**Тема 10. Сервисные программы и информационная безопасность.**

**Лекция 30 Виды угроз информационной безопасности. Подходы и способы защиты информационной безопасности**

Основной источник угроз – злоумышленники, хакеры, специализированные киберподразделения, использующие любые киберсредства, чтобы пробить защиту и проникнуть в базы данных, содержащие необходимую информацию. Находя узкие места и ошибки в работе программного обеспечения, они получают несанкционированную возможность получения данных из информационных баз.

Очень часто, учитывая неопытность пользователей, для получения нужной информации злоумышленники используют самый простой способ – использование спам-рассылок. Но иногда могут осуществляться и более серьезные виды кибератак.

**Виды угроз информационной безопасности**

Угрозы классифицируются по различным признакам:

По аспекту информационной безопасности, на который они направлены:

* Угрозы доступности.
* Угрозы целостности.
* Угрозы конфиденциальности.

По степени воздействия на информационную систему:

* Пассивные.
* Активные.

По природе возникновения:

* Непреднамеренные или преднамеренные.
* Естественные или искусственные.

По расположению источника:

* Внутренние угрозы.
* Внешние угрозы.

Угрозы могут быть направлены на базу данных, программные комплексы, аппаратуру или поддерживающую инфраструктуру.

Например, существуют открытые публичные организации, для которых не существует угроз конфиденциальности, потому что вся информация находится в общем доступе. Но для большинства компаний несанкционированный доступ представляет серьезную опасность.

Если угрозы направлены на взлом используемых вами программных комплексов, чаще всего на уровне пользователя вы не сможете на это повлиять. Единственный способ – не использовать некоторые программы. Использовать их можно, если проникновение злоумышленника не будет чревато утечкой важной информации и не повлечет существенных потерь для вас.

Безопасность от угроз, направленных на аппаратуру, инфраструктуру или от угроз природного характера, обеспечивает хостинг-компания, которая была выбрана вами в качестве арендодателя серверов. Подходите к выбору хостинг-компании внимательно и ответственно, она должна на высоком уровне обеспечить надёжность аппаратной и инфраструктурной составляющей.

**К основным видам угроз информационной безопасности относятся:**

* Внутренние сбои или отказ информационной системы.
* Отказ поддерживающей инфраструктуры.

**К основным угрозам в поддерживающей инфраструктуре относятся:**

* Сбой в работе, связанный с намеренным или случайным выходом из строя электрических систем, систем связи, водоснабжения, теплоснабжения и кондиционирования.
* Обвал, разрушение или повреждение зданий и сооружений.
* Невыполнение обслуживающим персоналом своих должностных обязанностей, обусловленное забастовками, сбоями в работе транспортных служб, авариями, природными катаклизмами, террористическими актами и т.п.

**Угрозы целостности разделяют на**: угрозы статической и динамической целостности, а также угрозы целостности служебной информации и содержательных данных.

Служебной информацией являются пароли для доступа, маршруты передачи данных в локальной сети и другая информация подобного рода. Очень часто противоправные действия и хакерские атаки осуществляет лицо, являющееся сотрудником компании, владеющее необходимым объемом информации о режиме работы и мерах защиты.

**Виды угроз информационной безопасности.**

Для того чтобы нарушить статическую целостность злоумышленник:

* Вводит неверные данные.
* Изменяет исходные данные.

К угрозам динамической целостности относятся кражи, копирование данных, внесение дополнительной информации.

Что касается конфиденциальной информации, то ее разделяют на предметную и служебную.

Служебная информация, примером которой являются пароли пользователей, несет техническую функцию и не относится к конкретной предметной области. Однако, ее раскрытие представляет особую опасность, потому что может способствовать получению доступа ко всей базе данных.

Одна из угроз, от которых очень трудно найти эффективный способ защиты – злоупотребление служебными полномочиями. Во многих системах предусмотрено предоставление доступа привилегированному пользователю, которым может являться системный администратор, ко всем файлам и почте любого пользователя.

Ущерб может быть нанесен при сервисном обслуживании, потому что сервисный инженер получает неограниченный доступ и имеет возможность в обход защитных барьеров подобраться к любому файлу.

**Подходы и способы защиты информационной безопасности**

Различают следующие способы, обеспечивающие безопасность данных в информационных системах:

* **Препятствие** — физическая преграда, препятствующая доступу злоумышленников к секретной информации. К примеру, вход в здание, где находится сервер, хранящий важную информацию, разрешен только сотрудникам компании.
* **Управление доступом** — доступ к информации и ее использованию контролируется системой идентификации пользователей, с проверкой их полномочий. К примеру, секретная информация хранится в компьютерах, находящихся в помещении или на этаже, доступ на который имеется только у сотрудников, имеющих специальные пропуска или владеющих логином и паролем для доступа к базе данных. Причем уровень предоставляемых каждому сотруднику привилегий может быть разным, в зависимости от уровня занимаемой должности и выполняемого сотрудником функционала.
* **Криптография** — один из способов сохранения конфиденциальности информации и целостности данных с помощью шифрования путем преобразования текста в специальный алгоритм. Ярким примером являются электронно-цифровые подписи.
* **Защита от атак вирусных и вредоносных программ (вирусы, трояны, сетевые черви, логические бомбы)** — использование антивирусных программ, внешних накопителей информации, резервное копирование данных.
* **Регламентация** — это способ информационной защиты, помогающий практически исключить для злоумышленника получение доступа к хранимой конфиденциальной информации. Например, многие компании вводят запрет на использование сотрудниками личных флэшек, утверждают специальные правила и стандарты работы, регламентирующие сроки создания резервных копий данных и т.п.
* **Принуждение** — установление определенных правил при работе с программами, содержащими секретную информацию, нарушение которых влечет за собой материальную, административную, а в некоторых случаях и уголовную ответственность.
* **Побуждение** — призыв к сотрудникам о соблюдении порядка по работе с конфиденциальной информацией, во избежание нарушений сложившихся морально-этических норм.

Различают следующие виды средств защиты информации:

* **Технические средства**. Например, установка сигнализации, защитных оконных решеток, использование устройств, создающих помехи при попытке передачи данных по радиоканалам, специальные электронные пропуска в виде ключ-карт для входа в здания.
* **Программные средства**. Программы для кодирования и шифрования данных, антивирусные программы, бэкап-системы, системы идентификации пользователей.
* **Смешанные средства**. Комбинированный комплекс технических и программных средств, обеспечивающих защиту информации.
* **Организационные средства**. Законодательные акты, нормативные документы, специализированные правила, регламентирующие деятельность в сфере защиты информации, оснащение и соответствующая подготовка помещений с компьютерной техникой, проведение сетевых кабелей с учетом требований по информационной безопасности и организация других действий, способствующих ограничению доступа к базам данных.