**Что такое информационная безопасность?**

**1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ.**

**Информационная безопасность** – защищенность информации и соответствующей инфраструктуры от случайных или преднамеренных воздействий сопровождающихся нанесением ущерба владельцам или пользователям информации.

**Информационная безопасность** – обеспечение конфиденциальности, целостности и доступности информации.

**Цель защиты информации** – минимизация потерь, вызванных нарушением целостности или конфиденциальности данных, а также их недоступности для потребителей.

**2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.**

***Основные типы угроз информационной безопасности:***

**1. Угрозы конфиденциальности** – несанкционированный доступ к данным.  
**2. Угрозы целостности** – несанкционированная модификация, дополнение или уничтожение данных.  
**3. Угрозы доступности** – ограничение или блокирование доступа к данным.

***Источники угроз:***

**1. Внутренние:**

а) ошибки пользователей и сисадминов;  
б) ошибки в работе ПО;  
в) сбои в работе компьютерного оборудования;  
г) нарушение сотрудниками компании регламентов по работе с информацией.

**2. Внешние угрозы:**

а) несанкционированный доступ к информации со стороны заинтересованных организаций и отдельных лица;  
б) компьютерные вирусы и иные вредоносные программы;  
в) стихийные бедствия и техногенные катастрофы.

**3. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ.**

***Методы обеспечения безопасности информации в ИС:***

* **Препятствие —** физическое преграждение пути злоумышленнику к защищаемой информации.
* **Управление доступом –** регулирование использования информации и доступа к ней за счет системы идентификации пользователей, их опознавания, проверки полномочий и т.д.
* **Криптография –** шифрование информации с помощью специальных алгоритмов.
* **Противодействие атакам вредоносных программ** **–** предполагает использование внешних накопителей информации только от проверенных источников, антивирусных программ, брандмауэров, регулярное выполнение резервного копирования важных данных и т.д. (*вредоносных программ очень много и они делятся на ряд классов: вирусы, эксплойты, логические бомбы, трояны, сетевые черви и т.п.*).
* **Регламентация –** создание условий по обработке, передаче и хранению информации, в наибольшей степени обеспечивающих ее защиту (*специальные нормы и стандарты для персонала по работе с информацией, например, предписывающие в определенные числа делать резервную копию электронной документации, запрещающие использование собственных флеш-накопителей и т.д.*).
* **Принуждение –** установление правил по работе с информацией, нарушение которых карается материальной, административной или даже уголовной ответственностью(*штрафы, закон «О коммерческой тайне» и т.п.*).
* **Побуждение –** призыв к персоналу не нарушать установленные порядки по работе с информацией, т.к. это противоречит сложившимся моральным и этическим нормам.

***Средства защиты информации:***

* **Технические (аппаратные) средства –** сигнализация, решетки на окнах, генераторы помех воспрепятствования передаче данных по радиоканалам, электронные ключи и т.д.
* **Программные средства** – программы-шифровальщики данных, антивирусы, системы аутентификации пользователей и т.п.
* **Смешанные средства** – комбинация аппаратных и программных средств.
* **Организационные средства** – правила работы, регламенты, законодательные акты в сфере защиты информации, подготовка помещений с компьютерной техникой и прокладка сетевых кабелей с учетом требований по ограничению доступа к информации и пр.