимог:

– політика послуги визначає домен КЗЗ ОЕ й інші домени, а також механізми захисту, що використовуються для реалізації розподілу доменів, наведені при відповіді на питання 154;

– КЗЗ ОЕ з використанням атрибутів, наведених при відповіді на питання 153, та засобів і механізмів, наведених при відповіді на питання 154, підтримує домен для свого власного виконання з метою захисту засобів КЗЗ від зовнішніх впливів і несанкціонованої модифікації та/або втрати керування;

– описані обмеження, наведені при відповіді на питання 155, дотримання яких дозволяє гарантувати, що послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Програма випробувань функціональної послуги безпеки «Цілісність комплексу засобів захисту» рівня НЦ-3 – «КЗЗ із функціями диспетчера доступу» має передбачати перевірку таких вимог:

– програма має містити ті ж вимоги, що містить програма випробувань функціональної послуги «КЗЗ із гарантованою цілісністю» за винятком останньої. Замість неї програма має передбачити перевірку такої вимоги:

– КЗЗ ОЕ з урахуванням правил, наведених при відповіді на питання 156, гарантує, що послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

4.5.6 Програма випробування функціональної послуги «Самотестування»

Послуга «Самотестування» дозволяє КЗЗ перевірити та на підставі цього гарантувати правильність функціонування та цілісність певної множини функцій ОЕ. Функціональні послуги «Самотестування» ранжируються за рівнями 1 … 3 залежно від можливості виконання тестів у процесі запуску або штатної роботи:

– НТ-1 – самотестування за запитом;

– НТ-2 – самотестування при старті;

– НТ-3 – самотестування у реальному часі.

Спеціальні питання щодо послуги «Самотестування»

Питання 157. Чи існують в ОЕ можливість і відповідні засоби перевірки (з використанням певних процедур) правильності функціонування компонентів ОЕ, що входять до складу КЗЗ, при виконанні певних операцій.

Питання 158. Наведіть перелік властивостей ОЕ та процедур, реалізованих у функціональних компонентах ОЕ, що входять до складу КЗЗ, які можуть бути використані для оцінювання правильності функціонування КЗЗ.

Питання 159. Наведіть перелік тестів (у вигляді опису перевірок і очікуваних результатів), використаних для оцінювання правильності функціонування різних функціональних компонентів ОЕ, що входять до складу КЗЗ, при виконанні різних операцій.

Питання 160. Чи існує можливість виконання тестів, використаних для оцінювання правильності функціонування різних функціональних компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на питання 159, запитами користувачів, що відносяться до певних ролей (адміністраторів або користувачів, яким надані відповідні повноваження).

У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Самотестування» рівнів НТ-1, НТ-2 чи НТ-3.

Питання 161. На підставі яких атрибутів доступу об'єктів-користувачів, що визначають їх приналежність до певних ролей (адміністраторів або користувачів, яким надані відповідні повноваження), в яких функціональних модулях ОЕ, що входять до складу КЗЗ, і згідно з якими правилами здійснюється оброблення запитів на виконання тестування різних функціональних компонентів ОЕ, що входять до складу КЗЗ.

Питання 162. Чи існує можливість виконання тестів, використаних для оцінювання правильності функціонування різних функціональних компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на питання 159, при старті ОЕ. В яких функціональних модулях ОЕ, що входять до складу КЗЗ, і згідно з якими правилами здійснюється виконання тестів, використаних для оцінювання правильності функціонування різних функціональних компонентів ОЕ, що входять до складу КЗЗ, при старті ОЕ.

У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Самотестування» рівня НТ-2 чи НТ-3.

Питання 163. Чи існує можливість виконання тестів, використаних для оцінювання правильності функціонування різних функціональних компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на питання 159, у процесі штатного функціонування ОЕ. В яких функціональних модулях ОЕ, що входять до складу КЗЗ, і згідно з якими правилами здійснюється виконання тестів, використаних для оцінювання правильності функціонування різних функціональних компонентів ОЕ, що входять до складу КЗЗ, у процесі штатного функціонування ОЕ.

У випадку позитивної відповіді на це питання можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Самотестування» рівня НТ-3.

Програма випробувань функціональної послуги безпеки «Самотестування» рівня НТ-1 – «Самотестування за запитом» має передбачати перевірку таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, описує властивості ОЕ та реалізовані процедури, наведені при відповіді на питання 158, що можуть бути використані для оцінювання правильності функціонування КЗЗ;

– КЗЗ ОЕ здатний, з використанням засобів і згідно правил, наведених при відповіді на питання 161, виконувати наведений при відповіді на питання 159 набір тестів із метою оцінювання правильності функціонування своїх критичних функцій за запитом користувачів, що мають відповідні повноваження та відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги «Розмежування обов'язків» рівня НО-1 або вище, наведеною при відповіді на питання 140, 141.

Програма випробувань функціональної послуги безпеки «Само тестування» рівня НТ-2 – «Самотестування при старті» має передбачати перевірку таких вимог:

– програма має містити ті ж вимоги, що містить програма випробувань функціональної послуги «Самотестування за запитом».

Додатково програма має передбачити перевірку такої вимоги:

– КЗЗ ОЕ здатний при старті виконувати наведений при відповіді на питання 159 набір тестів із метою оцінювання правильності функціонування своїх критичних функцій із використанням засобів і за правилами, наведеними при відповіді на питання 162.

Програма випробувань функціональної послуги безпеки «Самотестування» рівня НТ-3 – «Самотестування у реальному часі» має передбачати перевірку таких вимог:

– програма має містити ті ж вимоги, що містить програма випробувань функціональної послуги «Самотестування при старті».

Додатково програма має передбачити перевірку такої вимоги:

– КЗЗ ОЕ здатний у процесі штатного функціонування виконувати наведений при відповіді на питання 159 набір тестів із метою оцінювання правильності функціонування своїх критичних функцій із використанням засобів і за правилами, наведеними при відповіді на питання 162.

4.5.7 Програма випробування функціональної послуги «Ідентифікація й автентифікація при обміні»

Послуга «Ідентифікація й автентифікація при обміні» дозволяє КЗЗ (компонентам КЗЗ) установити та перевірити ідентичність іншого КЗЗ (компонента КЗЗ) перед початком або у процесі взаємодії. Функціональні послуги «Ідентифікація й автентифікація при обміні» ранжируються за рівнями 1 … 3 залежно від повноти реалізації:

НВ-1 – автентифікація вузла;

НВ-2 – автентифікація джерела даних;

НВ-3 – автентифікація підтвердження.

Спеціальні питання щодо послуги «Ідентифікація й автентифікація при обміні»

Питання 164. Чи існує в ОЕ можливість обміну (з використанням відповідних інтерфейсних процесів) між різними компонентами ОЕ через незахищене середовище пасивними об'єктами будь-якого з типів. Якщо така можливість існує, то наведіть цю підмножину типів пасивних об'єктів.

У цьому випадку в ОЕ може бути реалізована послуга «Ідентифікація й автентифікація при обміні» рівнів НВ-1, НВ-2 чи НВ-3.

Питання 165. Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ, засоби та відповідні механізми, що забезпечують виконання взаємної ідентифікації й автентифікації різних КЗЗ (компонентів КЗЗ) перед ініціалізацією (початком) обміну даними з іншим КЗЗ (компонентом КЗЗ). Функціонування засобів, що забезпечують реалізацію послуги «Ідентифікація й автентифікація при обміні», повинно обов'язково передбачати виконання таких дій:

– отримання інформації автентифікації, необхідної для генерації/перевірки запитів автентифікації сторонами взаємодії (ініціатором і верифікатором);

– генерація та передача запитів автентифікації стороною-ініціатором;

– перевірка й оброблення запитів автентифікації стороною-верифікатором.

При цьому функціонування механізмів, що реалізують послугу, може ґрунтуватися на одному з таких принципів:

– знання загального секрету;

– підтвердження довіреною третьою стороною;

– контекст запиту автентифікації.

Якщо у складі КЗЗ існують засоби, що реалізують механізми, які функціонують на підставі зазначених принципів, то це означає, що засобами КЗЗ може бути реалізована послуга «Ідентифікація й автентифікація при обміні» рівнів НВ-1, НВ-2 чи НВ-3.

Питання 166. З використанням яких атрибутів КЗЗ (компонентів КЗЗ), виконується взаємна ідентифікація й автентифікація різних КЗЗ (компонентів КЗЗ) перед ініціалізацією (початком) обміну даними з іншим КЗЗ (компонентом КЗЗ).

Питання 167. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на питання 165), з використанням яких саме механізмів реалізовані засоби виконання взаємної ідентифікації й автентифікації різних КЗЗ (компонентів КЗЗ) перед ініціалізацією (початком) обміну даними з іншим КЗЗ (компонентом КЗЗ) із застосуванням наведених при відповіді на питання 166 атрибутів. Наведіть опис протоколу виконання автентифікації та структуру наборів даних автентифікації, що використовуються при цьому.

Питання 168. Чи існує можливість забезпечення, з використанням засобів, наведених при відповіді на питання 167, встановлення джерела кожного експортованого (переданого) й імпортованого (прийнятого) об'єкта кожного з наведених при відповіді на питання 164.

У випадку позитивної відповіді на дане питання можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Ідентифікація й автентифікація при обміні» рівня НВ-2 чи НВ-3.

Питання 169. З використанням яких атрибутів переданих пасивних об'єктів, а також КЗЗ (компонентів КЗЗ), реалізується зазначена при відповіді на питання 168 можливість установлення джерела кожного експортованого (переданого) й імпортованого (прийнятого) об'єкта кожного типу.

Питання 170. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на питання 165), з використанням яких саме механізмів реалізовані засоби встановлення джерела кожного експортованого (переданого) й імпортованого (прийнятого) об'єкта при обміні даними з іншим КЗЗ (компонентом КЗЗ) із використанням наведених при відповіді на питання 169 атрибутів. Наведіть опис протоколу встановлення джерела кожного експортованого (переданого) й імпортованого (прийнятого) об'єкта при обміні даними з іншим КЗЗ (компонентом КЗЗ) і структуру наборів даних, що використовуються при цьому.

Питання 171. Чи існує можливість забезпечення, з використанням засобів і протоколів, наведених при відповіді на питання 170, однозначного підтвердження джерела кожного експортованого (переданого) й імпортованого (прийнятого) об'єкта незалежною третьою стороною. У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Ідентифікація й автентифікація при обміні» рівня НВ-3.

Питання 172. З використанням яких атрибутів переданих пасивних об'єктів і КЗЗ (компонентів КЗЗ), наведених при відповіді на питання 169, реалізується зазначена при відповіді на питання 171 можливість однозначного підтвердження джерела кожного експортованого (переданого) й імпортованого (прийнятого) об'єкта незалежною третьою стороною. Наведіть опис протоколу підтвердження джерела кожного експортованого (переданого) й імпортованого (прийнятого) об'єкта незалежною третьою стороною та структуру наборів даних, що використовуються при цьому.

Спільними для всіх рівнів функціональної послуги безпеки «Ідентифікація й автентифікація при обміні» є перевірки таких вимог:

– політика послуги, що реалізується КЗЗ об'єкта експертизи (ОЕ), визначає множину атрибутів КЗЗ, наведену при відповіді на питання 166 і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ (компонентом КЗЗ), наведені при відповіді на питання 167;

– КЗЗ (компонент КЗЗ), перш ніж почати обмін даними з іншим КЗЗ (компонентом КЗЗ), здатний ідентифікувати й автентифікувати цей КЗЗ (компонент КЗЗ) із використанням захищеного механізму та засобів, наведених при відповіді на питання 167;

– підтвердження ідентичності виконується на підставі затвердженого протоколу автентифікації, наведеного при відповіді на питання 167.

Програма випробувань функціональної послуги безпеки «Ідентифікація й автентифікація при обміні» рівня НВ-1 – «Автентифікація вузла» має передбачати перевірку спільних для всіх рівнів вимог.

Програма випробувань функціональної послуги безпеки «Ідентифікація й автентифікація при обміні» рівня НВ-2 – «Автентифікація джерела даних» має передбачати перевірку таких вимог:

– КЗЗ ОЕ використовує захищені механізми та протокол, наведені при відповіді на питання 170, для встановлення, з використанням атрибутів,

наведених при відповіді на питання 169, джерела кожного експортованого й імпортованого об’єкта кожного з наведених при відповіді на питання 164 типів.

Програма випробувань функціональної послуги безпеки «Ідентифікація й автентифікація при обміні» рівня НВ-3 – «Автентифікація з підтвердженням» має передбачати перевірку таких вимог:

– КЗЗ ОЕ використовує захищені механізми та протокол, наведені при відповіді на питання 170, для встановлення, з використанням атрибутів, наведених при відповіді на питання 169, джерела кожного експортованого й імпортованого об’єкта кожного з наведених при відповіді на питання 164 типів;

– використаний протокол, опис якого наведено при відповіді на питання 172, забезпечує можливість однозначного підтвердження джерела об’єкта незалежною третьою стороною.

4.5.8 Програма випробування функціональної послуги «Автентифікація відправника»

Послуга «Автентифікація відправника» дозволяє однозначно встановити приналежність певного об’єкта певному користувачу, тобто той факт, що об’єкт був створений або відправлений цим користувачем. Функціональні послуги «Автентифікація відправника» ранжируються за рівнями 1, 2 залежно від можливості підтвердження результатів перевірки незалежною третьою стороною:

НА-1 – базова автентифікація відправника;

НА-2 –автентифікація відправника з підтвердженням.

Спеціальні питання щодо послуги «Автентифікація відправника»

Питання 173. Чи існує в ОЕ можливість обміну (з використанням відповідних інтерфейсних процесів) між різними користувачами через незахищене середовище пасивними об’єктами будь-якого з типів. Якщо така можливість існує, то наведіть цю підмножину типів пасивних об’єктів.

Питання 174. Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ, засоби та відповідні механізми, що забезпечують можливість однозначно встановити приналежність певного об’єкта певного типу певному користувачу, тобто той факт, що об’єкт був створений або відправлений цим користувачем.

Функціонування засобів, що забезпечують реалізацію послуги «Автентифікація відправника», повинно обов’язково передбачати виконання таких дій:

– генерація підтверджень авторства (маркерів причетності), однозначно пов’язаних із переданими об’єктами (повідомленнями);

– передача та збереження підтверджень авторства (маркерів причетності);

– перевірка підтверджень авторства (маркерів причетності).

При цьому обов’язковим є застосування механізмів, заснованих на використанні криптографічних перетворень. Використаний вигляд

підтверджень (маркерів причетності) визначається типом використаних криптографічних алгоритмів і містить:

– захищені конверти повідомлень, у процесі генерації та перевірки яких використовуються симетричні криптографічні алгоритми;

– електронні цифрові підписи повідомлень, у процесі генерації та перевірки яких використовуються несиметричні криптографічні алгоритми.

Якщо засобів, що реалізують механізми, які функціонують на підставі зазначених принципів, у складі КЗЗ немає, то це означає, що послуга «Автентифікація відправника» засобами КЗЗ ОЕ не реалізується.

Питання 175. З використанням яких атрибутів користувачів, переданих пасивних об’єктів та інтерфейсних процесів виконується зазначене при відповіді на питання 173 встановлення приналежності певного об’єкта певного типу певному користувачу.

Питання 176. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на питання 174), з використанням яких саме механізмів реалізовані засоби встановлення приналежності певного об’єкта певному користувачу з використанням наведених при відповіді на питання 175 атрибутів. Наведіть опис протоколу виконання встановлення приналежності певного об’єкта певному користувачу та структуру наборів даних, що використовуються при цьому.

Питання 177. Чи існує можливість забезпечення, з використанням засобів і протоколів, наведених при відповіді на питання 176, однозначного підтвердження приналежності певного об’єкта певного типу певному користувачу незалежною третьою стороною.

У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Автентифікація відправника» рівня НА-2.

Питання 178. З використанням яких атрибутів користувачів, переданих пасивних об’єктів й інтерфейсних процесів, наведених при відповіді на питання 175, реалізується зазначена при відповіді на питання 177 можливість однозначного підтвердження приналежності певного об’єкта певного типу певному користувачу незалежною третьою стороною. Наведіть опис протоколу підтвердження приналежності об’єкта певному користувачу незалежною третьою стороною та структуру наборів даних, що використовуються при цьому.

Спільними для всіх рівнів функціональної послуги безпеки «Ідентифікація й автентифікація при обміні» є перевірки таких вимог:

– політика послуги, що реалізується КЗЗ об’єкт ОЕ, визначає множину властивостей й атрибутів переданих об’єктів, користувачів-відправників й інтерфейсних процесів різного типу, наведену при відповіді на питання 175, а також процедури, наведені при відповіді на питання 176, які дозволяють однозначно встановити, що об’єкт кожного з наведених при відповіді на питання 173 типів був відправлений (створений) певним користувачем;

– установлення приналежності виконується на підставі затвердженого протоколу, опис якого наведено при відповіді на питання 164, з використанням механізмів і засобів, наведених при відповіді на питання 164;

– атрибути користувача-відправника, використані у протоколі встановлення приналежності, автентифіковані з використанням засобів реалізації послуги «Ідентифікація й автентифікація» рівня НИ-1 або вище згідно політики цієї послуги, наведеної при відповіді на питання 125.

Програма випробувань функціональної послуги безпеки «Автентифікація відправника» рівня НА-1 – «Базова автентифікація відправника» має передбачати перевірку спільних для всіх рівнів вимог.

Програма випробувань функціональної послуги безпеки «Автентифікація відправника» рівня НА-2 – «Автентифікація відправника з підтвердженням» має передбачати перевірку таких вимог:

– використаний протокол підтвердження приналежності, опис якого наведено при відповіді на питання 178, забезпечує можливість однозначного підтвердження приналежності об’єкта певного типу незалежною третьою стороною.

4.5.9 Програма випробування функціональної послуги «Автентифікація отримувача»

Послуга «Автентифікація отримувача» дозволяє однозначно установити факт отримання певного об’єкта певним користувачем. Функціональні послуги «Автентифікація отримувача» ранжируються за рівнями 1, 2 залежно від можливості підтвердження результатів перевірки незалежною третьою стороною:

НП-1 – базова автентифікація отримувача;

НП-2 – автентифікація отримувача з підтвердженням.

Спеціальні питання щодо послуги «Автентифікація отримувача»

Питання 179. Чи існує в ОЕ можливість обміну (з використанням відповідних інтерфейсних процесів) між різними користувачами через незахищене середовище пасивними об’єктами будь-якого з типів. Якщо така можливість існує, то наведіть цю підмножину типів пасивних об’єктів.

Питання 180. Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ, засоби та відповідні механізми, що забезпечують можливість однозначно установити факт отримання певного об’єкта певного типу (з урахуванням відповіді на питання 180) певним користувачем. Функціонування засобів, що забезпечують реалізацію послуги «Автентифікація отримувача», обов’язково передбачає виконання дій:

– генерація підтверджень отримання (маркерів причетності), однозначно пов’язаних з отриманими об’єктами (повідомленнями);

– передача та збереження підтверджень отримання (маркерів причетності);

– перевірка підтверджень отримання (маркерів причетності).

При цьому обов’язковим є застосування механізмів, заснованих на використанні криптографічних перетворень. Використаний вигляд

підтверджень (маркерів причетності) визначається типом використаних криптографічних алгоритмів і містить:

– захищені конверти повідомлень про отримання, у процесі генерації та перевірки яких використовуються симетричні криптографічні алгоритми;

– електронні цифрові підписи повідомлень про отримання, у процесі генерації та перевірки яких використовуються несиметричні криптографічні алгоритми.

Питання 181. З використанням яких атрибутів користувачів, переданих пасивних об'єктів й інтерфейсних процесів виконується зазначене при відповіді на питання 179 встановлення факту отримання певного об'єкта певного типу певним користувачем.

Питання 182. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на питання 180), з використанням яких саме механізмів реалізовані засоби встановлення факту отримання певного об'єкта певного типу певним користувачем з використанням наведених при відповіді на питання 181 атрибутів. Наведіть опис протоколу виконання встановлення факту отримання певного об'єкта певним користувачем і структуру наборів даних, що використовуються при цьому.

Питання 183. Чи існує можливість забезпечення, з використанням засобів і протоколів, наведених при відповіді на питання 182, однозначного підтвердження факту отримання певного об'єкта певного типу певним користувачем незалежною третьою стороною.

У випадку позитивної відповіді можна стверджувати, що засобами КЗЗ може бути реалізована послуга «Автентифікація відправника» рівня НП-2.

Питання 184. З використанням яких атрибутів користувачів, переданих пасивних об'єктів і інтерфейсних процесів, наведених при відповіді на питання 181, реалізується зазначена при відповіді на питання 183 можливість однозначного підтвердження факту отримання певного об'єкта певного типу певним користувачем незалежною третьою стороною. Наведіть опис протоколу підтвердження факту отримання певного об'єкта певним користувачем незалежною третьою стороною та структуру наборів даних, що використовуються при цьому.

Спільними для всіх рівнів функціональної послуги безпеки «Автентифікація отримувача» є перевірки таких вимог:

– політика послуги, що реалізується КЗЗ ОЕ, визначає множину властивостей і атрибутів переданих об'єктів, користувачів-отримувачів й інтерфейсних процесів різного типу, наведену при відповіді на питання 181, а також процедури, наведені при відповіді на питання 182, які дозволяють однозначно встановити, що об'єкт кожного з наведених при відповіді на питання 179 типів був отриманий певним користувачем;

– установлення отримувача виконується на підставі затвердженого протоколу, опис якого наведено при відповіді на питання 182, з використанням механізмів і засобів, наведених при відповіді на питання 182;

– атрибути користувача-отримувача, використані у протоколі встановлення отримувача, автентифіковані з використанням засобів реалізації послуги

«Ідентифікація й автентифікація» рівня НИ-1 або вище згідно політики цієї послуги, наведеної при відповіді на питання 125.

Програма випробувань функціональної послуги безпеки «Автентифікація отримувача» рівня НП-1 – «Базова автентифікація отримувача» має передбачати перевірку спільних для всіх рівнів вимог.

Програма випробувань функціональної послуги безпеки «Автентифікація отримувача» рівня НП-2 – «Автентифікація отримувача з підтвердженням» має передбачати перевірку таких вимог:

– додатково визначені властивості, атрибути та процедури, наведені при відповіді на питання 184, що можуть бути використані для однозначного підтвердження факту отримання об’єкта певного типу незалежною третьою стороною;

– використаний протокол підтвердження отримувача, опис якого наведено при відповіді на питання 186, забезпечує можливість однозначного підтвердження факту отримання об’єкта певного типу незалежною третьою стороною.

Питання для самоконтролю

1. Цілі й основні положення державної експертизи комплексної системи захисту інформації в інформаційно-телекомунікаційних системах.
2. Дайте характеристику змісту спеціальних питань у програмі випробування функціональних послуг безпеки критеріїв конфіденційності.
3. Дайте характеристику змісту спеціальних питань у програмі випробування функціональних послуг безпеки критеріїв цілісності.
4. Дайте характеристику змісту спеціальних питань у програмі випробування функціональних послуг безпеки критеріїв доступності.
5. Дайте характеристику змісту спеціальних питань у програмі випробування функціональних послуг безпеки критеріїв спостережності.

Розділ 5

ОЦІНКА КРИТЕРІЇВ ГАРАНТІЙ БЕЗПЕКИ

5.1 Загальні відомості щодо критеріїв гарантій безпеки

Крім функціональних критеріїв, які дозволяють оцінювати наявність послуг безпеки у системі, застосовують критерії гарантій, які дозволяють оцінювати коректність реалізованих послуг. Відповідно до НД ТЗІ 2.5-004, критерії гарантій встановлюють вимоги до коректності реалізованих послуг безпеки інформації, які забезпечуються комплексом засобів захисту (КЗЗ) як складовою частиною комплексної системи захисту інформації (КСЗІ) в інформаційно-телекомунікаційних системах (ІТС).

Вводиться сім рівнів гарантій. Ієрархія рівнів гарантій відображає поступово зростаючу міру впевненості щодо того, що надавані послуги дозволяють протистояти певним загрозам, а механізми, що їх реалізують, у свою чергу, реалізовано коректно, і вони можуть забезпечувати сподіваний споживачем рівень захищеності інформації під час експлуатації системи.

Гарантії забезпечуються у перебігу як розроблення, так і оцінювання. У перебігу розроблення гарантії забезпечуються діями розробника щодо забезпечення правильності (коректності) розроблення. У перебігу оцінювання гарантії забезпечуються шляхом перевірення дотримання розробником вимог щодо критеріїв, аналізування документації, процедур розроблення й постачання, а також іншими діями експертів, які здійснюють оцінювання.

Нормативними документами встановлено, що рівень гарантій реалізації послуг безпеки, наприклад, для глобальних мереж повинен бути не нижчий Г2.

Критерії гарантій встановлюють вимоги щодо архітектури комплексу засобів захисту, середовища розроблення, послідовності розроблення, середовища функціонування, експлуатаційної документації, випробувань комплексу. Більшість цих вимог має пряме відношення до технічної експлуатації системи інформаційної безпеки.

Архітектура. Програмне забезпечення, призначене для реалізації комплексу засобів захисту, має максимальним чином будуватися за модульним принципом.

Склад послуг безпеки, а також механізмів захисту, які реалізують кожну з послуг, визначається політикою безпеки інформації в ІТС й має відповідати її вимогам. Якщо не всі вимоги політики безпеки реалізуються комплексом засобів захисту, вони повинні підтримуватися організаційними й іншими заходами захисту КСЗІ. У складі комплексу засобів захисту не повинні міститися послуги й використовуватися засоби, які мають не передбачені політикою безпеки функції. Використання таких засобів можливе за умови вилучання цих функцій чи гарантування унеможливлення їхньої активізації.

Мають бути описані особливості архітектури компонентів КСЗІ й їхнє призначення. Стиль описування – неформалізований.

Середовище розроблення. Має бути визначено всі стадії й етапи життєвого циклу ІТС, а для кожної стадії й етапу – перелік та обсяги необхідних робіт і порядок їхнього виконання. Якщо певні роботи потребують створення особливих умов, – це повинно бути зазначено окремо. Всі стадії й етапи робіт має бути задокументовано. Види та зміст документів встановлено державними стандартами. Це стосується і стадії технічної експлуатації WEB-сторінки.

На всіх стадіях життєвого циклу мають існувати процедури керування конфігурацією ІТС. Ці процедури мають визначати технологію відстеження та внесення змінень в апаратне та програмне забезпечення КСЗІ, тестове покриття й документацію та гарантувати, що без дотримання цієї технології жодне змінення не може бути внесено. Технологія відстеження та внесення змінень повинна гарантувати незмінну відповідність між документацією й реалізацією поточної версії комплексу засобів захисту.

Послідовність розроблення. Для всіх стадій життєвого циклу ІТС, зокрема для стадії технічної експлуатації, мають бути розроблені функціональні специфікації КСЗІ.

На підготовчому етапі створення КСЗІ має бути здійснено обстеження середовищ функціонування ІТС, за результатами якого визначаються об’єкти захисту, здійснюється класифікація інформації й розробляється модель загроз для інформації й концепція політики безпеки інформації в ІТС. На підставі цих даних мають бути сформульовані функціональні специфікації вимог із захисту інформації в ІТС. Ці специфікації мають бути викладені в окремому розділі технічного завдання на створення ІТС чи в окремому технічному завданні на створення КСЗІ.

Функціональні специфікації політики безпеки й моделі політики безпеки мають, як мінімум, містити перелік та опис послуг безпеки, надаваних комплексом засобів захисту, а також правила розмежування доступу до захищених об’єктів ІТС.

Функціональні специфікації проекту архітектури КСЗІ мають містити модель захисту чи ескізний проект, де враховано всі істотні загрози та для кожної з них визначено можливі варіанти її блокування (попередження) за допомогою комплексу засобів захисту або організаційними, або іншими заходами захисту. Якщо існує неоднозначність, повинні надаватися додаткові аргументи на користь вибору того чи іншого варіанта.

Функціональні специфікації детального проекту КСЗІ мають містити принципи побудови, функціональні можливості, опис функціонування кожного механізму захисту та взаємодії механізмів між собою у складі комплексу засобів захисту. Мають бути розроблені документи, які регламентували б використання засобів комплексу засобів захисту, а також організаційних та інших заходів захисту, які входять до КСЗІ. Як здійснення детального проекту можуть розглядатися технічний, робочий або техно-робочий проекти.

Функціональні специфікації всіх рівнів надаються в описовому неформалізованому вигляді.

Має бути неформально подана відповідність специфікацій КСЗІ всіх рівнів. Таким підтвердженням може бути дотримання власником ІТС і суб’єктами

господарювання, які беруть участь у створенні ІТС і КСЗІ, встановленого нормативними документами із захисту інформації порядку. Наприклад, підтвердженням відповідності між специфікаціями КСЗІ різних рівнів деталізації може бути узгодження в установленому порядку відповідних документів: моделі загроз, технічного завдання, технічного проекту тощо, висновок приймальної комісії щодо цього під час випробувань КСЗІ чи окремих її компонентів, результати контролю за виконаними роботами на етапах створення ІТС із боку системи керування якістю виробництва, якщо у власника та розробників ІТС таку систему впроваджено, й інше.

Окремі етапи робіт мають бути задокументовані відповідно до вимог НД ТЗІ 1.4-001-2000 [36] у вигляді окремих розділів плану захисту інформації у глобальній мережі чи вимог інших нормативно-правових актів і нормативних документів із ТЗІ.

Середовище функціонування. Мають існувати засоби інсталяції, генерації й запуску комплексу засобів захисту, які гарантують, що експлуатація ІТС розпочинається з безпечного стану, а також документи й інструкції, які регламентують порядок керування цими процедурами. Якщо можливі є різні варіанти конфігурації комплексу засобів захисту, то всі вони повинні бути описані в інструкціях.

Розробник апаратного, програмного, програмно-апаратного забезпечення КСЗІ повинен шляхом впровадження технічних, організаційних чи фізичних заходів безпеки гарантувати, що забезпечення, яке ним поставляється, відповідає еталону.

Документація. Документація на комплекс заходів захисту у вигляді окремих документів чи розділів інших документів має містити опис послуг безпеки, реалізованих комплексом заходів захисту, а також настанови для різних категорій користувачів – адміністратора безпеки, адміністратора баз даних, адміністратора послуг, звичайного користувача тощо – стосовно використання послуг безпеки.

Вимоги щодо складу й змісту документації на інші компоненти КСЗІ, організаційні чи інші заходи захисту визначаються технічним завданням на створення КСЗІ.

Випробування. Випробування комплексу засобів захисту можуть провадитись як самостійно, так і у складі КСЗІ. Для проведення випробувань розробник комплексу засобів захисту має підготувати програму й методику випробувань, розробити процедури та тести випробувань всіх механізмів, які реалізують послуги безпеки.

Розробник комплексу засобів захисту має надати доведення тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування з тим, аби здобуті результати можна було перевірити шляхом повторення тестування.

Розробник комплексу засобів захисту має усунути чи нейтралізувати всі знайдені “слабкі місця” та виконати повторне тестування КЗЗ для підтвердження того, що виявлені недоліки було усунуто й не виникли нові “слабкі місця ”.

Програма й методика випробувань комплексу засобів захисту, тестове покриття, результати випробувань комплексу входять до складу обов'язкового комплекту документації, яка надається організатору експертизи під час проведення державної експертизи КСЗІ в ІТС.

Далі наведемо рівні гарантій безпеки для рівнів Г1 – Г4 згідно з НД ТЗІ 2.5-004-99.

5.2 Рівні гарантій безпеки за національними стандартами

5.2.1 Вимоги гарантій для рівня Г-І

Архітектура

КЗЗ має реалізувати політику безпеки. Всі його компоненти повинні бути чітко визначені.

Середовище розроблення

Процес розроблення.

Розробник повинен визначити всі стадії життєвого циклу ІТС, розробити, запровадити та підтримувати у робочому стані документально оформлені методики своєї діяльності на кожній стадії. Мають бути документовані всі етапи кожної стадії життєвого циклу й їх граничні вимоги.

Управління конфігурацією.

Розробник повинен розробити, запровадити та підтримувати у робочому стані документовані методики щодо управління конфігурацією ІТС на всіх стадіях її життєвого циклу. Система управління конфігурацією має забезпечувати управління внесенням змін в апаратне забезпечення. програми постійних запам'ятовуючих пристроїв, вихідні тексти, об'єктні коди, тестове покриття та документацію. Система управління конфігурацією має гарантувати постійну відповідність між всією документацією та реалізацією поточної версії КЗЗ.

Послідовність розроблення.

Функціональні специфікації (політика безпеки).

На стадії розроблення технічного завдання Розробник повинен розробити функціональні специфікації ІТС. Представлені функціональні специфікації мають включати у себе неформалізований опис політики безпеки, що реалізується КЗЗ. Політика безпеки має містити перелік й опис послуг безпеки, що надаються КЗЗ.

Проект архітектури.

На стадії розроблення ескізного проекту Розробник повинен розробити проект архітектури КЗЗ. Поданий проект має містити перелік й опис компонентів КЗЗ і функцій, що реалізуються ними. Повинні бути описані будь-які використані зовнішні послуги безпеки. Зовнішні інтерфейси КЗЗ мають бути описані у термінах винятків, повідомлень про помилки та кодів повернення.

Стиль специфікації: неформалізований.

Детальний проект.

На стадіях розроблення технічного проекту або робочого проекту Розробник повинен розробити детальний проект КЗЗ. Поданий детальний проект має містити перелік усіх компонентів КЗЗ і точний опис функціонування кожного механізму. Мають бути описані призначення та параметри інтерфейсів компонентів КЗЗ.

Стиль специфікації: неформалізований.

Середовище функціонування.

Розробник повинен подати засоби інсталяції, генерації та запуску ІТС, які гарантують, що експлуатація ІТС починається з безпечного стану. Розробник повинен подати перелік усіх можливих параметрів конфігурації, які можуть бути використані у процесі інсталяції, генерації та запуску.

Документація.

Вимоги до документації є спільними 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 опису функцій безпеки мають бути викладені основні, необхідні для правильного використання послуг безпеки, принципи політики безпеки, що реалізуються КЗЗ оцінюваної ІТС, а також самі послуги.

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

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 й адміністратора. Настанови адміністратору та настанови користувачу можуть бути об’єднані у настанови з установлення й експлуатації.

Випробування комплексу засобів захисту.

Розробник повинен подати для перевірки програму та 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.

5.2.2 Вимоги гарантій для рівня Г-2

Архітектура. Без змін.

Середовище розроблення.

Процес розроблення.
Без змін.
Управління конфігурацією.
Без змін.
Послідовність розроблення.
Функціональні специфікації (політика безпеки).
Без змін.
Функціональні специфікації (модель політики безпеки).
Показ відповідності політиці безпеки.
Функціональні специфікації повинні включати модель політики безпеки.
Стиль специфікації: неформалізований.
Проект архітектури.
Додатково: показ відповідності моделі політики безпеки.
Детальний проект.
Додатково:
Показ відповідності проекту архітектури.
Стиль специфікації: неформалізований на весь КЗЗ.
Середовище функціонування.
Без змін.
Документація.
Без змін.
Випробування комплексу засобів захисту.
Додатково: розробник повинен усунути або нейтралізувати всі знайдені «слабкі місця» та виконати повторне тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені та не з'явилися нові «слабкі місця».

5.2.3 Вимоги гарантій для рівня Г-3

Архітектура
Додатково: КЗЗ повинен складатися з добре визначених і максимально незалежних компонентів. Кожен із компонентів повинен бути спроектований відповідно до принципу мінімуму повноважень.
Середовище розроблення.
Процес розроблення.
Додатково: розробник повинен описати стандарти кодування, яких необхідно дотримуватися у процесі реалізації, і повинен гарантувати, що всі вихідні коди компілюються відповідно до цих стандартів. Будь-яка з використаних під час реалізації мов програмування має бути добре визначена. Всі залежні від реалізації параметри мов програмування або компіляторів повинні бути документовані.
Управління конфігурацією.
Без змін.
Послідовність розроблення.
Функціональні специфікації (політика безпеки).
Без змін.

Функціональні специфікації (модель політики безпеки).

Додатково: стиль специфікації: частково формалізований.

Проект архітектури.

Додатково: стиль специфікації: частково формалізований.

Детальний проект.

Без змін.

Реалізація.

Показ відповідності детальному проекту.

Розробник повинен подати вихідний код частини КЗЗ.

Середовище функціонування.

Додатково: має існувати система технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне та програмно-апаратне забезпечення КЗЗ, яке поставляється Замовнику, точно відповідає еталонній копії.

Документація.

Без змін.

Випробування комплексу засобів захисту.

Без змін.

5.2.4 Вимоги гарантій для рівня Г-4

Архітектура

Додатково: критичні для безпеки компоненти КЗЗ повинні бути захищені від не критичних для безпеки за рахунок використання механізмів захисту, які надаються програмно-апаратними засобами більш низького рівня.

Середовище розроблення.

Процес розроблення.

Додатково: розробник повинен розробити, запровадити та підтримувати у робочому стані документально оформлені методики забезпечення фізичної, технічної, організаційної та кадрової безпеки.

Управління конфігурацією.

Система управління конфігурацією повинна базуватися на автоматизованих засобах.

Система управління конфігурацією також повинна бути використана для генерації КЗЗ із вихідного коду та обліку всіх змін із появою нових версій.

Система управління конфігурацією повинна бути здатна видавати звіти про стан елементів конфігурації.

Послідовність розроблення.

Функціональні специфікації (політика безпеки).

Без змін.

Функціональні специфікації (модель політики безпеки).

Додатково:

Демонстрація відповідності політиці безпеки.

Стиль специфікації: формалізований.

Проект архітектури.

Без змін.

Детальний проект.

Додатково. Стиль специфікацій: частково формалізований.

Реалізація.

Без змін.

Середовище функціонування.

Без змін.

Документація.

Без змін.

Випробування комплексу засобів захисту.

Додатково: розробник повинен виконати тести з подолання механізмів захисту та довести, що КЗЗ відносно або абсолютно стійкий до такого роду атак із боку розробника.

5.3 Вимоги гарантій засобів захисту за міжнародними стандартами

5.3.1 Загальна характеристика вимог гарантій безпеки

Вимоги гарантій безпеки (ВГБ) – вимоги безпеки, які у «Загальних критеріях» представляють собою характеристику ІТ-продукту, що показує, наскільки ефективно забезпечується заявлений рівень безпеки, а також ступінь коректності реалізації засобів захисту. Як і функціональні вимоги безпеки, ВГБ детально структуровані та регламентують усі етапи проектування, створення й експлуатації ІТ – продукту надто детально. Структура вимог гарантій аналогічна функціональним вимогам.

Клас ВГБ – верхній рівень формальної структури вимог гарантій безпеки. Містить наступні елементи: назва класу, опис класу, розділи вимог гарантій безпеки.

Вимоги розподілені на такі класи ВГБ.

– дистрибуція;

– розроблення;

– документація;

– процес розроблення:

– тестування;

– оцінка вразливостей.

Розділ «ВГБ» – це складова частина класу ВГБ. Структура розділу містить такі елементи:

– назва та позначення розділу [*family name*];

– мета [*objectives*];

– ранжирування вимог [*component leveling*];

– опис застосування [*application notes*);

– вимоги [*assurance component*].

Кожен розділ має свою унікальну назву та семисимвольний ідентифікатор, який складається з трисимвольного ідентифікатора класу, знаку підкреслення

та трисимвольного позначення розділу. Ранжирування стандартних вимог подано у вигляді впорядкованих списків.

Структура ВГБ складається з таких елементів**:**

– назва вимоги;

– мета;

– опис застосування;

– об’єднані вимоги;

– елементи вимоги.

Вимоги гарантій використовуються у ході кваліфікаційного аналізу ІТ-продукту відповідного рівня гарантій.

5.3.2 Класи вимог гарантій безпеки

Клас управління проектом включає у себе такі розділи «ВГБ»: засоби управління проектом; управління версіями; конфігурація проекту.

Розділ ***«Засоби управління проектом»*** включає у себе такі вимоги гарантій безпеки:

– застосування автоматизованих засобів управління проектом;

– повна автоматизація управління проектом і контролю версій.

Розділ **«*Управління версіями»*** включає у себе такі вимоги гарантій безпеки:

– нумерація версій;

– ідентифікація компонентів;

– контроль цілісності версій;

– авторизація виробників при поновленні версій;

– контроль цілісності й автентичності дистрибутивів системи.

Розділ «***Конфігурація проекту»*** включає у себе такі вимоги гарантій безпеки:

– основні компоненти проекту (алгоритми, тексти, документація);

– включення до складу об’єкта виявлених помилок й уразливості;

– включення до складу проекту інструментальних засобів розроблення.

Клас дистрибуція включає у себе такі розділи «ВГБ»: постачання, установлення, настроювання, запуск.

Розділ **«*Постачання»*** включає у себе такі вимоги гарантій безпеки:

– регламентована процедура постачання;

– виявлення спотворень у процесі постачання;

– захист від спотворень у процесі постачання.

Розділ «***Установлення, настроювання, запуск»*** включає у себе такі ВГБ:

– регламентовані процедури установлення, настроювання, запуску;

– протоколювання процесу установлення, настроювання, запуску.

Клас розроблення включає у себе такі розділи «ВГБ»: загальні функціональні специфікації; архітектура захисту; форма подання продукту на сертифікацію; структура засобів захисту; часткові специфікації засобів захисту; відповідність описів різного рівня; політика безпеки.

Розділ **«*Загальні функціональні специфікації»*** включає у себе такі вимоги гарантій безпеки:

– неформальні специфікації для засобів захисту;
– неформальні специфікації для усіх інтерфейсів засобів захисту;
– напівформальні специфікації для засобів захисту;
– формальні специфікації для засобів захисту.

Розділ «***Архітектура захисту»*** включає у себе такі вимоги гарантій безпеки:

– опис архітектури захисту;
– відповідність архітектури захисту та політики безпеки;
– напівформальний опис архітектури захисту;
– відповідність напівформального опису архітектури захисту та політики безпеки;
– формальний опис архітектури захисту й доведення її відповідності політиці безпеки.

Розділ «***Форма надання продукту на сертифікати»*** включає у себе такі вимоги гарантій безпеки:

– опис реалізації обмеженої підмножини засобів захисту;
– повний опис реалізації усіх засобів;
– структурований опис реалізації усіх засобів захисту.

Розділ «***Структура засобів захисту»*** включає у себе такі вимоги гарантій безпеки: модальність; ієрархічнісгь; мінімізація складності.

Розділ «***Часткові специфікації засобів захисту»*** включає у себе такі вимоги гарантій безпеки:

– неформальні часткові специфікації засобів захисту;
– напіворормальні часткові специфікації засобів захисту;
– формальні часткові специфікації засобів захисту.

Розділ «***Відповідність описів різного рівня»*** включає у себе такі вимоги гарантій безпеки:

– неформальне підтвердження відповідності;
– напівформальне підтвердження відповідності;
– формальне доведення відповідності.

Розділ «***Політика безпеки»*** включає у себе такі вимоги гарантій безпеки:

– неформальний опис політики безпеки;
– напівформальний опис політики безпеки;
– формальна модель політики безпеки .

Клас документація (включає у себе такі розділи «ВГБ»: керівництво адміністратора; керівництво користувача.

Розділ «***Керівництво адміністратора»*** включає у себе вимогу гарантій безпеки – адміністрування засобів захисту.

Розділ «***Керівництво користувача»*** включає у себе вимогу гарантій безпеки – використання засобів захисту.

Клас процес розроблення включає у себе такі розділи «ВГБ»: безпека середовища розроблення; виправлення помилок і ліквідація вразливостей; технологія розроблення; засоби розроблення.

Розділ «***Безпека середовища розроблення»*** включає у себе такі вимоги гарантій безпеки:

– застосування заходів безпеки у ході розроблення;

– підтвердження заходів безпеки у ході розроблення.

Розділ ***«Виправлення помилок і ліквідація вразливостей»*** включає у себе такі вимоги гарантій безпеки:

– виправлення виявлених помилок і ліквідація вразливостей;

– регулярне виправлення помилок і ліквідація вразливостей;

– гарантоване виправлення виявлених помилок і ліквідація виявлених уразливостей.

Розділ ***«Технологія розроблення»*** включає у себе такі вимоги гарантій безпеки:

– визначена розробником технологія розроблення;

– стандартизована технологія розроблення;

– технологія розроблення, яка дозволяє оцінювати продукт, що розробляється.

Розділ **«*Засоби розроблення»*** включає у себе такі вимоги гарантій безпеки:

– використання певного набору засобів розроблення;

– використання основних засобів розроблення, що відповідають певним стандартам;

– використання тільки засобів розроблення, що відповідають певним стандартам.

Клас тестування включає у себе такі розділи «ВГБ»: повнота тестування; глибина тестування; методика тестування; незалежне тестування.

Розділ ***«Повнота тестування»*** включає у себе такі вимоги гарантій безпеки:

– обґрунтування повноти тестування;

– аналіз повноти тестування;

– суворий аналіз повноти тестування.

Розділ «***Глибина тестування»*** включає у себе такі вимоги гарантій безпеки:

– архітектура;

– функціональні специфікації.

Розділ ***«Методика тестування»*** включає у себе такі вимоги гарантій безпеки:

– функціональне тестування й протоколювання результатів тестів;

– тестування у відповідності з певною методикою.

Розділ ***«Незалежне тестування»*** включає у себе такі вимоги гарантій безпеки:

– готовність продукту до незалежного тестування;

– вибіркове незалежне тестування;

– повне незалежне тестування.

Клас оцінка вразливостей включає у себе такі розділи «ВГБ»: аналіз прихованих каналів; аналіз можливостей неправильного використання засобів захисту; аналіз стійкості засобів захисту; аналіз продукту на наявність уразливостей.

Розділ ***«Аналіз прихованих каналів»*** включає у себе такі вимоги гарантій безпеки:

– пошук і документування прихованих каналів;

– пошук прихованих каналів на основі певних методик;

– вичерпний пошук прихованих каналів.

Розділ ***«Аналіз можливостей неправильного використання засобів захисту»*** включає у себе такі вимоги гарантій безпеки:

– аналіз керівництв адміністрування;

– підтвердження повноти керівництв із адміністрування та безпеки їхнього застосування;

– незалежний аналіз можливостей неправильного використання засобів захисту.

Розділ ***«Аналіз стійкості засобів захисту»*** включає у себе вимогу гарантій безпеки – оцінка стійкості засобів захисту.

Розділ ***«Аналіз продукту на наявність уразливостей»*** включає у себе такі вимоги гарантій безпеки;

– виявлення вразливостей розробником продукту;

– незалежний аналіз уразливостей;

– систематичний незалежний аналіз уразливостей на основі заданих методик;

– вичерпний аналіз уразливостей.

5.4 Рівні вимог гарантій безпеки

Визначення рівнів гарантій. Рівні гарантій у «Загальних критеріях» – це сім стандартизованих наборів вимог гарантій безпеки, що регламентують застосування різноманітних методів і технологій розроблення, тестування, контролю та верифікації ІТ-продукту:

– функціональне тестування;

– структурне тестування;

– методичне тестування та перевірка;

– методичне розроблення, тестування й аналіз;

– напівформальні методи розроблення та тестування;

– напівформальні методи верифікації розроблення та тестування;

– формальні методи верифікації розроблення та тестування.

Кожен із рівнів визначає ступінь відповідності ІТ-продукту кожній вимозі гарантій (гарантії зростають від першого рівня до сьомого). Назви рівнів відображають можливості засобів контролю та верифікації, що застосовуються у ході розроблення й аналізу ІТ- продукту (табл. 5.1).

Функціональне тестування. Рівень функціонального тестування – *перший рівень гарантій* для випадків, коли загрозам безпеці не надається великого значення. Пропонується використати його у тих ситуаціях, коли все, що необхідно, це незалежна гарантія того, що до складу ІТ-продукту входять засоби захисту персональної або подібної інформації. Відповідає таким вимогам гарантій безпеки.

Таблиця 5.1 – Рівні гарантій безпеки

Вимоги гарантій	**Номери рівнів гарантій**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1. Управління проектом							
Засоби керування проектом				1	1	2	2
Керування версіями	1	2	3	4	4	5	5
Конфігурація проекту			1	2	3	3	3
2 Дистрибуція							
Постачання		1	1	2	2	2	3
Установлення, настроювання запуск	1	1	1	1	1	1	1
3. Розроблення							
Загальні функціональні специфікації	1	1	1	2	3	3	4
Архітектура захисту		1	2	2	3	4	5
Форма подання продукту на сертифікацію				1	2	3	3
Структура засобів захисту					1	2	3
Часткові специфікації засобів захисту				1	1	2	2
Відповідність описів різного рівня	1	1	1	1	2	2	3
Політика безпеки _				1	3	3	3
4 Документація							
Керівництво адміністратора	1	1	1	1	1	1	1
Керівництво користувача	1	1	1	1	I	1	1
5. Процес розроблення							
Безпека середовища розроблення			1	1	1	7	2
Виправлення помилок і ліквідація вразливостей							
Технологія розроблення				1	2	2	3
Засоби розроблення				1	2	3	3
6. Тестування							
Повнота тестування		1	2	2	2	3	3
Глибина тестування			1	1	2	2	3
Методика тестування		1	1	1	1	2	2
Незалежне тестування	1	2	2	2	2	7	3
7. Оцінка вразливостей							
Аналіз прихованих каналів					1	2	2
Аналіз можливостей неправильного використання засобів захисту			1	2	2	3	3
Аналіз стійкості засобів захисту		1	1	1	1	1	1
Аналіз продукту на наявність вразливостей		1	1	2	3	4	4

У класі ВГБ: управлінця проектом у розділі «ВГБ»: управління версіями – нумерація версій (ACM_CAP.1).

У класі ВГБ: дистрибуція

– у розділі «ВГБ»: установлення, настроювання, запуск – регламентовані процедури установлення, настроювання, запуску.

У класі ВГБ: розроблення:

– у розділі «ВГБ»: загальні функціональні специфікації – неформальні специфікації для засобів захисту;

– у розділі «ВГБ»: відповідність описів різного рівня – неформальне підтвердження відповідності.

У класі ВГБ: документація:

– у розділі «ВГБ»: керівництво адміністратора – адміністрування засобів захисту;

– у розділі «ВГБ»: керівництво користувача – використання засобів захисту.

У класі ВГБ: тестування у розділі «ВГБ»: незалежне тестування – готовність продукту до незалежного тестування.

Аналіз ІТ-продукту на відповідність даному рівню гарантій забезпечується дослідженням функцій захисту та перевіркою функціональних специфікацій, інтерфейсів та документації.

Результати аналізу підтверджуються незалежним тестуванням засобів захисту ІТ-продукту на відповідність специфікаціям і документації.

Сертифікація ІТ-продукту на даний рівень гарантій є підтвердженням відповідності властивостей ІТ-продукту його документації та специфікаціям, а також наявності працездатності захисту проти загроз безпеці.

Структурне тестування. Рівень структурного тестування – другий рівень гарантій, призначений для використання при обставинах, коли розробники або користувачі згодні задовольнитися низьким або помірним ступенем незалежного підтвердження гарантій рівня безпеки, який необхідно забезпечити. Особливо рекомендують застосування даного рівня для успадкованих систем, які вже знаходяться в експлуатації.

Другий рівень гарантій відповідає наступним вимогам гарантій безпеки.

У класі ВГБ: управління проектом у розділі ВГН: управління версіями – ідентифікація компонентів управління.

У класі ВГВ: дистрибуцій:

– у розділі «ВГБ»: постачання – регламентована процедура поставки;

– у розділі «ВГБ»: установлення, настроювання, запуск – регламентовані процедури установлення, настроювання, запуску.

У класі ВГБ: розроблення:

– у розділі «ВГБ»: загальні функціональні специфікації – неформальні специфікації засобів захисту;

– у розділі «ВГБ»: архітектура захисту – опис архітектури захисту;

– у розділі «ВГБ»: відповідність описів різного рівня – неформальне підтвердження відповідності.

У класі ВГБ: документація:

– у розділі «ВГБ»: керівництво адміністратора – адміністрування засобів захисту;

– у розділі «ВГБ»: керівництво користувача використання засобів захисту.

У класі ВГБ: тестування:

– у розділі «ВГБ»: повнота тестування – обґрунтування повноти тестування;

– у розділі «ВГБ»: методика тестування – функціональне тестування й протоколювання результатів тестів;

– у розділі «ВГБ»: незалежне тестування – вибіркове незалежне тестування.

У класі ВГБ: оцінка вразливостей:

– у розділі аналіз стійкості засобів захисту – оцінка стійкості засобів захисту;

– у розділі «ВГБ»: аналіз продукту на наявність уразливостей – виявлення вразливостей розробником продукту.

Розроблення продукту відповідно до вимог даного рівня не вимагає від виробника ніяких додаткових витрат, порівняно з розробленням звичайних комерційних або промислових продуктів, окрім надання результатів тестування.

Для другого рівня аналіз повинен проводитися не тільки у відношенні функціональних специфікацій, інтерфейсів і документів, але й для архітектури захисту ІТ- продукту.

Крім незалежного тестування засобів захисту ІТ-продукту результати аналізу підтверджуються протоколами тестування функціональних специфікацій, наданих розробником, а також незалежним вибірковим контролем результатів цих випробувань і глибини проведеного тестування, і незалежним підтвердженням пошуку розробником явних уразливостей. Крім того, для цього рівня необхідна наявність документованого складу конфігурації продукту та доведення безпеки процедури поставки.

Даний рівень розширює вимоги попереднього за рахунок включення у матеріали, що підтверджують аналіз результатів тестів, проведених розробником ІТ-продукту, необхідністю здійснення аналізу вразливостей і незалежного тестування з використанням більш детальних специфікацій.

Методичне тестування та перевірка. Рівень методичного тестування та перевірки – третій рівень гарантій, призначений для використання при обставинах, коли розробникам або користувачам потрібна помірний ступінь належного підтвердження властивостей ІТ-продукту, а також повне та послідовне дослідження властивостей продукту та контроль у процесі створення, але без проведення дорогого зворотного проектування [*reengineering*].

Відповідає наступним вимогам гарантій безпеки.

У класі ВГБ: управління проектом:

– у розділі «ВГБ»: управління версіями – контроль цілісності версії;

– у розділі «ВГБ»: конфігурація проекту – основні компоненти проекту (алгоритми, вихідні тексти, тексти, документація).

У класі ВГБ: дистрибуція:

– у розділі «ВГБ»: постачання – регламентована процедура поставки;

– у розділі «ВГБ»: установлення, настроювання, запуск – регламентовані процедури установлення, настроювання, запуску.

У класі ВГБ: розроблення:

– у розділі «ВГБ»: загальні функціональні специфікації – неформальні специфікації для засобів захисту;

– у розділі «ВГБ»: архітектура захисту – відповідність архітектури захисту політиці безпеки;

– у розділі «ВГБ»: відповідність описів різною рівня – неформальне підтвердження відповідності.

У класі ВГБ: документація:

– у розділі «ВГБ»: керівництво адміністратора – адміністрування засобів захисту;

– у розділі «ВГБ»: керівництво користувача – використання засобів захисту.

У класі ВГБ: процес розроблення

– у розділі «ВГБ»: безпека середовища розроблення – застосування заходів безпеки у ході розроблення.

У класі ВГБ: тестування:

– у розділі «ВГБ»: повнота тестування – аналіз повноти тестування;

– у розділі «ВГБ»: глибина тестування – архітектура;

– у розділі «ВГБ»: методика тестування – функціональне тестування й протоколювання результатів тестів;

– у розділі «ВГБ»: незалежне тестування – вибіркове незалежне тестування.

У класі ВГБ: оцінка вразливостей:

– у розділі «ВГБ»: аналіз можливостей неправильного використання засобів захисту — аналіз керівництв із адміністрування;

– у розділі аналіз стійкості засобів захисту – оцінка стійкості засобів захисту;

– у розділі «ВГБ»: аналіз продукту на наявність уразливостей – виявлення вразливостей розробником продукту.

Цей рівень дозволяє отримати максимальний ступінь гарантій, який не потребує ніяких змін у звичайній процедурі розроблення, оскільки всі регламентовані ним заходи, спрямовані на забезпечення гарантій, застосовуються на етапі проектування.

Для цього рівня проводяться ті ж види аналізу, що й для другого рівня, але на доповнення до матеріалів тестування специфікацій функцій захисту від розробника вимагається надання результатів архітектури захисту ІТ-продукту. Вимоги до процесу створення продукту доповнюються використанням засобів управління конфігурацією проекту.

Рівень розширює вимоги попереднього за рахунок більш повного тестування функцій захисту та засобів їхньої реалізації, а також застосуванням заходів, які дають упевненість у тому, що ІТ-продукт не був підмінений у процесі розроблення.

Методичне розроблення, тестування та аналіз. Рівень методичного розроблення, тестування й аналізу – четвертий рівень гарантій, призначений для використання при обставинах, коли розробники або користувачі вимагають помірного або високого ступеню незалежного підтвердження гарантій захисту ІТ- продукту та готові нести певні додаткові витрати.

Відповідає наступним вимогам гарантій безпеки.

У класі ВГБ: управління проектом:

– у розділі «ВГБ»: засоби управління проектом – застосування автоматизованих засобів управління проектом;

– у розділі «ВГБ»: управління версіями – авторизація розробників при поновленні версій;

– у розділі «ВГБ»: конфігурація проекту – включення до складу конфігурації проекту виявлених помилок й уразливостей.

У класі ВГБ: дистрибуція:

– у розділі «ВГБ»: постачання – виявлення спотворень у процесі поставки;

– у розділі «ВГБ»: установлення, настроювання, запуск – регламентовані процедури установлення, настроювання, запуску.

У класі ВГБ: розроблення:

– у розділі «ВГБ»: загальні функціональні специфікації – неформальні специфікації для усіх інтерфейсів засобів захисту;

– у розділі «ВГБ»: архітектура захисту – відповідність архітектури захисту політиці безпеки;

– у розділі ВГВ: форма надання продукту на сертифікацію – опис реалізації обмеженої підмножини засобів захисту;

– у розділі «ВГБ»: часткові специфікації засобів захисту – неформальні часткові специфікації засобів захисту;

– у розділі «ВГБ»: відповідність описів різною рівня – неформальне підтвердження відповідності;

– у розділі «ВГБ»: політика безпеки – неформальний опис політики безпеки.

У класі ВГБ: документація:

– у розділі керівництво адміністратора – адміністрування засобів захисту;

– у розділі «ВГБ»: керівництво користувача – використання засобів захисту.

У класі ВГБ: процес розроблення:

– у розділі «ВГБ»: безпека середовища розроблення – застосування заходів безпеки у ході розроблення;

– у розділі «ВГБ»: технологія розроблення – визначена розробником технологія розроблення;

– у розділі «ВГБ»: засоби розроблення – використання певного набору засобів розроблення.

У класі ВГБ: тестування:

– у розділі «ВГБ»: повнота тестування – аналіз повноти тестування;

– у розділі «ВГБ»: глибина тестування – архітектура;

– у розділі «ВГБ»: методика тестування – функціональне тестування й протоколювання результатів тестів;

– у розділі «ВГБ»: незалежне тестування – вибіркове незалежне тестування.

У класі ВГБ: оцінка вразливостей:

– у розділі «ВГБ»: аналіз можливостей неправильного використання засобів захисту – підтвердження повноти керівництв з адміністрування й безпеки їхньою застосування;

– у розділі «Аналіз стійкості засобів захисту» – оцінка стійкості засобів захисту;

– у розділі «ВГБ»: аналіз продукту на наявність уразливостей – незалежний аналіз уразливостей.

Цей рівень, незважаючи на достатню сильні вимоги, не потребує від розробника спеціальних знань у галузі розроблення захищених систем і застосування спеціальних методів і технологій, які відрізняються від загальноприйнятих. Це найвищий рівень гарантій, на який можна розраховувати без значних додаткових економічних витрат.

На відміну від попередніх рівнів для сертифікації продукції на четвертий рівень гарантій аналізу піддаються всі інтерфейси без виключення, усі часткові специфікації, а також деталі реалізації засобів захисту. Крім того, повинна бути представлена неформальна політика безпеки.

Додатково до попереднього рівня результати аналізу піддаються незалежним дослідженням уразливостей засобів захисту, які демонструють стійкість системи проти слабких атак. Вимоги до процесу створення продукту розширюються додатковими вимогами застосування автоматизованих засобів управління конфігурацією.

Даний рівень відрізняється від попереднього посиленням вимог до процесу проектування та розроблення, а також підсиленням заходів, які гарантують, що ІТ-продукт не був підміненим у процесі створення.

Напівформальні методи розроблення та тестування. Рівень напівформальних методів розроблення та тестування – п’ятий рівень гарантій, призначений для використання у тих випадках, коли розробники або користувачі вимагають високого ступеню незалежного підтвердження гарантій засобів захисту, а також суворого застосування певних технологій розроблення ІТ-продукту, але без надмірних витрат.

Відповідає наступним вимогам гарантій безпеки.

У класі ВГБ: управління проектом:

– у розділі «ВГБ»: засоби управління проектом – застосування автоматизованих засобів управління проектом;

– у розділі «ВГБ»: управління версіями – авторизація розробників при поновленні версій;

– у розділі «ВГБ»: конфігурація проекту – включення до складу конфігурації проекту інструментальних засобів розроблення.

У класі ВГБ: дистрибуція:

– у розділі «ВГБ»: постачання – виявлення спотворень у процесі поставки;

– у розділі «ВГБ»: установлення, настроювання, запуск – регламентовані процедури установлення, настроювання, запуску.

У класі ВГВ: розроблення:

– у розділі «ВГБ»: загальні функціональні специфікації – напівформальні специфікації для засобів захисту;

– у розділі «ВГБ»: архітектура захисту – папівформальний опис архітектури захисту;

– у розділі «ВГБ»: форма надання продукту на сертифікацію – повний опис реалізації усіх засобів захисту;

– у розділі «ВГБ»: структура засобів захисту – модульність;

– у розділі «ВГБ»: часткові специфікації засобів захисту – неформальні часткові специфікації засобів захисту;

– у розділі «ВГБ»: відповідність описів різного рівня – напівформальне підтвердження відповідності;

– у розділі «ВГБ»: політика безпеки – формальна модель політики безпеки.

У класі ВГБ: документація:

– у розділі керівництво адміністратора – адміністрування засобів захисту;

– у розділі «ВГБ»: керівництво користувача – використання засобів захисту.

У класі ВГБ: процес розроблення:

– у розділі «ВГБ»: безпека середовища розроблення – застосування заходів безпеки у ході розроблення;

– у розділі «ВГБ»: технологія розроблення – стандартизована технологія розроблення;

– у розділі «ВГБ»: засоби розроблення – використання основних засобів розроблення, що відповідають певним стандартам.

У класі ВГБ: тестування:

– у розділі «ВГБ»: повнота тестування – аналіз повноти тестування;

– розділі «ВГБ»: глибина тестування – функціональні специфікації;

– у розділі «ВГБ»: методика тестування – функціональне тестування й протоколювання результатів і тестів;

– у розділі «ВГБ»: незалежне тестування – вибіркове незалежне тестування.

У класі ВГБ: оцінка вразливостей:

– у розділі «ВГБ»: аналіз прихованих каналів – пошук і документування прихованих каналів;

– у розділі «ВГБ»: аналіз можливостей неправильного використання засобів захисту – підтвердження повноти керівництв із адміністрування й безпеки їхнього заснування;

– у розділі «ВГБ»: аналіз стійкості засобів захисту – оцінка стійкості засобів захисту;

– у розділі «ВГБ»: аналіз продукту на наявність уразливостей – систематичний аналіз уразливостей на основі заданих методик.

Цей рівень вимагає від розробника застосування певних технологій і методів розроблення, проте їх використання може обмежуватися проектуванням і реалізацією засобів захисту.

На відміну від попередніх рівнів аналізу піддаються всі засоби захисту без виключення. Крім того, необхідна наявність формальної моделі політики безпеки та папівформальне представлення функціональних специфікацій та архітектури захисту, а також напівформальна демонстрація їхньої взаємної відповідності. Архітектура ІТ-продукту повинна відповідати вимогам модульності.

Додатково до попередніх рівнів для підтвердження результатів аналізу необхідне тестування розробником часткових специфікацій, а аналіз уразливостей повинен демонструвати стійкість проти атак помірної сили, крім

того, необхідна незалежна перевірка проведеного розробником аналізу схованих каналів.

Вимоги до процесу розроблення доповнюються необхідністю розширення складу конфігурації продукту, керованої за допомогою автоматичних засобів.

Таким чином, цей рівень посилює вимоги попереднього у частині напівформального опису процесу проектування та реалізації, більш структуррованої архітектури захисту, більш ретельного аналізу прихованих каналів, більш повного контролю у процесі розроблення.

Напівформальні методи верифікації розроблення та тестування. Рівень напівформальних методів верифікації розроблення та тестування – шостий рівень гарантій, призначений для використання у ситуаціях із високим ступенем ризику, де цінність інформації, що захищається, виправдовує високі додаткові витрати.

Відповідає наступним вимогам гарантій безпеки.

У класі ВГБ: управління проектом:

– у розділі «ВГБ»: засоби управління проектом – повна автоматизація управління проектом і контролю версій;

– у розділі «ВГБ»: управління версіями – контроль цілісності й автентичності дистрибутиву системи;

– у розділі «ВГБ»: конфігурація проекту – включення до складу конфігурації проекту інструментальних засобів розроблення.

У класі ВГБ: дистрибуція:

– у розділі «ВГБ»: постачання – виявлення спотворень у процесі поставки;

– у розділі «ВГБ»: установлення, настроювання, запуск – регламентовані процедури установлення, настроювання, запуску.

У класі «ВГБ»: розроблення:

– у розділі «ВГБ»: загальні функціональні специфікації – напівформальні специфікації для засобів захисту;

– у розділі «ВГБ»: архітектура захисту – відповідність напівформального опису архітектури захисту політиці безпеки;

– у розділі «ВГБ»: форма падання продукту на сертифікацію – структурований опис реалізації усіх засобів захисту;

– у розділі «ВГБ»: структура засобів захисту – ієрархічність;

– у розділі «ВГБ»: часткові специфікації засобів захисту – напівформальні часткові специфікації засобів захисту;

– у розділі «ВГБ»: відповідність описів різною рівня – напівформальне доведення відповідності;

– у розділі «ВГБ»: політика безпеки – формальна модель політики безпеки.

У класі «ВГБ»: документація:

– у розділі керівництво адміністратора – адміністрування засобів захисту;

– у розділі «ВГБ»: керівництво користувача – використання засобів захисту.

У класі «ВГБ»: процес розроблення:

– у розділі «ВГБ»: безпека середовища розроблення – підтвердження заходів безпеки у ході розроблення;

– у розділі «ВГБ»: технологія розроблення – стандартизована технологія розроблення;

– у розділі «ВГБ»: засоби розроблення – використання тільки засобів розроблення, що відповідають певним стандартам.

У класі ВГБ: тестування:

– у розділі «ВГБ»: повнота тестування – суворий аналіз повноти тестування;

– у розділі «ВГБ»: глибина тестування – функціональні специфікації;

– у розділі «ВГБ»: методика тестування – тестування у відповідності з певною методикою;

– у розділі «ВГБ»: незалежне тестування – вибіркове незалежне тестування.

У класі ВГБ: оцінка вразливостей:

– у розділі «ВГБ»: аналіз прихованих каналів – пошук прихованих каналів на основі певних методів;

– у розділі аналіз можливостей неправильного використання засобів захисту – незалежний аналіз можливостей неправильного використання засобів захисту;

– у розділі аналіз стійкості засобів захисту – оцінка стійкості засобів захисту;

– у розділі «ВГБ»: аналіз продукту на наявність уразливостей – вичерпний аналіз уразливостей.

Даний рівень вимагає суворого та послідовного застосування певних методів проектування та розроблення, які дозволяють забезпечувати гарантії захисту при експлуатації в умовах підвищеного ризику.

Вимоги цього рівня доповнюють попередні необхідністю структурного опису реалізації продукту та напівформального подання часткових специфікацій, а також вимогою багаторівневої архітектури.

Для підтвердження результатів аналізу, крім заходів, передбачених таким рівнем, аналіз уразливостей має демонструвати стійкість системи проти сильних атак, мають бути отримані незалежні підтвердження проведення розробником систематичного пошуку схованих каналів.

Вимоги до процесу розроблення розширюються необхідністю структурування цього процесу та повної автоматизації управління конфігурацією проекту.

Рівень розширює вимоги попереднього застосуванням більш глибокого аналізу, структуризацією представлення ІТ-продукту, багаторівневою архітектурою, посиленням аналізу вразливостей, застосуванням систематичного пошуку схованих каналів, а також удосконаленням управління конфігурацією та середовища розроблення.

Рівень формальних методів верифікації розроблення та тестування – сьомий рівень гарантій, призначений для використання у ситуаціях із виключно високим ступенем ризику, (або) там, де цінність об’єктів, які захищаються, виправдовує високі додаткові витрати. Практичне застосування цього рівня на даний час обмежене компаніями ІТ-продуктами, в яких сконцентровані засоби захисту, та які легко піддаються формальному аналізу.

Сьомий рівень гарантій відповідає таким вимогам гарантій безпеки.

У класі ВГБ: управління проектом:

– у розділі «ВГБ»: засоби управління проектом – повна автоматизація управління проектом і контролю версій;

– у розділі «ВГБ»: управління версіями – контроль цілісності й автентичності дистрибутива типа системи;

– у розділі «ВГБ»: конфігурація проекту – включення до складу конфігурації проекту інструментальних засобів розроблення.

У класі ВГБ: дистрибуція:

– у розділі «ВГБ»: постачання – захист від спотворень у процесі поставки;

– у розділі «ВГБ»: установлення, настроювання, запуск – регламентовані процедури установлення, настроювання, запуску.

У класі ВГБ: розроблення:

– у розділі «ВГБ»: загальні функціональні специфікації – формальні специфікації для засобів захисту;

– у розділі «ВГБ»: архітектура захисту – формальний опис архітектури захисту й доведення її відповідності політиці безпеки;

– у розділі «ВГБ»: форма надання продукту на сертифікацію – структурований опис реалізації усіх засобів захисту;

– у розділі «ВГБ»: структура засобів захисту – мінімізація складності;

– у розділі «ВГБ»: часткові специфікації засобів захисту – напівформальні часткові специфікації засобів захисту;

– у розділі «ВГБ»: відповідність описів різного рівня – формальне доведення відповідності;

– у розділі «ВГБ»: політика безпеки – формальна модель політики безпеки.

У класі ВГБ: документація:

– у розділі «ВГБ»: керівництво адміністратора – адміністрування засобів захисту;

– у розділі «ВГБ»: керівництво користувача – використання засобів захисту.

У класі ВГБ: процес розроблення:

– у розділі «ВГБ»: безпека середовища розроблення – підтвердження заходів безпеки у ході розроблення;

– у розділі «ВГБ»: технологія розроблення – технологія розроблення, яка дозволяє оцінювати продукт, що розроблюється;

– у розділі «ВГБ»: засоби розроблення – використання тільки засобів розрозроблення відповідають певним стандартам.

У класі ВГБ: тестування:

– у розділі «ВГБ»: повнота тестування – суворий аналіз повноти тестування;

– у розділі «ВГБ»: методика тестування – тестування у відповідності з певною методикою;

– у розділі «ВГБ»: глибина тестування – реалізація;

– у розділі «ВГБ»: незалежне тестування – повне незалежне тестування.

У класі ВГБ: оцінка вразливостей:

– у розділі «ВГБ»: аналіз схованих каналів – пошук схованих каналів на основі певних методів;

– у розділі «ВГБ»: аналіз можливості неправильного використання засобів захисту (ЗЗ) – незалежний аналіз можливостей неправильного використання ЗЗ;

– у розділі «ВГБ»: аналіз стійкості засобів захисту – оцінка стійкості засобів захисту;

– у розділі «ВГБ»: аналіз продукту на наявність уразливостей – вичерпний аналіз уразливостей .

На відміну від попередніх рівнів необхідне формальне подання функціональних специфікацій та архітектури захисту, а також формальна та напівформальна демонстрація відповідності між ними. Архітектура системи повинна бути не тільки модульною, але й простою та зрозумілою.

Додатково до попередніх рівнів результати аналізу вимагають підтвердження тестуванням форми реалізації, а також обґрунтованих незалежним підтвердженням усіх результатів, проведених розробником випробувань. Таким чином, цей рівень підсилює вимоги попереднього за рахунок більш послідовного аналізу з використанням формального опису системи на різних рівнях подання та формального доведення взаємної відповідності цих описів, а також всеохоплюючого тестування.

Накоплений практичний досвід і теорія захищених систем забезпечили розвиток «Загальних критеріїв». У 1999 році вийшла версія 2.1, у 2005 році – версія 2.3, а у 2009 році – версія 3.1. Найбільших змін зазнала частина 3 «Вимоги гарантій безпеки», де наведені методи забезпечення гарантій. Суть змін зводиться до наступного.

У класах *оцінювання завдання безпеки* й *оцінювання профілю захищеності* систематизовані вимоги до описів, що використовуються для формулювання цілей безпеки та профілів захищеності. Проведені переопрацювання спрямовані на доведення таких вимог до якості визначення описів припущень, загроз, політики безпеки організації, завдань безпеки, які б сприяли досягненню основної мети формування загальної специфікації об’єкта оцінювання: демонстрації того, як об’єкт оцінювання задовольняє вимогам до нього.

Чотири класи: управління проектом, дистрибуція, документація та процес розроблення, реорганізовані у два класи: *процес розроблення*, що описує вимоги, які відносяться до процесу розроблення об’єкта оцінювання, та *документація*, що описує всі вимоги, які відносяться до його впровадження та використання.

У версії 3.1 клас *розроблення* відображає збалансовану шкалу посилення вимог гарантій та відповідно обсягів роботи. Текст описує як принципи, що покладені в основу аналізу безпеки, так і те, яким чином ефективно сконцентрувати зусилля з їхнього втілення.

Клас *оцінювання вразливостей* тепер складається тільки з одного розділу «Аналіз уразливостей». Оцінювач повинен враховувати стійкість послуг безпеки до атак.

Питання для самоконтролю

1. Охарактеризуйте загальну структуру критеріїв гарантій безпеки НД ТЗІ 2.5-004-99.

2. Поясніть зміст вимог до рівня гарантій ГІ (Г2-Г7) за НД ТЗІ 2.5-004-99.

3. Поясніть різницю між рівнями гарантій реалізації політики безпеки Г1 і Г2. Наведіть приклади.

4. Поясніть різницю між рівнями гарантій реалізації політики безпеки Г та Г3. Наведіть приклади.

5. Поясніть різницю між рівнями гарантій реалізації політики безпеки Г3 та Г4. Наведіть приклади.

6. Опишіть структуру та надайте коротку характеристику вимог гарантій безпеки відповідно до міжнародного Стандарту ISO 15408.

7. Охарактеризуйте структуру вимог до гарантій безпеки класу «Управління проектом».

8. Охарактеризуйте структуру вимог до гарантій безпеки класу «Дистрибуція».

9. Охарактеризуйте структуру вимог до гарантій безпеки класу «Розроблення».

10. Охарактеризуйте структуру вимог до гарантій безпеки класу «Документації».

11. Охарактеризуйте структуру вимог до гарантій безпеки класу «Процес розроблення».

12. Охарактеризуйте структуру вимог до гарантій безпеки класу «Тестування».

13. Охарактеризуйте структуру вимог до гарантій безпеки класу «Оцінка управління».

14. Опишіть структуру та надайте стислу характеристику рівнів гарантій безпеки відповідно до міжнародного стандарту ISO 15408.

15. Охарактеризуйте структуру вимог до гарантій безпеки рівня «Функціональне тестування».

16. Охарактеризуйте структуру вимог до гарантій безпеки рівня «Структурне тестування».

17. Охарактеризуйте структуру вимог до гарантій безпеки рівня «Методичне розроблення та перевірка».

18. Охарактеризуйте структуру вимог до гарантій безпеки рівня «Методичне розроблення, тестування й аналіз».

19. Охарактеризуйте структуру вимог до гарантій безпеки рівня «'Напівформальні методи розроблення та тестування».

20. Охарактеризуйте структуру вимог до гарантій безпеки рівня «Напівформальні методи верифікації розроблення та тестування».

21. Охарактеризуйте структуру вимог до гарантій безпеки рівня «Формальні методи верифікації розроблення та тестування».

Додаток 1

ТЕРМІНИ ТА ВИЗНАЧЕННЯ У СФЕРІ ОЦІНКИ ІНФОРМАЦІЙНОЇ ЗАХИЩЕНОСТІ ТЕЛЕКОМУНІКАЦІЙ

У цьому навчальному посібнику застосовуються терміни та визначення, встановлені ДСТУ 3396.2-97, НД ТЗІ 1.1-003-99 і НД ТЗІ 2.6-001-11.

Зокрема, використано такі терміни та визначення.

Верифікація – одинична дія у процесі проведення оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки, яка передбачає виконання детального дослідження змісту матеріалів із метою прийняття рішення про достатність наведених у них аргументів на користь коректності доказів.

Випробування – експериментальне визначення кількісних та/або якісних характеристик властивостей об'єкта експертизи за результатом впливу на нього під час його функціонування.

Внутрішньосистемний інтерфейс – визначена Розробником сукупність засобів, методів і правил взаємодії між складовими частинами (підсистемами, компонентами, модулями) об'єкта експертизи.

Дослідження – одинична дія у процесі проведення експертизи, яка передбачає виконання поглибленого аналізу змісту матеріалів на предмет відповідності висунутим вимогам із використанням спеціальних знань і досвіду Експерта.

Ефективність – властивість об'єкта експертизи, що характеризується мірою досягнення цілей, поставлених під час його створення.

Засіб випробувань – програмний, програмно-апаратний або апаратний засіб, що використовується з метою здійснення перевірок у процесі проведення випробувань.

Засіб технічного захисту інформації від несанкціонованого доступу – програмний, апаратний або програмно-апаратний засіб, який створюється як окремий продукт виробництва, має необхідну проектну та/або експлуатаційну документацію та забезпечує самостійно або у комплексі з іншими засобами захист від загроз несанкціонованого доступу для інформації, оброблюваної в інформаційно-телекомунікаційній системі.

Захищений від несанкціонованого доступу компонент обчислювальної системи – програмний, апаратний або програмно-апаратний засіб, в якому додатково до основного призначення передбачено функції захисту інформації від загроз несанкціонованого доступу.

Захищеність інформації – характеристика рівня безпеки інформації, оброблюваної у певній інформаційно-телекомунікаційній системі (ІТС).

Зовнішній інтерфейс – визначена Розробником сукупність засобів, методів і правил взаємодії між об'єктом експертизи й іншими відносно нього об'єктами (користувачами, процесами, системами тощо).

Інформаційна модель процесу – модель процесу, подана у вигляді опису істотних для розгляду вхідних, вихідних і внутрішніх параметрів процесу та зв'язків між ними, яка дозволяє моделювати зміну вихідних параметрів процесу залежно від зміни певних його вхідних і внутрішніх параметрів.

Інформаційна система – організаційно-технічна система, в якій реалізується технологія оброблення інформації з використанням технічних і програмних засобів.

Інформаційний ресурс – будь-які дані в електронному вигляді, які обробляються або зберігаються в інформаційно-телекомунікаційній системі.

Інформаційно-телекомунікаційна система – сукупність інформаційних і телекомунікаційних систем, які у процесі оброблення інформації діють як єдине ціле.

Комплекс технічного захисту інформації – сукупність організаційних, інженерних і технічних заходів і засобів, призначених для захисту від витоку інформації з обмеженим доступом технічними каналами на об'єктах інформаційної діяльності.

Комплексна система захисту інформації (КСЗІ) – сукупність організаційних та інженерно-технічних заходів, програмно-апаратних засобів, які забезпечують захист інформації в інформаційно-телекомунікаційних системах у відповідності з вимогами нормативно-правових документів у галузі захисту інформації.

Метод випробувань – визначений (встановлений) спосіб виконання перевірок у процесі проведення випробувань.

Методика випробувань – визначені (встановлені) способи проведення випробувань.

Методика експертизи – визначені (встановлені) способи проведення експертних робіт у ході експертизи.

Методика перевірки дотримання вимог до рівня гарантій – визначені (встановлені) способи проведення перевірки дотримання вимог до рівня гарантій коректності реалізації функціональних послуг безпеки.

Об'єкт експертизи – засіб технічного захисту інформації від несанкціонованого доступу, захищений від несанкціонованого доступу компонент обчислювальної системи або комплексу засобів захисту комплексної системи захисту інформації, комплексна система захисту інформації, стосовно яких здійснюється експертиза у сфері технічного захисту інформації.

Об'єкт інформаційної діяльності – будівлі, приміщення, транспортні засоби чи інші інженерно-технічні споруди, функціональне призначення яких передбачає обіг інформації з обмеженим доступом.

Оцінювання – визначення міри відповідності характеристик об'єкта експертизи заданим критеріям і вимогам.

Перевірка – одинична контрольна дія у процесі проведення експертизи.

Працездатність – характеристика стану об'єкта експертизи (складової частини, компонента), що відображає його здатність виконувати певні функції із заданою ефективністю та протягом потрібного часу.

Програма випробувань – документована сукупність вимог, що підлягає перевірці у процесі проведення випробувань.

Програма експертизи – документована сукупність вимог, що підлягає перевірці у процесі проведення експертизи.

Програма перевірки рівня гарантій – документована сукупність вимог, що підлягають перевірці у процесі експертизи оцінюваного об'єкта експертизи, на відповідність вимогам до рівня гарантій коректності реалізації функціональних послуг безпеки.

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

Тестова процедура – документально зафіксована послідовність виконання перевірок у процесі проведення випробувань.

Тестове покриття – міра, що характеризує здатність тестових даних випробовувати вимоги до об'єкта експертизи.

Тестові дані – дані, що використовуються як вхідні у процесі проведення випробувань об'єкта експертизи.

Технічний захист інформації (ТЗІ) – діяльність, спрямована на запобігання витоку інформації технічними каналами, її блокування та (чи) порушення цілісності. ТЗІ є важливою складовою протидії втраті, зміні, модифікації та перехопленню інформації, що становить державну таємницю, або конфіденційної інформації з обмеженим доступом. З метою забезпечення ТЗІ на об'єкті інформаційної діяльності використовуються організаційні й інженерно-технічні заходи.

Технічний канал витоку інформації – сукупність носіїв інформації, середовища її поширення та засобів технічної розвідки.

Функціональна послуга безпеки – сукупність функцій, що визначені відповідно до вимог НД ТЗІ 2.5-004-99 і забезпечують захист інформації від певної загрози або від множини загроз.

Функціональна специфікація об'єкта експертизи – впорядкований перелік реалізованих в об'єкті експертизи функціональних послуг безпеки згідно з НД ТЗІ 2.5-004-99 разом із описом їх політики або іншим чином визначений перелік функцій захисту з описом їх політик згідно вимог міжнародних стандартів.

Література

1. Рекомендація МСЕ-Т X.800 (ISO 7498-2). Архітектура безпеки взаємодії відкритих систем для застосувань МККТ (Security Architecture for Open System Interconnection for CCIT applications). – Женева, 1991. – 48 с.
2. Закон України „Про захист інформації в інформаційно-телекомунікаційних системах”.
3. «Положення про державну експертизу у сфері технічного захисту інформації». Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 16.05.2007, № 93. Зареєстровано в Міністерстві юстиції України 16.07.2007 за № 820/14087. – 13 с.
4. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О.М. Новіков. – К.: Видавнича група ВНУ, 2009. – 608 с.
5. ДСТУ ISO 15408-1: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 1. Вступ і загальна модель.
6. ДСТУ ISO 15408-2: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 2. Функціональні вимоги безпеки.
7. ДСТУ ISO 15408-3: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 3. Вимоги до забезпечення захисту.
8. ДСТУ ISO 17799: 2005. Інформаційні технології. Методи захисту. Практичні рекомендації з управління інформаційної безпеки.
9. Тардаскіна Т.М. Менеджмент інформаційної безпеки в галузі зв’язку: навч. посіб. / Т.М. Тардаскіна, В.Г. Кононович; За заг. ред. М.В. Захарченка. – Одеса: ОНАЗ ім. О.С. Попова, 2011. – 272 с.
10. Зайцев А.П. Технические средства и методы защиты информации: Учебник для вузов / [А.П Зайцев., А.А. Шелупанов, Р.В. Мещеряков и др.]; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009. – 508 с.
11. CCITT Recommendation X.200 (ISO 7498). Reference model of open systems interconnection for CCITT applications. Geneva, 1988. – 49 p.
12. Кононович В. Г. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Частина 3. Архітектура безпеки. Концепція захисту інформації : [навч. посібник для вузів, затверджено Міністерством транспорту та зв’язку України] / Кононович В. Г. – Одеса: ОНАЗ, 2009. – 194 с.
13. Тардаскін М.Ф. Технічний захист комерційної таємниці підприємства зв’язку: навч. посіб. / М.Ф. Тардаскін, В.Г. Кононович. – Одеса: ОНАЗ, 2002.
14. Богуш В.М. Теоретичні основи захищених інформаційних технологій: навч. посіб. / В.М. Богуш, О.А. Довидьков, В.Г. Кривуца. – К.: ДУІКТ, 2010. – 454 с.
15. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу [Електронний ресурс] / Затверджено наказом № 22 ДСТСЗІ СБУ від 28.04.1999. – 30 с. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40393&cat_id=38835.
16. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу [Електронний ресурс] / Затверджено наказом № 22 ДСТСЗІ СБУ від 28.04.1999. – 19 с. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=403968&cat_id=38835.
17. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах НД від несанкціонованого доступу [Електронний ресурс] / Затверджено наказом № 22 ДСТСЗІ СБУ від 28.04.1999. – 57 с. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=403868&cat_id=38835.
18. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс] / Затверджено наказом № 22 ДСТСЗІ СБУ від

28.04.1999. – К.: ДСТСЗІ СБ України, 1999. – 20 с. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=403818&cat_id=38835.

19. НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження і модернізації засобів технічного захисту інформації від несанкціонованого доступу [Електронний ресурс] / Затверджено наказом № 60 ДСТСЗІ СБУ від 20.12.2000 – 16 с. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=39726&cat_id=38835.

20. НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 [Електронний ресурс] / Затверджено наказом № 84 ДСТСЗІ СБУ від 13.12.2002. – К.: ДСТСЗІ СБ України, 2002. – 30 с. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=39565&cat_id=38835.

21. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу / Затверджено наказом № 33 ДСТСЗІ СБУ від 02.04.2003. – К.: ДСТСЗІ СБ України, 2003. – 16 с. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=39560&cat_id=38835.

22. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах / Затверджено наказом Адміністрації Держспецзв'язку № 112 від 04.07.2008. – К.: Адм. Держспецзв'язку, 2003. – 9 с. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=72978&cat_id=38835.

23. НД ТЗІ 2.7-009-09. Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу / Затверджено наказом Адміністрації ДССЗЗІ України від 24.07.2009, № 172. – К.: Адм. Держспецзв'язку, 2009. – 175 с. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=78972&cat_id=38835.

24. НД ТЗІ 2.7-010-09. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу / Затверджено наказом Адміністрації ДССЗЗІ України від 24.07.2009, № 172. – К.: Адм. Державної служби спеціального зв'язку та захисту інформації України, 2009. – 137 с. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=78972&cat_id=38835.

25. Бабак В.П. Інформаційна безпека та сучасні мережеві технології. Англо-українсько-російський словник // В.П. Бабак, О.Г. Корченко. – К.: НАУ, 2003. – 670 с.

26. Рекомендация МСЭ-Т Е.408. Требования к безопасности сетей электросвязи. – 30 с.

27. ДСТУ ISO/IEC 15408-1:2010. Інформаційні технології. Методи захисту. Критерії оцінювання ІТ-безпеки. Частина 1. Вступ і загальна модель. – 72 с.

28. ДСТУ ISO/IEC 15408-2:2010. Інформаційні технології. Методи захисту. Критерії оцінювання ІТ-безпеки. Частина 2. Функціональні компоненти безпеки. – 240 с.

29. ДСТУ ISO/IEC 15408-3:2010. Інформаційні технології. Методи захисту. Критерії оцінювання ІТ-безпеки. Частина 3. Компоненти гарантій безпеки. – 201 с.

30. Мартемьянов Ю.Ф., Экспертные методы принятия решений: учебн. пособ. / Ю.Ф. Мартемьянов, Т.Я. Лазарева. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2010. – 41 с.

31. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко. – М.: Компания «АйТи» ; ДМК «Пресс», 2004. – 302 с.

32. Колпаков В.М. Теория и практика принятия управленческих решений: учеб. пособ. / В.М.Колпаков. – К.: МАУП, 2000. – 504 с.

33. Литвак И Г. Экспертные оценки и принятие решений / И Г. Литвак. – М.: Патент, 1996. – 184 с.

34. Петренко А.А. Оціни свій ризик / А.А. Петренко, С.А. Петренко // IT Manager. – 2002. – № 6.

35. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы средств / В.Ф.Шаньгин. – М.: ДМК Пресс, 2008. – 544 с.

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

37. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах / Затверджено наказом Адміністрації ДССЗЗІ України від 25.03.2011, № 65. – К.: Адм. Державної служби спеціального зв'язку та захисту інформації України, 2011. – 104 с.

38. НД ТЗІ ТПКО-95. Тимчасове положення про категоріювання об'єктів / Затверджено наказом Державного комітету країни з питань державних секретів та технічного захисту інформації від 10.07.95 № 35. – К., 1995. – 9 с.

39. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах / Затверджено постановою Кабінету Міністрів України від 29 березня 2006 р. № 373. – К., 2006. – 6 с.

40. НД ТЗІ 2.5-007-2007. Требования к комплексу средств защиты информации, которая представляет государственную тайну, от несанкционированного доступа при обработке ее в автоматизированных системах класса «1».

41. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – К., 2005. – 21 с.

42. ДСТУ 3396 1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

43. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. – К., 1999. – 16 с.

44. ДСТУ ISO/IEC TR 13335-2:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 2. Керування та планування безпеки інформаційних технологій. – К., 2003. – 18 с.

45. Положення про технічний захист інформації в Україні / Затверджене Указом Президента України від 27 вересня 1999 р. № 1229/99. – К., 1999. – 6 с.

46. ГОСТ 34.201-89. Виды, комплектность и обозначение документов при создании автоматизированных систем. – М., 1989. – 7 с.

47. РД 50-34.698-90. Методические указания. Автоматизированные системы. Требования к содержанию документов. – М., 1990. – 24 с.

Навчальне видання

Сергій Михайлович Горохов,
Наталія Володимирівна Кондратьєва,
Володимир Григорович Кононович,
Сергій Володимирович Стайкуца

ПРОГРАМИ ТА МЕТОДИКИ ДЕРЖАВНОЇ ЕКСПЕРТИЗИ ІНФОРМАЦІЙНОЇ ЗАХИЩЕНОСТІ ТЕЛЕКОМУНІКАЦІЙ

Навчальний посібник

Редактор *Л.А. Кодрул*
Комп'ютерне верстання *Ж.А. Гардиман*

Видавець і виготовлювач ОНАЗ ім. О.С. Попова
(Свідоцтво ДК № 3633 від 27.11.09)
м. Одеса, вул. Ковальська, 1

Здано до набору 14.12.11. Підписано до друку 11.05.12.
Обсяг 11,7 ум.-друк. арк.
Формат 90х60/16. Зам. № 4853. Наклад 300 прим.
Віддруковано на видавничому устаткуванні фірми RISO
в друкарні редакційно-видавничого центру ОНАЗ ім. О.С. Попова
Одеса, 65021, вул. Ковалевського, 5
Тел. (0482) 705-04-94