**Лекція 7. Формування завдання та варіанту побудови КСЗІ**

**Вступ.**

**Питання 1. Формування завдання на створення КСЗІ.**

**Питання 2. Аналіз ризиків реалізації загроз для інформації згідно вимог ISO/IEC 27005-2011.**

**Питання 3. Вибір варіанту побудови та складу КСЗІ та звітування.**

**Контрольні питання.**

**Вступ.**

Останні кроки 1-го етапу «Формування вимог до КСЗІ в ІТС» складаються 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.

**Питання 1.**

Під час кроку формування завдання на створення КСЗІ в ІТС визначаються завдання захисту інформації та відповідні ним напрями забезпечення її захисту, в результаті чого визначається конкретний варіант забезпечення безпеки інформації.

Завданнями захисту інформації можуть бути:

* забезпечення необхідних властивостей інформації (конфіденційності, цілісності, доступності) під час створення та експлуатації ІТС;
* своєчасне виявлення та ліквідація загроз для ресурсів ІТС, причин та умов, які спричиняють (можуть привести до) порушення її функціонування та розвитку;
* створення механізму та умов оперативного реагування на загрози для безпеки інформації, інші прояви негативних тенденцій у функціонуванні ІТС;
* ефективне попередження загроз для ресурсів ІТС шляхом комплексного впровадження правових, морально-етичних, фізичних, організаційних, технічних та інших заходів забезпечення безпеки;
* керування засобами захисту інформації, керування доступом користувачів до ресурсів ІТС, контроль за їхньою роботою з боку персоналу СЗІ, оперативне сповіщення про спроби НСД до ресурсів ІТС;
* реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації;
* створення умов для максимально можливого відшкодування та локалізації збитків, що завдаються неправомірними (несанкціонованими) діями фізичних та юридичних осіб, впливом зовнішнього середовища та іншими чинниками, зменшення негативного впливу наслідків порушення безпеки на функціонування ІТС.

Концепція безпеки інформації розкриває основні напрями забезпечення безпеки інформації та розробляється на підставі аналізу таких чинників:

* правових засад;
* вимог безпеки інформації;
* загроз для інформації.

За результатами аналізу формулюються загальні положення безпеки, які впливають на технологію обробки інформації в ІТС:

* мета і пріоритети, яких необхідно дотримуватись в ІТС під час забезпечення безпеки інформації;
* загальні напрями діяльності, необхідні для досягнення цієї мети;
* аспекти діяльності у галузі безпеки інформації, які повинні вирішуватися на рівні організації в цілому;
* відповідальність посадових осіб та інших суб’єктів взаємовідносин в ІТС, їхні права і обов'язки щодо реалізації завдань безпеки інформації.

Вибір основних рішень з безпеки інформації розглядається на 3-х рівнях:

* правовому;
* організаційному;
* технічному.

На правовому рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо виконання вимог нормативно-правових актів з безпеки інформації.

Цей рівень забезпечується виконанням таких заходів:

* підтримка керівництвом організації заходів з безпеки інформації в ІТС, визначення відповідальності посадових осіб, організаційної структури, комплектування і розподіл обов'язків співробітників СЗІ;
* розробка політики безпеки, плану захисту та іншої документації згідно вимог нормативно-правових актів з безпеки інформації;
* визначення процедури доведення до персоналу і користувачів ІТС основних положень політики безпеки інформації, їхнього навчання та підвищення кваліфікації з питань безпеки інформації;
* система контролю за своєчасністю, ефективністю і повнотою реалізації в ІТС рішень з безпеки інформації, дотриманням персоналом і користувачами положень політики безпеки.

На організаційному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо організації та впровадження режимних заходів, регламентації доступу та навчання персоналу.

Цей рівень забезпечується виконанням таких заходів:

* застосування режимних заходів на об’єктах ІТС;
* забезпечення фізичного захисту обладнання ІТС, носіїв інформації, інших ресурсів;
* визначення порядку виконання робіт з безпеки інформації, взаємодії з цих питань з іншими суб’єктами системи ТЗІ в Україні;
* регламентація доступу користувачів і персоналу до ресурсів ІТС;
* організація навчання та підвищення кваліфікації персоналу і користувачів ІТС з питань безпеки інформації;
* реалізація окремих положень політики безпеки, найбільш критичних з точки зору забезпечення захисту аспектів (наприклад, організація віддаленого доступу до ІТС, використання мереж передачі даних загального користування, зокрема Інтернет тощо).

На технічному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо застосування інженерно-технічних і програмно-апаратних засобів реалізації вимог безпеки.

Під час розгляду різних варіантів реалізації рекомендується враховувати наступні аспекти:

* інженерно-технічне обладнання приміщень, в яких розміщуються компоненти ІТС;
* реєстрація санкціонованих користувачів ІТС, авторизація користувачів в системі;
* керування доступом до інформації і механізмів, що реалізують послуги безпеки, включаючи вимоги до розподілу ролей користувачів і адміністраторів;
* виявлення та реєстрація небезпечних подій з метою здійснення повсякденного контролю;
* перевірка і забезпечення цілісності критичних даних на всіх стадіях їхньої обробки в ІТС;
* забезпечення конфіденційності інформації, у тому числі використання криптографічних засобів;
* резервне копіювання критичних даних, супроводження архівів даних і ПЗ;
* відновлення роботи ІТС після збоїв, відмов, особливо для систем із підвищеними вимогами до доступності інформації;
* захист ПЗ, окремих компонентів і ІТС в цілому від внесення несанкціонованих доповнень і змін;
* забезпечення функціонування засобів контролю.

**Питання 2.**

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). *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*. *До них відносяться активи, вразливості, загрози та збитки.*

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

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

Загрози - реалізація яких можлива за допомогою використання вразливостей.

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

**Керування ризиками** – це процес послідовного виконання трьох основних етапів:

**1 - визначення початкових ризиків (в незахищеній ІТС);**

**2 - застосування засобів захисту для скорочення ризиків;**

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

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

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

1) визначення критеріїв;

2) аналіз ризиків;

3) обробка ризиків;

4) прийняття ризиків.

*Кінцевою метою керування ризиком є ​​мінімізація ризику*. Мета мінімізації ризику полягає в тому, що застосування ефективних заходів захисту призводить до прийняття залишкового ризику.

**Мінімізація ризику** складається з трьох частин:

1 - визначення областей, де ризик неприйнятний;

2 - вибір ефективних заходів захисту;

3 - оцінювання заходів захисту та визначення прийнятності залишкового ризику.

**Визначення критеріїв оцінки ризиків**

На цьому етапі використовуються дані обстеження всіх середовищ ІТС з метою визначення того, які інформаційні та технічні ресурси зі складу ІТС і з якою детальністю повинні розглядатися в процесі керування ризиком. Крім того, необхідно розробити критерії оцінки ризиків, впливу на активи та прийняття ризиків.

Критерії оцінки ризику повинні розроблятися, враховуючи наступне:

- стратегічна цінність обробки інформації;

- критичність інформаційних активів;

- нормативно-правові вимоги та договірні зобов'язання;

- важливість доступності, конфіденційності та цілісності інформації.

Крім того, критерії оцінки ризиків можуть використовуватися також для визначення пріоритетів для обробки ризиків.

Критерії впливу повинні розроблятися, виходячи з міри збитку, враховуючи наступне:

- цінність інформаційного активу, на який виявлений вплив;

- порушення властивості інформації (втрата конфіденційності, цілісності або доступності);

- погіршення бізнес-операції;

- втрата цінності бізнесу та фінансової цінності;

- порушення планів і кінцевих термінів;

- збиток для репутації;

- порушення нормативно-правових вимог або договірних зобов'язань.

Критерії прийняття ризику повинні встановлюватися з урахуванням:

- критеріїв якості бізнес-процесів;

- нормативно-правових і договірних аспектів;

- операцій;

- технологій;

- фінансів;

- соціальних і гуманітарних чинників.

При розробці критеріїв прийняття ризику слід враховувати, що вони можуть:

- включати багато порогових значень з бажаним рівнем ризику, але за умови, що при певних обставинах керівництво прийматиме риски, що знаходяться вище вказаного рівня;

- визначатися як кількісне співвідношення оціненої вигоди до оціненого ризику для бізнесу;

- включати вимоги для майбутньої додаткової обробки, наприклад, ризик може бути прийнятий, якщо є згода на дії щодо його зниження до прийнятного рівня у рамках певного періоду часу.

Аналіз ризиків складається з таких заходів:

- ідентифікація ризиків;

- вимірювання ризиків;

- оцінювання ризиків.

**Ідентифікація ризиків**

Метою ідентифікації ризику є визначення випадків нанесення потенційної шкоди та отримання уявлень про те, як, де і чому могла статися ця шкода. Для цього необхідно виконати ідентифікацію наявних засобів захисту, вразливостей системи і можливих наслідків реалізації загроз.

Ідентифікація наявних засобів захисту

Ідентифікація усіх наявних засобів захисту має бути зроблена для того, щоб уникнути їх дублювання або непотрібної роботи. Одночасно слід провести перевірку справності і правильності функціонування засобів захисту.

Будь-який дефект засобів захисту може стати причиною вразливості. Одним із способів кількісно оцінити дії засобу захисту - подивитися, як він зменшує вірогідність загрози та використання вразливості.

Наявний або запланований засіб захисту можна ідентифікувати як неефективний, недостатній або необгрунтований. Якщо його визнали необгрунтованим або недостатнім, необхідно визначити, чи потрібно засіб захисту вилучити, замінити ефективнішим або залишити без змін, наприклад, із-за нестачі грошей на новий.

Ідентифікація вразливостей системи

Необхідно ідентифікувати всі вразливості, які можуть бути використані потенційними загрозами для нанесення збитку. Навіть та вразливість, яка не відповідає ніякій загрозі і тому не вимагає засобів захисту, повинна знаходитися під контролем на предмет можливих змін.

Зрозуміло, що аналіз загроз повинен розглядатися у тісному зв'язку з вразливостями ІТС. Завданням даного етапу управління ризиками є складання переліку можливих вразливостей системи і класифікація цих вразливостей з урахуванням їх «сили».

Градацію вразливостей можна розбити по таких рівнях: високий, середній та низький.

Джерелами складання такого переліку уразливостей можуть стати:

- загальнодоступні, регулярно друковані списки вразливостей ;

- списки вразливостей, що друкуються виробниками ПЗ;

- результати тестів на проникнення (проводяться адміністратором безпеки);

- аналіз звітів сканерів вразливостей (проводяться адміністратором безпеки).

У загальному випадку вразливості можна класифікувати таким чином:

- вразливості ОС і ПЗ (програмні помилки), виявлені виробником або незалежними експертами;

- вразливості системи, пов'язані з помилками в адмініструванні (наприклад, незакриті міжмережевим екраном порти з уразливими сервісами, загальнодоступні незаблоковані мережеві ресурси тощо);

- вразливості, джерелами яких можуть стати інциденти, не передбачені політикою безпеки, а також події стихійного характеру.

Як приклад поширеної вразливості ОС і ПЗ можна привести переповнювання буфера. До речі, абсолютну більшість з нині існуючих шкідливих програм реалізують клас вразливостей на переповнювання буфера.

**Ідентифікація наслідків реалізації загроз**

Мають бути ідентифіковані усі можливі наслідки реалізації загроз. Наслідком може бути втрата інформації, ресурсів ІТС, несприятливі операційні умови, втрата бізнесу, збиток, нанесений репутації тощо. Наслідки можуть бути тимчасовими або постійними, як у разі руйнування активів.

**Вимірювання ризиків**

Вимірювання ризиків складається з таких заходів:

- розробка методології вимірювання;

- оцінка наслідків реалізації загроз;

- оцінка вірогідності ризиків;

- вимір рівня ризиків.

**Розробка методології вимірювання**

Методологія вимірювання ризиків може бути якісною або кількісною, або їх комбінацією, залежно від обставин. На практиці якісна оцінка часто використовується першою для отримання загальних відомостей про рівень ризиків і виявлення їх основних значень. Надалі може виникнути необхідність в здійсненні кількісного аналізу значень ризиків, оскільки він є швидшим і менш витратним.

Якісна оцінка - використовує шкалу кваліфікації атрибутів для опису величини можливих наслідків (наприклад, низький, середній і високий) і вірогідності виникнення цих наслідків. Перевага якісної оцінки полягає в простоті її розуміння усім персоналом, а недоліком є залежність від суб'єктивного підходу.

Кількісна оцінка - використовує шкалу з числовими значеннями наслідків і вірогідностей з урахуванням отримання даних з різних джерел. Якість аналізу залежить від точності та повноти числових значень і обгрунтованості використовуваних моделей. У більшості випадків кількісна оцінка використовує фактичні дані за минулий період, забезпечуючи перевагу в тому, що вона може бути безпосередньо пов'язана з цілями захисту інформації і проблемами організації.

При розробці методології виміру ризику використовуються методи системного аналізу, в результаті виходять оцінки гранично допустимого та реального ризику здійснення загроз протягом деякого часу.

**Оцінка наслідків реалізації загроз**

Оцінці наслідків реалізації загроз повинне передувати визначення цінності активів (ресурсів ІТС). У свою чергу, цінність активів визначається з урахуванням їх важливості для бізнесу, первинної та відновлювальної вартості. Відновлювальна вартість активів визначається з урахуванням вартості:

- бізнес-втрат або компрометації активів;

- відновлення або заміни активів.

Оцінка збитків, який може завдати діяльності організації реалізація загроз безпеки, здійснюється з урахуванням можливих наслідків порушення конфіденційності, цілісності, доступності інформації та спостереженості ІТС.

**Оцінка вірогідності ризиків**

Використовуючи якісні або кількісні методи оцінки необхідно також оцінити вірогідність кожного сценарію реалізації загрози. Необхідно розглянути, як часто виникають загрози та наскільки легко можуть бути використані вразливості, з урахуванням наступного:

- наявний досвід і статистика вірогідності загроз;

- для джерел навмисних загроз: мотивація, можливості та доступні ресурси для можливих порушників, а також сприйняття привабливості та вразливості активів можливим порушником;

- для джерел випадкових загроз: географічні чинники, наприклад, близькість до підприємства зі шкідливим виробництвом, можливість екстремальних кліматичних умов і чинники, які можуть вплинути на помилки персоналу та збої устаткування;

- властивості окремих вразливостей та їх сукупності;

- наявні засоби контролю і те, наскільки ефективно вони знижують вразливості.

В ідеалі для кожної із загроз повинно бути отримано значення вірогідності її здійснення протягом деякого часу. Це допоможе співвіднести оцінку можливого збитку з витратами на захист. На практиці для більшості загроз неможливо отримати достовірні дані про вірогідність реалізації загрози та доводиться обмежуватися якісними оцінками.

**Вимір рівня ризиків**

При вимірі рівня ризиків визначаються значення вірогідності та наслідків ризиків. Ці значення можуть бути якісними або кількісними. Вимір ризиків грунтується на оцінених наслідках і вірогідності. Виміряний ризик є комбінацією вірогідності небажаного сценарію реалізації загрози та його наслідків.

Для прикладу ідентифікуємо значення цінності активів, використовуючи числову шкалу від 0 до 4. Наступним кроком ідентифікуємо кожен вид загрози, кожного активу, з яким пов'язаний цей вид загрози, щоб зробити можливою оцінку рівнів загроз і вразливостей.

Цінність ресурсів ІТС, рівні загроз і вразливостей приводимо до табличної форми (матриці), щоб для кожної комбінації ідентифікувати відповідну міру ризику на основі шкали від 0 до 8. Значення заносяться в матрицю структурованим чином.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Рівень **загрози** | | Низька (Н) | | | Середня (С) | | | Висока (В) | | |
| Рівень вразливості | | Н | С | В | Н | С | В | Н | С | В |
| Значення  **ресурсів ІТС** | 0 | 0 | 1 | 2 | 1 | 2 | 3 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 2 | 3 | 4 | 3 | 4 | 5 |
| 2 | 2 | 3 | 4 | 3 | 4 | 5 | 4 | 5 | 6 |
| 3 | 3 | 4 | 5 | 4 | 5 | 6 | 5 | 6 | 7 |
| 4 | 4 | 5 | 6 | 5 | 6 | 7 | 6 | 7 | 8 |

Для кожного активу розглядаються вразливості та загрози, що відповідають їм. Тепер відповідний рядок в таблиці встановлює значення цінності ресурсів ІТС, а відповідна колонка - вірогідність виникнення загрози та уразливості. Наприклад, якщо актив має цінність 3, загроза є «високою», а уразливість «низької», то міра ризику дорівнюватиме 5.

Аналогічна матриця є результатом розгляду вірогідності реалізації загрози з урахуванням впливу на ресурси ІТС. Отриманий в результаті ризик вимірюється за шкалою від 0 до 8 і може бути оцінений по відношенню до критеріїв прийняття ризику.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Вірогідність  реалізації загрози | | Дуже низька | Низька | Середня | Висока | Дуже висока |
| **Вплив на ресурси ІТС** | **Дуже низьке** | **0** | **1** | **2** | 3 | 4 |
| **Низьке** | **1** | **2** | 3 | 4 | 5 |
| **Середнє** | **2** | 3 | 4 | 5 | **6** |
| **Високе** | 3 | 4 | 5 | **6** | **7** |
| **Дуже високе** | 4 | 5 | **6** | **7** | **8** |

Таблиця може бути використана також, щоб зв'язати чинники наслідків для ресурсів ІТС з вірогідністю виникнення загрози (враховуючи аспекти вразливості). Перший крок полягає в оцінюванні наслідків для ресурсів ІТС за заздалегідь визначеною шкалою, наприклад, від 1 до 5, для кожного ресурсу (колонка 2), що знаходиться під загрозою. Другий крок полягає в оцінюванні вірогідності виникнення загрози за заздалегідь визначеною шкалою, наприклад, від 1 до 5, для кожної загрози (колонка 3).

Третій крок полягає в обчисленні міри ризику шляхом множення значень колонок 2 і 3. Нарешті, загрози можуть бути ранжирувані в порядку відповідної міри ризику. Відмітимо, що значення «1» в колонках 2 і 3 відповідає найменшим наслідкам і вірогідності загрози, а в колонці 5 - найбільшій небезпеці.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вид загрози | Наслідки для активів | Вірогідність загрози | Міра ризику | Ранг небезпеки |
| 1 | 2 | 3 | 4 | 5 |
| А | 5 | 2 | 10 | 2 |
| Б | 2 | 4 | 8 | 3 |
| В | 3 | 5 | 15 | 1 |
| Г | 1 | 3 | 3 | 5 |
| Д | 4 | 1 | 4 | 4 |
| Е | 2 | 4 | 8 | 3 |

У широкому сенсі міра ризику може розглядатися як опис видів несприятливих дій, впливу яких може зазнати система, і ймовірностей того, що ці дії можуть відбутися. Результат цього процесу повинен визначити ступінь ризику для певних цінностей. Цей результат важливий, оскільки є основою для вибору засобів захисту і рішень по мінімізації ризику.

**Оцінювання ризиків**

Виміряні ризики для їх оцінювання повинні порівнюватися з прийнятими в організації критеріями їх оцінки. Критерії оцінки ризику, які використовуються для ухвалення рішень, повинні враховувати цілі організації, характер бізнесу, думки зацікавлених сторін тощо.

Рішення, пов'язані з оцінкою ризику, зазвичай грунтуються на його прийнятному рівні. Сукупність безлічі ризиків низького та середнього рівня може дати у результаті загальний ризик більш високого рівня.

Оцінювання ризиків грунтується на розумінні суті ризику, отриманому на етапі його аналізу, для ухвалення рішень про майбутні дії. Рішення повинні включати наступне:

- чи мають бути зроблені якісь дії;

- пріоритети при обробці ризиків з урахуванням їх виміряних рівнів.

Оцінювання ризиків проводиться за допомогою різноманітних інструментальних засобів, а також методів моделювання процесів захисту інформації. На підставі результатів аналізу виявляються найбільш високі ризики, що переводять потенційну загрозу в розряд реально небезпечних і, отже, вимагають прийняття додаткових заходів захисту.

Коли намічені заходи прийняті, необхідно перевірити їх дієвість, наприклад, зробити автономне та комплексне тестування програмно-технічного механізму захисту. Якщо перевірка виявила, що в результаті проведеної роботи залишкові ризики знизилися до прийнятного рівня, то можна визначити дату найближчої переоцінки, якщо ні - слід проаналізувати допущені помилки і провести повторне оцінювання ризиків.

**Обробка ризиків**

Обробка ризиків здійснюється у такій послідовності:

- вибір варіанту обробки ризику;

- реалізація обраного варіанту;

- оцінка залишкового ризику.

Для обробки ризиків є 4 варіанти:

1) зниження;

2) збереження;

3) уникнення;

4) перенесення.

Зниження ризику

Якщо рівень ризику є неприйнятним, приймається рішення про зниження ризику, що реалізується шляхом впровадження необхідних заходів і засобів захисту. Їх ефективність при обробці ризику повинна бути такою, щоб залишковий ризик став прийнятним.

Засоби ТЗІ можуть забезпечувати один або декілька варіантів захисту від негативних дій: їх виключення, попередження, зменшення їх впливу, стримування, виправлення. Під час вибирання засобів важливо «зважувати» вартість їх придбання, реалізації, функціонування, адміністрування та технічної підтримки по відношенню до цінності активів.

Існують обмеження, які можуть впливати на вибирання засобів ТЗІ. Наприклад, вони можуть понизити продуктивність роботи системи. Тому необхідно приймати таке рішення, яке задовольняє вимогам продуктивності і в той же час гарантує достатній рівень захисту. Результатом цього кроку є складання переліку можливих засобів ТЗІ з порівняльним аналазом їх вартості, недоліків, переваг та пріоритетів реалізації.

**Збереження ризику**

Ризик може бути збережений, якщо його рівень відповідає критеріям прийняття ризику. У такому разі немає необхідності реалізовувати додаткові засоби захисту.

**Уникнення ризику**

Якщо витрати на обробку ризику перевищують бюджет, може бути прийняте рішення про уникнення цього ризику, що може бути реалізоване як відмова від діяльності, пов’язаної з цим ризиком, або зміна її умов. Наприклад, відносно ризиків, що викликаються стихійними лихами, найбільш вигідною альтернативою може бути фізичне переміщення засобів обробки інформації туди, де ймовірність таких ризиків дуже мала.

**Перенесення ризику**

Якщо витрати на обробку ризику перевищують бюджет, може бути прийняте рішення про перенесення ризику, що може бути реалізоване за допомогою систем аутсорсингу та/або страхування. Вибір цих систем залежить від вартості їх використання.

Аутсорсинг - це передача компанією частини її завдань або процесів стороннім більш професійним виконавцям на умовах субпідряду. Для цього необхідно укласти договір із сторонньою організацією для проведення зовнішнього моніторингу системи та запобігання загрозам, перш ніж вони приведуть до збитків.

Страхування - це можливість відшкодування збитків, що можуть виникнути у наслідок реалізації загроз, для чого також необхідно укласти договір із страховою організацією.

**Прийняття ризиків**

Керівництвом організації повинно бути прийнято та задокументовано рішення про прийняття ризиків і відповідальності за це рішення.

В деяких випадках рівень залишкового ризику може не відповідати критеріям прийняття ризику, оскільки вживані критерії не враховують усіх обставин. У таких випадках керівництво може прийняти ризики, але зобов'язано їх прокоментувати та включити обгрунтування для рішення, пов’язаного з перевищенням стандартного критерію прийняття ризику.

*Рішення щодо прийняття ризику можуть внести поправки до вибору заходів і засобів захисту*. Коли властивості запропонованих заходів і засобів захисту відомі, можна повторно провести перевірку залишкового ризику та визначити, чи досягнуто рівень прийнятності ризику або необхідно змінити рішення щодо його прийнятності, щоб відобразити інформацію про властивості запропонованих заходів і засобів захисту.

Після того, як всі заходи і засоби захисту реалізовані, перевірені та визначені ефективними, результати перевірки прийнятності ризику повинні бути повторно вивчені. Ризик, пов'язаний зі співвідношенням загроза/вразливість, повинен тепер бути скорочений до прийнятного рівня або усунуто. Якщо ці умови не дотримані, то рішення, прийняті на попередніх кроках, повинні бути переглянуті, щоб визначити належні заходи захисту.

**Питання 3.**

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:

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

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

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

Після цього необхідно здійснити первинне (попереднє) оцінювання допустимих витрат на блокування загроз, виходячи з вибраного варіанту побудови КСЗІ і виділених на це коштів.

На етапі проектування КСЗІ, після формування пропозицій щодо складу заходів і засобів захисту, здійснюється оцінка залишкового ризику для кожної пропозиції (наприклад, за критерієм «ефективність/вартість»), вибирається найбільш оптимальна серед них і первинна оцінка уточнюється.

Якщо залишковий ризик не відповідає критеріям прийнятності, вносяться відповідні зміни до складу заходів і засобів захисту, після чого всі процедури виконуються повторно до одержання прийнятного результату.

На підставі визначених завдань і функцій ІТС, результатів аналізу її середовищ функціонування, моделей загроз і порушників та результатів аналізу ризиків визначаються компоненти ІТС (наприклад, ЛОМ, спеціалізований АРМ, Інтернет-вузол тощо), для яких необхідно або доцільно розробляти свої власні політики безпеки, відмінні від загальної політики безпеки в ІТС.

Визначаються загальна структура та склад КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, обмеження щодо середовищ функціонування ІТС та використання її ресурсів для реалізації завдань захисту, припустимі витрати на створення КСЗІ, умови створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальні вимоги до застосування в ІТС (окремих її підсистемах, компонентах) організаційних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ.

Для ІТС формується перелік необхідних функціональних послуг захисту (далі - ФПЗ) від НСД та вимог до рівнів реалізації кожної з них, визначається рівень гарантій реалізації послуг. Визначені вимоги складають профіль захищеності інформації в ІТС або її компоненті.

ФПЗ є ієрархічними в тому розумінні, що їх реалізація забезпечує зростаючу захищеність від загроз відповідного типу (конфіденційності - К, цілісності - Ц і доступності - 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.

Кожна послуга є набором функцій, які дозволяють протистояти певній множині загроз. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, хоча й не є точними підмножинами один одного. Рівні починаються з першого й зростають до певного значення, унікального для кожного виду послуг.

**Звітування.**

Останній етап формування завдання на створення КСЗІ 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.

**Контрольні питання**

1. Що визначається під час формування завдання на створення КСЗІ?
2. Що розкриває концепція безпеки інформації?
3. На яких рівнях розглядається вибір основних рішень з безпеки інформації?
4. На підставі аналізу яких чинників розробляється концепція безпеки інформації?
5. Які повинні бути вироблені підходи на правовому рівні забезпечення безпеки інформації?
6. Які повинні бути вироблені підходи на організаційному рівні забезпечення безпеки інформації?
7. Які повинні бути вироблені підходи на технічному рівні забезпечення безпеки інформації?
8. Що визначається в результаті аналізу ризиків реалізації загроз?
9. Що відноситься до вхідних параметрів аналізу ризиків?
10. Що таке активи?
11. Що таке вразливості?
12. Що таке збитки?
13. За допомогою чого можлива реалізація загроз?
14. З яких трьох основних етапів складається процес керування ризиками?
15. Що уточнюється по завершенні аналізу ризиків реалізації загроз?
16. З яких 4-х етапів складається керування ризиками згідно стандарту?
17. Що є кінцевою метою керування ризиком? ​​
18. У чому полягає мета мінімізації ризику?
19. З яких трьох частин складається мінімізація ризику?
20. Яку умовну назву має стандарт щодо керування ризиками інформаційної безпеки?
21. Які необхідно розробити критерії стосовно ризиків згідно стандарту?
22. Для визначення чого також можуть використовуватися критерії оцінки ризиків?
23. З яких трьох заходів складається аналіз ризиків згідно стандарту?
24. З ідентифікації чого складається ідентифікація ризиків згідно стандарту?
25. По яких рівнях можна розбити градацію вразливостей системи?
26. З яких чотирьох заходів складається вимірювання ризиків згідно стандарту?
27. Якою може бути методологія вимірювання ризиків?
28. Що повинно передувати оцінці наслідків реалізації загроз?
29. З урахуванням чого визначається цінність активів?
30. З урахуванням чого визначається відновлювальна вартість активів?
31. Що визначається при вимірі рівня ризиків?
32. З чим повинні порівнюватися виміряні ризики для їх оцінювання?
33. У якій послідовності здійснюється обробка ризиків?
34. Які чотири варіанти має процес обробки ризику згідно стандарту?
35. Коли ризик може бути збережений?
36. Як реалізується варіант уникнення ризику?
37. Які варіанти захисту від негативних дій можуть забезпечувати засоби ТЗІ?
38. Яке приймається рішення, якщо рівень ризику є неприйнятним?
39. Якою повинна бути ефективність заходів і засобів захисту при обробці ризику?
40. Яке приймається рішення, якщо витрати на обробку ризику перевищують бюджет?
41. За допомогою яких систем може бути реалізоване перенесення ризиків?
42. Яке рішення повинно бути прийнято та задокументовано керівництвом організації?
43. Вибір чого необхідно здійснити після завершення аналізу всіх можливих ризиків?
44. Чим характеризується мінімальний варіант побудови КСЗІ?
45. Чим характеризується оптимальний варіант побудови КСЗІ?
46. Чим характеризується максимальний варіант побудови КСЗІ?
47. Який документ складається після формування завдань на створення КСЗІ?