МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Харківський національний університет внутрішніх справ

Факультет № 4

Кафедра інформаційних технологій

ТЕКСТ ЛЕКЦІЇ

з дисципліни «Вступ у спеціальність»

за темою «Загрози безпеці інформації та інформаційних ресурсів»

Галузь знань: 12 «Інформаційні технології»

Спеціальність: 125 «Кібербезпека»

Ступень вищої освіти: бакалавр

Харків

2017 рік

Текст лекції призначений для використання при вивченні курсу «Вступ у спеціальність» в рамках підготовки бакалаврів за спеціальністю 125 «Кібербезпека» в Харківському національному університеті внутрішніх справ.

СХВАЛЕНО

Науково-методичною радою Харківського національного університету внутрішніх справ

_____ Протокол № ____

(дата, місяць, рік)

ЗАТВЕРДЖЕНО

Вченою радою факультету № 4 Харківського національного університету внутрішніх справ

_____ Протокол № ____

(дата, місяць, рік)

_____ _____

(підпис) (П.І.Б.)

ПОГОДЖЕНО

Секцією науково-методичної ради ХНУВС з технічних дисциплін

_____ Протокол № ____

(дата, місяць, рік)

_____ _____

(підпис) (П.І.Б.)

ЗАТВЕРДЖЕНО

На засіданні кафедри інформаційних технологій факультету № 4 ХНУВС

_____ Протокол № ____

(дата, місяць, рік)

_____ _____

(підпис) (П.І.Б.)

Рецензент:

Носов В.В., професор кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ к.т.н., доцент.

Розробник: Тулупов Володимир Володимирович – м. Харків: Харківський національний університет внутрішніх справ, 2017 р.

План лекції

1. Основні характеристики інформаційної системи як об’єкту захисту.
2. Класифікація загроз безпеці інформації.
3. Ранжування джерел загроз безпеці інформації.
4. Класифікація уразливостей безпеці інформації.
5. Ранжування уразливостей.
6. Класифікація актуальних загроз безпеці інформації.

Література:

Основна:

1. Носов, В.В., Манжай, А.В. Організація та забезпечення безпеки інформації [Текст]: навчальний посібник / В.В. Носов, А.В. Манжай. – Харків: ХНУВС, 2007. – 216 с., іл.
2. Антонюк А. О. Основи захисту інформації в автоматизованих системах: навч. посіб. / А. О. Антонюк. – К.: Академія, 2003. – 242 с.
3. Богуш В. М. Інформаційна безпека держави: навч. посіб. / В. М. Богуш, О. К. Юдін. – К.: МК-Прес, 2005. – 432 с.
4. Завгородний В. И. Комплексная защита информации в компьютерных системах: учеб. пособие / В. И. Завгородний. – М.: Логос ; ПБОЮЛ Н. А. Егоров, 2001. – 264 с.

Додаткова:

5. Герасименко В.А. Защита информации в автоматизированных системах обработки данных / В.А. Герасименко. В 2-х кн.: Кн.1. – М.: Энергоатомиздат, 1994. – 400 с.
6. Герасименко В.А. Защита информации в автоматизированных системах обработки данных / В.А. Герасименко. В 2-х кн.: Кн.2. – М.: Энергоатомиздат, 1994. – 176 с.

Текст лекції

1. Основні характеристики інформаційної системи як об’єкта захисту

Для інформаційних систем як об’єктів безпеки властиві наступні такі характеристики як конфіденційність, доступність та цілісність інформації (даних) в інформаційній системі.

Конфіденційність[1] *інформації (даних) в інформаційній системі* – це властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом інформаційної системи. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Доступність у загальному смислі представляється як можливість проникнення куди-небудь. Для інформаційної системи – це властивість ресурсу системи, яка полягає в тому, що користувач і (або) процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не

[1] *Конфіденційність* – це властивість не підлягати розголосові; довірчість, секретність, суто приватність.

очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, і в той час, коли він йому необхідний.

Доступність даних в інформаційній системі – це властивість даних, що полягає у можливості їхнього читання користувачем або програмою. Визначається рядом факторів: можливістю працювати за терміналом, володінням паролем, знанням мови запитів і т.ін.

Цілісність – це внутрішня єдність, зв'язаність усіх частин чого-небудь, єдине ціле.

В інформаційній системі – це стан даних або інформаційної системи системи, в якій дані та програми використовуються встановленим чином, що забезпечує:

– стійку роботу системи;

– автоматичне відновлення у випадку виявлення системою потенційної помилки;

– автоматичне використання альтернативних компонентів замість тих, що вийшли з ладу.

Для інформаційної системи можна розглядати такі поняття як цілісність даних, цілісність інформації, цілісність бази даних цілісність інформаційної системи і т.ін.[2]

Забезпечення безпеки інформації повинно носити комплексний характер, засновуватися на всебічному аналізі можливих негативних наслідків і при якому важливо не упустити будь-які суттєві аспекти. Виникає наступний ланцюжок: джерело загрози – фактор (уразливість) загроза (дія) – наслідки (атака).

Джерело загрози – це потенційні антропогенні, техногенні або стихійні носії загрози безпеці.

Загроза (дія) – це можлива небезпека (потенційна або така, що існує реально) вчинення будь-якого діяння (дії або бездіяльності), спрямованого проти об'єкта захисту (інформаційних ресурсів), яке наносить збиток власнику або користувачу, що проявляється як небезпека спотворення або втрати інформації.

Фактор (уразливість) – це властиві об'єкту інформатизації причини, які призводять до порушення безпеки інформації на конкретному об'єкті та зумовлені вадами процесу функціонування об'єкта інформатизації, властивостями архітектури інформаційно-телекомунікаційної системи, протоколами обміну та інтерфейсами, що застосовуються програмним забезпеченням і апаратними засобами, умовами експлуатації.

Наслідки (атака) – це можливі наслідки реалізації загрози (можливі дії) при взаємодії джерела загрози через наявні фактори (уразливості) .

---

[2] *Цілісність інформації* – це властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і (або) процесом. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації (видалення).

Цілісність даних в інформаційній системі – це стан, при якому дані, що зберігаються в системі, в точності відповідають даним у вихідних документах; властивість, що має відношення до набору даних і означає, що дані не можуть бути змінені або зруйновані без санкції на доступ. Цілісність даних вважається збереженою, якщо дані не спотворені і не зруйновані (стерті). *Семантична цілісність даних* – це стан даних, коли вони зберігають свій інформаційний зміст та однозначність інтерпретації в умовах випадкових впливів.

Цілісність бази даних – це стан бази даних, коли всі значення даних правильні в тому сенсі, що відображають стан реального світу (в межах заданих обмежень по точності та часовій узгодженості) і підпорядковуються правилам взаємної несперечливості.[2]

Цілісність системи – це властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки.

Атака – це завжди пара «джерело-фактор», що реалізує загрозу та приводить до збитків.

2. Класифікація загроз безпеці інформації

Виділяють три основні види *загроз безпеці інформації***:** загрози безпеці інформації при забезпеченні конфіденційності, доступності та цілісності.

Загрози безпеці інформації при забезпеченні конфіденційності:

– крадіжка (копіювання) інформації та засобів її оброблення;
– втрата (ненавмисна втрата, витік) інформації та засобів її оброблення.

Загрози безпеці інформації при забезпеченні доступності:

– блокування інформації;
– знищення інформації та засобів її оброблення.

Загрози безпеці інформації при забезпеченні цілісності:

– модифікація (спотворення) інформації;
– заперечення автентичності інформації;
– нав'язування фальшивої інформації.

3. Ранжування джерел загроз безпеці інформації

Носіями загроз безпеці інформації є *джерела загроз.*

Джерелами загроз можуть бути як суб'єкти (особистість), так і об'єктивні прояви. Джерела загроз можуть знаходитися як усередині організації – внутрішні джерела, так і ззовні її – зовнішні джерела. Поділ джерел на суб'єктивні та об'єктивні виходить з міркувань стосовно вини або ризику збитку інформації.

Усі джерела загроз безпеці інформації діляться на три групи:

– обумовлені діями суб'єкта (антропогенні джерела загроз);
– обумовлені технічними засобами (техногенні джерела загроз);
– обумовлені стихійними джерелами.

Антропогенним джерелом загроз можна вважати суб'єкта, який має доступ (санкціонований або несанкціонований) до роботи зі штатними засобами об'єкта, що підлягає захисту.[3] Суб'єкти, дії яких можуть привести до порушення безпеки інформації, можуть бути як внутрішніми, так і зовнішніми.

Внутрішні джерела (суб'єкти) представляють собою висококваліфікованих спеціалістів у галузі розробки та експлуатації програмного забезпечення та технічних засобів, знайомі зі специфікою завдань, що вирішуються, структурою та основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного обладнання та технічних засобів мережі.[4]

Зовнішні джерела можуть бути випадковими або навмисними та мати різний рівень кваліфікації.

Друга група містить джерела загроз, що визначаються технократичною діяльністю людини, є особливо актуальною в сучасних умовах, так як очікується різке зростання числа техногенних катастроф, викликаних фізичним та моральним старінням існуючого обладнання.

Технічні засоби, що є джерелами потенційних загроз безпеці інформації, також можуть бути зовнішніми та внутрішніми.

---

[3] *Антропогенними джерелами загроз* виступають суб'єкти, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини. Ця група джерел загроз найбільш численна та представляє найбільший інтерес із точки зору організації захисту, так як дії суб'єкта завжди можна оцінити, спрогнозувати та прийняти адекватні заходи. Методи протидії у цьому випадку керовані й залежать від волі організаторів захисту інформації.

[4] Особливу групу внутрішніх антропогенних джерел складають особи з порушеною психікою та спеціально впроваджені та завербовані агенти, які можуть бути з числа основного, допоміжного та технічного персоналу, а також представників служби захисту інформації. Кваліфікація антропогенних джерел загроз безпеці інформації відіграє важливу роль для оцінки їхнього впливу та враховується при ранжируванні джерел загроз.

Третя група джерел загроз об'єднує обставини, що складають непереборну силу, тобто такі обставини, які носять об'єктивний і абсолютний характер, що розповсюджується на всіх.[5]

Усі джерела загроз мають різну *міру небезпеки,* яку можна оцінити, якщо провести їхнє ранжирування. При цьому, оцінка міри небезпеки здійснюється за непрямими показниками.[6]

Кожний показник оцінюється експертно-аналітичним методом за п'ятибальною системою. Причому, 1 відповідає мінімальній мірі впливу показника, який оцінюється на небезпеку використання джерела, а 5 – максимальній.

Необхідні умови готовності джерела визначаються, виходячи джерела загрози з можливості реалізації тієї чи іншої загрози в конкретних умовах розташування об'єкт а, при цьому передбачається:

– загроза реалізована – тобто умови сприятливі або можуть бути сприятливими для реалізації загрози;

– загроза помірно реалізована – тобто умови сприятливі для реалізації загрози, проте довгострокові спостереження не припускають можливості її активізації у період існування й активної діяльності об'єкта захисту;

– загроза слабо реалізована – тобто існують об'єктивні причини на самому об'єкті або в його оточенні, що перешкоджають реалізації загрози;

– загроза не реалізована – тобто відсутні передумови для реалізації передбачуваної подій.

Результати ранжирування відносно конкретного об'єкта захисту зводяться в таблицю, яка дозволяє визначити найбільш небезпечні для даного об'єкта джерела загроз безпеці інформації.

4. Класифікація уразливостей безпеці інформації

Уразливості, властиві об'єкту інформатизації, обумовлюються недоліками процесу функціонування, властивостями архітектури автоматизованих систем, протоколами обміну та інтерфейсами, програмним забезпеченням і апаратною платформою, умовами експлуатації та розташування.[7]

Джерела загроз можуть використовувати уразливості для порушення безпеки інформації, нанесення збитків власникові, користувачеві інформації).

Уразливості безпеці інформації можуть бути: об'єктивними, суб'єктивними, випадковими.

Об'єктивні уразливості залежать від особливостей побудови та технічних характеристик обладнання, що застосовується на об'єкті захисту. Повне усунення цих уразливостей неможливе, але вони можуть суттєво послаблятися технічними та інженерно-технічними методами відбивання загроз безпеці інформації.

---

[5] До непереборної сили в законодавстві та договірній практиці відносять стихійні лиха або інші обставини, які неможливо передбачити або їм запобігти або можливо передбачити, але не можливо запобігти їм при сучасному рівні знань і можливостей людини. Стихійні джерела потенційних загроз (природні катаклізми) інформаційній безпеці є зовнішніми по відношенню до об'єкта захисту.

[6] Критеріями порівняння (показників) може бути:

– можливість виникнення джерела, визначаючи міру доступності до можливості використати фактор (уразливість) (для антропогенних джерел), віддаленість від фактора (уразливості) (для техногенних джерел) або особливості обстановки (для випадкових джерел);

– готовність джерела, що визначає міру кваліфікації та привабливість здійснення діяння зі сторони джерела загрози (для антропогенних джерел) або наявність необхідних умов (для техногенних та стихійних джерел).

– фатальність визначає міру непереборності наслідків реалізації загрози.

[7] Загрози, як можливі небезпечності здійснення будь-якої дії, спрямованої проти об'єкта захисту, проявляються не самі по собі, а через уразливості (фактори), що призводять до порушення безпеки інформації на конкретному об'єкті інформатизації.

Суб'єктивні уразливості залежать від дій співробітників і, в основному, вилучаються організаційними та програмно-апаратними методами.

Випадкові уразливості залежать від особливостей середовища, яке оточує об'єкт захисту, та непередбачених обставин. Ці факти передбачувані і їх усунення можливе тільки при проведення комплексу організаційних та інженерно-технічних заходів із протидії загрозам інформаційній безпеці.

5. Ранжирування уразливостей

Усі уразливості мають різну міру небезпеки, яку можна кількісно оцінити на основі ранжирування. При цьому критеріями порівняння (показниками) можна вибрати:

– фатальність, що визначає міру впливу уразливості на непереборність наслідків реалізації загрози. Для об'єктивних уразливостей – це інформативність, тобто здатність уразливості повністю (без спотворення) передати корисний інформаційний сигнал;

– доступність, що визначає зручність (можливість) використання уразливості джерелом загроз (малогабаритні розміри, складність, вартість необхідних засобів, можливість використання не спеціалізованої апаратури);

– кількість, що визначає кількість елементів об'єкта, яким характерна та чи інша уразливість.

Результати аналізу із зазначенням коефіцієнтів небезпеки кожної уразливості зводиться в таблицю.

6. Класифікація актуальних загроз

При проведенні аналізу актуальних загроз експертно-аналітичним методом визначаються об'єкти захисту, що піддаються впливу цієї чи іншої загрози, характерні джерела цих загроз і уразливості, що сприяють реалізації загроз.

На основі аналізу складається таблиця взаємозв'язку джерел загроз і уразливостей, із яких визначаються можливі наслідки реалізації загроз (атаки) та обчислюється коефіцієнт небезпеки цих атак як добуток коефіцієнтів небезпеки відповідних загроз та джерел загроз, визначених раніше. При цьому передбачається, що атаки,які мають коефіцієнт небезпеки менше 0,1 (припущення експертів), в подальшому можуть не розглядатися із-за малої ймовірності їх здійснення на об'єкті захисту.

Така матриця складається окремо для кожної загрози. І після виявлення найбільш актуальних загроз приймаються заходи з вибору методів і засобів для відбивання.