КСЗІ-2021 8-й семестр (весна).

**Заняття 1.**

**Мета заняття:** Надання студентам груп КБ-41, КБ-42 загальних основ вивчення матеріалу дисципліни «Комплексні системи захисту інформації: проектування, впровадження, супровід», та порядку викладання, звітності, нарахування балів і самостійного отримання і виконання завдань викладача.

**Вступ. Мова отримання та контроля знань.**

|  |  |
| --- | --- |
| **Дисципліна СТЗІ викладається з використанням мов:**  **1. Державної**, бо **стаття 10 Конституції України встановлює, що державною мовою в Україні є українська мова**… В Україні гарантується вільний розвиток, використання і захист російської, інших мов національних меншин України.  **2.** **ЄС, Англії та США**, бо відповідно Закону України від 1 липня 2010 року «Про засади внутрішньої і зовнішньої політики» (стаття 11) однією з основоположних засад зовнішньої політики України є «забезпечення інтеграції України в європейський політичний, економічний, правовий простір з метою набуття членства в ЄС».  **3. Руської**, бо Резолюція Генеральної Асамблеї ООН про територіальну цілісність України № 68/262, що була ухвалена 27 березня 2014 року встановила, що Росія є державою-агресором і державою-окупантом. Потрібно володіти мовою агресора, розуміти її таємний зміст та адекватно протидіяти інформаційним загрозам протидіючі агресору його-ж зброєю. | Taras Shevchenko selfportrait oil 1840 (crop).png  **Шевченко Тарас Григорович**  **(1814 - 1861).**  Уильям Шекспир — лучшие стихотворения  **William Shakespeare**  **(1564—1616).**  У Лондоні розмістили плакати-пародії про роль Путіна у Brexit  *Фото:@Pr0ud\_Bear* Лондон. 08.11.2018 22:01  **Автори плаката група «сатириків-офіцерів з ГРУ РФ". Джерело: https://tvrain.ru/news/** |

Приклад державного підходу і системності викладу вивчення дисципліни є узятий зразок виконання державних стандартів України інформаційної безпеки. А саме:

**ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ**

**ДСТУ 3396.0-96**

**Захист інформації**

**Технічний захист інформації**

**Основні положення – ДЕРЖАВНА МОВА.**

**Information protection**

**Technical protection of information**

**Basic principles – АНГЛІЙСЬКА МОВА.**

**Защита информации**

**Техническая защита информации**

**Основные положения – РОСІЙСЬКА МОВА.**

Дисципліна «Комплексні системи захисту інформації: проектування, впровадження, супровід» (КСЗІ) займає одне з провідних місць в системі підготовки студентів напряму 125 «Кібербезпека».

На сучасному етапі розвитку інформаційних систем захист інформації повинен бути не тільки систематизованим в цільовому, просторово-часовому й організаційному сенсі, але й представляти собою комплексне охоплення методів і засобів, які дозволять забезпечити захист від максимального числа можливих загроз.

Комплексний розгляд існуючих загроз до інформації, а також методів і засобів протидії цим загрозам, дозволяє кожному вищому навчальному закладу викладати матеріал дисципліни за принципом «from the general to the specific». При цьому, як правило, курс КСЗІ завершується сплайновою подобою звуження комплексного охоплення інформаційного захисту до рівня обмеженої спеціалізації кафедр та факультетів.

Ми ознайомимся з деякими найбільш повними джерелами інформації, в яких викладався курс КСЗІ:

1. Замула О.А. Нормативно-правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації. : учб. посіб. / О. А. Замула, Ю. І. Горбенко, О. І. Шумов ; Харк. нац. ун-т радіоелектрон. - Х. : ХНУРЕ, 2010. - 248 с.
2. Гребенніков В.В. Комплексні системи захисту інформації: проектування, впровадження, супровід. : збірник лекцій / Ужгород: Ужгородський національний університет, 2019. – 612с.
3. Комплексні системи захисту інформації [Текст]: конспект лекцій для студентів напрямку підготовки 125 «Кібербезпека» денної форми навчання / уклад. В.М. Мельник. – Луцьк: Луцький НТУ, 2016. – 68 с.
4. Комплексні системи захисту інформації [Текст] : навч. посіб. / [Ю. Є. Яремчук та ін.] ; Вінницький національний технічний університет. - Вінниця : ВНТУ, 2018. - 117 с. - Бібліогр.: с. 116-117. - 50 (1-й запуск 1-20) прим.

В результаті дослідження інформаційних джерел та з дозволу автора більш 50 відсотків матеріалу – Гребеннікова Вадима Вікторовича - було прийнято рішення обрати матеріал Ужгородського національного університету в якості лекційної основи дистанційного курсу КСЗІ для студентів факультету комп'ютерних наук, напряму підготовки "Кібербезпека".

Автор більш 50-ти відсотків змісту лекційного матеріалу - Гребенніков Вадим Вікторович старший викладач з інформаційної безпеки, полковник, ветеран державної служби спеціального зв'язку та захисту інформації України, відмічений державною нагородою «За бездоганну службу» та багатьма відомчими нагородами, зокрема, «Хрестом заслуги» І і ІІ ступенів, автор багатьох наукових праць-посібників, таких як: «Нормативно-правове забезпечення інформаційної безпеки», «Європейська криптологія», «Американська криптологія», «Російська криптологія», «Стеганографія» та багатьох інших.

Не останню роль у виборі дистанційного курсу зіграло й те, що на території Ужгорода століттями свято зберігаються основи джерельної державної мови, яка є важливим елементом фундаменту української незалежності.

Текст цих лекцій дозволяє розвивати тематику КСЗІ, доповнюючи практичними дослідженнями і довідковими даними.

При цьому важливо пам’ятати, що студенти факультету комп'ютерних наук є особливою групою обдарованої молоді, яка велику частину свого життя "проживає" у віртуальному просторі комп'ютерних програм, алгоритмів і мов. Практика показує, що для них такі "приземлені" науки, як фізика и хімія менш привабливі, ніж іноземні мови та інформатика.

Автор даного курсу допускає наявність в числі його опонентів людей, які, володіючи доступом до інформаційної бази та адмінресурсу, здатні більш дохідливо запропонувати виклад матеріалу занять. Тому авторське трактування цілком допускає її подальше розширення в співавторстві з передовими дослідниками комплексних систем захисту інформації.

Слід зазначити, що динаміка розвитку як кібер-технологій, так і кіберзлочинів вкрай динамічна. Автор орієнтується не на ортодоксальний конспект лекцій, а на рівень розвитку аудиторії слухачів, їх інтелектуальні здібності і науковий прогрес комп'ютерних технологій.

**«Конспект викладача - контролюючим, сучасні знання – учням»,** - тільки такий адаптивне-динамічний процес у ВНЗ дозволить вивести Україну в число передових індустріальних держав світу.



**Питання 2. Актуальність проблеми забезпечення безпеки інформації.**

Проблеми захисту інформації від стороннього доступу і небажаного впливу на неї виникли з того часу, коли людині з яких-небудь причин не хотілося ділитися нею ні з ким або ні з кожною людиною.

Цінним стає та інформація, володіння якою дозволить її наявному й потенційному власникам отримати будь-який виграш.

З переходом на використання технічних засобів зв'язку, інформація піддається впливу випадкових процесів (збоїв обладнання, помилок операторів і т.д.), які можуть привести до її руйнування, зміни на помилкову, а також створити передумови до доступу до неї сторонніх осіб.

З появою складних автоматизованих систем управління, пов'язаних з автоматизованим введенням, зберіганням, обробкою і поширенням інформації, проблеми її захисту набувають ще більшого значення.

Цьому сприяє:

1. Збільшення обсягів інформації, що накопичується, зберігається та обробляється за допомогою ЕОМ та інших засобів обчислювальної техніки.

2. Зосередження в єдиних базах даних інформації різного призначення і приналежності.

3. Розширення кола користувачів, що мають доступ до ресурсів обчислювальної системи, і масивів даних, що знаходяться в ній.

4. Ускладнення режиму функціонування технічних засобів, обчислювальної системи (широке впровадження багатопрограмного режиму поділу часу і реального часу).

5. Автоматизація міжмашинного обміну інформацією, в т.ч. й на великих відстанях.

6. Збільшення кількості технічних засобів і зв'язків в автоматизованих системах управління (АСУ) і обробки даних.

7. Поширення ПЕОМ, що у свою чергу розширюють можливості не тільки користувача, але і порушника.

8. Індустрія переробки інформації досягла глобального рівня.

9. Поява електронних грошей створило передумови для розкрадання великих сум.

10. З'явилося дивне переродження науково-технічних працівників. Хакери - прекрасні знавці інформаційної техніки. Кракери. Фракери - прихильники електронного журналу Phrack.

Останнім часом широкого поширення набув новий комп'ютерний злочин - створення комп'ютерних вірусів.

**1.1 Предмет захисту.**

Властивості інформації.

Інформація - це результат відображення і обробки в людській свідомості різноманіття навколишнього світу. Це відомості про оточуючих людини предмети, явища природи, діяльність інших людей. Відомості, якими обмінюється людина через машину з іншою людиною або машиною і є предметом захисту. Однак, захисту підлягає та інформація, яка має ціну. Для оцінки потрібно розподіл інформації на категорії не тільки відповідно до її цінності, а й важливістю. Відомо наступний розподіл інформації за рівнем важливості:

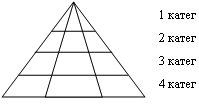
1. Життєве-важлива, незамінна інформація, наявність якої необхідно для функціонування організацій.

2. Важлива інформація, яка може бути замінена або відновлена, але процес відновлення дуже важкий і пов'язаний з великими витратами.

3. Корисна інформація - це інформація, яку важко відновити, однак організація може ефективно функціонувати і без неї.

4. Неістотна інформація.

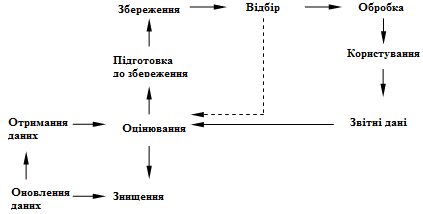
Модель предмета захисту:



Відповідно до принципів поділу, інформацію, що оброблюють в автоматизованих системах (АСОД), для ілюстрації можна уявити за категоріями важливості і секретності у вигляді піраміди, що складається з декількох шарів по вертикалі (ІЗОД).

Вершиною піраміди є найбільш важлива інформація державної таємниці особливої важливості, а фундаментом - несуттєва інформація, але у свою чергу вона пов'язана з обробкою більш важливої ​​інформації. Кожен шар даної піраміди, поділений на частини по горизонталі, відображає принцип розподілу інформації за функціональною ознакою і повноважень її користувачів.

Безпека інформації в АС інтерпретується як небезпека її несанкціонованого: отримання, модифікації та ін. за весь час перебування в АС, а також безпеку дій, для здійснення яких використовується інформація.

У інформації в АС є свій життєвий цикл:  
  


Безпечні технології - це технології, які не завдають матеріальних збитків суб'єктам, які мають пряме або непряме відношення до них. Суб'єктом може бути держава, фізичні особи та ін.

Технологія - це сукупність методів переробки (перетворення вихідної сировини, будь-якими засобами з метою отримання кінцевої продукції).

Для правильної побудови системи захисту необхідно визначити:

1. Види впливу на інформацію.

2. Що з себе являє автоматизована система.

3. Які існують загрози безпеки автоматизованих систем.

4. Заходи протидії загрозам безпеки.

5. Принцип побудови систем захисту.

**Види впливу на інформацію:**

1. Порушення конфіденційності.

А) З інформацією ознайомлюються суб'єкти, яким вона не належить. Рівень допуску до інформації визначає її власник.

Порушення конфіденційності може відбутися через неправильну роботу системи, обмеження доступу або наявності побічного каналу доступу.

Б) Несанкціоноване тиражування. Під захистом розуміється захист авторських прав і прав власності на інформацію.

2. Порушення цілісності.

Причини:

- втрата інформації;

- вихід з ладу носія.

Спотворення:

- порушення смислової значущості;

- порушення логічної зв'язаності;

- втрата достовірності.

3. Блокування інформації.

Користувач не може отримати доступ до інформації. При відсутності доступу, сама інформація не втрачається.

Причини:

- відсутність обладнання;

- відсутність фахівця;

- відсутність ПО.

4. Порушення контролю за інформаційним процесом. Порушення спостереженості.

**2. Типові структури автоматизованих систем і об'єкти захисту в них.**

АСУ - організаційно-технічні системи, що представляють собою сукупність компонентів:

1. Технічні засоби обробки і передачі даних

2. Системне і прикладне ПО

3. Інформація на різних носіях

4. Персонал і користувачі системи

Типові Структури АС:

Автономні робочі станції (АРС).

Один або кілька ПК, не пов'язаних між собою. На будь-якому з них користувачі працюють окремо в часі. Обмін інформацією здійснюється через змінні носії.

Об'єкти захисту в автономних робочих станціях (АРС):

- АРС;

- змінні носії інформації;

- користувачі і обслуговуючий персонал;

- пристрої візуального представлення інформації;

- джерела побічного електромагнітного випромінювання і наведень.

ЛВС - створюються для колективної обробки інформації або спільного використання ресурсу. Устаткування розміщено в межах одного приміщення, будівлі або групи близько розташованих будівель.

**Локальні системи колективного користування (ЛСКК).**

Структура ЛСКК:

- без виділеного сервера або тимчасової мережі. Не вимагає централізованого управління; будь-який користувач робить доступними свої дані; використовується однотипна ОС.

- з виділеним сервером. Вимагає централізованого адміністративного управління; на РС і сайти можуть використовувати:

- багатотермінальні системи на базі малих і великих комп'ютерів.

Основні ресурси зосереджені на сервері; РС - це термінали; загальне керівництво здійснює адміністратор; на центральному комп'ютері і РС використовуються різні ОС.

- багатосегментні ЛС - складаються з декількох сегментів, кожний з яких є мережею з виділеним сервером. Об'єднання здійснюється через міст, в якості якого може використовуватися або виділений сервер, або спеціальної пристрій. Будь-яким сегментом управляє свій адміністратор. У будь-якому сегменті може використовуватися своя ОС.

- змішані мережі - включають всі вищерозглянуті системи.

Об'єкти захисту:

- всі робочі станції (РС);

- сервер і центральний комп'ютер;

- локальні канали зв'язку;

- реквізити доступу.

**Глобальні системи колективного користування (ГСКК).**

ГСКК - спільна обробка інформації і спільне використання ресурсів.

Відмінності від ЛСКП:

1. Можуть знаходитися на значній відстані один від одного.

2. Канали зв'язку не належать власнику системи.

3. Канали зв'язку є комутованими і взаємопов'язаними.

4. Для використання каналів зв'язку необхідний пристрій сполучення.

5. Подібні системи відкриті і підключитися до них можуть всі бажаючі.

Об'єкти захисту:

- РС;

- глобальні канали зв'язку;

- інформація, що передається по глобальних каналах зв'язку;

- інформація про реквізити доступу в ГСКП.

**3. Загрози безпеці інформації - їх російське тлумачення.**

Загроза - це потенційно можлива подія, дія, процес або явище, яке може привести до поняття збитку чиїмось інтересам.

Порушення безпеки - це реалізація загрози.

Природні загрози - це загрози, викликані впливом на АС об'єктивних фізичних процесів, стихійних природних явищ, що не залежать від людини.

Природні поділяються на:

• природні (стихійні лиха, магнітні бурі, радіоактивне випромінювання, опади);

• технічні. Пов'язані з надійністю технічних засобів, обробки інформації та систем забезпечення.

Штучні поділяють на:

• ненавмисні - вчинені через незнання і без злого умислу, з цікавості або недбалості;

• навмисні.

**Канали проникнення в систему і їх класифікація:**

1. За способом:

- прямі;

- непрямі.

2. За типом основного засобу для реалізації загрози:

- людина;

- апаратура;

- програма.

3. За способом отримання інформації:

- фізичний;

- електромагнітний;

- інформаційний.

**Заходи протидії загрозам:**

1. Правові та законодавчі.

Закони, укази, нормативні акти, які регламентують правила поводження з інформацією та визначають відповідальність за порушення цих правил.

2. Морально-етичні.

Норми поведінки, які традиційно склалися або складаються в суспільстві в міру поширення обчислювальної техніки. Невиконання цих норм веде до падіння авторитету, престижу організації, країни, людей.

3. Адміністративні або організаційні.

Заходи організаційного характеру, які регламентують процеси функціонування АС, діяльність персоналу з метою максимального утруднення або виключення реалізації погроз безпеки:

- організація явного або прихованого контролю за роботою користувачів;

- організація обліку, зберігання, використання, знищення документів і носіїв інформації;

- організація охорони та надійного пропускного режиму;

- заходи, здійснювані при підборі і підготовці персоналу;

- заходи щодо проектування, розробки правил доступу до інформації;

- заходи при розробці, модифікації технічних засобів.

4. Фізичні.

Застосування різного роду технічних засобів охорони і споруд, призначених для створення фізичних перешкод на шляхах проникнення в систему.

5. Технічні.

Засновані на використанні технічних пристроїв і програм, що входять до складу АС і виконують функції захисту:

- засоби автентифікації;

- апаратне шифрування;

- інші.

**4. Принципи побудови систем захисту:**

1. **Принцип системності** - системний підхід передбачає необхідність врахування всіх взаємопов'язаних і змінюються в часі елементів, умов і факторів, істотно значущих для розуміння і вирішення проблеми забезпечення безпеки.

2. **Принцип компетентності** - передбачає побудову системи з різнорідних засобів, що перекривають всі існуючі канали реалізації загрози безпеці і не містять слабких місць на стику окремих компонентів.

3. **Принцип безперервної захисту** - захист повинен існувати без розриву в просторі і часі. Це безперервний цілеспрямований процес, який передбачає не тільки захист експлуатації, але і проектування захисту на стадії планування системи.

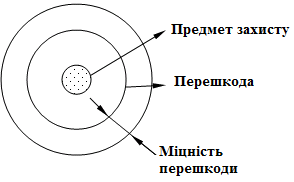
4. **Принцип розумної достатності.** Вкладення коштів в систему захисту повинно бути побудовано таким чином, щоб отримати максимальну віддачу.

5. **Принцип гнучкості управління і застосування.** При проектуванні системи захист може вийти або надлишкової, або недостатньої. Система захисту повинна бути легко настроюється.

6. **Принцип відкритості алгоритмів і механізмів захисту.** Знання алгоритму **механізму захисту не дозволяє здійснити злом системи.**

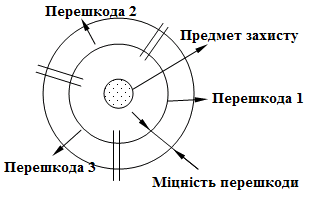
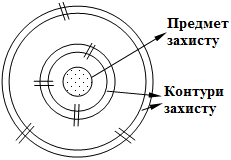
**7. Принцип простоти застосування захисних заходів і засобів**. Всі механізми захисту повинні бути інтуїтивно зрозумілі і прості у використанні. Користувач повинен бути вільний від виконання малозрозумілої багато-об’ємної рутинної роботи і не повинен володіти спеціальними знаннями. Раб… .

**Модель елементарного захисту.**



Міцність захисної перешкоди є достатньою, якщо очікуваний час подолання її порушником більше часу життя предмета захисту, або більше часу виявлення і блокування його доступу при відсутності шляхів прихованого обходу цієї перешкоди.

**Модель багатоланкового захисту.**

  
  
**Модель багаторівневого захисту.**  
  


**Джерела інформації:**

1. *Щеглов А. Ю.* Защита компьютерной информации от несанкционированного доступа. –СПб.: Наука и техника, 2004. –384 с.
2. *Варламов О. О.* Системный подход к созданию модели компьютерных угроз информационной безопасности.// Материалы VI Международной научно-практической конференции «Информационная безопасность»- Таганрог: Издательство ТРТУ, 2004 С. 61-65 .
3. *Домарев В. В.* Безопасность информационных технологий. Системный подход: - К.: ООО ТИД ДС, 2004.-992с.
4. *И. В. Машкина, Е. А. Рахимов.* Модель объекта информатизации// Материалы VI Международной научно-практической конференции «Информационная безопасность»- Таганрог: Издательство ТРТУ, 2004. С.
5. *Абалмазов Э.И.* Методы и инженерно-технические средства противодействия информационным угрозам//Гротек, 1997, 248 с.

**Завдання на самопідготовку:**

* 1. **При кольоровому виділенні основних та додаткових питань наприкінці матеріалу надати схему класифікації інформації щодо рівня доступу.**