Восьмий семестр.

Лекція 1. Стислий зміст сьомого семестру

Вступ.

Питання I. 6 етапів створення КСЗІ та її документації.

Питання II. Формування вимог до КСЗІ в ІТС.

Питання III. Керування доступом та забезпечення функцій захищеності інформації.

Контрольні питання.

Вступ.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом та умовами експлуатації ІТС.

Створення комплексів технічного захисту інформації від витоку технічними каналами здійснюється, якщо в ІТС обробляється інформація, що становить державну таємницю, або коли необхідність цього визначено власником інформації.

Створення комплексу засобів захисту від несанкціонованого доступу (далі – КЗЗ) здійснюється в усіх ІТС, де обробляється інформація, яка належить до державних інформаційних ресурсів, належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначено законодавством, а також в ІТС, де така необхідність визначена власником інформації.

Рішення щодо необхідності вжиття заходів захисту від спеціальних впливів на інформацію приймається власником інформації в кожному випадку окремо.

Питання I.

Роботи зі створення КСЗІ виконуються організацією-власником (розпорядником) ІТС з дотриманням вимог нормативно-правових актів щодо провадження діяльності у сфері захисту інформації.

**2. Після чого створюється служба захисту інформації в ІТС?**

Після прийняття рішення про необхідність створення КСЗІ в ІТС для організації цих робіт створюється Служба захисту інформації (далі - СЗІ) в ІТС (2).

**1. Яку назву має НД ТЗІ, що визначає етапи створення КСЗІ?**

**4. Скільки є етапів створення КСЗІ згідно НД ТЗІ?**

НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення КСЗІ в ІТС» визначає 6 етапів створення КСЗІ (1) та її документації:

**5. Яку назву має перший етап створення КСЗІ?**

1. Формування вимог до КСЗІ в ІТС

1.1. Обґрунтування необхідності створення КСЗІ і призначення СЗІ:

- наказ про порядок проведення робіт зі створення КСЗІ

- наказ про створення СЗІ

- положення про СЗІ

- перелік інформації, що підлягає обробленню в ІТС та потребує захисту

**15. Для чого створюються комісії на першому етапі створення КСЗІ?**

1.2. Категоріювання ІТС:

- наказ про призначення комісії з категоріювання

- акт категоріювання

1.3. Обстеження середовищ функціонування ІТС:

- наказ про призначення комісії з обстеження

- акт обстеження

- формуляр ІТС

1.4. Опис моделі порушника політики безпеки інформації: модель порушника

1.5. Опис моделі загроз для інформації: модель загроз

1.6. Формування завдання на створення КСЗІ: звіт за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ

**6. Яку назву має другий етап створення КСЗІ?**

2. Розробка політики безпеки інформації в ІТС

2.1. Вибір варіанту КСЗІ

2.2. Складання політики безпеки

2.3. Складання плану захисту

2.4. Складання календарного плану робіт із захисту інформації

**7. Яку назву має третій етап створення КСЗІ?**

3. Розробка Технічного завдання на створення КСЗІ:

- складання технічного завдання та погодження його з органами Держспецзв’язку

**8. Яку назву має четвертий етап створення КСЗІ?**

4. Розробка проекту КСЗІ:

- складання документів ескізного проекту КСЗІ

- складання документів технічного проекту КСЗІ

- складання документів робочого проекту КСЗІ

**9. Яку назву має п’ятий етап створення КСЗІ?**

5. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС

5.1. Підготовка КСЗІ до введення в дію:

- інструкція про порядок введення в експлуатацію КСЗІ

5.2. Навчання користувачів:

**16. Які адміністратори входять до складу СЗІ?**

- інструкція адміністратора безпеки в ІТС

- інструкція системного адміністратора ІТС

- інструкція користувача ІТС

- правила управління паролями в ІТС

- правила видачі, вилучення та обміну персональних ідентифікаторів, інших атрибутів розмежування доступу в ІТС

5.3. Комплектування КСЗІ

5.4. Будівельно-монтажні роботи:

- наказ про призначення комісії з приймання робіт

- акт приймання робіт

5.5. Пусконалагоджувальні роботи:

- акт інсталяції та налагоджування АВПЗ і КЗЗ від НСД

- акт завершення пусконалагоджувальних робіт

5.6. Попередні випробування КСЗІ:

- наказ про створення комісії з проведення випробувань

- програма та методика попередніх випробувань

- протокол про проведення попередніх випробувань

- акт завершення попередніх випробувань

5.7. Дослідна експлуатація КСЗІ:

- наказ про введення ІТС в дослідну експлуатацію

- акт завершення дослідної експлуатації

- акт завершення робіт зі створення КСЗІ

5.8. Державна експертиза КСЗІ:

- заявка на проведення державної експертизи КСЗІ

- експертний висновок щодо відповідності КСЗІ вимогам НД ТЗІ

- атестат відповідності КСЗІ вимогам НД ТЗІ

- наказ про дозвіл на обробку в ІТС інформації, яка підлягає захисту

**10. Яку назву має шостий етап створення КСЗІ?**

6. Супровід КСЗІ здійснюється з виконанням вимог наступної документації:

- наказ про порядок забезпечення захисту інформації в ІТС

- інструкція щодо забезпечення правил обробки ІзОД в ІТС

- інструкція з антивірусного захисту інформації в ІТС

- інструкція про порядок використання засобів КЗІ в ІТС

- інструкція про порядок обліку та використання машинних носіїв інформації

- інструкція з правил управління паролями в ІТС

- інструкція про порядок створення і зберігання резервних копій інформаційних ресурсів ІТС

- інструкція про порядок проведення контролю режиму обробки та захисту інформації в ІТС

- інструкція про порядок супроводу та модернізації КСЗІ в ІТС

- інструкція про порядок відновлювальних та ремонтних робіт ІТС

- інші інструкції.

Питання II.

Етап 1. Формування вимог до КСЗІ в ІТС

**3. Які готуються накази після прийняття рішення про необхідність створення КСЗІ?**

Після прийняття рішення про необхідність створення КСЗІ відповідальний за ТЗІ організації-власника (розпорядника) ІТС готує для керівника організації 3 накази:

1) про створення Служби захисту інформації в ІТС (далі - СЗІ), порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000 «Типове положення про СЗІ в АС»;

2) про призначення комісії з категоріювання ІТС, завдання та повноваження якої визначено в НД ТЗІ 1.6-005-2013 «Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці»;

3) про призначення комісії з обстеження середовищ функціонування ІТС, завдання та повноваження якої визначено в ДСТУ 3396.1-96 «Технічний захист інформації. Порядок проведення робіт».

**17. Який документ складає СЗІ після свого призначення?**

Після призначення СЗІ складає «Положення про СЗІ в ІТС», що має бути оформлене у вигляді окремого документа згідно рекомендацій НД ТЗІ 1.4-001-2000 та затверджене керівником організації-власника (розпорядника) ІТС.

Положення повинно складатись з таких розділів:

* загальні положення;
* завдання СЗІ;
* функції СЗІ;

- повноваження та відповідальність СЗІ;

- взаємодія СЗІ з іншими підрозділами організації та зовнішніми підприємствами, установами, організаціями;

- штатний розклад та структура СЗІ;

- організація та фінансування робіт СЗІ.

Категоріювання ІТС

Об’єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься ІзОД, підлягають обов’язковому категоріюванню. Об’єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься тільки відкрита інформація, категоріюванню не підлягають.

**18. Що таке об’єкт інформаційної діяльності?**

Об’єктами категоріювання є об’єкти інформаційної діяльності (далі - ОІД), в тому числі об’єкти електронно-обчислювальної техніки (далі - ЕОТ) ІТС. ОІД - це інженерно-технічна споруда (приміщення), транспортний засіб, де здійснюється озвучення та/або обробка технічними засобами ІзОД.

Категоріювання ІТС здійснюється комісією організації-власника (розпорядника) ІТС для визначення необхідного рівня захисту інформації, що обробляється на об’єктах ЕОТ ІТС.

**20. За якою ознакою здійснюється категоріювання ОІД?**

Категоріювання здійснюється за ознакою ступеня обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на ОІД.

**19. Яку назву має нормативний документ, який визначає категорії ОІД?**

**21. Скільки є категорій об’єктів інформаційної діяльності?**

Згідно ТПКО-95 «Тимчасове положення про категоріювання об'єктів» установлюються 4 категорії об'єктів, на яких обробляється технічними засобами та/або озвучується ІзОД, що:

**22. Яка ІзОД відноситься до першої категорії?**

- становить державну таємницю, для якої встановлено гриф секретності «особливої важливості» - перша (І);

**23. Яка ІзОД відноситься до другої категорії?**

- становить державну таємницю, для якої встановлено гриф секретності «цілком таємно» - друга (ІІ);

**24. Яка ІзОД відноситься до третьої категорії?**

- становить державну таємницю, для якої встановлено гриф секретності «таємно», а також інформація, що містить відомості, які становлять іншу передбачену законом таємницю - третя (ІІІ);

**25. Яка ІзОД відноситься до четвертої категорії?**

- не становить державної таємниці - четверта (ІV).

Категоріювання ОІД четвертої категорії здійснюється згідно вимог НД ТЗІ 1.6-005-2013 «Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці».

**26. Яким може бути категоріювання?**

Категоріювання може бути первинним, черговим або позачерговим. Первинне категоріювання здійснюється у разі створення ІТС, де буде оброблятися ІзОД.

**27. Через скільки років здійснюється чергове категоріювання?**

Чергове - не рідше ніж один раз на 5 років.

**28. У якому разі здійснюється позачергове категоріювання?**

Позачергове - у разі зміни ознаки, за якою була встановлена категорія ІТС.

Комісія з категоріювання визначає ступень обмеження доступу до інформації, яка оброблятиметься в ІТС, та з урахуванням цього ступеня встановлює категорію ІТС. Встановлена категорія зазначається в Акті категоріювання ІТС, який складається комісією за результатами її роботи. Акт категоріювання є чинним протягом 5 років з моменту проведення категоріювання, якщо не змінилась ознака, за якою була встановлена категорія об’єкта.

В акті зазначається:

1. Підстава для категоріювання (рішення про створення КСЗІ, закінчення терміну дії акта категоріювання, зміна ознаки, за якою була встановлена категорія, та реквізити наказу про призначення комісії з категоріювання.

2. Вид категоріювання: первинне, чергове, позачергове (у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання, та реквізити акту, яким було встановлено цю категорію).

3. В ІТС здійснюється обробка ІзОД.

4. Ступінь обмеження доступу до ІзОД, що обробляється в ІТС (передбачена законом таємниця; службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, інша конфіденційна інформація, вимога щодо захисту якої встановлена законом).

5. Встановлена комісією категорія.

ОБСТЕЖЕННЯ СЕРЕДОВИЩ ФУНКЦІОНУВАННЯ ІТС

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.

**29. Які середовища ІТС підлягають обстеженню?**

Під час проведення обстеження ІТС необхідно вивчити такі середовища:

- обчислювальне;

- інформаційне;

- користувацьке;

- фізичне (у разі обробки інформації, що становить державну таємницю).

**30. З чого складається обчислювальне середовище?**

При обстеженні обчислювального середовища ІТС повинні бути проаналізовані й описані:

* обладнання - ЕОМ та їхні складові частини (процесори, монітори, термінали, робочі станції та ін.), периферійні пристрої;

- програмне забезпечення - вихідні, завантажувальні модулі, утиліти, СКБД, операційні системи та інші системні програми, діагностичні і тестові програми тощо;

- види і характеристики каналів зв'язку;

- особливості взаємодії окремих компонентів, їх взаємний вплив один на одного, можливі обмеження щодо використання засобів тощо.

При обстеженні інформаційного середовища аналізу підлягає вся інформація, що обробляється, а також зберігається в ІТС. Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, за типом їхнього представлення в ІТС, визначені й описані види її представлення в ІТС. Класифікація є підставою для визначення власником (розпорядником) інформації або ІТС методів і способів захисту кожного окремого виду інформації.

**31. Який документ складається за результатами обстеження інформаційного середовища?**

За результатами обстеження інформаційного середовища складається «Перелік інформації, що підлягає автоматизованому обробленню в ІТС і потребує захисту», який оформлюється як окремий документ, затверджений керівником організації-власника (розпорядника) відповідної інформації, або як розділ у інших документах (Політика безпеки, План захисту, Технічне завдання на створення КСЗІ тощо).

У переліку має бути наведено перелік інформаційних ресурсів (видів інформації), що підлягають обробленню в ІТС, класифікований за такими ознаками:

* назва відповідного інформаційного ресурсу, який визначається цільовим призначенням відповідної інформації;
* характеристики інформації відповідно до встановленого законодавством правового режиму та режиму доступу (ІДТ, КІВД, КІ, ВІВД, 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 373 і вимог власника (розпорядника) інформації;
* вимоги (за наявності) щодо обмеження доступу до інформації користувачів ІТС різних категорій, визначені з урахуванням, наприклад, вимог «Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в АС» або «Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію».

При обстеженні користувацького середовища 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.

**32. Який експлуатаційний документ складається за результатами обстеження обчислювального, інформаційного та користувацького середовищ?**

За результатами обстеження середовищ функціонування ІТС складається «Формуляр ІТС», який оформлюється як окремий документ і складається з таких розділів:

- загальні відомості про ІТС;

- склад технічних засобів ІТС;

- склад програмного забезпечення;

- відомості про програмно-апаратний КЗЗ від НСД;

- відомості про впровадження, випробування та приймання в експлуатацію;

- посадові особи, відповідальні за технічне обслуговування;

- посадові особи, відповідальні за забезпечення захисту інформації;

- реєстрація проведених робіт (технічне обслуговування, ремонт, модернізація тощо);

- відмітки про проведення перевірок КСЗІ;

- перелік технічних та експлуатаційних документів КСЗІ.

**34. У якому разі здійснюється обов’язкове обстеження фізичного середовища ІТС?**

У разі обробки в ІТС таємної інформації здійснюється також обстеження фізичного середовища, під час якого аналізується взаємне розміщення засобів обробки інформації ІТС на ОІД, комунікацій, систем життєзабезпечення і зв’язку, а також режим функціонування цих об’єктів.

Порядок проведення обстеження повинен відповідати ДСТУ 3396.1-96 «Технічний захист інформації. Порядок проведення робіт», а в частині, що стосується захисту інформації від витоку технічними каналами, - НД ТЗІ 3.1-001-07 «Створення комплексу технічного захисту інформації. Передпроектні роботи».

**33. Який підсумковий документ складається за результатами обстеження всіх середовищ?**

За результатами комісія складає «Акт обстеження середовищ функціонування ІТС», який затверджується керівником організації-власника (розпорядника) ІТС і складається з таких розділів:

- клас і склад обчислювальної системи,

- перелік і характеристики інформаційних ресурсів,

- перелік і повноваження користувачів,

- опис фізичного середовища (до акту додаються генеральний і ситуаційний плани, схеми систем життєзабезпечення та заземлення).

Останній крок 1-го етапу складається з таких робіт:

1. Формування завдання на створення КСЗІ в ІТС.

2. Аналіз ризиків реалізації загроз для інформації в ІТС.

3. Вибір варіанту побудови та складу КСЗІ в ІТС.

4. Оформлення звіту за результатами проведеної роботи.

Під час цього кроку здійснюється аналіз ризиків, який передбачає вивчення моделей загроз і порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди).

**35. Що визначається в результаті аналізу ризиків реалізації загроз?**

В результаті аналізу ризиків реалізації загроз визначається перелік суттєвих загроз для ІТС.

Аналіз ризиків полягає в моделюванні картини появи несприятливих умов з урахуванням всіх можливих чинників, що визначають ризики, які називаються вхідними параметрами.

**36. Що відноситься до вхідних параметрів аналізу ризиків?**

До них відносяться активи, вразливості, загрози та збитки.

**37. Що таке активи?**

Активи - ключові компоненти ІТС, що залучені в технологічні процеси та мають певну цінність.

**38. Що таке вразливості?**

Вразливості - слабкості в засобах захисту, викликані помилками або недосконалістю процедур, які можуть бути використані для проникнення в ІТС або пошкодження активів.

**39. За допомогою чого можлива реалізація загроз?**

Загрози - реалізація яких можлива за допомогою використання вразливостей.

**40. Що таке збитки?**

Збитки - втрати після реалізації загрози з урахуванням витрат на відновлення пошкоджених активів.

**41. З яких трьох основних етапів складається процес керування ризиками?**

Керування ризиками – це процес послідовного виконання трьох основних етапів:

- визначення початкових ризиків (в незахищеній ІТС);

- застосування засобів захисту для скорочення ризиків;

- прийняття залишкових ризиків.

З метою підвищення ефективності аналізу ризиків він проводиться по різних напрямах:

- для об'єктів ІТС;

- для процесів, процедур і програм обробки інформації;

- для каналів зв'язку;

- для побічних електромагнітних випромінювань і наведень;

- для механізмів керування системою захисту.

Процес аналізу ризиків включає оцінку:

- можливих втрат в результаті реалізації загроз;

- вірогідності виявлення вразливостей системи, що впливає на оцінку можливих втрат;

- витрат на впровадження заходів і засобів захисту, які скорочують ризик до прийнятного рівня.

Витрати на КСЗІ необхідно співвіднести з цінністю інформаційних ресурсів, які піддаються ризику, а також зі збитком, який може бути нанесений організації в результаті реалізації загроз.

**42. Що уточнюється по завершенні аналізу ризиків реалізації загроз?**

По завершенні аналізу ризиків реалізації загроз уточнюються допустимі залишкові ризики та витрати на заходи захисту інформації.

**47. Яку умовну назву має стандарт щодо керування ризиками інформаційної безпеки?**

На даний час керування ризиками інформаційної безпеки визначає міжнародний стандарт ISO/IEC 27005-2011 «Інформаційна технологія. Методи забезпечення безпеки. Керування ризиками інформаційної безпеки».

**43. З яких 4-х етапів складається керування ризиками згідно стандарту?**

Згідно вимог цього стандарту керування ризиками складається з 4-х етапів:

1) визначення критеріїв;

2) аналіз ризиків;

3) обробка ризиків;

4) прийняття ризиків.

**44. Що є кінцевою метою керування ризиком?** ​​

Кінцевою метою керування ризиком є ​​мінімізація ризику.

**45. У чому полягає мета мінімізації ризику?**

Мета мінімізації ризику полягає в тому, що застосування ефективних заходів захисту призводить до прийняття залишкового ризику.

**46. З яких трьох частин складається мінімізація ризику?**

Мінімізація ризику складається з 3-х частин:

- визначення областей, де ризик неприйнятний;

- вибір ефективних заходів захисту;

- оцінювання заходів захисту та визначення прийнятності залишкового ризику.

**48. Вибір чого необхідно здійснити після завершення аналізу всіх можливих ризиків?**

Після завершення аналізу всіх можливих ризиків необхідно здійснити вибір варіанту побудови КСЗІ в залежності від ступеня обмеження доступу до інформації, яка обробляється в ІТС, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є у розпорядженні власника ІТС.

Характеристика можливих варіантів побудови КСЗІ:

**49. Чим характеризується мінімальний варіант побудови КСЗІ?**

- мінімальний - досягнення необхідного рівня захищеності інформації за мінімальних затрат і допустимого рівня обмежень на технологію її обробки в ІТС;

**50. Чим характеризується оптимальний варіант побудови КСЗІ?**

- оптимальний - досягнення необхідного рівня захищеності інформації за допустимих затрат і заданого рівня обмежень на технологію її обробки в ІТС;

**51. Чим характеризується максимальний варіант побудови КСЗІ?**

- максимальний - досягнення максимального рівня захищеності інформації за необхідних затрат і мінімального рівня обмежень на технологію її обробки в ІТС.

**52. Який документ складається після формування завдань на створення КСЗІ?**

Етап завершується оформленням «Звіту за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ», який затверджується керівником організації-власника (розпорядника) ІТС.

Звіт повинен містити 2 розділи:

- формалізований або неформалізований опис результатів аналізу ризиків, пов’язаних з реалізацією загроз для інформації в ІТС;

- формулювання, з урахуванням результатів виконаного аналізу ризиків, завдань на створення КСЗІ в ІТС.

Питання III.

КЕРУВАННЯ ДОСТУПОМ.

**53. Які є види або принципи керування доступом?**

Є два види або принципи керування доступом в ІТС: довірче та адміністративне.

**54. Що дозволяє робити КЗЗ при довірчому керуванні доступом?**

Довірче керуванням доступом - це таке керування, при якому КЗЗ дозволяє звичайним користувачам управляти потоками інформації в системі між іншими користувачами і об'єктами свого домену (наприклад, на підставі права володіння об'єктами). Тобто визначення повноважень користувачів не вимагає адміністративного втручання.

**55. Що дозволяє робити КЗЗ при адміністративному керуванні доступом?**

Адміністративне керуванням доступом - це таке керування, при якому КЗЗ дозволяє тільки спеціально уповноваженим користувачам (адміністраторам) управляти потоками інформації в системі між користувачами і об'єктами.

Прикладом реалізації адміністративного керування доступом може служити механізм, коли у вигляді атрибутів доступу використовуються мітки, що відображають міру конфіденційності інформації (об'єкта) і рівень допуску користувача. Таким чином, КЗЗ на підставі порівняння міток об'єкта і користувача визначає, чи можна виконати запит користувача.

**56. Що не може змінювати звичайний користувач при адміністративному керуванні доступом?**

Система, що реалізує адміністративне керування, повинна гарантувати, що потоки інформації всередині системи установлюються адміністратором і не можуть бути змінені звичайним користувачем. З іншого боку, система, що реалізує довірче керування доступом, дозволяє звичайному користувачу модифікувати, в т. ч. створювати нові потоки інформації всередині системи.

ЗАБЕЗПЕЧЕННЯ ПОСЛУГ БЕЗПЕКИ (ФУНКЦІЙ ЗАХИЩЕНОСТІ)

З точки зору забезпечення безпеки інформації ІТС або КЗЗ можна розглядати як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти деякій множині загроз.

Існує певний перелік послуг, які на підставі практичного досвіду визнані «корисними» для забезпечення безпеки інформації.

**57. Яку назву має НД ТЗІ, що визначає вимоги до реалізації послуг безпеки?**

Вимоги до реалізації даних послуг наведені в НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в КС від НСД».

Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного. Рівні починаються з першого (1) і зростають до значення n, де n - унікальне для кожного виду послуг.

**58. З яких груп складаються функціональні послуги безпеки?**

Функціональні послуги розбиті на 4 групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із 4-х основних типів: конфіденційність (К), цілісність (Ц), доступність (Д) і спостережність (Н).

**59. Захист інформації від чого реалізують послуги конфіденційності?**

1. Реалізація послуг конфіденційності дозволяє забезпечити захист інформації від несанкціонованого ознайомлення з нею (компрометації). Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні. Принципи, що лежать в основі реалізації послуг, визначаються політикою конфіденційності.

**60. Захист інформації від чого реалізують послуги цілісності?**

2. Реалізація послуг цілісності дозволяє забезпечити захист інформації від несанкціонованої модифікації (включаючи її знищення). Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні. Принципи, що лежать в основі реалізації послуг, визначаються політикою цілісності.

**61. Захист інформації від чого реалізують послуги доступності?**

3. Реалізація послуг доступності забезпечується в ІТС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

**62. Захист ІТС від чого реалізують послуги спостереженості?**

4. Реалізація послуг спостережності забезпечується в ІТС такими послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача.

Всі послуги є більш-менш незалежними. Якщо ж така залежність виникає, тобто реалізація якої-небудь послуги неможлива без реалізації іншої, то цей факт відбивається як необхідні умови для даної послуги (або її рівня). За винятком послуги «аналіз прихованих каналів» залежність між функціональними послугами безпеки та гарантіями відсутня.

**64. На підставі чого кожний клас АС поділяється на підкласи?**

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.

**65. Яка є кількість груп підкласів та сумарна кількість підкласів?**

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

**63. Як розшифровується термін «СФПЗ»?**

«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.

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

**11. Скільки ієрархічних класів має автоматизована система згідно НД ТЗІ?**

- номер класу ІТС (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.

**13. Що таке автоматизована система класу «2» згідно НД ТЗІ?**

Наприклад, СФПЗ ІТС 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}

**12. Що таке автоматизована система класу «1» згідно НД ТЗІ?**

А СФПЗ ІТС класу «1» номер 2 з підвищеними вимогами до забезпечення конфіденційності, цілісності і 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}

**14. Що таке автоматизована система класу «3» згідно НД ТЗІ?**

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 класу чи підкласу ІТС.

**Контрольні питання:**

1. **Яку назву має НД ТЗІ, що визначає етапи створення КСЗІ?**
2. **Після чого створюється служба захисту інформації в ІТС?**
3. **Які готуються накази після прийняття рішення про необхідність створення КСЗІ?**
4. **Скільки є етапів створення КСЗІ згідно НД ТЗІ?**
5. **Яку назву має перший етап створення КСЗІ?**
6. **Яку назву має другий етап створення КСЗІ?**
7. **Яку назву має третій етап створення КСЗІ?**
8. **Яку назву має четвертий етап створення КСЗІ?**
9. **Яку назву має п’ятий етап створення КСЗІ?**
10. **Яку назву має шостий етап створення КСЗІ?**
11. **Скільки ієрархічних класів має автоматизована система згідно НД ТЗІ?**
12. **Що таке автоматизована система класу «1» згідно НД ТЗІ?**
13. **Що таке автоматизована система класу «2» згідно НД ТЗІ?**
14. **Що таке автоматизована система класу «3» згідно НД ТЗІ?**
15. **Для чого створюються комісії на першому етапі створення КСЗІ?**
16. **Які адміністратори входять до складу СЗІ?**
17. **Який документ складає СЗІ після свого призначення?**
18. **Що таке об’єкт інформаційної діяльності?**
19. **Яку назву має нормативний документ, який визначає категорії ОІД?**
20. **За якою ознакою здійснюється категоріювання ОІД?**
21. **Скільки є категорій об’єктів інформаційної діяльності?**
22. **Яка ІзОД відноситься до першої категорії?**
23. **Яка ІзОД відноситься до другої категорії?**
24. **Яка ІзОД відноситься до третьої категорії?**
25. **Яка ІзОД відноситься до четвертої категорії?**
26. **Яким може бути категоріювання?**
27. **Через скільки років здійснюється чергове категоріювання?**
28. **У якому разі здійснюється позачергове категоріювання?**
29. **Які середовища ІТС підлягають обстеженню?**
30. **З чого складається обчислювальне середовище?**
31. **Який документ складається за результатами обстеження інформаційного середовища?**
32. **Який експлуатаційний документ складається за результатами обстеження обчислювального, інформаційного та користувацького середовищ?**
33. **Який підсумковий документ складається за результатами обстеження всіх середовищ?**
34. **У якому разі здійснюється обов’язкове обстеження фізичного середовища ІТС?**
35. **Що визначається в результаті аналізу ризиків реалізації загроз?**
36. **Що відноситься до вхідних параметрів аналізу ризиків?**
37. **Що таке активи?**
38. **Що таке вразливості?**
39. **За допомогою чого можлива реалізація загроз?**
40. **Що таке збитки?**
41. **З яких трьох основних етапів складається процес керування ризиками?**
42. **Що уточнюється по завершенні аналізу ризиків реалізації загроз?**
43. **З яких 4-х етапів складається керування ризиками згідно стандарту?**
44. **Що є кінцевою метою керування ризиком? ​​**
45. **У чому полягає мета мінімізації ризику?**
46. **З яких трьох частин складається мінімізація ризику?**
47. **Яку умовну назву має стандарт щодо керування ризиками інформаційної безпеки?**
48. **Вибір чого необхідно здійснити після завершення аналізу всіх можливих ризиків?**
49. **Чим характеризується мінімальний варіант побудови КСЗІ?**
50. **Чим характеризується оптимальний варіант побудови КСЗІ?**
51. **Чим характеризується максимальний варіант побудови КСЗІ?**
52. **Який документ складається після формування завдань на створення КСЗІ?**
53. **Які є види або принципи керування доступом?**
54. **Що дозволяє робити КЗЗ при довірчому керуванні доступом?**
55. **Що дозволяє робити КЗЗ при адміністративному керуванні доступом?**
56. **Що не може змінювати звичайний користувач при адміністративному керуванні доступом?**
57. **Яку назву має НД ТЗІ, що визначає вимоги до реалізації послуг безпеки?**
58. **З яких груп складаються функціональні послуги безпеки?**
59. **Захист інформації від чого реалізують послуги конфіденційності?**
60. **Захист інформації від чого реалізують послуги цілісності?**
61. **Захист інформації від чого реалізують послуги доступності?**
62. **Захист ІТС від чого реалізують послуги спостереженості?**
63. **Як розшифровується термін «СФПЗ»?**
64. **На підставі чого кожний клас АС поділяється на підкласи?**
65. **Яка є кількість груп підкласів та сумарна кількість підкласів?**
66. **Яку умовну назву має підклас з підвищеними вимогами до конфіденційності інформації в АС класу 2?**
67. **Яку умовну назву має підклас з підвищеними вимогами до цілісності інформації в АС класу 3?**
68. **Яку умовну назву має підклас з підвищеними вимогами до доступності інформації в АС класу 3?**
69. **Яку умовну назву має підклас з підвищеними вимогами до конфіденційності та цілісності інформації в АС класу 2?**
70. **Яку умовну назву має підклас з підвищеними вимогами до конфіденційності та доступності інформації в АС класу 2?**
71. **Яку умовну назву має підклас з підвищеними вимогами до цілісності та доступності інформації в АС класу 3?**
72. **Яку умовну назву має підклас з підвищеними вимогами до конфіденційності, цілісності та доступності інформації в АС класу 1?**
73. **Яку умовну назву має СФПЗ АС класу 2 номер 5 з підвищеними вимогами до конфіденційності інформації?**
74. **Яку умовну назву має СФПЗ АС класу 3 номер 1 з підвищеними вимогами до цілісності інформації?**
75. **Яку умовну назву має СФПЗ АС класу 3 номер 2 з підвищеними вимогами до доступності інформації?**
76. **Яку умовну назву має СФПЗ АС класу 2 номер 4 з підвищеними вимогами до конфіденційності та доступності інформації?**
77. **Яку умовну назву має СФПЗ АС класу 2 номер 3 з підвищеними вимогами до забезпечення конфіденційності та цілісності інформації?**
78. **Яку умовну назву має СФПЗ АС класу 3 номер 2 з підвищеними вимогами до цілісності та доступності інформації?**

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

**Домашнє завдання складається з трьох етапів:**

1. Прочитати матеріал Лекції 1.

2. Виділити жовтим фоном текст, який на вашу думку містить найбільш важливі правила, моменти (та ін.), А також виділити бірюзовим кольором текст з менш важливим, але з необхідним вмістом для фахівця з кібербезпеки.

3. З фінального розділу "Контрольні питання" перенести кожне з 79-ти (!) питань до тексту лекції і поставити це питання перед початком того тексту, що містить відповідь на це питання.

**Наприклад:**

… Питання I.

Роботи зі створення КСЗІ виконуються організацією-власником (розпорядником) ІТС з дотриманням вимог нормативно-правових актів щодо провадження діяльності у сфері захисту інформації.

**2.Після чого створюється служба захисту інформації в ІТС?**

Після прийняття рішення про необхідність створення КСЗІ в ІТС для організації цих робіт створюється Служба захисту інформації (далі - СЗІ) в ІТС (2).

НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення КСЗІ в ІТС»…