ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ ИМЕНИ А.Ф. МОЖАЙСКОГО

Математического и программного обеспечения

УТВЕРЖДАЮ

Начальник 27 кафедры

полковник

С. Войцеховский

«___» _____ 20__ г.

Автор: старший преподаватель 27 кафедры
кандидат технических наук
подполковник С.Краснов

Лекция № 6

по учебной дисциплине
«Защита информации»
на тему

Тема: «МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Рассмотрено и одобрено
на заседании кафедры № 27

« ___ » августа 201__ г.

протокол № __

Санкт-Петербург 201_

Содержание занятия и время

Введение – 5 мин.

Учебные вопросы (основная часть):

1. Понятие метода защиты информации и характеристика основных методов ЗИ. – 30 мин.
2. Программно-аппаратные методы ЗИ.– 50 мин.

Заключение – 3-5 мин.

Литература:

Основная:

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.
2. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.

Дополнительная:

1. Вихорев С.В. Классификация угроз информационной безопасности. - http://www2.cnews.ru/comments/security/elvis_class.shtml
2. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах./ Под ред. профессора Хомоненко А.Д. – Спб.:НТЦ им. Л.Т. Тучкова, 2005. – 149 с.

Материально техническое обеспечение:

1. Технические средства обучения: ПЭВМ, мультимедиа проектор, экран, программное обеспечение.
2. Приложения (слайды).
3. Наглядные средства обучения – доска, мел.

Организационно-методические указания:

Цель лекции: *Дать знания в области основных методов защиты информации.*

Во введении сформулировать тему лекции, цель и название изучаемых вопросов. При этом произвести опрос курсантов по пройденному материалу.

Применяемым методическим приемом является рассказ.

В основной части сконцентрировать внимание курсантов на основных группах методов ЗИ, возможности применения комплексного подхода при построении системы информационной безопасности объекта ВТ.

В заключительной части обобщить изложенный материал и осуществить контрольный опрос.

1. Дайте определение метода защиты информации?
2. Перечислите основные группы методов ЗИ?
3. Какие методы относятся к программно-аппаратным методам ЗИ?

Отвечаю на вопросы по теме занятия, даю задание на самостоятельную подготовку.

Лекция № 6

РАЗДЕЛ II МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 3. «Основные методы защиты информации»

В. 1. Понятие метода защиты информации и характеристика основных методов ЗИ.

В соответствии с «Современным словарём иностранных слов», *метод* – приём, способ или образ действия. В соответствии с [2 – Большаков А.А., Петряев А.Б., Платонов В.В., Ухлинов Л.М. Основы обеспечения безопасности данных в компьютерных системах и сетях. Часть 1. Методы, средства и механизмы защиты данных] *метод (способ) защиты данных* – совокупность приёмов и операций, реализующих функции защиты данных.

В соответствии с Государственным Стандартом Российской Федерации Р 50922-96 [4] под ***методом* (способом) *защиты информации*** понимают порядок и правила применения определенных принципов и средств защиты информации. Это определение мы и будем использовать в дальнейшем.

Уменьшить отрицательное, дестабилизирующее воздействие угроз на АС возможно различными *методами*, направленными, с одной стороны, на устранение ИУ, а с другой – на устранение или существенное ослабление уязвимостей. Эти методы должны быть направлены и на устранение последствий реализации угроз.

Их можно разделить на следующие основные группы:

- правовые (законодательные);
- экономические;
- организационные (административные);
- инженерно-технические;
- технические;
- программно – аппаратные.

Правовые (законодательные) методы представляют собой законодательные акты государства, которыми регламентируются правила использования данных ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Этим они препятствуют несанкционированному использованию информации и являются сдерживающим фактором для потенциальных нарушителей. Эти методы являются базисом для реализации всех остальных методов защиты.

Экономические методы воздействуют на антропогенные ИУ и позволяют их сократить, а также подключать механизмы ликвидации последствий реализации угроз. Так к примеру возможно применение системы коэффициентов и надбавок для сотрудников работающих с конфиденциальной информацией; страхование оборудования и информации; возмещение убытков и компенсация ущерба.

Организационные (административные) методы защиты ориентированы в основном на работу с персоналом – это меры организационного характера, вытекающие из политики безопасности и регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельности персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

Кроме того *организационные* методы защиты могут включать:

- выбор местоположения и размещения;
- мероприятия по разработке правил доступа пользователей к ресурсам системы

(разработка политики безопасности; пользователь должен знать, что ему разрешено делать в АС и подписать соответствующий документ) и определение ответственности сотрудников за нарушение политики безопасности и нанесение вреда компании (компрометация имиджа, разглашение коммерческой тайны);

- мероприятия, осуществляемые при подборе и подготовке персонала;
- физическая защита, организация охраны и надежного пропускного режима к АС;
- организацию учета, хранения, использования и уничтожения оборудования, документов и носителей с информацией;
- распределение реквизитов разграничения доступа (паролей, ключей, шифрования и т. п.);
- организацию явного и скрытого контроля за работой пользователей по выполнению требований по защите;
- взаимодействие с компетентными органами;
- противопожарную охрану и другие.

Инженерно-технические методы связаны с оптимальным построением зданий, сооружений, инженерных коммуникаций, транспортных магистралей с учётом требований безопасности информации. Это довольно дорогостоящие методы, но они как правило, реализуются ещё на этапе строительства или реконструкции объекта информатизации, способствуют повышению его общей живучести и дают высокий эффект при устранениии источников угроз. А некоторые источники угроз, например обусловленные стихийными бедствиями или техногенного характера, вообще не устранимы другими методами. Кроме того, они позволяют уменьшить влияние объективных и случайных уязвимостей.

К ним относятся следующие мероприятия:

- защита помещений от разрушений;
- электрозащита оборудования и зданий;
- оптимальное размещение оборудования и инженерных коммуникаций;
- применение технических средств визуального наблюдения, связи и охранной сигнализации;
- оптимальное построение зданий, сооружений, сетей инженерных коммуникаций с учётом требований безопасности информации (экранирование помещений, разделение трасс силовых и коммуникационных кабелей и т.д.).

Технические методы предназначены для устранения воздействий преднамеренных ИУ (нарушителей) по добыванию информации специальными техническими средствами. Они основаны на использовании специальных технических средств защиты информации и контроля обстановки для предотвращения вышеуказанных угроз. К ним относятся следующие мероприятия:

- резервирование каналов связи;
- использование выделенных каналов связи;
- создание системы пространственного зашумления;
- создание системы линейного зашумления;
- создание системы акустического зашумления;
- экранирование узлов и оборудования;
- использование источников бесперебойного питания;
- контроль каналов связи;
- контроль отсутствия средств съёма информации и другие.

Например, для защиты акустической (речевой) информации используются пассивные и активные методы.

Пассивные методы защиты акустической (речевой) информации направлены на:

- ослабление акустических (речевых) сигналов на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;
- ослабление информационных электрических сигналов в соединительных линиях ВТСС, имеющих в своем составе электроакустические преобразователи (обладающие микрофонным эффектом), до величин, обеспечивающих невоможность их выделения средством разведки на фоне естественных шумов;
- исключение (ослабление) прохождения сигналов высокочастотного навязывания во вспомогательные технические средства, имеющие в своем составе электроакустические преобразователи (обладающие микрофонным эффектом);
- обнаружение излучений акустических закладок и побочных электромагнитных излучений диктофонов в режиме записи;
- обнаружение несанкционированных подключений к телефонным линиям связи.

Активные методы защиты акустической (речевой) информации направлены на:

- создание маскирующих акустических и вибрационных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения информационного акустического сигнала средством разведки;
- создание маскирующих электромагнитных помех в соединительных линиях ВТСС, имеющих в своем составе электроакустические преобразователи (обладающие микрофонным эффектом), с целью уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;
- электромагнитное подавление диктофонов в режиме записи;
- ультразвуковое подавление диктофонов в режиме записи;
- создание маскирующих электромагнитных помех в линиях электропитания ВТСС, обладающих микрофонным эффектом, с целью уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;
- создание прицельных радиопомех акустическим и телефонным радиозакладкам с целью уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;
- подавление (нарушение функционирования) средств несанкционированного подключения к телефонным линиям;
- уничтожение (вывод из строя) средств несанкционированного подключения к телефонным линиям.

Методы защиты телефонных разговоров

- подача во время разговора в телефонную линию синфазного маскирующего низкочастотного сигнала (метод синфазной низкочастотной маскирующей помехи);
- подача во время разговора в телефонную линию маскирующего высокочастотного сигнала звукового диапазона (метод высокочастотной маскирующей помехи);
- подача во время разговора в телефонную линию маскирующего высокочастотного ультразвукового сигнала (метод ультразвуковой маскирующей помехи);
- поднятие напряжения в телефонной линии во время разговора (метод повышения напряжения);
- подача во время разговора в линию напряжения, компенсирующего постоянную составляющую телефонного сигнала (метод "обнуления");

- подача в линию при положенной телефонной трубке маскирующего низкочастотного сигнала (метод низкочастотной маскирующей помехи);
- подача в линию при приеме сообщений маскирующего низкочастотного (речевого диапазона) с известным спектром (компенсационный метод);
- подача в телефонную линию высоковольтных импульсов (метод "выжигания").

Основные характеристики устройств активной защиты телефонной линии

Наименование характеристик	Тип устройства					
	«Прокруст»	«Протон»	«Цикада-М»	Sel SP-17/P	Гром-ЗИ-6	Кзот-06
Метод синфазной низкочастотной маскирующей помехи	-	-	•	-	-	-
Метод высокочастотной маскирующей помехи	•	•	-	•	•	•
Метод ультразвуковой маскирующей помехи	-	-	•	-	•	-
Метод повышения напряжения	•	-	-	-	-	-
Метод "обнуления"			•	-	-	-
Метод низкочастотной маскирующей помехи	•	•	-	-	-	•
Метод "выжигания"	-	-	-	-	-	-
Индикация	световая	световая	световая	световая	световая, звуковая	световая
Габаритные размеры, мм	62*155*195	205*60*285	68*176*170	152*104*34	150*200*50	210*85*32
Вес, кг	1	2,3		0,6	1,5	0.75
Напряжение питания, В	220	220	220	220/12	220	9
Примечание	Цифровая индикация напряжения в линии	Цифровая индикация напряжения в линии		Частотный диапазон помехи8 … 10 кГ. Уровень сигнала помехи 70 дБ	Цифровая индикация уменьшения напряжения в линии	Цифровая индикация напряжения в линии

Защита от перехвата компьютерной информации от ПЭМИ осуществляется пассивными и активными методами ЗИ.

Пассивные методы защиты информации направлены на:

- ослабление побочных электромагнитных излучений (информационных сигналов) ТСПИ на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;
- ослабление наводок побочных электромагнитных излучений (информационных сигналов) ТСПИ в посторонних проводниках и соединительных линиях ВТСС, выходящих за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;

- исключение (ослабление) просачивания информационных сигналов ТСПИ в цепи электропитания, выходящие за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов.

Активные методы защиты информации направлены на:

- создание маскирующих пространственных электромагнитных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала ТСПИ;
- создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях ВТСС с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала ТСПИ.

В. 2. Программно-аппаратные методы защиты информации.

Наибольший эффект достигается при применении совокупности организационных и программно-аппаратных методов защиты информации.

Программно-аппаратные методы защиты информации играют ключевую роль как при обеспечении ИБ на автономных ЭВМ так и при построении комплексной системы ИБ АС и вычислительных сетей. На основе программно-аппаратных методов защиты создаются программно-аппаратные средства защиты, которые могут сочетать в себе не один, а несколько методов защиты информации. Многие из этих средств имеют действующие сертификаты ФСТЭК России.

Простота реализации и администрирования, высокая эффективность применения, приемлемые цены делают эти методы, и средства защиты на их основе, очень привлекательными для пользователей во всём мире.

Задача защиты информации от несанкционированного доступа решалась во все времена на протяжении истории человечества. Уже в Древнем мире выделилось два основных метода решения этой задачи, существующие и по сегодняшний день: *криптография и стеганография*. В последние десятилетия в связи с высокими темпами развития и внедрения новых информационных технологий (ЭВМ, вычислительных сетей) и автоматизации доступа к информации получил применение новый метод – *эталонных характеристик.*

К *основным программно-аппаратным методам защиты информации* можно отнести следующие:

- криптографические;
- стеганографические;
- эталонных характеристик.

Суть ***криптографического*** метода защиты информации заключается в преобразовании открытых данных в зашифрованные при помощи шифра.

Суть ***стеганографического*** метода защиты информации заключается в том, что скрываемое сообщение встраивается в некоторый безобидный, не привлекающий внимания объект, который затем открыто транспортируется адресату. При стеганографии скрывается сам факт существования тайного сообщения.

Суть метода ***эталонных характеристик*** заключается в анализе аппаратно-программной среды и формировании её уникального идентификатора. Только субъект, обладающий этим уникальным идентификатором, будет иметь (не иметь) право доступа к информации.

Под аппаратно-программной средой понимают: состав устройств, программ, носителей информации, установленный определённый порядок действий, правил и характеристики производительности компьютерных подсистем. *Подсистема* – набор

устройств и программ АС выполняющих единую задачу. **Доступ к информации** – получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.

Программно-аппаратные **методы** предназначены для устранения проявления угроз, непосредственно связанных с процессом обработки и передачи информации. К ним в соответствии с [14] относятся следующие мероприятия:

- разграничение (ограничение) доступа пользователей к ресурсам АС;
- управление потоками информации;
- маскирование структуры и назначение сети;
- блокирование неиспользуемых сервисов;
- подтверждение подлинности информации;
- преобразование информации при её передаче и хранении;
- контроль целостности данных;
- обеспечение конфиденциальности данных;
- мониторинг целостности аппаратно-программного обеспечения;
- резервирование ресурсов и компонентов АС;
- регистрация и анализ событий, происходящих в АС.

Сопоставление описанных выше угроз безопасности информации и группы методов их парирования позволяет решить, какими способами, какие угрозы целесообразно предотвращать, а также определить рациональное соотношение групп методов при распределении денежных средств.