Розділ 16. Проектування, створення, супровід комплексних систем захисту інформації (КСЗІ)

16.1. Дослідження середовищ функціонування ІС – середовища користувачів, обчислювальної системи, фізичного середовища, інформаційного середовища та побудова моделі загроз.

16.2. Проведення аудиту інформаційної безпеки (ІБ) та визначення її рівня на основі звіту з аудиту ризиків ІБ.

16.3. Вибір методів та засобів забезпечення необхідного рівня ІБ.

16.1. Дослідження середовищ функціонування інформаційної системи (ІС) – середовища користувачів, обчислювальної системи, фізичного середовища, інформаційного середовища та побудова моделі загроз

Розгляд даного питання зробимо, спираючись на поради (рекомендації) щодо створення **комплексних систем захисту інформації (КСЗІ)** в **інформаційно-телекомунікаційних системах (ІТС)**, які використовуються для надання послуг доступу до мережі Інтернет від Державної служби спеціального зв'язку та захисту інформації України, розроблених на основі **НД ТЗІ 3.7-003-05** «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі») (https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet)

Комплексна система захисту інформації (КСЗІ) – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС.

До складу КСЗІ входять заходи та засоби, які реалізують методи, механізми захисту інформації від несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів та ін;

Для організації робіт зі створення КСЗІ в ІТС **створюється служба захисту інформації, порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000**.

Комплекс засобів захисту (КЗЗ) – сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

Етапи створення КСЗІ

Дозволяється виключати окремі етапи робіт або поєднувати декілька етапів, а також включати нові етапи робіт. За необхідністю дозволяється змінювати послідовність виконання окремих етапів – виконувати одночасно

декілька етапів робіт, окремі етапи виконувати до завершення попередніх і т.п., якщо це не призводить до зниження якості робіт і не суперечить цілям їх виконання.

1 Формування загальних вимог до КСЗІ в ІТС

1.2 Обстеження середовищ функціонування ІТС

1.2.1 Під час виконання цих робіт ІТС розглядається як організаційно-технічна система, яка поєднує:

– обчислювальну систему;

– фізичне середовище;

– середовище користувачів;

– оброблювану інформацію і технологію її обробки (далі – середовища функціонування ІТС).

1.2.2 Метою обстеження є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт.

Слід враховувати, що середовища функціонування є множинами, що перетинаються, окремі їхні елементи можуть входити одночасно до різних середовищ і мати в них різні якості. Наприклад, програмне забезпечення може розглядатись обчислювальною системою як об’єкт-процес, а в інформаційному середовищі – як пасивний об’єкт КС.

1.2.3 Обстеження виконується, коли розроблена концепція ІТС (основні принципи і підходи побудови), визначені основні завдання і характеристики ІТС, функціональних комплексів ІТС та існує варіант(и) їх реалізації.

1.2.4 **При обстеженні обчислювальної системи** ІТС повинні бути проаналізовані й описані:

– загальна структурна схема і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо);

– види і характеристики каналів зв'язку;

– особливості взаємодії окремих компонентів, їх взаємний вплив один на одного;

– можливі обмеження щодо використання засобів та ін.

Мають бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів, їхні властивості і характеристики, в тому числі ті, що встановлюються за умовчанням та ін.

Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІТС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

1.2.5 **При обстеженні інформаційного середовища** аналізу підлягає вся інформація, що обробляється, а також зберігається в ІТС (дані і програмне забезпечення). Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, визначені й описані види (в термінах об'єктів КС) її представлення в ІТС.

Для кожного виду інформації і типу об'єкта, в якому вона міститься, ставляться у відповідність властивості захищеності інформації (конфіденційність, цілісність, доступність) чи КС (спостережність), яким вони повинні задовольняти.

Аналіз технології обробки інформації повинен виявити особливості обігу електронних документів, мають бути визначені й описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків та місця їх призначення, принципи та методи керування інформаційними потоками, складені структурні схеми потоків. Фіксуються види носіїв інформації та порядок їх використання під час функціонування ІТС.

Для кожного структурного елемента схеми інформаційних потоків фіксуються склад інформаційних об'єктів, режим доступу до них, можливий вплив на нього (елементу) елементів середовища користувачів, фізичного середовища з точки зору збереження властивостей інформації.

1.2.6 **При обстеженні фізичного середовища** здійснюється аналіз взаємного розміщення засобів обробки інформації ІТС на об'єктах інформаційної діяльності, комунікацій, систем життєзабезпечення і зв'язку, а також режим функціонування цих об'єктів.

Порядок проведення обстеження повинен відповідати ДСТУ 3391.

Аналізу підлягають такі **характеристики фізичного середовища**:

– територіальне розміщення компонентів ІТС (генеральний план, ситуаційний план);

– наявність охорони території та перепускний режим;

– наявність категорійованих приміщень, в яких мають розміщуватися компоненти ІТС;

– режим доступу до компонентів фізичного середовища ІТС;

– вплив чинників навколишнього середовища, захищеність від засобів технічної розвідки;

– наявність елементів комунікацій, систем життєзабезпечення і зв'язку, що мають вихід за межі контрольованої зони;

– наявність та технічні характеристики систем заземлення;

– умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації;

– наявність проектної та експлуатаційної документації на компоненти фізичного середовища.

1.2.7 **При обстеженні середовища користувачів** здійснюється аналіз:

– функціонального та кількісного складу користувачів, їхніх функціональних обов'язків та рівня кваліфікації;

– повноважень користувачів щодо допуску до відомостей, які обробляються в ІТС, доступу до ІТС та її окремих компонентів;

– повноважень користувачів щодо управління КСЗІ;

– рівня можливостей різних категорій користувачів, що надаються (можуть бути доступними) їм засобами ІТС.

– наявності СЗІ в ІТС.

1.2.8 Результати обстеження середовищ функціонування ІТС оформлюються у вигляді акту і включаються, у разі необхідності, до відповідних розділів плану захисту інформації в ІТС (далі – План захисту), який розробляється згідно з НД ТЗІ 1.4-001.

1.2.9 За результатами обстеження середовищ функціонування ІТС затверджується перелік об'єктів захисту (з урахуванням рекомендацій НД ТЗІ 1.4-001, НД ТЗІ 2.5-007, НД ТЗІ 2.5-008, НД ТЗІ 2.5-010 щодо класифікації об'єктів), а також визначаються потенційні загрози для інформації і розробляються **модель загроз** та **модель порушника**. **Побудова моделей** здійснюється відповідно до положень **НД ТЗІ 1.1-002, НД ТЗІ 1.4-001** та **НД ТЗІ 1.6-003**. **Модель загроз для інформації** та **модель порушника** рекомендується оформляти у вигляді окремих документів (або поєднаних в один документ) Плану захисту.

2 Розробка політики безпеки інформації в ІТС

2.1 На цьому етапі здійснюється вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій і т.п., які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій;

2.2 Політика безпеки може розроблятись для ІТС в цілому або, якщо мають місце особливості функціонування окремих компонентів КСЗІ, для окремої компоненти, для окремої функціональної задачі, для окремої технології обробки інформації тощо.

2.3 Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.1-002-99 та рекомендаціями НД ТЗІ 1.4-001-2000.

3 Розробка технічного завдання на створення КСЗІ

3.1 ТЗ на створення КСЗІ в ІТС є засадним організаційно-технічним документом, який визначає вимоги із захисту оброблюваної в ІТС інформації, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію в складі ІТС.

3.3 Для оформлення ТЗ на КСЗІ можуть бути використані такі варіанти:

– у вигляді окремого розділу ТЗ на створення ІТС;

– у вигляді окремого (часткового) ТЗ.

3.4 Перший варіант рекомендується застосовувати для вперше створюваних ІТС. Другий варіант рекомендується застосовувати у випадку модернізації КСЗІ, модернізації діючих ІТС, а також для ІТС, які вже мають затверджене ТЗ на створення, в якому не міститься окремого розділу із захисту інформації.

Вимоги в частині захисту від НСД мають бути викладені відповідно до НД ТЗІ 2.5-004-99 Згідно з цим документом в процесі оцінки захищеності ІТС розглядаються вимоги двох видів: вимоги до функцій (послуг) забезпечення безпеки і вимоги до рівня гарантій. Відповідно, в ТЗ на КСЗІ повинні бути зазначені вимоги обох видів.

3.7 Для будь-якого варіанту розроблення та оформлення ТЗ на КСЗІ його зміст, порядок погодження та затвердження повинен відповідати НД ТЗІ 3.7-001-99 та ГОСТ 34.602.

4 Розробка проекту КСЗІ

4.1.1 Проект КСЗІ розробляється на підставі та у відповідності до ТЗ на створення ІТС (доповнення до нього, окремого ТЗ на створення КСЗІ).

4.1.2 Під час розробки проекту КСЗІ обґрунтовуються і приймаються проектні рішення, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних заходів і способів захисту інформації.

4.1.3 Проект КСЗІ виконується на таких стадіях створення ІТС: ескізний проект, технічний проект, робочий проект.

Можливо вилучати етап “Ескізний проект КСЗІ”, а також поєднувати етапи “Технічний проект КСЗІ” і “Робочий проект КСЗІ” в один етап “Техноробочий проект КСЗІ”.

4.1.4 Для всіх стадій розробки проекту КСЗІ склад документації визначається ТЗ на КСЗІ, види та зміст – ГОСТ 34.201, НД ТЗІ 2.5-004-99. Документація на програмні засоби виконується згідно з комплексом стандартів ЄСПД, на технічні засоби – згідно з комплексом стандартів ЄСКД.

4.2 Ескізний проект КСЗІ

4.2.1 На цьому етапі здійснюється розробка попередніх проектних рішень КСЗІ та, у разі необхідності, її окремих складових частин, а також розроблення, оформлення, узгодження та затвердження документації на КСЗІ.

4.2.2 Визначаються: функції КСЗІ в цілому та функції її окремих складових частин; склад комплексу технічного захисту інформації від спеціальних впливів (за наявності); організаційних, правових та інших заходів захисту; склад КЗЗ; узагальнена структура КСЗІ та схема взаємодії складових частин.

4.3 Технічний проект КСЗІ

4.3.1 Розробка проектних рішень КСЗІ

Виконується розробка: загальних проектних рішень, необхідних для реалізації вимог ТЗ на КСЗІ; рішень щодо структури КСЗІ (організаційної структури, структури технічних і програмних засобів), алгоритмів функціонування та умов використання засобів захисту; рішень щодо архітектури КЗЗ та механізмів реалізації, визначених функціональним профілем послуг безпеки інформації.

4.3.2 Розробка документації на КСЗІ

Виконується розроблення, оформлення, узгодження та затвердження документації в обсязі, передбаченому ТЗ на КСЗІ.

4.4 Робочий проект КСЗІ

4.4.1 На цьому етапі здійснюється розроблення, оформлення та затвердження робочої та експлуатаційної документації КСЗІ та, у разі необхідності, її окремих складових частин.

Робоча документація містить детальні рішення щодо реалізації технічного проекту КСЗІ, щодо забезпечення управління КСЗІ і взаємодії її компонентів, а також документацію, необхідну для тестування, проведення пусконалагоджувальних робіт, проведення випробувань КСЗІ.

4.4.4 До складу робочої документації на КЗЗ повинні входити описи процедур інсталяції та ініціалізації комплексу, налагодження всіх механізмів розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, контролю за діями користувачів, а також контролю цілісності програмного забезпечення

4.4.5 Експлуатаційна документація включає опис порядку функціонування КСЗІ та настанови (інструкції) щодо забезпечення цього порядку обслуговуючим персоналом і користувачами, порядку супроводження КСЗІ впродовж життєвого циклу ІТС.

5 Введення КСЗІ в дію та оцінка захищеності інформації в ІТС

5.1 Підготовка КСЗІ до введення в дію

5.1.1 Проводяться роботи з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІТС.

5.1.2 Здійснюється створення СЗІ (призначаються відповідальні особи за захист інформації), якщо цього не було зроблено на попередніх етапах.

5.1.4 Створення СЗІ та розробка Плану захисту здійснюється згідно з НД ТЗІ 1.4-001-2000.

5.2 Навчання користувачів

Проводиться навчання користувачів ІТС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів та користувачів, які мають повноваження щодо управління засобами КСЗІ та ін.) в частині, що їх стосується, основним положенням документів Плану захисту, які необхідні їм для дотримання правил політики безпеки інформації, експлуатації засобів захисту інформації тощо, перевірка їх уміння користуватись впровадженими технологіями захисту інформації і реєстрація результатів навчання.

5.5 Пусконалагоджувальні роботи

5.5.2 Монтаж ОТЗ ІТС, кабельного обладнання, мереж живлення та заземлення здійснюється згідно з конструкторською документацією робочого проекту.

5.5.8 Здійснюється згідно з документацією робочого проекту інсталяція, ініціалізація та перевірка працездатності КЗЗ.

Під час інсталяції мають бути задіяні механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, контролю за діями користувачів, а також контролю цілісності програмного забезпечення.

5.6 Попередні випробування

5.1. Метою попередніх випробувань є перевірка працездатності КСЗІ та визначення можливості прийняття її у дослідну експлуатацію.

Під час випробувань перевіряються працездатність КСЗІ та відповідність її вимогам ТЗ.

5.6.2 Попередні випробування проводяться згідно з програмою та методиками випробувань. Програму й методики випробувань готує розробник КСЗІ, а узгоджує замовник ІТС. Програма та методики випробувань, протоколи випробувань розробляються та оформлюються згідно з вимогами РД 50-34.698.

5.6.3 Попередні випробування організовує замовник ІТС, а проводить розробник КСЗІ спільно із замовником. Для проведення попередніх випробувань замовником ІТС створюється комісія. Головою комісії призначається представник замовника.

5.6.4 Результати попередніх випробувань оформлюються “Протоколом випробувань”, де міститься висновок щодо можливості прийняття КСЗІ у дослідну експлуатацію, а також перелік виявлених недоліків, необхідних заходів з їх усунення, і рекомендовані терміни виконання цих робіт.

5.6.5 Після усунення недоліків у випадку їх наявності та коригування проектної, робочої, експлуатаційної документації КСЗІ оформлюється акт про приймання КСЗІ у дослідну експлуатацію.

5.7 Дослідна експлуатація

5.7.1 Під час дослідної експлуатації КСЗІ:

– відпрацьовуються технології оброблення інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів;

– співробітники СЗІ та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів;

– здійснюється (за необхідністю) доопрацювання програмного забезпечення, додаткове налагоджування та конфігурування КЗЗ;

– здійснюється (за необхідністю) коригування робочої та експлуатаційної документації.

5.7.2 За результатами робіт за довільною формою складається акт про завершення дослідної експлуатації, який містить висновок щодо можливості (неможливості) представлення КСЗІ на державну експертизу.

5.8 Державна експертиза КСЗІ

5.8.1 Державна експертиза КСЗІ є окремим етапом приймальних випробувань ІТС.

5.8.2 Державна експертиза проводиться з метою визначення відповідності КСЗІ технічному завданню, вимогам НД із захисту інформації та визначення можливості введення КСЗІ в складі ІТС в експлуатацію.

Державна експертиза КСЗІ в ІТС проводиться згідно з Положенням про державну експертизу в сфері технічного захисту інформації, яке затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16 травня 2007 року N 93 (у редакції наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 13 жовтня 2017 року N 565).

Надання послуг щодо проведення Державної експертизи КСЗІ (оцінювання захищеності інформації) підлягає ліцензуванню відповідно до Переліку послуг у галузі технічного захисту інформації, господарська діяльність щодо надання яких підлягає ліцензуванню.

5.8.3 Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такий самий, як і для попередніх випробувань. Якщо в силу якихось причин усунути недоліки в ході експертизи неможливо, це оформлюється актом, до якого вноситься перелік необхідних доробок та рекомендації щодо їх виконання. Після завершення передбачених актом робіт проводиться повторна експертиза.

5.8.4 Для інтегрованих ІТС може проводитись державна експертиза кожної складової частини (модуля) КСЗІ окремо.

5.8.5 Якщо інтегрована КСЗІ має у своєму складі типові модулі, які створювались за єдиним ТЗ, то експертиза таких модулів КСЗІ виконується в два етапи: на першому проводиться у повному обсязі експертиза одного обраного типового модуля, а на другому – здійснюється перевірка відповідності умов експлуатації типовим на кожному конкретному об’єкті для всіх модулів КСЗІ цього типу.

5.8.6 Введення до складу діючої КСЗІ нового (оціненого) модуля здійснюється без проведення повторної експертизи всієї КСЗІ. Проводиться оцінювання взаємодії нового модуля зі складовими частинами КСЗІ, які вже знаходяться в експлуатації.

5.8.7 Допускається розпочинати і проводити державну експертизу КСЗІ паралельно з роботами етапів проектування.

16.2. Проведення аудиту інформаційної безпеки та визначення на основі звіту з аудиту ризиків ІБ

Мета процесу аудиту та аналізу ризиків полягає у визначенні рівня ризиків інформаційної системи.

Згідно **НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу** визначені наступні поняття щодо ризику інформаційної безпеки.

Створення КСЗІ має починатись з аналізу об'єкта захисту і можливих загроз. Передусім мають бути визначені ресурси АС, що підлягають захисту. Загрози мають бути визначені в термінах ймовірності їх реалізації і величини можливих збитків. На підставі аналізу загроз, існуючих в системі вразливостей,

ефективності вже реалізованих заходів захисту для всіх ресурсів, що підлягають захисту, мають бути оцінені ризики. **Ризик** являє собою функцію ймовірності реалізації певної загрози, виду і величини завданих збитків. **Величина ризику** може бути виражена в грошовому вимірі або у вигляді формальної оцінки (високий, низький і т. ін.). На підставі виконаної роботи мають бути вироблені заходи захисту, перетворення яких в життя дозволило б знизити рівень остаточного ризику до прийнятного рівня. Підсумком даного етапу робіт повинна стати сформульована або скоригована політика безпеки.

На підставі проведеного аналізу ризиків сформульованої політики безпеки розробляється план захисту, який включає в себе опис послідовності і змісту всіх стадій і етапів життєвого циклу КСЗІ, що мають відповідати стадіям і етапам життєвого циклу автоматизованої системи (АС). **Вартість заходів щодо захисту інформації має бути адекватною розміру можливих збитків.**

Згідно **НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі** визначені наступні поняття щодо **аналізу ризиків** інформаційної безпеки.

Основою для проведення аналізу ризиків і формування вимог до КСЗІ є розробка моделі загроз для інформації та моделі порушника.

Аналіз ризиків

Аналіз ризиків передбачає вивчення моделі загроз для інформації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації в АС. Під час проведення аналізу ризиків необхідним є виконання наступних робіт.

1. Визначення компонентів і ресурсів АС, які необхідно враховувати при аналізі. Повинні бути визначені критичні з точки зору безпеки компоненти і ресурси АС, які можуть бути об'єктами атаки або самі є потенційним джерелом порушення безпеки інформації (об’єкти захисту). Для цього використовуються відомості п.3 додатку, одержані в результаті обстеження середовищ функціонування АС.

2. Ідентифікація загроз з об’єктами захисту. Встановлюється відповідність моделі загроз і об’єктів захисту, тобто складається матриця загрози/компоненти (ресурси) АС. Кожному елементу матриці повинен бути зіставлений опис можливого впливу загрози на відповідний компонент або ресурс АС. У процесі упорядкування матриці може уточнюватися список загроз і об’єктів захисту, внаслідок чого коригуватись модель загроз.

3. Оцінка ризиків. Повинні бути отримані оцінки гранично припустимого й існуючого (реального) ризику здійснення кожної загрози впродовж певного проміжку часу, тобто ймовірності її здійснення впродовж цього інтервалу. Для оцінки ймовірності реалізації загрози рекомендується вводити декілька дискретних ступенів (градацій). Оцінку слід робити за припущення, що кожна подія має найгірший, з точки зору власника інформації, що потребує захисту, закон розподілу, а також за умови відсутності заходів захисту інформації. На

практиці для більшості загроз неможливо одержати достатньо об’єктивні дані про ймовірність їхньої реалізації і доводиться обмежуватися якісними оцінками. У цьому випадку значення ймовірності реалізації загрози визначається в кожному конкретному випадку експертним методом або емпіричним шляхом, на підставі досвіду експлуатації подібних систем, шляхом реєстрації певних подій і визначення частоти їхнього повторення тощо. Оцінка може мати числове або смислове значення (наприклад, ймовірність реалізації загрози – незначна, низька, висока, неприпустимо висока). У будь-якому випадку існуючий ризик не повинен перевищувати гранично допустимий для кожної загрози. Перевищення свідчить про необхідність впровадження додаткових заходів захисту. Мають бути розроблені рекомендації щодо зниження ймовірності виникнення або реалізації загроз та величини ризиків.

4. Оцінювання величини можливих збитків, пов'язаних з реалізацією загроз. Виконується кількісна або якісна оцінка збитків, що можуть бути нанесені АС (організації) внаслідок реалізації загроз. Доцільно, щоб ця оцінка складалась з величин очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від втрати керованості АС внаслідок реалізації загрози. Для одержання оцінки можуть бути використані такі ж методи, як і при аналізі ризиків. Величина можливих збитків визначається розміром фінансових втрат або, у разі неможливості визначення цього, за якісною шкалою (наприклад, величина збитків – відсутня, низька, середня, висока, неприпустимо висока).

5. Вибір варіанту побудови КСЗІ. В залежності від конфіденційності інформації, яка обробляється в АС, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є у розпорядженні власника АС, а також інших чинників обґрунтовується пропозиція щодо доцільності застосування варіантів побудови КСЗІ. Можливі наступні варіанти:

– досягнення необхідного рівня захищеності інформації за мінімальних затрат і допустимого рівня обмежень на технологію її обробки в АС;

– досягнення необхідного рівня захищеності інформації за допустимих затрат і заданого рівня обмежень на технологію її обробки в АС;

– досягнення максимального рівня захищеності інформації за необхідних затрат і мінімального рівня обмежень на технологію її обробки в АС.

Якщо інформація становить державну таємницю, то необхідно застосовувати, як правило, третій варіант.

6 Оцінювання витрат на КСЗІ. Здійснюється первинне (попереднє) оцінювання допустимих витрат на блокування загроз, виходячи з вибраного варіанту побудови КСЗІ і виділених на це коштів. На етапі проектування КСЗІ, після формування пропозицій щодо складу заходів і засобів захисту, здійснюється оцінка залишкового ризику для кожної пропозиції (наприклад, за критерієм “ефективність/вартість”), вибирається найбільш оптимальна серед них і первинна оцінка уточнюється.

Якщо **залишковий ризик** перевищує гранично допустимий, вносяться відповідні зміни до складу заходів і засобів захисту, після чого всі процедури виконуються повторно до одержання прийнятного результату.

Основні підходи до аудиту та аналізу ризиків

Управління ризиками складається з трьох етапів:

– оцінка;

– зменшення;

– застосування заходів після оцінки ризику.

Управління ризиками – це процес, що дозволяє менеджерам здійснювати баланс між економічною та операційною вартістю ризику. Тому управління ними – це одне з головних завдань організації, оскільки воно дозволяє знайти баланс між вартістю засобів захисту інформації та вартістю ймовірної шкоди.

Основні компоненти управління ризиками

– Ресурси – інформація та підтримуючі засоби, які потрібні організації для ведення бізнесу. Це, наприклад, інформація/дані, паперові документи, програмне забезпечення, фізичне обладнання, служби, люди та їх знання, імідж та репутація організації. Кожному ресурсу інформаційної системи має бути присвоєно певне значення, що використовується визначення його важливості для бізнесу та необхідності тієї чи іншої рівня захисту. Значення можуть виражатися в термінах потенційного впливу на бізнес небажаних подій, що призводять до втрати конфіденційності, цілісності та доступності. Потенційний вплив включає фінансові втрати, падіння доходів та акцій на ринку або падіння престижу, що може призвести до фінансових втрат.

– Загроза – будь-які обставини чи події, які можуть спричинити порушення політики безпеки та/або заподіяння збитків автоматизованій системі. Загрози можуть бути ненавмисними (повінь, пожежа, землетрус), навмисними або випадковими. Результатом реалізації загрози можуть бути такі події, як руйнування, пошкодження чи модифікація, крадіжка, видалення чи втрата, розкриття об'єкта, використання чи впровадження нелегального об'єкта, переривання служби. Щоб загроза завдала шкоди, необхідна реалізація певної вразливості системи.

– Вразливість системи – неможливість системи протистояти реалізації певної загрози чи сукупності загроз. Як правило, вразливість виникає внаслідок погано відпрацьованих процедур, помилок некваліфікованого персоналу, внаслідок некоректної конфігурації системи. Щоб вразливість була використана, вона має бути відома чи реалізована загрозою.

– Ризик – функція ймовірності реалізації певної загрози, виду та величини зазнаних втрат. Рівень ризику безпеки визначається комбінацією значень ресурсів, оцінених рівнів відповідних загроз та асоційованих із нею вразливостей.

– Аналіз ризику – процес визначення загроз безпеки інформації та їх характеристик, слабких сторін комплексної системи захисту інформації (відомих та ймовірних), оцінки потенційних збитків від реалізації загроз та ступеня їхньої прийнятності для експлуатації автоматизованої системи.

– Базовий аналіз ризиків – аналіз ризиків, який проводиться відповідно до вимог базового рівня безпеки. Методи даного класу застосовуються у випадках, коли до інформаційної системи не висувається підвищених вимог у галузі ІБ.

– Повний аналіз ризиків – аналіз ризиків для інформаційних систем, які висувають підвищені вимоги до ІБ.

– Ризик порушення інформаційної безпеки – можливість реалізації загрози.

– Оцінка ризиків – ідентифікація ризиків, вибір параметрів для їх опису та отримання оцінок за цими параметрами.

– Управління ризиками – процес визначення контрзаходів відповідно до оцінки ризиків.

– Система управління інформаційною безпекою (СУІБ) або **Система менеджменту інформаційної безпеки (СМІБ)** – комплекс заходів, спрямованих на забезпечення режиму інформаційної безпеки на всіх стадіях життєвого циклу автоматизованих систем.

– Клас ризиків – безліч загроз ІХ, виділених за певною ознакою.

Процес оцінки ризиків

Оцінка ризику включає такі кроки:

1. Визначення характеристик системи.
2. Ідентифікація небезпек.
3. Ідентифікація вразливостей.
4. Аналіз контролю.
5. Визначення ймовірностей.
6. Аналіз впливу.
7. Визначення ризику.
8. Рекомендації щодо контролю.
9. Результуюча документація.

Крок 1. Визначення характеристик системи

На даному етапі збирається інформація, яка включає відомості про апаратуру; програмному забезпеченні, системних інтерфейсах (внутрішніх та зовнішніх з'єднаннях), даних, персоналі, що підтримує та використовує систему, призначенні системи (процесах, що виробляються системою), критичності системи та даних, їх чутливості.

Для збору цієї інформації можуть використовуватися запитальники, інтерв'ю, огляд документів, автоматичні пристрої сканування.

Крок 2. Ідентифікація загроз

Джерело загроз визначається як будь-яка обставина чи подія, які потенційно можуть завдати шкоди ІТ-системі. Спільними джерелами загроз можуть бути природа, люди та обладнання.

Крок 3. Аналіз вразливостей

Для визначення системних вразливостей використовуються джерела загроз та результати тестування системної безпеки. Потім слідує розробка контрольного списку вимог щодо безпеки. Необхідно відзначити, що типи вразливостей та методика їх визначення залежать від структури IT-інфраструктури.

Знаходження джерел вразливостей

Вразливості (як технічного, і нетехнічного характеру) ідентифікуються шляхом застосування технологій збору інформації. Іншим джерелом даних про вразливість є інтернет. Розробники часто публікують у Мережі відомі системні вразливості разом із засобами, призначеними для їх усунення або зменшення. Водночас можуть застосовуватись інші документовані джерела.

Тестування системної безпеки

Для оцінки дійсної наявності вразливостей можуть застосовуватись автоматичні засоби сканування, тести та оцінка безпеки, тести на проникнення. Автоматичні засоби сканування можуть бути використані для сканування мережі щодо наявності вразливих системних служб. Разом з тим слід зауважити, що не всі потенційні вразливості, визначені в такий спосіб, становлять реальну загрозу інформаційній безпеці організації.

Тест та оцінка безпеки включає розробку та виконання тестування. Призначення цього методу – протестувати ефективність контролю безпеки системи.

Тести проникнення використовуються з метою оцінки рівня контролю безпеки, здатності протистояти атакам на інформаційну систему.

Крок 4. Аналіз засобів захисту (контролю)

На цьому кроці проводиться аналіз засобів, що застосовуються або плануються до застосування засобів захисту інформації.

Крок 5. Ранжування частот появи

На цьому кроці необхідно визначити можливість реалізації потенційної вразливості. При цьому ймовірність описується як висока, середня та низька.

Крок 6. Аналіз впливу

На цьому кроці визначається величина впливу (висока, середня та низька), яку може зробити успішна реалізація загрози.

Крок 7. Визначення ризику

На цьому етапі оцінюється рівень ризику для системи. При цьому ризик виражається як функція від ймовірності того, що джерело загроз намагається реалізувати вразливість. Для вимірювання ризику розробляються шкали ризику та матриця рівнів ризику.

Визначення ризику одержують множенням класів (rating) ймовірностей загроз та впливу загроз.

Дана матриця (3x3) є матрицею оцінки загроз (високої, середньої, низької) та впливу загрози (висока, середня, низька). Залежно від вимог організації та кількості градацій бажаної оцінки ризику можна використовувати матриці 4x4 або 5x5.

Крок 8. Рекомендації щодо засобів захисту (контролю)

Метою цих рекомендацій є зменшення рівня ризику в інформаційній системі до допустимого рівня.

Виходом 8-го кроку є рекомендації щодо засобів захисту (контролю) та альтернативні рішення для зменшення ризику.

Крок 9. Результуюча документація

Після закінчення оцінки ризику результати подаються у вигляді звіту.

Зменшення ризиків

Процес зменшення ризику

Після того, як отримані результати оцінки ризиків, виникає завдання розділити ризики на прийнятні та неприйнятні. Для неприйнятних ризиків необхідно застосовувати процедури їхнього зменшення.

У загальному випадку зменшення ризику може бути досягнуто шляхом застосування однієї або комбінації наступних операцій, таких як прийняття ризику, ухилення від нього, обмеження, планування, дослідження та підтвердження, передача ризику.

Загальна схема процесу зменшення ризику ілюструє ці питання. Відповідні точки застосування дій засобів захисту малюнку позначені словом “так”.

Основним методом зниження ризику є застосування засобів захисту (контролю). Для зменшення ризику використовується наступна методологія, що описує підхід до застосування засобів захисту:

– Крок 1. Привласнення пріоритетів діям. Результат кроку 1 – ранжовані (від високого до низького) ризики.

– Крок 2.Оцінка рекомендованих варіантів захисту. Результат – перелік відповідних засобів захисту.

– Крок 3. Проведення аналізу витрат та результатів. Результат кроку 3 – аналіз витрат та результатів, що описує вартість та результати застосування засобів захисту.

– Крок 4. Вибір засобів захисту. Результат кроку 4 – список вибраних коштів.

– Крок 5. Призначення відповідальних. Результат – список відповідальних осіб.

– Крок 6. Розробка плану реалізації захисту. На цьому етапі розробляється план реалізації (застосування) засобів захисту (план дій). Результат кроку 6 – план застосування засобів захисту.

– Крок 7. Застосування вибраних засобів захисту. Результат – залишковий ризик.

При застосуванні рекомендованих засобів для зменшення ризику керівництво організації розглядає технічні, управлінські та операційні засоби захисту або їхню комбінацію, щоб максимізувати ефективність захисту для своєї ІТ-системи та організації.

Залишковий ризик

Застосування засобів захисту не гарантує знищення ризику. Тому завжди залишається певний рівень його, який називається залишковим ризиком. Загальна схема отримання залишкового ризику ілюструється малюнком.

Обчислення та оцінювання

Тенденції розвитку організацій показують, що з часом їх комп'ютерні мережі розширюватимуться та оновлюватимуться, компоненти мереж змінюватимуться та доповнюватимуться, прикладне та системне програмне забезпечення замінюватиметься чи оновлюватимуться новими версіями. Крім того, великі зміни зачіпають персонал організації та, відповідно, політику безпеки. Ці зміни означають, що з'являються нові ризики, і ризики, які раніше зазнали зменшення, знову стають значними. Тому процес управління ризиками має бути безперервним та еволюціонуючим

16.3. Вибір методів та засобів забезпечення необхідного рівня ІБ

Системний підхід до опису інформаційної безпеки пропонує виділити такі складові інформаційної безпеки:

1. Законодавча, нормативно-правова та наукова база.
2. Структура та завдання органів (підрозділів), що забезпечують безпеку ІТ.
3. Організаційно-технічні та режимні заходи та методи (Політика інформаційної безпеки).
4. Програмно-технічні способи та засоби забезпечення інформаційної безпеки.

Метою реалізації інформаційної безпеки будь-якого об'єкта є побудова **Системи забезпечення інформаційної безпеки** даного об'єкта (**СЗІБ**). Для побудови та ефективної експлуатації СЗІБ необхідно:

– виявити вимоги захисту інформації, специфічні для цього об'єкта захисту;

– врахувати вимоги національного та міжнародного Законодавства;

– використовувати напрацьовані практики (стандарти, методології) побудови подібних СЗІБ;

– визначити підрозділи, відповідальні за реалізацію та підтримку СЗІБ;

– розподілити між підрозділами відповідальності у здійсненні вимог СЗІБ;

– на базі управління ризиками інформаційної безпеки визначити загальні положення, технічні та організаційні вимоги, що становлять Політику інформаційної безпеки об'єкта захисту;

– реалізувати вимоги Політики інформаційної безпеки, запровадивши відповідні програмно-технічні способи та засоби захисту інформації;

– реалізувати **Систему менеджменту (управління) інформаційної безпеки (СМІБ)**;

– використовуючи СМІБ організувати регулярний контроль ефективності СЗІБ та за необхідності перегляд та коригування СЗІБ та СМІБ.

Як очевидно з останнього етапу робіт, процес реалізації СЗІБ безперервний і циклічно (після кожного перегляду) повертається до першого етапу, повторюючи послідовно й інші. Так СЗІБ коригується для ефективного виконання своїх завдань захисту інформації та відповідності новим вимогам інформаційної системи, що постійно оновлюється.

1. Організаційно-технічні та режимні заходи та методи

Для опису технології захисту інформації конкретної інформаційної системи зазвичай будується так звана **Політика інформаційної безпеки** або Політика безпеки інформаційної системи, що розглядається.

Політика безпеки (інформації в організації) (англ. Organizational security policy) – сукупність документованих правил, процедур, практичних прийомів або керівних принципів у сфері безпеки інформації, якими керується організація у своїй діяльності.

Політика безпеки інформаційно-телекомунікаційних технологій (англ. ICTsecurity policy) – правила, директиви, практика, що склалася, які визначають, як у межах організації та її інформаційно-телекомунікаційних технологій управляти, захищати та розподіляти активи, у тому числі критичну інформацію.

Для побудови Політики інформаційної безпеки рекомендується окремо розглядати такі напрямки захисту інформаційної системи:

– Захист об'єктів інформаційної системи.

– Захист процесів, процедур та програм обробки інформації.

– Захист каналів зв'язку (акустичні, інфрачервоні, дротові оптичні, радіоканали та ін.).

– Пригнічення побічних електромагнітних випромінювань та наведень (ПЕМВН).

– Управління системою захисту.

При цьому в кожному з перерахованих вище напрямків **Політика інформаційної безпеки має описувати такі етапи створення засобів захисту інформації**:

1. Визначення інформаційних та технічних ресурсів, що підлягають захисту.

2. Виявлення повної множини потенційно можливих загроз та каналів витоку інформації.

3. Проведення оцінки вразливості та ризиків інформації за наявної множини загроз та каналів витоку.

4. Визначення вимог до системи захисту.

5. Здійснення вибору засобів захисту інформації та їх характеристик.

6. Впровадження та організація використання обраних заходів, способів та засобів захисту.

7. Здійснення контролю цілісності та управління системою захисту.

Політика інформаційної безпеки оформляється як документованих вимог на інформаційну систему. Документи зазвичай поділяють за рівнями опису (деталізації) процесу захисту.

Документи верхнього рівня Політики інформаційної безпеки відображають позицію організації до діяльності в галузі захисту інформації, її прагнення відповідати державним, міжнародним вимогам та стандартам у цій галузі. Подібні документи можуть називатися «**Концепція ІБ**», «**Регламент управління ІБ**», «**Політика ІБ**», «**Технічний стандарт ІБ**» тощо. зовнішнього та внутрішнього використання.

Відповідно до стандарту **ISO/IEC 27002,** на **верхньому рівні Політики інформаційної безпеки** мають бути оформлені такі документи: «**Концепція забезпечення ІБ**», «**Правила допустимого використання ресурсів інформаційної системи**», «**План забезпечення безперервності бізнесу**».

До середнього рівня відносять документи щодо окремих аспектів інформаційної безпеки. Це вимоги на створення та експлуатацію засобів захисту інформації, організацію інформаційних та бізнес-процесів організації за конкретним напрямом захисту інформації. Наприклад: Безпека даних, Безпека комунікацій, Використання засобів криптографічного захисту, Контентна фільтрація тощо. Подібні документи зазвичай видаються у вигляді внутрішніх технічних та організаційних політик (стандартів) організації. Усі документи середнього рівня політики інформаційної безпеки є конфіденційними.

У політику інформаційної безпеки **нижнього рівня** входять регламенти робіт, посібники з адміністрування, інструкції з експлуатації окремих послуг інформаційної безпеки.

2. Організаційний захист об'єктів інформаційних систем

Організаційний захист – це регламентація виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, що виключає або суттєво ускладнює неправомірне оволодіння конфіденційною інформацією та прояв внутрішніх та зовнішніх загроз. Організаційний захист забезпечує:

– організацію охорони, режиму, роботу з кадрами, документами;

– використання технічних засобів безпеки та інформаційно-аналітичну діяльність з виявлення внутрішніх та зовнішніх загроз підприємницької діяльності.

До основних організаційних заходів належать:

– організація режиму та охорони. Їхня мета – виключення можливості таємного проникнення на територію та у приміщення сторонніх осіб;

– організація роботи зі співробітниками, яка передбачає добір та розстановку персоналу, включаючи ознайомлення зі співробітниками, їх вивчення, навчання правил роботи з конфіденційною інформацією, ознайомлення із заходами відповідальності за порушення правил захисту інформації та ін.;

– організація роботи з документами та документованою інформацією, включаючи організацію розробки та використання документів та носіїв

конфіденційної інформації, їх облік, виконання, повернення, зберігання та знищення;

– організація використання технічних засобів збору, обробки, накопичення та зберігання конфіденційної інформації;

– організація роботи з аналізу внутрішніх та зовнішніх загроз конфіденційної інформації та вироблення заходів щодо забезпечення її захисту;

– організація роботи з проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання та знищення документів та технічних носіїв.

У кожному даному випадку організаційні заходи носять специфічну для цієї організації форму і зміст, створені задля забезпечення безпеки інформації у конкретних умовах.

3. Програмно-технічні способи та засоби забезпечення інформаційної безпеки.

Класифікація засобів захисту.

– Засоби захисту від несанкціонованого доступу (НСД):
  - Засоби авторизації.
  - Мандатне керування доступом.
  - Виборче керування доступом.
  - Управління доступом на основі ролей.
  - Журналювання (так само називається Аудит).
– Системи аналізу та моделювання інформаційних потоків (CASE-системи).
– Системи моніторингу мереж:
  - Системи виявлення та запобігання вторгненням (IDS/IPS).
  - Системи запобігання витоку конфіденційної інформації (DLP-системи).
– Аналізатори протоколів.
– Антивірусні засоби.
– Міжмережеві екрани.
– Криптографічні засоби:
  - Шифрування.
  - Цифровий підпис.
– Системи резервування:
  - Резервне копіювання.
  - Відмовостійкий кластер.
  - Резервний Центр обробки даних (ЦОД) для катастрофостійкої ІС.
– Системи безперебійного живлення:
  - Джерела безперебійного живлення.
  - Резервні лінії електроживлення.
  - Генератори електроживлення.

- Системи автентифікації на основі:
  - Паролі.
  - Ключі доступу (фізичного або електронного).
  - Сертифікат.
  - Біометричні дані.
- Засоби запобігання злому корпусів та крадіжок обладнання.
- Засоби контролю та управління доступом до приміщень.
- Інструментальні засоби аналізу систем захисту.
- Засоби захисту від ПЕМВН.