**Лекція 10. Побудова і структура гарантій**

**реалізації послуг безпеки**

**Вступ.**

**Питання 1. Критерії гарантій реалізації послуг безпеки включають такі вимоги до КЗЗ.**

**Питання 2. Випробування КЗЗ.**

**Питання 3. Класифікація АС і стандартні функціональні профілі захищеності оброблюваної інформації від НСД.**

**Контрольні питання.**

**Вступ.**

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в ІТС, є також критерії гарантій, які дозволяють оцінити коректність реалізації послуг безпеки згідно вимог НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в КС від НСД».

Критерії гарантій мають сім iєрархічних рівнів гарантій. Iєрархiя рівнів гарантій відбиває поступово наростаючу міру упевненості в тому, що послуги, які надаються, дозволяють протистояти певним загрозам, а механізми, що їх реалізують, в свою чергу, коректно реалізовані, і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації ІТС.

Гарантії повинні забезпечуватися як в процесі розробки КСЗІ, так і в процесі її оцінки. В процесі розробки гарантії забезпечуються діями розробника щодо забезпечення правильності (коректностi) розробки. В процесі оцінки гарантії забезпечуються шляхом перевірки додержання розробником вимог критеріїв, аналізу документації, процедур розробки і постачання.

**Питання 1.**

Критерії гарантій реалізації послуг безпеки включають такі вимоги до КЗЗ:

- архітектура;

- середовище розробки;

- послідовність розробки;

- випробування;

- середовище функціонування;

- якість документації.

Для того, щоб ІТС одержала певний рівень гарантій реалізації необхідних послуг безпеки (якщо вона не може одержати більш високий), повинні бути задоволені всі вимоги, визначені для даного рівня в кожному з розділів вимог.

**1.1 Вимоги до архітектури**

Вимоги до архітектури КЗЗ забезпечують гарантії реалізації політики безпеки інформації у повному обсязі.

Це більшою мірою відносяться до архітектури ПЗ. Додержання цих вимог забезпечується розробником на стадіях проектування КЗЗ. Передусім, вимоги до архітектури покликані забезпечити структурованість КЗЗ відповідно до принципів якісного проектування ПЗ (модульність, iнкапсуляція і приховування даних).

Для самих низьких рівнів критеріїв гарантій від розробника вимагається просто описати складові компоненти КЗЗ та їх призначення.

Для більш високих (проміжних) рівнів вимагається логічне поділення вихідного коду на окремі незалежні компоненти (модулі), що ідентифікуються, та ізоляція компонентів КЗЗ, критичних для безпеки. Внутрішні деталі і дані, використовувані всередині кожного модуля, повинні бути приховані від усіх зовнішніх об'єктів. Послуги КЗЗ повинні бути доступні тільки через зовнішній документований інтерфейс.

Для самих верхніх рівнів Розробник під час проектування ПЗ повинен зосередити зусилля на зменшенні обсягу КЗЗ до мінімального набору компонентів. Мінімізація обсягу є однією з вимог концепції диспетчера доступу і дозволяє виділити у складі КЗЗ ядро захисту.

Програмне забезпечення, призначене для реалізації КЗЗ, повинне максимальним чином будуватися за модульним принципом.

Склад послуг безпеки, а також механізмів захисту, що реалізують кожну з послуг, визначається політикою безпеки інформації в ІТС і повинен відповідати її вимогам. Якщо не всі вимоги політики безпеки реалізуються КЗЗ, то вони повинні підтримуватися організаційними та іншими заходами захисту. У складі КЗЗ не повинні міститися послуги та використовуватися засоби, які мають не передбачені політикою безпеки функції. Використання таких засобів можливе за умови вилучення цих функцій або гарантування неможливості їх активізації.

Мають бути описані особливості архітектури компонентів КСЗІ та їх призначення. Стиль опису – неформалізований, вимоги щодо детального опису не висуваються.

**1.2 Середовище розробки**

Вимоги до середовища розробки КЗЗ забезпечують гарантії повної керованості процесів розробки та супроводження ІТС з боку розробника.

Процес розробки. Від розробника вимагається визначити всі стадії життєвого циклу ІТС, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії. Мають бути визначені всі стадії та етапи життєвого циклу ІТС, а для кожної стадії та етапу – перелік і обсяги необхідних робіт та порядок їх виконання. Якщо для якихось робіт вимагається створення особливих умов – це повинно бути визначено окремо. Всі стадії та етапи робіт повинні бути задокументовані. Види та зміст документів встановлено державними стандартами.

На всіх стадіях життєвого циклу повинні існувати процедури керування конфігурацією ІТС. Ці процедури повинні визначати технологію відслідковування та внесення змін в апаратне та програмне забезпечення КСЗІ, тестове покриття і документацію та гарантувати, що без дотримання цієї технології ніякі зміни не можуть бути внесені. Технологія відслідковування та внесення змін повинна гарантувати постійну відповідність між документацією й реалізацією поточної версії КЗЗ (інших компонентів КСЗІ).

Крім того, повинні бути документовані стандарти, які використовувались під час розробки ПЗ. Використовувані мови програмування і компілятори мають відповідати вимогам національних, міждержавних або міжнародних стандартів. В іншому випадку слід надати повне визначення і опис мови, яка використовувалась. Додатково має бути документовано використання залежних від реалізації або апаратури опцій мови програмування.

Для більш високих рівнів гарантій вимоги до середовища розробки включають вимоги необхідності документування використовуваних методик фізичної, технічної, організаційної і кадрової безпеки.

Керування конфігурацією.

Керування конфігурацією є необхідною і невід'ємною частиною будь-якої спроби розробки, а особливо захищених ІТС. Додержання вимог даного розділу критеріїв гарантій дозволяє забезпечити впевненість Експертної комісії в тому, що розробник може повністю керувати конфігурацією оцінюваної ІТС.

Розробник повинен розробити, запровадити і підтримувати в дієздатному стані документовані методики керування конфігурацією ІТС на всіх стадіях її життєвого циклу. При цьому Розробник може розробити і використати систему керування конфiгурацією, що найкраще відображає і складність ІТС, і розміри організації Розробника.

Критерії керування, можливе використання засобів автоматизації і належний рівень формалізації процедур і перевірок визначаються Розробником (і підтверджуються Експертною комісією) таким чином, щоб бути настільки сумісним з іншими компонентами середовища розробки, наскільки це можливо. Важливо, щоб усі процедури, ролі і відповідальність всього персоналу, задіяного в керуванні конфiгурацією, були чітко визначені і документовані.

Система керування конфігурацією повинна бути орієнтована на вирішення чотирьох основних завдань: визначення конфігурації, регулювання конфiгурації, облік стану і перевірка якості конфігурації

Визначення конфігурації.

ІТС повинна ідентифікуватися в термінах своєї конфiгурації: апаратне забезпечення, програмне забезпечення і документація на ІТС (наприклад, функціональні специфікації, технічний і робочий проекти, документація з тестування). Кожний елемент конфігурації одержує унікальне і значиме ім'я (ідентифікатор), під яким він існує в ІТС протягом всього її життєвого циклу. Повинні використовуватися загальні для всього проекту угоди щодо позначення, маркірування, нумерації і каталогізації елементів конфігурації Особливу увагу слід приділяти угодам щодо ПЗ (наприклад, для визначення того, є елемент вихідним чи об'єктним кодом).

Розмір елементів конфігурації може варіюватися відповідно до їх складності та очікуваної частоти зміни. Шляхом ретельного вибору розміру кожного елемента конфігурації система керування конфігурацією може краще ізолювати ті елементи, що змінюються частіше від тих, що змінюються рідше, ізолювати ті елементи, що є критичними для безпеки від тих, що не є такими, і групувати окремі малі елементи ІТС в єдиний великий елемент конфігурації для зменшення загального числа елементів конфігурації Ефективність контролю за змінами залежить від вдалого виділення елементів конфiгурації: має досягатись рівновага між керуванням великим числом малих елементів конфігурації і групуванням надто великого числа елементів ІТС в один елемент конфігурації

Регулювання конфігурації.

Контроль внесення будь-яких змін до ІТС є основною функцією системи керування конфігурацією ІТС. Керування внесенням змін до конфігурації ІТС слід здійснювати протягом всього життєвого циклу ІТС. Процес внесення змін і набір використовуваних процедур мають бути визначені і документовані.

Необхідно мати відповідальних осіб, роль і відповідальність яких має бути документована, які відповідали б за оцінку і затвердження запропонованих змін і безпосередньо за їх внесення. Це дозволяє гарантувати, що в разі необхідності елементи конфігурації можуть бути зафіксовані в певному стані і що ефекти від пропонованих змін будуть враховані раніше, ніж будуть затверджені дані зміни.

Облік стану.

Завдання керування конфігурацією щодо обліку стану включає в себе фіксування інформації за статусом кожного елемента конфігурації Вона включає і вихідне визначення елемента, і будь-які зміни, внесені до елемента (наприклад, поширення, усунення помилок) протягом всього життєвого циклу. При збереженні записів за кожним елементом конфігурації поточний стан (статус) кожного елемента може бути доступним зацікавленому персоналу, а також можуть бути одержані історичні дані для використання в процесі перевірки конфігурації

Перевірка якості конфігурації.

Контроль за конфiгурацiєю здійснюється шляхом взаємозв'язаних переглядів і перевірок інформації за станом всіх елементів конфігурації з метою одержання впевненості, що система керування конфігурацією працює належним чином. Контроль за конфігурацією робить можливим наступну адаптацію і настроювання процесу керування конфігурацією відповідно до умов, що змінюються (вхідними вимогами). Перегляди і перевірки також дають гарантію того, що стандарти, політика і процедури, прийняті в організації, присутні і в системі керування конфігурацією

Відповідно до Критеріїв система керування конфігурацією включає в себе технічні та організаційні заходи. Система керування конфігурацією повинна охоплювати розробку програмно-апаратного забезпечення, документації та їх супровід.

Для найнижчих рівнів критеріїв гарантій у розробника має бути базова система керування конфiгурацією. Базова система керування конфiгурацією дозволяє ідентифікувати ІТС, керувати внесенням змін і вести їх архів. Система керування конфігурацією повинна включати технічні або організаційні документовані методики керування програмним, апаратним, програмно-апаратним забезпеченням, опрацюванням документації і тестів в необхідному обсязі.

Для більш високих рівнів критеріїв гарантій система керування конфігурацією повинна додатково мати можливість генерувати версію КЗЗ із вихідного коду і відзначати будь-які відмінності. Частиною системи мають бути засоби генерації звітів про помилки та інші проблеми, а також про їх усунення. Для даних рівнів система керування конфігурацією повинна використовувати засоби автоматизації та організаційні процедури, що їх доповнюють.

Для найбільш високих рівнів критеріїв гарантій система керування конфігурацією повинна додатково забезпечувати керування всіма засобами (наприклад, мовами програмування, компіляторами, бібліотеками часу виконання тощо), які використовувались в процесі розробки ІТС.

**1.3 Послідовність розробки**

Вимоги до процесу проектування КЗЗ забезпечують гарантії точного опису ІТС на кожній стадії її розробки та реалізації згідно вимог політики безпеки. Для всіх стадій життєвого циклу ІТС повинні бути розроблені функціональні специфікації КСЗІ.

Рівні деталізації.

Вимоги до гарантій передбачають наявність чотирьох основних рівнів деталізації ІТС у процесі її створення: функціональна специфікація, проект архітектури, детальний проект, реалізація. Експертна комісія виконує аналіз для визначення коректності опису ІТС для кожного рівня деталізації і його відповідності опису попереднього рівня. Для кожної конкретної ІТС розробник можуть спільно визначити необхідні рівні деталізації процесу розробки, які можна розглядати як функціональну специфікацію, проект архітектури і детальний проект. В документах, в яких наведені описи для кожного рівня деталізації, можуть використовуватись посилання на інші документи.

Стиль специфікації.

В залежності від рівня гарантій і рівня деталізації передбачається можливість використання трьох способів (стилів) специфікації: неформалiзований, частково формалізований і формалізований. Неоднозначність специфікацій зменшується з використанням більш високого рівня формалізації.

Неформалiзована специфікація має стиль текстового документа мовою повсякденного спілкування (російська, українська). Для неформалiзованої специфікації вимагається представити визначення термінів, що використовуються в контексті, які відрізняються від звичайних, що використовуються у повсякденній мові.

Частково формалізована специфікація складається мовою з обмеженим синтаксисом і доповнюється поясненнями, написаними мовою повсякденного спілкування. Мова з обмеженим синтаксисом може являти собою повсякденну мову з жорсткою структурою речення і ключовими словами, що мають спеціальне значення, або бути дiаграматичною (наприклад, діаграми потоків даних, станів або переходу). Для побудови частково формалізованої специфікації як на базі діаграм, так і на базі мови повсякденного спілкування, необхідно сформулювати набір угод, що визначають обмеження синтаксису.

Формалізовані специфікації мають представлення, яке базується на добре встановлених математичних концепціях, і супроводжуються поясненнями звичайною мовою. Ці математичні концепції використовуються для визначення синтаксису і семантики подань і несуперечливих правил доказу, які підтримуються логічними посиланнями. Властивості, критичні для безпеки, повинні виражатися мовою формалізованої специфікації. Формалізовані представлення повинні дозволяти описати і ефект (результат) виконання функції, і всі зв'язані з нею виняткові або помилкові умови. Якщо використовуються ієрархічні специфікації, то необхідно показати, що кожний рівень включає властивості, встановлені для попереднього рівня.

Вимоги до відповідності специфікацій рівня.

Критерії гарантій включають вимоги до відповідності специфікацій рівня деталізації. Рівень зусиль, необхідних для досягнення такої відповідності, зростає разом з рівнем гарантій. Для його характеристики використовують терміни «показати», «продемонструвати» або «довести».

Якщо від розробника вимагається показати повну відповідність між представленнями ІТС, це означає, що є необхідністю наявність відповідності тільки між основними елементами кожної специфікації. Прикладом може бути використання таблиці, елементи якої відображають відповідність, або використання належного представлення діаграми проекту.

Якщо від розробника вимагається продемонструвати повну відповідність між представленнями ІТС, то вимагається наявність відповідності між більш дрібними елементами кожної специфікації. Демонстрація відповідності виконується на основі аналізу з використанням структурованого наукового підходу, що дає переконливі аргументи на користь того, що існує повна відповідність між елементами двох специфікацій.

Якщо від розробника вимагається довести повну відповідність між представленнями ІТС, то необхідним є наявність відповідності між ще більш дрібними елементами кожної специфікації. Відповідність між елементами має бути виражена формально.

Функціональні специфікацїi.

Функціональні специфікації політики безпеки й моделі політики безпеки повинні, як мінімум, містити перелік й опис послуг безпеки, що надаються КЗЗ, а також правила розмежування доступу до захищених об’єктів ІТС.

Політика безпеки описує ІТС як набір послуг безпеки. Кожна послуга описується відповідно до вимог функціональних критеріїв для певного рівня даної послуги і з урахуванням необхідних умов. Для всіх рівнів гарантій політика безпеки подається у стилі неформалiзованої специфікації і показується її відповідність більш деталізованій специфікації. Фактично, політика безпеки може бути визначена в технічному завданні на ІТС.

Модель політики безпеки дозволяє точніше виразити вимоги політики безпеки. Стиль специфікації моделі політики безпеки варіюється залежно від рівнів гарантій від неформалiзованого до формалізованого. Для всіх рівнів гарантій показується відповідність моделі політики безпеки більш деталізованій специфікації.

Функціональні специфікації проекту архітектури КСЗІ повинні містити модель захисту (ескізний проект), де враховані всі суттєві загрози і для кожної з них визначено можливі варіанти її блокування (попередження) за допомогою КЗЗ або організаційними чи іншими заходами захисту. Якщо існує неоднозначність, повинні надаватися додаткові аргументи на користь вибору того чи іншого варіанту.

Функціональні специфікації детального проекту КСЗІ повинні містити принципи побудови, функціональні можливості, опис функціонування кожного механізму захисту та взаємодії механізмів між собою у складі КЗЗ. Повинні бути розроблені документи, що регламентують використання засобів КЗЗ, а також організаційних та інших заходів захисту, які входять до КСЗІ. Як реалізація детального проекту може розглядатися технічний, робочий або техно-робочий проекти.

Має бути підтверджена (показана) відповідність специфікацій КСЗІ всіх рівнів. Формальних доказів відповідності не вимагається. 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 або окремих її компонентів, результати контролю за виконаними роботами на етапах створення ІТС з боку системи управління якістю виробництва, якщо у власника та розробників ІТС така система впроваджена та ін.

Проект архітектури.

Проект архітектури є старшим або верхнім рівнем специфікації проекту, який відображає функціональну специфікацію в основні компоненти проекту ІТС. Для кожного з основних компонентів ІТС проект архітектури описує його призначення і функції, визначає послуги безпеки, що реалізуються ним. Взаємодія всіх компонентів також визначається на даному етапі. Ця взаємодія представляється на рівні зовнішніх інтерфейсів, потоків даних, керування тощо. Проект архітектури описує, яку функцію виконує кожний компонент. Опис того, як компонент виконує свої функції всередині, не вимагається.

Детальний проект.

Детальний проект є нижнім і найбільш детальним рівнем специфікації, який поділяє проект архітектури на менші за обсягом проекти його компонент. Детальний проект повинен мати достатню міру деталізації, щоб дозволити почати реалізацію. Для кожного компонента детальний проект повинен містити опис його призначення і функцій. Має бути визначений порядок взаємодії всіх компонентів. Ця взаємодія представляється на рівні зовнішніх інтерфейсів потоків даних, керування і т. ін. Детальний проект описує і те, яку функцію виконує кожний компонент, і те, як він це робить, включаючи алгоритми і внутрішні інтерфейси. Для детального проекту допускається наявність деяких проміжних специфікацій, кожна з яких характеризується більшою рівнем деталізації порівняно з попередніми.

Реалізація.

Реалізація є завершальним представленням ІТС, що складаються з програмного, програмно-апаратного і апаратного забезпечення. Кожний компонент реалізації повинен бути створений і документований відповідно до вимог процесу проектування. Інтерфейси та інші компоненти, що згадуються, повинні бути описані в документації. Для найбільш високих рівнів гарантій вимагається представлення обраних дільниць вихідного коду.

**1.4 Середовище функціонування**

Вимоги до середовища функціонування КЗЗ забезпечують гарантії його поставки замовнику без несанкціонованих модифікацій та його впровадження замовником згідно вимог розробника.

Оцінка ІТС забезпечує гарантії того, що ІТС правильно реалізує політику безпеки і правильно функціонує, і будується на припущенні, що функціонування ІТС починається з безпечного стану. Дотримання вимог даного розділу критеріїв гарантій дозволяє забезпечити впевненість, що це припущення є правильним для всіх оцінюваних ІТС.

Повинні існувати засоби інсталяції, генерації й запуску КЗЗ, які гарантують, що експлуатація ІТС починається з безпечного стану, а також, існувати документи (інструкції), які регламентують порядок керування цими процедурами. Якщо можливі різні варіанти конфігурації КЗЗ, то всі вони повинні бути описані в інструкціях.

Розробник апаратного, програмного, програмно-апаратного забезпечення КСЗІ повинен шляхом впровадження технічних, організаційних або фізичних заходів безпеки гарантувати, що забезпечення, яке ним поставляється, відповідає еталону.

По-перше, розробник повинен гарантувати, що конфігурація, яка поставляється замовнику, є сертифікованою конфігурацією.

По-друге, під час постачання розробник повинен забезпечити захист КЗЗ від несанкціонованої модифікації. Цей захист за своєю природою може бути технічний, організаційний або фізичний. Технічний захист може полягати, наприклад, у використанні шифрування або криптографічних контрольних сум, паролів, що відкривають доступ до критичного ПЗ, перевірок на відповідність ПЗ еталону тощо. Організаційний захист може полягати, наприклад, у перевірці конфігурації для досягнення впевненості в тому, що замовнику поставлена потрібна версія, для чого можуть застосовуватися процедури керування якістю, задіяні розробником при пакуванні КЗЗ. Фізичний захист може полягати, наприклад, у використанні вакуумної упаковки компонентів ПЗ і документації та використанні інших оболонок, що запобігають або фіксують спроби фізичного доступу.

По-третє, коли КЗЗ доставлений та його цілісність перевірена, замовнику необхідні інструкції з його інсталяції та ініціалізації. Наведені вказівки повинні описувати всі параметри конфiгурування та можливі обмеження.

**1.5 Документація**

Документація КЗЗ повинна містити опис послуг безпеки, що реалізуються КЗЗ, та настанови для користувачів з їх використання.

Для того, щоб замовник зміг повною мірою використати послуги безпеки, що надаються КЗЗ для реалізації політики безпеки, встановленої в його організації, йому необхідна відповідна документація, в якій були б описані ці послуги і дані вказівки щодо їх використання.

У складі експлуатаційної документації розробник повинен подати опис послуг безпеки, що реалізуються КЗЗ оцінюваної ІТС, настанови адміністратору та користувачу щодо послуг безпеки. Зміст цих документів залежить від політики безпеки, що реалізується ІТС. Ніяких особливих вимог до назв, формату або структур документів дані критерії не ставлять.

Документація може бути загальною або в ній можуть бути явно виділені документи (розділи), призначені для адміністратора безпеки і для звичайного користувача. В будь-якому випадку наведеної в документації інформації повинно бути достатньо для того, щоб і адміністратор, і звичайні користувачі мали змогу виконувати свої функції.

**Питання 2.**

Для проведення випробувань КЗЗ розробником складається програма й методика та розробляються процедури випробувань усіх механізмів захисту.

В плані випробувань повинна бути викладена стратегія випробувань розробника. План повинен надавати детальний опис всіх тестованих частин КЗЗ. Сюди входять зовнішні інтерфейси КЗЗ, всі політики, привілеї, механізми послуг захисту і специфічних викликів системних функцій, бібліотечного ПЗ тощо. План має також відображати середовище випробувань, будь-які особливі умови, що створюються для проведення випробувань, і засоби випробувань. Повинні бути наведені аргументи на користь повноти тестового покриття.

Програма і методика випробувань повинна визначати процедури тестування кожного елемента, визначеного у плані випробувань (наприклад, системних викликів). Для кожного окремого тесту має бути докладно описано використання засобів випробувань, необхідне оточення і особливі умови. Рівень деталізації процедур випробувань має бути достатнім для наступного повторення випробувань Експертною комісією. Розробник повинен також описати очікувані результати кожного тесту.

Для демонстрації того, що КЗЗ оцінюваної ІТС піддавався випробуванням, і доказу повноти цих випробувань розробник повинен надати Експертній комісії документально оформлені результати випробувань. Вимоги до випробувань визначають такі основні елементи планування і проведення випробувань розробником: план випробувань, програма і методика випробувань і результати випробувань (журнал випробувань, звіт, протокол випробувань).

Розробник КЗЗ повинен надати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування. Розробник КЗЗ повинен усунути або нейтралізувати всі знайдені «слабкі місця» і виконати повторне тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові «слабкі місця».

Програма та методика випробувань КЗЗ, тестове покриття, результати випробувань КЗЗ входять до складу обов’язкового комплекту документації, яка надається організатору експертизи під час проведення державної експертизи КСЗІ в АС.

Інформація, що міститься в документах, які представляють результати випробувань, дозволяє Експертній комісії оцінити реальну ефективність і повноту проведених випробувань, їх відповідність плану, програмі і методиці, а також організувати проведення сертифікаційних випробувань.

**Питання 3.**

В межах кожного класу АС класифікуються на підставі вимог до забезпечення певних властивостей інформації.

З точки зору безпеки інформація характеризується трьома властивостями: конфіденційністю, цілісністю та доступністю. Виходячи з цього, кожний клас АС (Х=1,2,3) поділяється на підкласи, які визначають підвищені вимоги до забезпечення однієї чи декілька цих властивостей.

Таким чином, кількість сполучень з трьох властивостей зумовлює наявність семи груп підкласів АС:

1) підклас Х.К - конфіденційності інформації;

2) підклас Х.Ц - цілісності інформації;

3) підклас Х.Д - доступності інформації;

4) підклас Х.КЦ - конфіденційності та цілісності інформації;

5) підклас Х.КД - конфіденційності та доступності інформації;

6) підклас Х.ЦД - цілісності та доступності інформації.

7) підклас Х.КЦД - конфіденційності, цілісності та доступності інформації.

Якщо врахувати наявність в кожній групі трьох класів АС, сумарна кількість підкласів становить 21.

НД ТЗІ 2.5-005-99 «Класифікація АС і стандартні функціональні профілі захищеності оброблюваної інформації від НСД» вводить таке поняття як «стандартний функціональний профіль захищеності» (далі - СФПЗ). Він являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.

Для кожного з підкласів кожного класу вводиться деяка кількість ієрархічних СФПЗ, яка може бути різною для кожного класу і підкласу АС. Профілі є ієрархічними в тому розумінні, що їх реалізація забезпечує наростаючу захищеність від загроз відповідного типу (К, Ц і Д). Зростання ступеня 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 реалізовувати КЗЗ проектованої або існуючої АС. Цей підхід дозволяє мінімізувати витрати на початкових етапах створення КСЗІ ІТС. Проте слід визнати, що для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.

СФПЗ 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 висуваються. Політика безпеки АС, що реалізує певний СФПЗ, має бути «успадкована» з документів, що встановлюють вимоги до порядку обробки певної інформації в АС.

НД ТЗІ 2.5-005-99 визначає стандартний підхід до визначення ФПЗ АС шляхом вибору з множини СФПЗ, який базується на таких припущеннях:

- усі АС можна віднести до одного з трьох класів за наступними ознаками: конфігурація апаратних засобів, їх фізичне розміщення, кількість категорій оброблюваної інформації, кількість користувачів і категорій користувачів;

- у межах класу АС можна віднести до одного з підкласів, що визначені за критерієм необхідності забезпечення К, Ц і Д;

- вимоги до безпеки АС різних класів суттєво відрізняються, що дозволяє сформувати для їх підкласів множини СФПЗ, що знаходяться у ієрархічній залежності;

- для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної ІТС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Клас АС** | **Кількість СФПЗ для підкласів АС** | | | | | | | **Загальна кількість СФПЗ** |
| **К** | **Ц** | **Д** | **КЦ** | **КД** | **ЦД** | **КЦД** |
| **1** | **2** | **2** | **4** | **2** | **4** | **4** | **4** | **22** |
| **2** | **6** | **5** | **4** | **6** | **4** | **4** | **5** | **34** |
| **3** | **6** | **5** | **4** | **6** | **4** | **4** | **5** | **34** |

Стандартний підхід визначення ФПЗ вимагає таких етапів:

1. Визначення підкласу АС.

2. Визначення призначення АС та вибір підказки, яку треба використовувати у цьому випадку для вибору одного із СФПЗ, використовуючи довідковий додаток «А» з НД ТЗІ 2.5-005-99. Якщо призначення АС відрізняється від наведених у НД ТЗІ 2.5-005-99 необхідно власноруч обрати підмножину СФПЗ відповідно до підкласу АС.

3. Аналіз сутності вимог, відібраних СФПЗ.

4. Вибір одного із СФПЗ, який найбільш відповідає політиці безпеки.

5. У випадку, коли жоден із СФПЗ не підходить повною мірою, необхідно змінити рівень послуги, що міститься у СФПЗ, або додати нову послугу.

Така властивість як спостереженість не використовується для розбиття АС на підкласи. Цей факт пояснюється тим, що послуги спостереженості є необхідною умовою для реалізації інших послуг безпеки, а з іншого боку завжди важливі для АС.

Алгоритм з'ясування необхідності та рівня послуги безпеки можна викласти у табличному вигляді:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№№** | **Запитання** | **Відповіді** | | **Результат** | | **Пере-хід**  **до** | **Група**  **відпо-**  **відей** |
| **Гру-па** | **Варіанти**  **відповіді** | **Рівень**  **послуги** | **Тип**  **\*** |
| 1 | Чи повинні користувачі (не адміністратори) мати можливість керувати потока-ми інформації від  захищених об'єк-тів ІТС до інших користувачів? | а) | Так. Ця можливість має бути надана користувачам (не адміністраторам) стосовно окремих захищених об’єкті | КД-1 або 2 | П | п.2 | а) |
| Так. Ця можливість має бути нада-  на користувачам (не адміністраторам) стосовно всіх захищених об’єктів | КД-3 або 4 | П | п.2 | б) |
| Ні. Таку можливість має бути виключено | Послуга не  потрібна | О | нас-тупної  таблиці | - |
| 2 | Захист від якого рівня загроз має забезпечувати  КСЗІ? | а) | НСД до захищеного об’єкту із застосуванням неавторизованого  процесу | КД-1 | О | нас-тупної  таблиці | - |
| НСД до захищеного об’єкту з боку  неавторизованого користувача | КД-2 | О | нас-тупної  таблиці | - |
| б) | НСД до захищеного об’єкту з боку  неавторизованого користувача | КД-3 | О | нас-тупної  таблиці | - |
| НСД до захищеного об’єкту з боку  неавторизованого/ авторизованого  користувача із застосуванням не-авторизованого процесу та/або  авторизованого користувача із застосуванням неавторизованого  процесу | КД-4 | О | нас-тупної  таблиці | - |

\*Примітка: «О» - остаточний результат, «П» - проміжний результат.

Згідно НД ТЗІ 2.5-005-99 кожний профіль має свій буквено-числовий ідентифікатор, який включає:

- номер класу АС (1 - ПЕОМ, 2 - ЛОМ, 3 - РОМ),

- букви, що характеризує види загроз, від яких забезпечується захист (К, Ц, Д),

- номер профілю.

Всі частини ідентифікатора відділяються один від одного крапкою.

Наприклад, СФПЗ АС класу «2» номер 1 з підвищеними вимогами до забезпечення конфіденційності інформації виглядає таким чином:

2.К.1 = { КД-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1 }

А СФПЗ АС класу «1» номер 2 з підвищеними вимогами до забезпечення конфіденційності, цілісності та доступності інформації виглядає таким чином:

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

Версія може служити, зокрема, для вказівки на підсилення певної послуги всередині профілю. Наприклад, нарощування можливостей реєстрації приведе до появи нової версії. Тим не менше, при внесенні деяких істотних змін, особливо додання нових послуг, може або привести до появи нового профілю, або до того, що профіль буде відноситись до іншого підкласу АС.

Найбільш складним профілем є профіль КЦД, до якого включається 22 послуги, причому це взагалі максимально можлива для профілів кількість послуг. Але не завжди є необхідність підтримувати відразу всі властивості інформації, що захищається, - іноді достатньо підтримувати лише деякі з них залежно від конкретної мети та завдань захисту інформації, а також очікуваних загроз інформації. Наприклад, у деяких випадках достатньо підтримувати властивість конфіденційності, яка може реалізуватися таким механізмом, як криптографія. Іноді, особливо в мережевих конфігураціях, найбільш важливою може бути підтримка властивості доступності.

ФПЗ по суті є варіантом технічної реалізації системи захисту інформації. За рахунок реалізації певного ФПЗ забезпечується виконання політики безпеки ІТС й зменшення збитку, що завдається АС впливом загроз. Вирішення завдання вибору оптимального ФПЗ включає формування множини припустимих варіантів ФПЗ, визначення сукупності показників якості та критерію оптимальності, а також вибір варіантів ФПЗ, оптимальних за цим критерієм.

Таким чином, завданням розробника КСЗІ є обстеження властивостей конкретної АС, як об'єкта захисту та вибір необхідного СФПЗ із списку, наведеного у НД ТЗІ 2.5-005-99. У випадку, коли жоден з наявних СФПЗ не підходить до конкретної АС, розробник має створити свій, найбільш придатний для нього ФПЗ, обґрунтувати й затвердити його.

**Контрольні питання**

Які вимоги до КЗЗ включають критерії гарантій реалізації послуг безпеки?

Скільки iєрархічних рівнів мають критерії гарантій реалізації послуг безпеки?

Що дозволяють оцінити критерії гарантій реалізації послуг безпеки?

Гарантії чого забезпечують вимоги до архітектури КЗЗ?

Гарантії чого забезпечують вимоги до середовища розробки КЗЗ?

Які процедури повинні існувати на всіх стадіях життєвого циклу ІТС?

Що є основною функцією системи керування конфігурацією ІТС?

Що повинна охоплювати система керування конфігурацією ІТС?

Що дозволяє базова система керування конфiгурацією ІТС?

Гарантії чого забезпечують вимоги до процесу проектування КЗЗ?

Гарантії чого забезпечують вимоги до середовища функціонування КЗЗ?

Що повинна містити документація КЗЗ?

Що складається та розробляється для проведення випробувань КЗЗ?

Як розшифровується термін «СФПЗ»?

На підставі чого кожний клас АС поділяється на підкласи?

Яка є кількість груп підкласів та сумарна кількість підкласів?

Яку назву має підклас з підвищеними вимогами до конфіденційності інформації в АС класу 2?

Яку назву має підклас з підвищеними вимогами до цілісності інформації в АС класу 3?

Яку назву має підклас з підвищеними вимогами до доступності інформації в АС класу 3?

Яку назву має підклас з підвищеними вимогами до конфіденційності та цілісності інформації в АС класу 2?

Яку назву має підклас з підвищеними вимогами до конфіденційності та доступності інформації в АС класу 2?

Яку назву має підклас з підвищеними вимогами до цілісності та доступності інформації в АС класу 3?

Яку назву має підклас з підвищеними вимогами до конфіденційності, цілісності та доступності інформації в АС класу 1?

Яку назву має СФПЗ АС класу 2 номер 5 з підвищеними вимогами до конфіденційності інформації?

Яку назву має СФПЗ АС класу 3 номер 1 з підвищеними вимогами до цілісності інформації?

Яку назву має СФПЗ АС класу 3 номер 2 з підвищеними вимогами до доступності інформації?

Яку назву має СФПЗ АС класу 2 номер 4 з підвищеними вимогами до конфіденційності та доступності інформації?

Яку назву має СФПЗ АС класу 2 номер 3 з підвищеними вимогами до забезпечення конфіденційності та цілісності інформації?

Яку назву має СФПЗ АС класу 3 номер 2 з підвищеними вимогами до цілісності та доступності інформації?

Яку назву має СФПЗ АС класу 1 номер 3 з підвищеними вимогами до конфіденційності, цілісності та доступності інформації?