Курс: **основы информационной безопасности**

Тема: **Общие методы обеспечения ИБ в АС, разграничение доступа**

Преподаватель: Пятков Антон Геннадьевич

Красноярск

Основные методы противодействия угрозам ИБ

- ✔ Организационные;
- ✔ Инженерно-технические;
- ✔ Технические;
- ✔ Программно-аппаратные.

Организационные методы - ориентированы на работу с персоналом, осуществление контроля, возложение персональной ответственности за выполнение мер защиты, кадровые вопросы.

Инженерно-технические методы - связаны с построением инженерных сооружений и коммуникаций, учитывающих требования безопасности.

Технические методы - применение специальных технических средств защиты информации и контроля обстановки.

Программно-аппаратные методы - направлены на устранение угроз, непосредственно связанных с процессом обработки и передачи информации.

! Наибольший эффект дает оптимальное сочетание всех выше перечисленных методов противодействия реализации угроз ИБ.

Виды мер противодействия угрозам ИБ

- ✔ **правовые (законодательные);**
- ✔ **морально-этические;**
- ✔ **технологические;**
- ✔ **организационные (административные и процедурные);**
- ✔ **физические;**
- ✔ **технические (программные, аппаратные, программно-аппаратные).**

К правовым мерам относятся действующие в стране нормативно-правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее получения, обработки и использования, а также устанавливающие ответственность за нарушения этих правил.

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Не обязательны, как требования нормативных актов, но их несоблюдение ведет обычно к падению авторитета или престижа человека, группы лиц или организации.

Технологические – разного рода технологические решения и приемы, основанные обычно на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.).

Организационные меры – меры административного и процедурного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей и обслуживающего персонала с системой таким образом, чтобы в затруднить или исключить возможность реализации угроз ИБ или снизить размер потерь в случае их реализации.

Физические меры защиты основаны на применении разного рода механических, электро-или электронно-механических устройств и сооружений, предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей, а также средств визуального наблюдения, связи и охранной сигнализации.

Технические меры защиты основаны на использовании различных электронных устройств и спец.программ, входящих в состав АС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты.

Основные механизмы защиты

- идентификация (именование и опознавание) и аутентификация (подтверждение подлинности) пользователей системы;
- разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователям;
- регистрация и оперативное оповещение о событиях в системе;
- криптографическое закрытие хранимых и передаваемых по каналам связи данных (теневое шифрование, VPN с шифрованием);
- контроль целостности и аутентичности (подлинности и авторства) данных;
- выявление и нейтрализация действий компьютерных вирусов;
- затирание остаточной информации на МНИ;
- выявление уязвимостей (слабых мест) системы;
- изоляция (защита периметра) компьютерных сетей (фильтрация трафика – Firewall, скрытие внутренней структуры и адресации, противодействие атакам на внутренние ресурсы и т.д.);
- обнаружение атак и оперативное реагирование (системы обнаружения вторжений – СОВ, группа реагирования на инциденты ИБ – ГРИБ);
- резервное копирование;
- маскировка (маскировка сервера Linux под сервер Windows и пр.).

ID –> KEY –> RIGHTS

Идентификация – процесс присвоения субъектам и объектам доступа идентификатора и/или сравнения предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Аутентификация – процесс опознавания субъекта или объекта путем сравнения введенных идентификационных данных с эталоном (образом), хранящимся в памяти системы для данного субъекта или объекта.

Авторизация – предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ.

Аутентификация пользователей осуществляется обычно путём проверки :

• знания ими паролей (секретных последовательностей символов);

• владения ими какими-либо специальными устройствами (карточками, ключевыми вставками...) с уникальными признакам;

• уникальных физических характеристик и параметров (отпечатков пальцев, особенностей радужной оболочки глаз, формы кисти рук, рисунки капилляров, клавиатурный подчерк,…) самих пользователей при помощи ных биометрических устройств.

Доступ

Объект доступа - единица информационного ресурса АС, доступ регламентируется ПРД

Субъект доступа - лицо или процесс, действия которого регламентируются правилами ПРД

Доступ к информации – ознакомление с информацией, её обработка (копирование, модификация или уничтожение).

Разграничение (контроль) доступа к ресурсам АС - такой порядок использования ресурсов АС, при котором субъекты получают доступ к объектам системы в строгом соответствии с установленными правилами разграничения доступа.

Правила разграничения доступа (ПРД) - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

Санкционированный доступ к информации - доступ к информации, не нарушающий ПРД

Несанкционированный доступ к информации (НСД) - доступ к информации, нарушающий ПРД с использованием штатных средств

Защита от НСД - предотвращение или существенное затруднение НСД

Матрица доступа - таблица, отображающая ПРД

Доступ

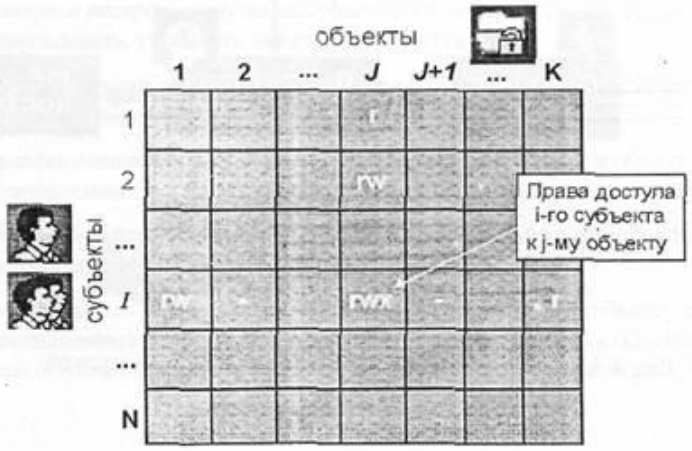
Нарушитель ПРД - субъект доступа, осуществляющий НСД к информации

Модель нарушителя ПРД - абстрактное (ф или неф) описание нарушителя ПРД

Комплекс средств защиты (КСЗ) - совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты АС от НСД к информации

Система разграничения доступа (СРД) - совокупность реализуемых ПРД в АС

Диспетчер доступа (ядро защиты) - технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа



Матрица доступа

Принцип распределения доступа

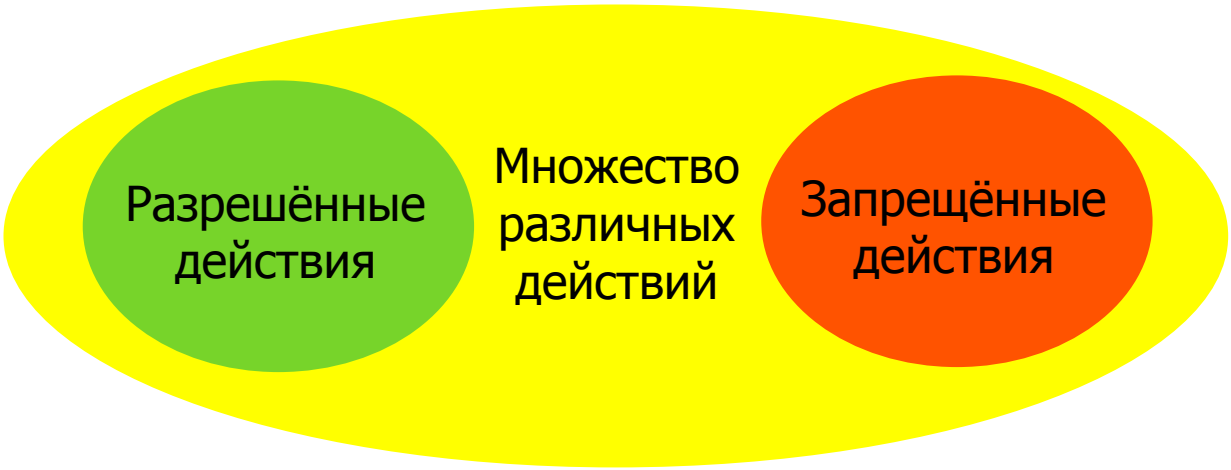
Разделение привилегий на доступ – объективно необходимое решение.

Основной принцип распределения прав доступа с точки зрения ИБ – **минимизация**.

Предоставлять пользователям только **минимально возможный** набор прав доступа, достаточный для выполнения пользователями их должностных обязанностей.

Для средств защиты информации (СЗИ) могут применяться подходы:

- ✔ коммунистический (запрещено всё, кроме того что явно разрешено);
- ✔ демократический (разрешено всё, кроме того что явно запрещено).



Принцип адекватности

При построении системы защиты необходимо стремиться к достижению адекватности мер по защите от угроз ИБ.

Нужно найти разумный баланс между защищённостью и функциональностью системы. ИБ не должно сковывать бизнес-процесс, но защищать его. Безопасность – ограничения.

На ИБ компании рекомендуется (мировая практика) тратить от 10% до 25% от расходов на ИТ-бюджет, но система защиты не должна обходиться дороже защищаемой информации (принцип адекватности).