Служба управления безопасностью

Администрирование ИС

Лекция 10

Безопасность информационной системы

Безопасность информационной системы – свойство, заключающееся в способности системы обеспечить *конфиденциальность и целостность информации*, т.е. защиту информации от несанкционированного доступа с целью ее раскрытия, изменения или разрушения.

В соответствии с общепринятым современным подходом выделяют следующие аспекты информационной безопасности:

- **доступность** (возможность за приемлемое время получить требуемую информационную услугу);
- **целостность** (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- **конфиденциальность** (защита от несанкционированного ознакомления).

Главная цель мер, предпринимаемых на административном уровне, состоит в том, чтобы *сформировать программу работ в области повышения доступности информационных сервисов и обеспечить ее выполнение*, выделяя необходимые ресурсы и контролируя фактическое состояние дел.

Первым этапом выработки подобной программы является анализ угроз и рисков.

Все **угрозы информационным системам** можно объединить в обобщающие их три группы.

1. **Угроза раскрытия** — возможность того, что информация станет известной тому, кому не следовало бы ее знать.
2. **Угроза целостности** — умышленное несанкционированное изменение (модификация или удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую.
3. **Угроза отказа в обслуживании** — возможность появления блокировки доступа к некоторому ресурсу вычислительной системы.

Выделяют следующие классы отказов:

1. Отказ пользователей – возникает по следующим причинам:

- *нежелание работать с информационной системой;*
- *невозможность работать с системой в силу отсутствия соответствующей подготовки;*
- *невозможность работать с системой в силу отсутствия технической поддержки.*

2. Внутренний отказ информационной системы – возникает по следующим причинам:

- *отступление (случайное или умышленное) от установленных правил эксплуатации;*
- *ошибки при (пере)конфигурировании системы;*
- *отказы программного и аппаратного обеспечения;*
- *разрушение данных;*
- *разрушение или повреждение аппаратуры.*

3. Отказ поддерживающей инфраструктуры – возникает по следующим причинам:

- *нарушение работы (случайное или умышленное) систем связи, электропитания, водоснабжения, кондиционирования;*
- *разрушение или повреждение помещений;*
- *невозможность или нежелание выполнения обслуживающим персоналом и/или пользователями своих обязанностей (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).*

По природе возникновения *угрозы* можно разделить на:

- ***Естественные угрозы*** — это угрозы, связанные с воздействиями на **ИС** объективных физических процессов или природных явлений.
- ***Искусственные угрозы*** — это угрозы **ИС**, связанные с деятельностью человека.

Пользователем **ИС** могут быть осуществлены следующие **<u>непреднамеренные</u> действия**, представляющие ***угрозу безопасности* ИС**:

- доведение до состояния частичного или полного отказа системы, разрушение аппаратных, программных, информационных ресурсов системы (*порча оборудования, носителей информации, удаление, искажение файлов с важной информацией или программ*);
- неправомерное включение оборудования или изменение режимов работы устройств и программ;
- запуск сервисных программ, способных при некомпетентном использовании вызывать потерю работоспособности системы или необратимые изменения в системе;
- нелегальное внедрение и использование неучтенных программ, не являющихся необходимыми для выполнения служебных обязанностей, с последующим необоснованным расходованием ресурсов (*загрузка процессора, захват оперативной памяти и памяти внешних носителей*);
- заражение компьютера вирусами;
- разглашение конфиденциальной информации;
- разглашение, передача или утрата атрибутов разграничения доступа (*паролей, ключей шифрования, идентификационных карточек, пропусков и т. п.)*;
- игнорирование организационных ограничений;
- некомпетентное использование, настройка или неправомерное отключение средств защиты информации;
- пересылка данных по ошибочному адресу абонента;
- ввод ошибочных данных;
- повреждение каналов связи.

Пользователем **ИС** могут быть осуществлены следующие **преднамеренные** действия, представляющие ***угрозу безопасности* ИС :**

- физическое разрушение системы или вывод из строя наиболее важных ее компонентов;
- отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (*электропитания, охлаждения и вентиляции, линий связи и т. п.);*
- дезорганизация функционирования системы (*изменение режимов работы устройств или программ, создание мощных активных радиопомех и т. п.);*
- внедрение агентов в число персонала, вербовка персонала или отдельных пользователей, имеющих определенные полномочия;
- применение подслушивающих устройств, дистанционная фото и видеосъемка и т. п.;
- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
- перехват данных, передаваемых по каналам связи, и их анализ с целью осуществления попыток проникновения в систему;
- хищение носителей информации;
- несанкционированное копирование носителей информации;
- хищение производственных отходов (*распечаток, записей, списанных носителей информации и т.п.*);
- чтение остатков информации из оперативной памяти и с внешних запоминающих устройств, чтение информации из областей оперативной памяти, используемых операционной системой;
- незаконное получение паролей и других реквизитов разграничения доступа (*агентурным путем, используя халатность пользователей, путем подбора, имитации интерфейса системы и т. п.)* с последующей маскировкой под зарегистрированного пользователя;
- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики;
- вскрытие шифров криптозащиты информации;
- внедрение аппаратных спецвложений, программ «***закладок***» и «***троянских коней***».

Формализованное описание или представления комплекса возможностей нарушителя по реализации тех или иных угроз безопасности информации называют ***моделью нарушителя***, при разработке которой делаются предположения:

- *о категориях лиц, к которым может принадлежать нарушитель;*
- *о мотивах действий нарушителя;*
- *о квалификации нарушителя и его технической оснащенности;*
- *о характере возможных действий нарушителя.*

По отношению к **ИС *нарушители*** могут быть:

Внутренние нарушители - могут быть лица из следующих категорий персонала:

- пользователи системы;
- персонал, обслуживающий технические средства (инженеры, техники);
- сотрудники отделов разработки и сопровождения программного обеспечения (прикладные и системные программисты);
- технический персонал, обслуживающий здание (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здание и помещения, где расположены компоненты **ИС**);
- сотрудники службы безопасности **ИС**;
- руководители различных уровней должностной иерархии.

Посторонние лица, которые могут быть ***внешними нарушителями***:

- клиенты;
- посетители;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжение и т. п.);
- представители конкурирующих организаций или лица, действующие по их заданию;
- лица, случайно или умышленно нарушившие пропускной режим (без цели нарушения безопасности **ИС**).

Можно выделить ***три основных мотива нарушений*** :

- безответственность;
- самоутверждение;
- корыстный интерес.

Нарушители классифицируются по следующим признакам:

1. **По уровню знаний об ИС.**
2. **По уровню возможностей** - нарушители определяются, как:

- *применяющие чисто агентурные методы получения сведений;*
- *применяющие пассивные средства (технические средства перехвата без модификации компонентов системы);*
- *использующие только штатные средства и недостатки систем защиты для ее преодоления, а также компактные магнитные носители информации, которые могут быть скрытно пронесены через посты охраны;*
- *применяющие методы и средства активного воздействия (модификация и подключение дополнительных механических средств, подключение к каналам передачи данных, внедрение программных «**закладок**» и использование специальных инструментальных и технологических программ).*

3. **По месту действия** - нарушители могут быть:

- *не имеющие доступа на контролируемую территорию организации;*
- *действующие с контролируемой территории без доступа в здания и сооружения;*
- *действующие внутри помещений, но без доступа к техническим средствам **ИС**;*
- *действующие с рабочих мест конечных пользователей **ИС**;*
- *имеющие доступ в зону данных (баз данных, архивов и т. п.);*
- *имеющие доступ в зону управления средствами обеспечения безопасности **ИС**.*

Система защиты — это совокупность специальных мер правового и административного характера, организационных мероприятий, программно-аппаратных средств защиты, а также специального персонала, предназначенных для обеспечения информационной безопасности .

Для построения эффективной ***системы защиты*** необходимо провести следующие работы :

- определить угрозы безопасности информации;
- выявить возможные каналы утечки информации и несанкционированного доступа (**НСД**) к данным;
- построить модель потенциального нарушителя;
- выбрать соответствующие меры, методы, механизмы и средства зашиты.

Проблема создания системы защиты информации включает две задачи:

- разработка системы защиты информации;
- оценка разработанной системы защиты информации.

Вторая задача решается путем анализа технических характеристик системы с целью установления, удовлетворяет ли система защиты информации комплексу требований. Такая задача в настоящее время решается **экспертным путем** с помощью сертификации средств защиты информации и аттестации системы защиты информации в процессе ее внедрения.

Основные методы защиты информации:

1. ***Создание препятствий*** — методы физического преграждения злоумышленнику пути к защищаемой информации (аппаратуре, носителям информации и т. д.).
2. ***Управление доступом*** — метод защиты информации регулированием использования всех ресурсов компьютерной информационной системы (элементов баз данных, программных и технических средств).
3. ***Защита от несанкционированного доступа к ресурсам компьютера*** — это комплексная проблема, подразумевающая решение следующих вопросов:
   - присвоение пользователю, терминалам, программам, файлам и каналам связи уникальных имен и кодов (идентификаторов);
   - выполнение процедур установления подлинности при обращениях к информационной системе, то есть проверка того, что лицо или устройство, сообщившее идентификатор, в действительности ему соответствует;
   - проверка полномочий, то есть проверка права пользователя на доступ к системе или запрашиваемым данным;
   - автоматическая регистрация в специальном журнале всех как удовлетворенных, так и отвергнутых запросов к информационным ресурсам с указанием идентификатора пользователя, терминала, времени и сущности запроса, то есть ведение аудита.
4. ***Маскировка*** — метод защиты информации путем ее криптографического закрытия.
5. ***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.
6. ***Принуждение*** — метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Рассмотренные методы обеспечения безопасности реализуются на практике за счет применения различных средств защиты, таких как технические, программные, организационные, законодательные.

Средства обеспечения информационной безопасности

Средства обеспечения информационной безопасности **в зависимости от способа их реализации** можно разделить на следующие классы методов:

- **аппаратные методы**, реализующие физическую защиту системы от несанкционированного доступа, аппаратные функции идентификации периферийных терминалов системы и пользователей, режимы подключения сетевых компонентов и т. д.

К техническим средствам физической защиты информации (ЗИ) относят механические, электронно-механические, электромеханические, оптические, акустические, лазерные, радио и другие устройства, системы и сооружения, предназначенные для создания физических препятствий на пути к защищаемой информации и способные выполнять самостоятельно или в комплексе с другими средствами функции защиты информации.

Средства обеспечения информационной безопасности

- **организационные методы** подразумевают рациональное конфигурирование, организацию и администрирование системы. В первую очередь это касается сетевых информационных систем, их операционных систем, полномочий сетевого администратора, набора обязательных инструкций, определяющих порядок доступа и работы в сети пользователей;

- **технологические методы**, включающие в себя технологии выполнения сетевого администрирования, мониторинга и аудита безопасности информационных ресурсов, ведения электронных журналов регистрации пользователей, фильтрации и антивирусной обработки поступающей информации;

- **программные методы** - это самые распространенные методы защиты информации (*например, программы идентификации пользователей, парольной защиты и проверки полномочий, брандмауэры, криптопротоколы и т. д*.).

Без использования программной составляющей практически невыполнимы никакие, в том числе и первые три группы методов (то есть в чистом виде организационные, технологические и аппаратные методы защиты, как правило, реализованы быть не могут — все они содержат программный компонент).

Типы защиты сети

Типы защиты сети можно разбить на четыре основные категории:

- *физическая безопасность;*
- *защита пользователей;*
- *защита файлов;*
- *защита от вторжения извне.*

Типы защиты сети

Физическая безопасность

- Любому компьютеру, является ли он сервером в сети, рабочей станцией, ноутбуком или общедоступным терминалом в уличном киоске, необходимо обеспечить физическую защиту.

Защита пользователя

У защиты пользователя есть два аспекта:

- *предоставление пользователю доступа к тем ресурсам, в которых он нуждается;*
- *не предоставлять (и даже не показывать) пользователю те ресурсы, которые ему не требуются для работы. К таким ресурсам относятся наиболее конфиденциальная информация компании и личные данные пользователей.*

Управление доступом сводится к взаимному опознанию пользователя и системы и установлению факта допустимости использования ресурсов конкретным пользователем в соответствии с его запросом.

Типы защиты сети

Защита файлов

При обеспечении защиты файлов также имеется два аспекта:

- *управление доступом к файлу;*
- *защита целостности файла.*

Нарушитель, преднамеренно проникнувший в систему, может извлечь, изменить или уничтожить информацию в файлах. Поэтому необходим ввод некоторых ограничений на обработку файлов, содержащих важную информацию.

Защита от вторжения извне

Защита реализуется процедурами идентификации, установления подлинности и регистрации обращений.

Идентификация и подтверждение подлинности могут осуществляться в процессе работы неоднократно, чтобы исключить возможность входа в систему нарушителя, выдающего себя за истинного пользователя.

Модели администрирования сети и способы обеспечения безопасности

Администрирование сети можно организовать одним из четырех основных способов:

- *централизованно на всем предприятии;*
- *по отделам или группам («распределенное» администрирование);*
- *по операционным системам;*
- *в виде сочетания предыдущих способов.*

Модели администрирования небольших и крупных, сложных систем могут совпадать. Они будут отличаться масштабами, но не по сути.

Централизованное администрирование

В модели с централизованным администрированием один человек, группа или отдел занимается администрированием всей сети организации, ее пользователей и ресурсов.

Главным и очень серьезным недостатком централизованной схемы является ее недостаточная масштабируемость и отсутствие отказоустойчивости.

Производительность центрального компьютера всегда будет ограничителем количества пользователей, работающих с данным приложением, а отказ центрального компьютера приводит к прекращению работы всех пользователей.

Эта модель хорошо подходит небольшим и средним организациям, но может оказаться медленной и неэффективной для крупного или географически разбросанного предприятия.

Однако с точки зрения безопасности централизованное администрирование является наилучшим. Оно гарантирует, что системная политика и процедуры являются однообразными для всей организации.

Распределенное администрирование

При распределенном администрировании управление сетью осуществляется *на уровне отдела или рабочей группы*.

Хотя администрирование на этом уровне может быстро откликаться на нужды пользователей, часто это достигается за счет безопасности сети.

При наличии нескольких администраторов политика администрирования в разных рабочих группах будет отличаться.

Чем больше групп имеется в системе, тем больше доверительных отношений им требуется, что повышает возможность того, что в систему проникнет злоумышленник и воспользуется этими доверительными отношениями, чтобы добраться до совершенно секретной информации.

Администрирование по операционным системам

Когда администрирование домена производится по операционным системам, средства обеспечения безопасности значительно различаются в зависимости от используемых операционных систем.

Например, если имеется свой администратор у сервера Windows NT Server, свой — у сервера Novell Net Ware и свой — у систем UNIX, то администратор каждой системы будет сам обеспечивать ее безопасность.

Однако потребуется кто-то, кто будет разрешать различия во мнениях администраторов в случае возникновения проблем.

Смешанная модель администрирования

Смешанная модель администрирования сочетает элементы централизованной и распределенной моделей.

Центральный администратор (или группа) гарантирует проведение политики безопасности на всем предприятии, а администраторы на уровне отделов или рабочих групп выполняют повседневную работу.

При этом обычно *требуется больше затрат на штат*, чем может себе позволить небольшая организация, поэтому применение смешанной модели администрирования, как правило, ограничивается *крупными предприятиями*.

Заключение

Политика безопасности должна исполняться во всей организации.

Соответствие самому строгому уровню безопасности вместе с применением множества средств обеспечения безопасности при условии, что система неаккуратно спроектирована и плохо управляется, может привести к неэффективности защиты и сложности использования системы по её прямому назначению.

Необходимо помнить, что практически всегда повышение уровня безопасности системы требует увеличения времени и усилий администратора на управление им.

При построении системы защиты разумно придерживаться следующих принципов:

- **Актуальность.** Защищаться следует от реальных атак, а не от фантастических или же архаичных.
- **Разумность затрат.** Поскольку 100% защиты обеспечить нереально, необходимо найти тот рубеж, за которым дальнейшие траты на повышение безопасности превысят стоимость той информации, которую может украсть злоумышленник.