**Заняття 6. Фундаментальні державні джерела для розробки комплексних систем захисту інформації**

**Вступ.**

**Питання 1. Послуги у галузі ТЗІ і КЗІ: умови та джерела.**

**Питання 2. Отримання державного сертифікату відповідності розробленим комплексом засобів захисту.**

**Контрольні питання.**

**Вступ.**

Почнемо лекцію з питання ліцензування такого виду господарської діяльності як надання послуг у галузі технічного захисту інформації (далі - ТЗІ).

**Питання 1.**

Основним нормативно-правовим актом України визначає види господарської діяльності, що підлягають ліцензуванню, порядок їх ліцензування, встановлює державний контроль у сфері ліцензування, відповідальність суб'єктів господарювання та органів ліцензування за порушення законодавства у сфері ліцензування є Закон України «Про ліцензування видів господарської діяльності».

У Законі вживаються терміни, які мають таке значення:

- ліцензіат - суб’єкт господарювання, який має ліцензію на провадження встановленого законом виду господарської діяльності;

- ліцензійні умови - нормативно-правовий акт Кабінету Міністрів України, положення якого встановлюють вичерпний перелік вимог, обов’язкових для виконання ліцензіатом, та вичерпний перелік документів, що додаються до заяви про отримання ліцензії;

- ліцензія - документ, що надається органом ліцензування, на право провадження суб’єктом господарювання визначеного ним виду господарської діяльності, що підлягає ліцензуванню, в електронному вигляді (запис про наявність ліцензії у такого суб’єкта господарювання в Єдиному державному реєстрі юридичних осіб та фізичних осіб - підприємців) або на паперовому носії;

- ліцензування - засіб державного регулювання провадження видів господарської діяльності, що підлягають ліцензуванню, спрямований на реалізацію єдиної державної політики у сфері ліцензування.

Дія цього Закону не поширюється на порядок видачі, переоформлення та анулювання ліцензій на здійснення таких видів господарської діяльності:

- банківську діяльність, яка здійснюється відповідно до Закону України «Про банки і банківську діяльність»;

- діяльність в галузі телебачення і радіомовлення, яка здійснюється відповідно до Закону України «Про телебачення і радіомовлення».

Згідно статті 5 Закону Експертно-апеляційна рада з питань ліцензування є постійно діючим колегіальним органом при спеціально уповноваженому органі з питань ліцензування та діє за регламентом, що затверджується спеціально уповноваженим органом з питань ліцензування.

Обов’язками Експертно-апеляційної ради з питань ліцензування є:

- розгляд апеляцій та інших скарг здобувачів ліцензії, ліцензіатів на дії органу ліцензування або інших заявників щодо порушення законодавства у сфері ліцензування;

- розгляд звернень органів ліцензування або спеціально уповноваженого органу з питань ліцензування щодо проведення позапланових перевірок додержання ліцензіатами вимог ліцензійних умов на підставах, передбачених пунктами 4 та 5 частини дев’ятої статті 19 цього Закону.

Згідно статті 7 Закону ліцензуванню підлягають такі види господарської діяльності:

8) діяльність у сфері телекомунікацій з урахуванням особливостей, визначених Законом України «Про телекомунікації» (згідно статті 21 Закону ліцензування діяльності у сфері телекомунікацій, передбачене цим пунктом, втрачає чинність з 1 січня 2018 року),

надання послуг у галузі КЗІ (крім послуг ЕЦП) та ТЗІ, за переліком, що визначається Кабінетом Міністрів України;

23) діяльність, пов’язана з розробленням, виготовленням, постачанням спеціальних технічних засобів для зняття інформації з каналів зв’язку та інших технічних засобів негласного отримання інформації (критерії належності та перелік технічних засобів негласного отримання інформації визначаються Кабінетом Міністрів України за поданням Служби безпеки України).

Згідно статті 9 Закону *ліцензіат зобов’язаний виконувати вимоги ліцензійних умов відповідного виду господарської діяльності, а здобувач ліцензії для її одержання - відповідати ліцензійним умовам*.

Ліцензійні умови та зміни до них розробляються органом ліцензування, що є центральним органом виконавчої влади, підлягають погодженню спеціально уповноваженим органом з питань ліцензування та затверджуються Кабінетом Міністрів України.

Ліцензійними умовами встановлюються зміст та форма:

1) заяви про одержання ліцензії;

2) документів, що додаються до заяви про одержання ліцензії;

3) опису документів, що подаються для одержання ліцензії;

4) документів щодо кожного місця провадження господарської діяльності.

Згідно статті 10 Закону документи, подання яких до органу ліцензування та видача яких органом ліцензування передбачені цим Законом, можуть бути подані до органу ліцензування та отримані від цього органу ліцензування за вибором здобувача ліцензії:

1) нарочно відповідно до пункту 3 частини другої статті 6 та у порядку, встановленому статтею 9 Закону України «Про адміністративні послуги»;

2) поштовим відправленням з описом вкладення (орган ліцензування надсилає поштові відправлення з повідомленням за місцезнаходженням здобувача ліцензії протягом одного робочого дня з дня оформлення відповідного документа, якщо інший строк надсилання не встановлено законом);

3) в електронному вигляді за допомогою телекомунікаційних засобів зв’язку.

Згідно статті 11 Закону здобувач ліцензії подає до органу ліцензування заяву про отримання ліцензії за визначеною ліцензійними умовами формою.

У заяві про отримання ліцензії повинна міститися інформація про:

1) здобувача ліцензії:

2) вид господарської діяльності (повністю або частково), зазначений у статті 7 цього Закону, на провадження якого здобувач ліцензії має намір одержати ліцензію;

3) бажаний спосіб одержання документів.

Підставою для прийняття рішення про відмову у видачі ліцензії за результатом розгляду заяви про отримання ліцензії є виявлення:

1) невідповідності здобувача ліцензії ліцензійним умовам, встановленим для провадження виду господарської діяльності, зазначеного в заяві про отримання ліцензії;

2) недостовірності даних у підтвердних документах, поданих здобувачем ліцензії.

Орган ліцензування на наступний робочий день після дня прийняття ним рішення про видачу ліцензії здобувачу ліцензії передає відомості про таке рішення в електронному вигляді до Єдиного державного реєстру юридичних осіб та фізичних осіб - підприємців у порядку, визначеному розпорядником цього реєстру.

Строк прийняття рішення про видачу ліцензії становить десять робочих днів з дня одержання органом ліцензування заяви про отримання ліцензії.

Набуття здобувачем ліцензії права на провадження виду господарської діяльності, що підлягає ліцензуванню, відбувається з моменту внесення даних про рішення органу ліцензування про видачу йому ліцензії до *Єдиного державного реєстру юридичних осіб та фізичних осіб - підприємців.*

У повідомленні про прийняття рішення про видачу ліцензії орган ліцензування зазначає розрахункові реквізити для внесення плати за видачу ліцензії.

Ліцензія на провадження здобувачем ліцензії визначеного ним виду господарської діяльності, що підлягає ліцензуванню, оформлюється органом ліцензування в електронному вигляді (запис про рішення органу ліцензування щодо видачі ліцензії суб’єкту господарювання в Єдиному державному реєстрі юридичних осіб та фізичних осіб - підприємців).

Ліцензія видається на необмежений строк.

Форму та зміст ліцензії визначає спеціально уповноважений орган з питань ліцензування.

Ліцензія на паперовому носії має бути підписана керівником органу ліцензування, який підписав рішення про видачу ліцензії (або уповноваженою ним посадовою особою), і завірена гербовою печаткою цього органу ліцензування.

Згідно статті 14 Закону за видачу ліцензії справляється разова плата в розмірі однієї мінімальної заробітної плати, виходячи з розміру мінімальної заробітної плати, що діє на день прийняття органом ліцензування рішення про видачу ліцензії, якщо інший розмір плати не встановлений законом (на даний час - 3200 грн.).

Переоформлення ліцензії є безоплатним.

Плата за видачу ліцензії вноситься ліцензіатом у строк не пізніше десяти робочих днів з дня отримання здобувачем ліцензії від органу ліцензування повідомлення про прийняте ним рішення про видачу ліцензії.

Документом, що підтверджує внесення плати за видачу ліцензії, є копія квитанції, виданої банком, копія платіжного доручення з відміткою банку, квитанція з платіжного термінала, квитанція (чек) з поштового відділення зв’язку.

Згідно статті 19 Закону державний нагляд за додержанням органами державної влади чи державними колегіальними органами вимог законодавства у сфері ліцензування здійснює спеціально уповноважений орган з питань ліцензування шляхом проведення планових та позапланових перевірок у порядку, встановленому Кабінетом Міністрів України за поданням спеціально уповноваженого органу з питань ліцензування.

Спеціально уповноважений орган з питань ліцензування складає акт перевірки у двох примірниках в останній день перевірки.

Один примірник акта видається керівнику органу ліцензування, діяльність якого перевірялася, другий - зберігається спеціально уповноваженим органом з питань ліцензування.

У разі виявлення порушення органом ліцензування законодавства у сфері ліцензування спеціально уповноважений орган з питань ліцензування протягом п’яти робочих днів з дня складення акта перевірки видає розпорядження про усунення порушень законодавства у сфері ліцензування.

Контроль за наявністю у ліцензіатів (суб’єктів господарювання) ліцензій здійснюють державні органи, на які згідно із законом покладено функції контролю за наявністю ліцензій.

Контроль за додержанням ліцензіатами вимог ліцензійних умов здійснюють у межах своїх повноважень органи ліцензування шляхом проведення планових і позапланових перевірок відповідно до Закону України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» з урахуванням особливостей, визначених цим Законом.

З метою забезпечення ліцензіатом присутності керівника, його заступника або іншої уповноваженої особи під час проведення органом ліцензування планової перевірки додержання ліцензіатом вимог ліцензійних умов, орган ліцензування вживає вичерпних заходів попереднього інформування (не менш як за десять робочих днів) ліцензіата про дату та місце проведення планової перевірки, зокрема за допомогою засобів поштового, телефонного, факсимільного та/або електронного поштового зв’язку.

Про проведення позапланової перевірки ліцензіат повідомляється у день перевірки.

Акт перевірки додержання ліцензіатом вимог ліцензійних умов складається в останній день проведення перевірки.

14 листопада 2000 року постановою Кабінету Міністрів України № 1698 (у редакції постанови Кабінету Міністрів України [від 27 липня 2011 року № 798](http://zakon1.rada.gov.ua/laws/show/798-2011-%D0%BF)) був затверджений  «Перелік органів ліцензування»:

|  |  |
| --- | --- |
| Орган ліцензування | Вид господарської діяльності |
| Адміністрація Держспецзв'язку | надання послуг у галузі ТЗІ і КЗІ |

16 листопада 2016 року № 821 постановою Кабінету Міністрів України був затверджений «Перелік послуг у галузі КЗІ (крім послуг ЕЦП) і ТЗІ, господарська діяльність щодо яких підлягає ліцензуванню»:

I. Послуги у галузі КЗІ (крім послуг ЕЦП), господарська діяльність щодо яких підлягає ліцензуванню

1. Розроблення і складення конструкторської та іншої технічної документації, виробництво криптосистем і засобів КЗІ (з наданням права провадження діяльності у галузі КЗІ, що становить державну таємницю; з наданням права провадження діяльності у галузі криптографічного захисту службової інформації).

2. Постачання, монтаж (встановлення), налаштування, технічне обслуговування (супроводження), ремонт та/або утилізація криптосистем і засобів КЗІ (з наданням права провадження діяльності у галузі КЗІ, що становить державну таємницю; з наданням права провадження діяльності у галузі криптографічного захисту службової інформації).

3. Тематичні та експертні дослідження криптосистем і засобів КЗІ (з наданням права провадження діяльності у галузі КЗІ, що становить державну таємницю; з наданням права провадження діяльності у галузі криптографічного захисту службової інформації).

II. Послуги у галузі ТЗІ, господарська діяльність щодо яких підлягає ліцензуванню

1. Оцінювання захищеності інформації, що не становить державної таємниці.

2. Оцінювання захищеності інформації усіх видів, у тому числі інформації, що становить державну таємницю.

3. Виявлення закладних пристроїв.

«Ліцензійні умови провадження господарської діяльності з надання послуг у галузі ТЗІ (згідно з переліком, що визначається Кабінетом Міністрів України)» були затверджені наказом Адміністрації Держспецз’язку від 14 жовтня 2014 року № 532, зареєстрованим в Міністерстві юстиції України 4 листопада 2014 року за № 1387/26164.

4.2. Провадження господарської діяльності з надання послуг, визначених цими Ліцензійними умовами, суб'єкт господарювання здійснює за умови наявності спеціалістів з повною чи базовою вищою освітою за напрямом підготовки «Інформаційна безпека» або повною чи базовою вищою інженерно-технічною освітою фахового спрямування відповідно до обраного виду послуг з додатковою підготовкою на курсах перепідготовки та підвищення кваліфікації фахівців з питань ТЗІ за напрямами підготовки відповідно до обраного виду послуг.

7.1. Залежно від правового режиму доступу до інформації встановлюються особливі умови надання послуг з технічного захисту:

- усіх видів інформації, у тому числі що становить державну таємницю;

- інформації, що не становить державної таємниці.

Наказом Адміністрації Держспецзв’язку від 28 березня 2013 року № 158 «Про надання адміністративних послуг у галузі технічного захисту інформації» були затверджені такі документи:

- Інформаційна картка адміністративної послуги Адміністрації Держспецзв’язку з видачі ліцензій (копії, дубліката) на провадження господарської діяльності з надання послуг у галузі ТЗІ;

- Технологічна картка адміністративної послуги Адміністрації Держспецзв’язку з видачі ліцензій (копії, дубліката) на провадження господарської діяльності з надання послуг у галузі ТЗІ.

Разом з тим, згідно «Положення про дозвільний порядок проведення робіт з ТЗІ для власних потреб», затвердженого наказом ДСТСЗІ СБУ від 23 лютого 2002 року № 9, зареєстрованим в Міністерстві юстиції України 13 березня 2002 року за № 245/6533, органи державної влади та місцевого самоврядування, які мають намір проводити роботи у галузі ТЗІ для власних потреб, можуть отримати такий дозвіл від Адміністрації Держспецз’язку у разі виконання вимог цього Положення. За відсутності у державного органу такого дозволу ці роботи повинні виконуватись тільки установою, що має ліцензію на право провадження діяльності у галузі ТЗІ.

Згідно статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» для створення КСЗІ, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері захисту інформації.

Тобто розроблений КЗЗ повинен пройти процедуру сертифікації в Українській державній системі сертифікації продукції (УкрСЕПРО) і отримати сертифікат відповідності, після чого він вноситься до Реєстру УкрСЕПРО. Здійснюється це згідно «Правил проведення робіт із сертифікації засобів захисту інформації», затверджених наказом Адміністрації Держспецз’язку та Державного комітету України з питань регуляторної політики підприємництва від 25.04.2007 № 75/91 і зареєстрованих у Міністерстві юстиції України 14.05.2007 за № 498/13765.

**Питання 2.**

**Для того, щоб розроблений КЗЗ отримав сертифікат відповідності він повинен відповідати вимогам НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в КС від НСД»,** тобто забезпечити:

- безперервний захист;

- «модульність» КЗЗ;

- атрибути доступу;

- керування доступом.

Крім того, КЗЗ від НСД повинен реалізувати:

- концепцію диспетчера доступу;

- реєстрацію дій користувачів;

- послуги безпеки (функції захищеності);

- гарантії реалізації послуг безпеки.

**1. Безперервний захист**

КЗЗ повинен забезпечити захист інформації в ІТС протягом всього періоду її існування. З моменту створення об'єкта ІТС (або його імпорту) до його знищення (або експорту) всі запити на доступ до нього (або від нього) повинен контролювати КЗЗ.

Головним аспектом є те, що не повинно існувати можливості одержати доступ до об'єкта (або від об'єкта) в обхід КЗЗ. Для безперервного захисту об'єктів КЗЗ повинен забезпечувати свою цілісність і керованість.

Другим аспектом є те, що особливе значення набуває визначення діючих за умовчанням правил, які визначають початкові умови, за яких починається існування об'єкта всередині ІТС.

**2. «Модульність» КЗЗ**

КЗЗ повинен мати модульну структуру. На рівні розгляду архітектури ІТС «модульність» означає, що КЗЗ має бути реалізований як набір відносно незалежних частин. Кожна з цих частин повинна взаємодіяти з іншими тільки через добре визначені iнтерфейси.

На рівні розгляду архітектури КЗЗ «модульність» означає, що КЗЗ має функціонувати як сукупність логічних груп програмного та апаратного забезпечення так, щоб кожна група вирішувала певні завдання. Для ПЗ, наприклад, в простішому випадку під цим слід розуміти, що подібні функції мають бути зосереджені в певних вихідних файлах.

Під більш жорсткими вимогами слід розуміти використання приховання даних та інших механізмів, що дозволяють мати впевненість, що кожний модуль вирішує єдине завдання. Будь-яка взаємодія між компонентами повинна здійснюватись тільки через відомі і описані канали (iнтерфейси).

**3. Атрибути доступу**

Для реалізації політики безпеки КЗЗ повинен забезпечити ізоляцію об'єктів всередині сфери управління та гарантувати розмежування запитів доступу і керування потоками інформації між об'єктами. Для цього всі об'єкти ІТС повинні мати атрибути доступу. Атрибути доступу об'єкта - це інформація, яка дозволяє КЗЗ iдентифікувати об'єкт і перевіряти легальність запитів доступу до нього.

Кожний об'єкт ІТС повинен мати певний набір атрибутів доступу, який включає унікальний iдентифікатор та іншу інформацію, що визначає його права доступу і/або права доступу до нього. Атрибут доступу - термін, що використовується для опису будь-якої інформації, яка використовується при керуванні доступом і зв'язана з користувачами, процесами або пасивними об'єктами. Відповідність атрибутів доступу і об'єкта може бути як явною, так і неявною. Атрибути доступу об'єкта є частиною його подання в ІТС.

Коли користувачі або процеси намагаються одержати доступ до пасивних об'єктів, механізми, що реалізують керування доступом, на підставі політики безпеки і перевірки атрибутів доступу можуть «прийняти рішення» про легальність запиту. Використовуючи набір атрибутів доступу відповідно до прийнятої політики безпеки, можна реалізувати довірче або адміністративне керування доступом, контроль за цілісністю та інші види керування доступом.

Для відображення функціональностi ІТС у простір, в якому не розглядаються права власності, використовується концепція матриці доступу. Проста матриця доступу – це таблиця, яка містить iдентифікатори користувачів, об'єктів та видів доступу до них.

Матриця доступу може бути:

- двомірною (наприклад, користувачі/об'єкти або процеси/об'єкти);

- тримірною (користувачі/процеси/об'єкти);

- повною, тобто містити вздовж кожної з осей всі існуючі iдентифікатори ІТС.

Повна матриця доступу дозволяє точно описати, хто (iдентифікатор користувача), через що (iдентифікатор процесу), до чого (iдентифікатор об'єкта), який вид доступу може одержати (iдентифікатор доступу).

**4. Керування доступом**

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

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.

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.

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.

Створення додаткових потоків інформації може бути зумовлене:

- модифікацією атрибутів доступу користувача, процесу або пасивного об'єкта;

- створенням нових об'єктів (включаючи копіювання існуючих);

- експортом або імпортом об'єктів.

Сталість атрибутів доступу

При адміністративному керуванні доступом звичайний користувач не може змінювати атрибути доступу об'єкта. Таким чином, якщо політика потоків інформації, створена адміністратором, визначає, що два користувача не можуть спільно використовувати інформацію, то жоден з них не спроможний передати іншому користувачу свої повноваження щодо доступу до існуючого об'єкта.

І навпаки, при довірчому керуванні доступом звичайний користувач може змінювати атрибути доступу об'єкта, що належить йому.

Створення нових об'єктів

Якщо при адміністративному керуванні доступом політика потоків інформації, створена адміністратором, визначає, що два користувачі не можуть спільно використовувати інформацію, то жоден з них не може створити об'єкт, доступний іншому. Додатково повинні існувати правила для визначення атрибутів доступу, що мають присвоюватись об'єкту, одержаному копіюванням існуючого.

І навпаки, при довірчому керуванні доступом звичайний користувач може створювати атрибути доступу для знову створеного об'єкту. Наприклад, система може дозволяти творцю об'єкта визначати користувачів, що можуть мати права доступу до об'єкта.

Експорт і імпорт об'єктів

*При адміністративному керуванні атрибути доступу об'єкта мають зберігатись під час його експорту на зовнішній носiй.* Додатково повинні існувати правила для присвоєння атрибутів доступу імпортованому об'єкту.

І навпаки, при довірчому керуванні доступом об'єкт може бути експортований без збереження атрибутів доступу. Додатково може існувати можливість імпорту звичайним користувачем об'єкта з наступним присвоєнням йому атрибутів доступу на розсуд користувача.

Проте, навіть відповідно до політики довірчого керування доступом, атрибути доступу об'єкта під час виконання деяких операцій, наприклад, під час його резервного копіювання, мають зберігатися. Якщо об'єкт буде коли-небудь відновлено з резервної копії, то його атрибути доступу також мають бути відновлені.

**5. Концепція диспетчера доступу**

При реалізації КЗЗ використовується концепція диспетчера доступу, що повинна забезпечити:

- безперервний і повний захист;

- захищеність від модифікації;

- невеликі розміри.

Це означає, що диспетчер доступу має бути завжди активним і повинен контролювати всі запити на доступ до будь-якого захищеного об'єкта, який піддається впливу. Диспетчер доступу має бути захищений від модифікацiї, що для програмної реалізації звичайно вважається ізоляцією домену КЗЗ від доменів інших процесів.

Диспетчер доступу не повинен складати весь КЗЗ, а повинен включати мінімально необхідний набір механізмів, що безпосередньо реалізують перевірку легальностi запитів на доступ і, можливо, реєстрацію цих запитів.

Головна мета диспетчера доступу - забезпечення єдиної точки проходження всіх запитів всередині ІТС. Це гарантія того, що потоки інформації між користувачами, процесами і об'єктами відповідають вимогам політики безпеки.

Класичний погляд на диспетчер доступу полягає в тому, що він служить бар'єром між користувачем і об'єктом, до якого він хоче одержати доступ. Диспетчер доступу дозволяє або забороняє доступ відповідно до того, чи є запит авторизованим*. Рішення приймається на підставі перевірки атрибутів доступу користувача, процесу і об'єкта*.

Узагальненням концепції диспетчера доступу є ідея герметизації, коли кожний об'єкт як би герметизовано диспетчером доступу, що утворює навкруги нього непрониклу оболонку. Кількість захищених (що знаходяться всередині оболонки) об'єктів може змінюватись від одного об'єкта до всіх об'єктів системи.

Диспетчер доступу повинен забезпечити неможливість доступу до об'єкта в обхід механізмів захисту, перевірку наявності у користувача і/або процесу прав доступу до об'єкта і реєстрації подій, що відбуваються.

**6. Реєстрація дій користувачів**

Коли користувач працює з ІТС, то система розглядає його не як фізичну особу, а як об'єкт, якому притаманні певні атрибути і поводження. КЗЗ повинен забезпечувати реєстрацію дій користувачів щодо використання ресурсів системи, а також інших дій і подій, які так або інакше можуть вплинути на дотримання реалізованої ІТС політики безпеки.

Система повинна надавати користувачам, що мають адміністративні повноваження, можливість проглядати та аналізувати дані реєстрації, що представляються у вигляді журналів реєстрації, виявляти небезпечні з точки зору політики безпеки події, встановлювати їх причини і користувачів, відповідальних за порушення політики безпеки.

**7. Послуги безпеки (функції захищеності)**

З точки зору забезпечення безпеки інформації ІТС або КЗЗ можна розглядати як набір функціональних послуг безпеки. Кожна послуга безпеки 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. Вимоги до реалізації даних послуг наведені *в НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в КС від НСД».*

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

**Функціональні 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 спостереженість (Н**).

1. Послуги конфіденційності реалізують 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.

2. Послуги цілісності реалізують захист інформації від несанкціонованої модифікації (спотворення, руйнування). Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні. Принципи, що лежать в основі реалізації послуг, визначаються політикою цілісності.

3. Послуги доступності реалізують захист інформації від несанкціонованого блокування доступу до неї. Також забезпечує можливості використання ІТС в цілому та окремих функцій та гарантує спроможність ІТС функціонувати в разі відмови її компонентів. Доступність забезпечується в ІТС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

4. Послуги спостереженості реалізують захист ІТС від несанкціонованого втручання в її роботу (виводу з ладу). Також забезпечує відповідальність користувача за свої дії та підтримує спроможності КЗЗ виконувати свої функції. Спостереженість 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.

**8. Гарантії реалізації послуг безпеки**

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в ІТС, є також критерії гарантій, які дозволяють оцінити коректність реалізації послуг безпеки.

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.

Критерії гарантій включають вимоги до архітектури КЗЗ, середовища та послідовностi його розробки, випробування КЗЗ, середовища його функціонування та якості 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.

**Контрольні питання**

1. Який нормативно-правовий акт є основним з питань ліцензування господарської діяльності?
2. Що таке ліцензія згідно закону?
3. Хто такий ліцензіат згідно закону?
4. Що таке ліцензування згідно закону?
5. Ліцензування яких видів господарської діяльності здійснюється відповідно до окремих законів?
6. Який орган розглядає скарги щодо порушення законодавства у сфері ліцензування згідно закону?
7. Вимоги якого документу зобов’язаний виконувати ліцензіат згідно закону?
8. Вимогам якого документу зобов’язаний відповідати здобувач ліцензії згідно закону?
9. Яким чином можуть бути подані документи до органу ліцензування згідно закону?
10. Виявлення чого є підставою для прийняття рішення про відмову у видачі ліцензії згідно закону?
11. Яким є строк прийняття рішення про видачу ліцензії з дня одержання заяви про її отримання згідно закону?
12. На який строк видається ліцензія згідно закону?
13. В якому реєстрі робиться запис про рішення органу ліцензування щодо видачі ліцензії суб’єкту господарювання згідно закону?
14. В якому розмірі справляється разова плата за видачу ліцензії згідно закону?
15. В якому розмірі справляється разова плата за переоформлення ліцензії згідно закону?
16. В який строк з дня отримання повідомлення про прийняте рішення про видачу ліцензії вноситься плата за її видачу згідно закону?
17. Яким шляхом здійснюється державний нагляд за додержанням органами влади вимог законодавства у сфері ліцензування згідно закону?
18. В який строк до початку планової перевірки інформується ліцензіат про її проведення згідно закону?
19. Коли повідомляється ліцензіат про проведення позапланової перевірки згідно закону?
20. Коли складається акт перевірки додержання ліцензіатом вимог ліцензійних умов згідно закону?
21. Який орган займається ліцензуванням господарської діяльності у галузі захисту інформації?
22. Надання яких послуг у галузі ТЗІ підлягає ліцензуванню?
23. Яку назву має НД ТЗІ, що визначає вимоги до розробки КЗЗ від НСД?
24. Що повинен забезпечити КЗЗ від НСД згідно вимог НД ТЗІ?
25. Що повинен робити КЗЗ з моменту створення об'єкта до його знищення?
26. Що повинен забезпечувати КЗЗ для безперервного захисту об'єктів?
27. Які є види або принципи керування доступом?
28. Що дозволяє робити КЗЗ при довірчому керуванні доступом?
29. Що дозволяє робити КЗЗ при адміністративному керуванні доступом?
30. Що не може змінювати звичайний користувач при адміністративному керуванні доступом?
31. При якому керуванні атрибути доступу об'єкта мають зберігатись під час його експорту на носiй?
32. Що таке атрибути доступу об'єкта?
33. Що таке проста матриця доступу?
34. Які ідентифікатори містить повна матриця доступу?
35. Що означає «модульність» КЗЗ на рівні розгляду архітектури ІТС?
36. Що означає «модульність» на рівні розгляду архітектури КЗЗ?
37. Що повинна забезпечити концепція диспетчера доступу?
38. Що є головною метою диспетчера доступу?
39. В чому полягає класичний погляд на диспетчер доступу?
40. На підставі чого приймає рішення диспетчер доступу?
41. Яка ідея є узагальненням концепції диспетчера доступу?
42. Що являє собою кожна послуга безпеки?
43. Яку назву має НД ТЗІ, що визначає вимоги до реалізації послуг безпеки?
44. З яких груп складаються функціональні послуги безпеки?
45. Захист інформації від чого реалізують послуги конфіденційності?
46. Захист інформації від чого реалізують послуги цілісності?
47. Захист інформації від чого реалізують послуги доступності?
48. Захист ІТС від чого реалізують послуги спостереженості?