Краснодарское высшее военное училище

Дисциплины

Разработка и эксплуатация защищенных автоматизированных систем

Групповое занятие

Занятие № 1/3. Построение комплексной защиты автоматизированных систем

Учебные вопросы:

1. Основы проектирования комплексной защиты информационной системы от НСД.

2. Критерии оценки защищенности автоматизированных систем.

3. Методы обеспечения информационной безопасности защищенных автоматизированных систем

4. Деятельность персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем.

1 Основы проектирования комплексной защиты информационной системы от НСД

На предыдущем занятии мы рассмотрели защиту информации от утечки по электромагнитным, электрическим и акустическим каналам.

При анализе общей проблемы безопасности информации еще выделяются такие направления, в которых преднамеренная или непреднамеренная деятельность человека, а также неисправности ТС, ошибки программного обеспечения могут привести к утечке, модификации или уничтожению информации. Такие направления относятся к несанкционированному доступу к информации (НСД).

Под НСД понимается доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых АС.

Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения АС.

СПОСОБЫ НДС. К основным способам НСД относятся:

непосредственное обращение к объектам доступа;

создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

модификация средств защиты, позволяющая осуществить НСД;

внедрение в технические средства или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции АС и позволяющих осуществить НСД.

Рассмотрим автоматизированную систему обработки информации как объект, в котором имеется некоторое множество возможных каналов несанкционированного доступа к предмету защиты. Для построения защиты информации в данной системе на каждом **возможном канале несанкционированного доступа** (**ВКНСД**), а если возможно, сразу на нескольких установить соответствующую преграду. Чем большее количество ВКНСД перекрыто средствами защиты и ниже вероятность их преодоления нарушителем, тем выше безопасность информации.

Структура защиты будет носить многозвенный и многоуровневый характер. Количество перекрываемых ВКНСД при этом будет зависеть от заданной квалификации нарушителя.

Нарушители могут быть:

- ***нарушитель-профессионал;***
- ***нарушитель высокой квалификации;***
- ***относительно квалифицированный нарушитель-непрофессионал;***
- ***безответственный пользователь.***

Поведение потенциального нарушителя может быть следующим:

1. Нарушитель может появиться в любое время и в любом месте периметра автоматизированной системы.

2. Квалификация и осведомленность нарушителя может быть на уровне разработчика данной системы.

3. Постоянно хранимая информация, включая секретную, принципы работы системы нарушителю известны.

4. Для достижения своей цели нарушитель выверит наиболее слабое звено в защите.

5. Нарушителем может быть законный пользователь системы.

6. Нарушитель действует один.

В этих условиях в систему построения защиты должны быть положены принципы:

1. Необходимо «построить» вокруг предмета защиты постоянно действующий замкнутый контур защиты.

2. Свойства преграды, составляющие защиту должны, по возможности, соответствовать ожидаемой квалификации и осведомленности нарушителя.

3. Для входа в систему законного пользователя необходима переменная секретная информация, известная только ему.

4. Итоговая прочность защитного контура определяется его слабейшим звеном.

5. При наличии нескольких законных пользователей полезно обеспечить разграничение их доступа к информации в соответствии с полномочиями и выполняемыми функциями.

Можно установить следующее распределение ВКНСД по классам:

1. Все ВКНСД, возможные в данной системе и в данный момент времени.

2. Все ВКНСД, кроме машинных носителей с остатками информации, подлежащей защите специальными криптографическими методами.

3. Только следующие ВКНСД:

- терминалы пользователей;
- аппаратура регистрации, документирования, отображения информации;
- машинные и бумажные носители информации;
- средства загрузки программного обеспечения;
- технологические пульты и органы управления;
- внутренний монтаж аппаратуры;
- линии связи между аппаратными средствами

Анализ возможных каналов НСД к информации показывает, что данные каналы необходимо разделить на 2 вида:

1. Контролируемые:

- *терминалы пользователей;*
- *аппаратура регистрации, документирования, отображения информации;*
- *средства загрузки программного обеспечения;*
- *технологические пульты и органы управления;*
- *внутренний монтаж аппаратуры;*
- *побочные наводки информации на сетях электропитания и заземления аппаратуры, вспомогательных и посторонних коммуникациях, размещенных вблизи ТС.*

2. Неконтролируемые:

- *машинные носители ПО и информации, выносимые за пределы системы;*
- *долговременные запоминающие устройства с остатками информации, выносимыми за пределы системы;*
- *внешние каналы связи;*

Основная тактика защиты информации от НСД заключаются в выполнении следующих задач:

- ***Предупреждении и контроле попыток НСД.***
- ***Своевременном обнаружении места и блокировки несанкционированных действий.***
- ***Регистрации и документировании событий.***
- ***Установление и устранение причины НСД.***
- ***Ведение статистики и прогнозирования НСД.***

2 Критерии оценки защищенности автоматизированных систем

Одним из необходимых условий проектирования систем защиты информации (СЗИ) от несанкционированного доступа (НСД) для автоматизированных систем (АС) является анализ потенциальных угроз безопасности с целью определения исходных данных и граничных условий для разработки средств защиты. Чем полнее и детальнее будет описано множество угроз, тем с большей вероятностью будут найдены адекватные средства и способы защиты.

С другой стороны, решение задачи эффективности средств защиты невозможно без системы критериев и показателей защищенности АС от НСД. При этом, если характеристики угроз являются исходными данными для проектирования системы защиты, то система критериев и показателей защищенности позволяет не только оценивать результаты разработки, но и контролировать ее ход.

Для решения этой задачи на этапе проектирования СЗИ выполняются следующие работы:

- ***анализ исходных данных и потенциальных угроз;***
- ***выявление уязвимых мест и каналов потенциальных нарушений безопасности АС;***
- ***построение модели потенциальных угроз;***
- ***определение вероятностей угроз;***
- ***оценка вероятного ущерба при реализации угроз;***
- ***построение модели защиты;***
- ***определение системы критериев и показателей защищенности;***
- ***оценка защищенности АС.***

Перечень угроз, оценка вероятностей их реализации, а также модель угроз являются основой для определения требований к СЗИ. На практике задача формального описания полного множества угроз чрезвычайно сложна вследствие очень большого числа факторов, влияющих на процессы хранения и обработки информации в современных АС. Поэтому для защищаемой системы определяют, как правило, не полный перечень угроз, а перечень классов угроз в соответствии с принятой классификацией. При этом классификация возможных угроз информационной безопасности АС проводится по ряду базовых признаков, например:

- ***по природе возникновения;***
- ***по степени преднамеренности проявления;***
- ***по непосредственному источнику угроз;***
- ***по положению источника угроз;***
- ***по степени зависимости от активности АС;***
- ***по степени воздействия на АС и т.п.***

В свою очередь, использование методов классификации угроз предопределяет классификацию методов защиты и обусловливает существование систем показателей защищенности классификационно-описательного типа.

Примером могут служить критерии и показатели защищенности, изложенные в руководящих документах (РД) Гостехкомиссии (ГТК) России, посвященных вопросам защиты информации в АС и средствах вычислительной техники (СВТ). РД ГТК определяют две группы требований к безопасности – ***показатели защищенности СВТ от НСД*** и ***критерии защищенности АС обработки информации***. Различие подходов к проблеме защищенности АС и СВТ обусловлено тем, что СВТ представляют собой элементы, на основе которых строятся АС и по отношению к которым можно говорить лишь о защищенности СВТ от НСД. При рассмотрении АС появляются дополнительные характеристики (например, полномочия пользователей, модель нарушителя, технология обработки информации и др.).

Применительно к СВТ в РД ГТК устанавливается классификация СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Конкретные перечни показателей определяют классы защищенности СВТ. Совокупность всех средств защиты составляет комплекс средств защиты (КСЗ).

РД ГТК устанавливает **семь** классов защищенности СВТ от НСД к информации. ***Самый низкий класс – седьмой, самый высокий – первый***. РД содержат требования к классам, являющиеся примером применения необходимых условий оценки качества защиты, при которых наличие определенного механизма класса защиты является основанием для отнесения СВТ к некоторому классу.

Относительно АС устанавливается **девять** классов защищенности от НСД, распределенных по **трем** группам. Каждый класс характеризуется определенной совокупностью требований к средствам защиты.

Являясь основным официальным документом, регламентирующим создание средств защиты от НСД, РД ГТК содержит исключительно описательные требования к КСЗ, причем ранжирование требований по классам защищенности значительно упрощено и сведено до определения наличия или отсутствия заданного набора механизмов защиты, что существенно снижает гибкость требований и возможность их практического применения.

В самом деле, разработчик решает на практике по сути задачу оптимального синтеза СЗИ для заданного множества угроз.

Необходимым условием решения задачи синтеза СЗИ является определение в явном виде функции эффективности **E= W(S,C). г**де **S** – параметры структуры, **C – параметры управления.**

Использование расчетных показателей эффективности позволяет автоматизировать процедуру оптимизации при синтезе СЗИ для заданных условий на этапах: ***проектирование***, ***создание дистрибутива (установщика программ)***, ***генерация конкретной версии***, ***настройка конкретной версии***.

При этом на этапах проектирования и создания дистрибутива описательные требования к СЗИ должны обеспечить разработку соответствующих аппаратных средств и дистрибутива программного обеспечения.

Анализ множества угроз с использованием моделей угроз, моделей защиты и расчетных показателей эффективности позволяет уточнить состав СЗИ и дистрибутива.

На этапе генерации конкретной версии уточняются состав и функции СЗИ. И если на этапе проектирования основными могут быть ограничения, накладываемые на процесс разработки и эксплуатации (например ограничения на полные затраты на разработку), то на этапе генерации конкретной версии определяющими становятся ограничения на процесс эксплуатации СЗИ.

Кроме того, если в составе СЗИ присутствуют средства параметрической настройки, обеспечивающие тонкую настройку СЗИ на этапе эксплуатации с целью минимизации влияния средств СЗИ на производительность базовой АС, можно рассматривать задачу параметрического синтеза СЗИ.

3. Методы обеспечения информационной безопасности защищенных автоматизированных систем

При разработке ЗАС должно быть предусмотрено:

- мониторинг показателей и разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;
- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;
- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;
- контроль за действиями персонала в защищенных информационных системах;
- формирование системы информационной безопасности.

Для обеспечения информационной безопасности защищенных автоматизированных систем используются следующие **методы**:

- ***управление доступом;***
- ***препятствие;***
- ***маскировка;***
- ***регламентация;***
- ***принуждение;***
- ***побуждение.***

Управление доступом – метод ЗИ регулированием использования всех ресурсов ЗАС. Управление доступом включает следующие функции защиты:

- *идентификация пользователей, персонала и ресурсов системы;*
- *аутентификация объектов и субъектов;*
- *проверка полномочий субъекта на соответствие регламенту безопасности;*
- *разрешение и создание условий работы в пределах регламента;*
- *регистрация обращений к защищаемым ресурсам;*
- *реагирование при попытках несанкционированных действий (отказ в запросе, задержка работы, отключение, сигнализация).*

Препятствие – метод физического преграждения пути злоумышленнику к ресурсам информационной системы.

Маскировка – методы криптографической защиты.

Регламентация – метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

Принуждение – метод защиты, при использовании которого пользователи и персонал ЗАС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение – такой метод защиты, который побуждает пользователей и персонал системы не нарушать сложившиеся моральные нормы.

Перечисленные методы ИБ реализуются на практике применением различных средств защиты, которые делятся на **два** класса:

Формальные – выполняющие защитные функции по заранее определенной процедуре без непосредственного участия человека;

Неформальные – определяются целенаправленной деятельностью человека либо регламентируют эту деятельность.

Средства защиты информации:

Технические средства реализуются в виде **электрических**, **электромеханических** и **электронных** устройств (делятся на ***аппаратные*** и **физические)**.

Под ***аппаратными*** средствами понимают устройства, встраиваемые непосредственно в аппаратуру ЗАС, или устройства, которые сопрягаются с этой аппаратурой по стандартному интерфейсу (электронные ключи, схемы аппаратного шифрования).

Физические средства реализуются в виде автономных устройств и систем (оборудование сигнализации, двери, решетки).

Программные средства представляют собой ПО, специально предназначенное для выполнения функций защиты информации. Программные средства по функциям делятся на:

- *средства контроля доступа,*
- *средства аудита,*
- *средства блокирования атак (межсетевые экраны),*
- *средства поиска уязвимостей (сканеры безопасности),*
- *средства анализа кодов программ,*

Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые на всех этапах жизненного цикла ЗАС (строительство помещений, проектирования ИС, монтаж и наладка оборудования, испытания и эксплуатация).

Законодательные средства защиты определяются законами и другими документами, регламентирующими правила использования, обработки и передачи ключевой информации и устанавливающими ответственность за нарушение правил.

Морально-этические средства защиты реализуются в виде всевозможных норм, которые складываются по мере развития информационных технологий. Эти нормы не являются обязательными как законы, но их несоблюдение может привести к потере авторитета или престижа человека или организации.

В настоящее время имеются следующие тенденции развития средств обеспечения информационной безопасности:

- ***аппаратная реализация основных функций защиты;***
- ***создание комплексных средств защиты, выполняющих несколько защитных функций;***
- ***унификация и стандартизация алгоритмов и технических средств.***

4. Деятельность персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем

Каждое лицо, входящее в состав персонала АСУ, должно применять соответствующие информационные модели и работать с техническими средствами и документацией, определяющей порядок его деятельности.

Персонал автоматизированных систем может быть условно разделен на **три** основные категории:

1. разработчиков средств программного, технического, информационного, лингвистического и организационно-технологического обеспечения системы;

2. персонал, обслуживающий систему;

3. пользователей системы.

В зависимости от характера каждой конкретной системы, этапов ее развития, а также видов выполняемых в определенный момент времени работ, отдельные лица, относящиеся к персоналу системы, могут выступать в ней в качестве представителей различных категорий (например, разработчика, представителя обслуживающего персонала и/или пользователя).

Администратор баз данных (АБД) – лицо, отвечающее за выработку требований к базе данных, реализацию, эффективное использование и сопровождение. В зависимости от сложности автоматизированной системы в ней может функционировать один АБД или несколько администраторов.

В процессе эксплуатации системы АБД руководит работой системных программистов и других лиц в части поддержания штатного режима функционирования системы. Используя соответствующие программные и аппаратные средства АБД контролирует работоспособность БД. АБД является ключевой фигурой в правильной организации и эффективном использовании БД.

Аналитик – специалист в области и конкретной прикладной области, в функции которого входит анализ проблем, оптимизация их решения и постановка задач на проектирование или совершенствование автоматизированных систем.

Системный интегратор – специалист по проектированию программно-аппаратных комплексов автоматизированных систем. Термин также применяется для определения характера деятельности специалистов, ориентированных на поддержку работы интегрированных вычислительных систем.

Администратор сети, системный администратор – специалист, отвечающий за нормальное функционирование и использование ресурсов автоматизированной системы и/или вычислительной сети.

Программист – специалист в области разработки, отладки или сопровождения работы средств программного обеспечения автоматизированных систем. В зависимости от характера деятельности программисты могут подразделяться на программистов – аналитиков, прикладных и системных программистов (см. ниже).

Некоторые разновидности должностей программистов:

Программист-аналитик – специалист, сочетающий функции **программиста** и **аналитика**.

Прикладной программист – программист, осуществляющий разработку и отладку прикладных программ. Квалифицированный прикладной программист должен быть одновременно специалистом в предметной области, с которой связаны разрабатываемые им программные продукты.

Системный программист – программист, в функции которого входит эксплуатация и сопровождение средств программного обеспечения системы, а также разработка отдельных (как правило, вспомогательных) программных модулей, совершенствующих ее работу.

По другим признакам различаются также:

Ведущий/главный программист – программист, осуществляющий руководство разработкой средств программного обеспечения (программ) и непосредственно участвующий в проектировании отдельных их частей.

Местный/собственный программист – программист, состоящий в штате сотрудников определенной автоматизированной системы или вычислительного центра.

Инженер. Квалификация специалиста с высшим техническим образованием, дополняется указанием области его профессиональной подготовки.

Некоторые разновидности инженерных должностей:

Инженер-программист – инженер, занимающийся разработкой и эксплуатацией средств программного обеспечения (см. также «программист»).

Инженер-системотехник – инженер, занимающийся ремонтом и поддержкой в рабочем состоянии аппаратных средств автоматизированных систем. В отечественной языковой практике в указанном значении используется также термин инженер-электронщик.

Инженер по эксплуатационному обслуживанию – специалист в области электроники или вычислительной техники, инженер по образованию, в функции которого входит организация эксплуатации и поддержка в исправном состоянии технических средств автоматизированной системы.

Инженер знаний – специалист по искусственному интеллекту с инженерным образованием, занимающийся разработкой баз знаний или экспертных систем.

Инженерия знаний – область информатики, связанная с теорией искусственного интеллекта, прикладная направленность которой ориентирована на создание экспертных систем различного назначения и, в частности, - разработку баз знаний, способов их актуализации и управления ими.

Оператор:

- Специалист, управляющий работой автоматизированного устройства.
- Лицо, ответственное за текущий контроль состояния аппаратных (технических) средств системы.
- Специалист, входящий в штат сотрудников организации (фирмы, предприятия), обслуживаемой автоматизированной системой, если они выполняют свои функциональные обязанности с использованием ее терминальных средств.

Пользователь – лицо, использующее услуги автоматизированной системы для получения информации или решения различных задач.

Виды пользователей:

Абонент – лицо, группа лиц или организация, имеющие право на пользование услугами системы в качестве ее внешних или конечных пользователей.

Внешний (***конечный***) ***пользователь*** – пользователь, обращающийся к информационным ресурсам автоматизированной системы или вычислительной сети для решения различных задач и, как правило, не входящий в состав персонала соответствующей системы.

Внутренний пользователь – пользователь, относящийся к персоналу системы, предоставляющей свои ресурсы в вычислительную сеть.

Диалоговый/интерактивный пользователь – пользователь, работающий с системой в диалоговом (интерактивном) режиме.

Терминальный пользователь – пользователь, взаимодействующий с автоматизированной системой со своего терминала, например, ПЭВМ.

Удаленный пользователь – пользователь, осуществляющий доступ к ресурсам системы с удаленного терминала с использованием каналов связи.

Зарегистрированный пользователь – пользователь, имеющий личный регистрационный номер или код, определяющий характер его прав при работе с системой коллективного пользования.

Привилегированный пользователь – пользователь, имеющий больше прав («привилегий») по сравнению с другими пользователями при работе с средствами и ресурсами автоматизированной системы.

Незарегистрированный пользователь:

Пользователь, не состоящий на учете в данной системе коллективного пользования.

Пользователь, работающий в системе не по графику или в условиях превышения установленных для него прав.

Тонкий клиент – пользователь маломощного ПК или рабочей станции, выполняющий с их помощью ограниченный круг видов работ и операций.

Хакер – лицо, осуществляющее систематические несанкционированные доступы в компьютерные системы и сети с целью развлечения, мошенничества или нанесения ущерба (в том числе путем разработки и распространения компьютерных вирусов). В более широком смысле этот термин распространяется также на программистов-любителей (иногда достаточно высококвалифицированных), а также программистов производящих несанкционированную переработку и/или распространение программных продуктов.