

# **Защита деловой информации**

**Обеспечение сохранности  
данных.  
Лекция 3.**

# **Информационная безопасность**

**Информационная безопасность (в узком смысле) – защита собственных информационных ресурсов.**

**Информационная безопасность (в широком смысле) – защита отдельных людей, сотрудников, общества от воздействия вредоносной информации.**

# Информационная безопасность

- Очевидно, что абсолютно безопасных систем не существует. Любую систему можно «взломать», если располагать достаточно большими материальными и временными ресурсами. Есть смысл оценивать лишь степень доверия, которое можно оказать той или иной системе, т. е. степень ее надежности для пользователя. Принято считать, что система, использующая достаточные аппаратные и программные средства для обеспечения одновременной обработки информации разной степени секретности группой пользователей без нарушения прав доступа, является надежной.
- Важным компонентом надежности системы является *политика безопасности* информации на предприятии. Она включает правила и нормы поведения при обработке, защите и распространении информации. В частности, правила определяют, в каких случаях пользователь имеет право работать с определенными наборами данных. Чем надежнее система, тем строже и разнообразнее правила, обеспечивающие политику безопасности.

# Информационная безопасность

- Дополнением политики безопасности является *механизм подотчетности*, который позволяет определять, кто работает в системе и что делает в каждый момент времени. *Средства подотчетности* делятся на три категории:
  - **идентификация и аутентификация,**
  - **предоставление надежного пути,**
  - **анализ регистрационной информации.**

# Идентификация и аутентификация.

- Каждый пользователь, прежде чем получить право совершать какие-либо действия в системе, должен идентифицировать себя. Обычный способ идентификации — ввод имени пользователя при входе в систему. В свою очередь система должна проверить подлинность личности пользователя, т. е. именно он является тем, за кого себя выдает. Стандартное средство проверки подлинности (аутентификации) — пароль, хотя могут использоваться также разного рода личные карточки, биометрические устройства (сканирование радужной оболочки глаза или отпечатков пальцев) или их комбинация.

# *Предоставление надежного пути.*

- Надежный путь связывает пользователя непосредственно с надежной вычислительной базой, минуя другие, потенциально опасные компоненты системы. Цель предоставления надежного пути — дать пользователю возможность убедиться в подлинности обслуживающей его системы.

# Анализ регистрационной информации.

- Он предусматривает наличие средств выборочного протоколирования как в отношении пользователей (слежение осуществляется только за подозрительными личностями), так и в отношении событий (вход-выход, обращение к удаленной системе, операции с файлами, смена привилегий и др.).  
*Протоколирование* помогает следить за пользователями и реконструировать прошедшие события. Реконструкция событий позволяет проанализировать случаи нарушений, понять, почему они стали возможны, оценить размеры ущерба и принять меры по исключению подобных нарушений в будущем. При протоколировании события записывается следующая информация: дата и время события; уникальный идентификатор пользователя — инициатора действия; тип события; результат действия (успех или неудача); источник запроса (например, имя терминала); имена затронутых объектов (например, открываемых или удаляемых файлов) и др.

# Определения.

- **Компьютерная безопасность** — это совокупность технологических и административных мер, которая обеспечивает доступность, целостность и конфиденциальность ресурсам, связанным с данным компьютером.
- **Безопасность данных** — это защита данных от несанкционированной модификации, разрушения или раскрытия их.
- **Безопасность коммуникаций** — это меры по предотвращению предоставления неавторизованным лицам информации, которая может быть выдана системой в ответ на запрос по каналам связи.
- **Безопасность программного обеспечения** — это программное обеспечение, которое осуществляет безопасную обработку данных в компьютерной системе, а также дает возможность безопасно использовать ресурсы системы.



# Информационная безопасность

Проведению в жизнь политики безопасности для информационной системы на базе компьютерной сети способствуют:

- невозможность миновать защитные средства при доступе в систему;
- невозможность перехода системы в небезопасное состояние;
- разделение обязанностей;
- разнообразие защитных средств;
- простота и управляемость информационной системы;
- обеспечение всеобщей поддержки мер безопасности.

# Информационная безопасность

- Среди экономических факторов угроз информационной безопасности наиболее существенными являются переход к рыночной экономике; критическое состояние отраслей промышленности; расширяющаяся кооперация с зарубежными странами.

- К организационно-техническим факторам угрозы информационной безопасности относят: недостаточную нормативно-правовую базу в сфере информационных отношений; рост объемов информации, передаваемой по открытым каналам связи; широкое использование в сфере государственного управления и кредитно-финансовой сфере незащищенных от утечки информации импортных технических и программных средств для хранения, обработки и передачи информации.

- Существуют различные виды угроз на объекты информационной безопасности: информационные, программно-математические, физические, радиоэлектронные и организационно-правовые

# Виды угроз на объекты информационной безопасности

## Виды угроз

Информационные	Программно-математические	Физические	Радиоэлектронные	Организационно-правовые
<p>Нарушение адреса и своевременности обмена. Несанкционированный доступ.</p> <p>Манипулирование информацией.</p> <p>Незаконное копирование данных и систем.</p> <p>Нарушение технологии информации.</p>	<p>Внедрение программ-вирусов. Установка программных и аппаратных закладных устройств.</p> <p>Уничтожение или модификация данных в информационных системах.</p>	<p>Уничтожение или разрушение средств обработки информации и связи.</p> <p>Уничтожение, разрушение или хищение машинных или других оригинальных носителей информации. Хищение программных и аппаратных ключей и средств криптографической защиты информации.</p> <p>Воздействие на персонал.</p> <p>Постановка "зараженных" компонентов информационных систем.</p>	<p>Перехват информации в технических каналах ее возможной утечки</p> <p>Внедрение электронных устройств перехвата информации в технических средствах и помещениях.</p> <p>Перехват, дешифрование и навязывание ложной информации в сетях передачи данных и линий связи.</p> <p>Воздействие на парольно-ключевые системы.</p> <p>Радиоэлектронное подавление линий связи и систем управления.</p>	<p>Невыполнение требований законодательства и задержки в принятии необходимых нормативно-правовых положений в информационной сфере.</p> <p>Неправомерное ограничение доступа к документам, содержащим важную для граждан и организаций информацию.</p>

# Информационная безопасность

- Для борьбы с угрозами информационной безопасности разрабатываются различные методы и средства защиты информации.
- Сложились два основных подхода к проблеме обеспечения информационной безопасности — *редукционистский* (фрагментарный) и *системный* (комплексный).
- *Редукционистский подход* ориентирован на избирательность относительно конкретной угрозы. Его отличительная черта — отсутствие единой защищенной среды обработки информации.
- *Системный подход* к защите информации в сложных автоматизированных системах охватывает все уровни обработки и передачи информации. Он целенаправленно проводится в жизнь на основе законодательно закрепленных норм и правил обеспечения информационной безопасности.