**Основные виды угроз информационной безопасности и средства защиты информации.**

**Информация – это знания,** которые он получает из различных источников с помощью органов чувств

Информационная безопасность, или ИБ, — это комплекс мер, которые нужны, чтобы защитить от утечки или взлома программы, компьютерные системы и данные.

Конфиденциа́льность (от лат. confidentia — доверие) — необходимость предотвращения разглашения, утечки какой-либо информации.

Защита информации (ЗИ) - комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности: целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.

Целью защиты информации является предотвращение нанесения ущерба пользователю, владельцу, собственнику информации.

Средства защиты информации:

**Технические** (аппаратные) средства — сигнализация, решетки на окнах, генераторы помех воспрепятствования передаче данных по радиоканалам, вход в здание или помещение по ключ-карте, электронные ключи и т. д.

**Программные средств**а — программы-шифровальщики данных, антивирусы, брандмауэры, бэкап-системы, 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.

**Законодательные средства** – законодательные акты страны, которыми регламентируются правила использования и обработки информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил;

**Морально-этические средства.**

Защита информации – деятельность, направленная на сохранение государственной, служебной, коммерческой или личной тайн, а также на сохранение носителей информации любого содержания.

Информационная безопасность направлена: – на предупреждение угроз как превентивных мер по обеспечению информационной безопасности в интересах упреждения возможности их возникновения; – на выявление угроз, которое выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению; – на обнаружение угроз, целью которого является определение реальных угроз и конкретных преступных действий; – на локализацию преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий; – на ликвидацию последствий угроз и преступных действий и восстановление статус-кво.

Система защиты информации – комплекс организационных и технических мероприятий по защите информации, проводимых на объекте управления с применением средств и способов в соответствии с концепцией, целью и замыслом защиты.

**Задачи информационной безопасности общества**

Выделяют четыре основные составляющие национальных интересов РФ в информационной сфере.

1. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечения духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

2. Информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации о государственной политике РФ, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

3. Развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

4. Защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

**Уровни формирования информационной безопасности**

Уровни формирования информационной безопасности Обеспечение информационной безопасности – это комплексная проблема, для решения которой требуется сочетание мер законодательного, 17 административного, процедурного и программнотехнического уровней. Соответственно выделяют три уровня формирования режима информационной безопасности: – законодательно-правовой; – административный (организационный); – программно-технический.

**Задания для самостоятельной работы**

**Записать в тетрадь Законы РФ информационной безопасности**

**Почему информацию надо защищать?**

**Какая информация называется защищаемой?**

**Какая информация называется цифровой?**

**Какие основные виды угроз существуют для цифровой информации?**

**Что надо сделать, чтобы быть спокойным за информацию в своем личном ПК?**