Тема занятия: **Информационная безопасность**

Вопрос 1: Понятие информационной безопасности:- что означает этот термин;- защита информации;- угрозы доступности

- **Информационная безопасность** – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации. Другими словами, это набор технологий, стандартов и методов управления, которые необходимы для защиты информационной безопасности.
- **Цель обеспечения информационной безопасности** – защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения.

Принципы защиты информации:

- **Конфиденциальность.** Это значит ввести в действие контроль, чтобы гарантировать достаточный уровень безопасности с данными предприятия, активами и информацией на разных этапах деловых операций для предотвращения нежелательного или несанкционированного раскрытия. Конфиденциальность должна поддерживаться при сохранении информации, а также при транзите через рядовые организации независимо от ее формата.
- **Целостность.** Целостность имеет дело с элементами управления, которые связаны с обеспечением того, чтобы корпоративная информация была внутренне и внешне последовательной. Целостность также гарантирует предотвращение искажения информации.
- **Доступность.** Доступность обеспечивает надежный и эффективный доступ к информации уполномоченных лиц. Сетевая среда должна вести себя предсказуемым образом с целью получить доступ к информации и данным, когда это необходимо. Восстановление системы по причине сбоя является важным фактором, когда речь идет о доступности информации, и такое восстановление также должно быть обеспечено таким образом, чтобы это не влияло на работу отрицательно.

Виды контроля безопасности

- **Административный.** Административный вид контроля состоит из утвержденных процедур, стандартов и принципов. Он формирует рамки для ведения бизнеса и управления людьми. Законы и нормативные акты, созданные государственными органами, также являются одним из видов административного контроля. Другие примеры административного контроля включают политику корпоративной безопасности, паролей, найма и дисциплинарные меры.
- **Логический.** Логические средства управления (еще называемые техническими средствами контроля) базируются на защите доступа к информационным системам, программном обеспечении, паролях, брандмауэрах, информации для мониторинга и контроле доступа к системам информации.
- **Физический.** Это контроль среды рабочего места и вычислительных средств (отопление и кондиционирование воздуха, дымовые и пожарные сигнализации, противопожарные системы, камеры, баррикады, ограждения, замки, двери и др.).

Угрозы информационной безопасности можно разделить на следующие:

- **Естественные** (катаклизмы, независящие от человека: пожары, ураганы, наводнение, удары молнии и т.д.).
- **Искусственные,** которые также делятся на:
  - непреднамеренные (совершаются людьми по неосторожности или незнанию);
  - преднамеренные (хакерские атаки, противоправные действия конкурентов, месть сотрудников и пр.).
- **Внутренние** (источники угрозы, которые находятся внутри системы).
- **Внешние** (источники угроз за пределами системы)

средства защиты информационной безопасности — это набор технических приспособлений, устройств, приборов различного характера, которые препятствуют утечке информации и выполняют функцию ее защиты.

Средства защиты информации делятся на:

- **Организационные.** Это совокупность организационно-технических (обеспечение компьютерными помещениями, настройка кабельной системы и др.) и организационно-правовых (законодательная база, статут конкретной организации) средств.
- **Программные.** Те программы, которые помогают контролировать, хранить и защищать информацию и доступ к ней.
- **Технические (аппаратные).** Это технические виды устройств, которые защищают информацию от проникновения и утечки.
- **Смешанные аппаратно-программные.** Выполняют функции как аппаратных, так и программных средств.

Информация сейчас подвергается все большему числу угроз и уязвимостей. Хакерские атаки, перехват данных по сети, воздействие вирусного ПО и прочие угрозы приобретают более изощренный характер и набирают огромный темп. Отсюда возникает необходимость внедрять системы информационной безопасности, которые могли бы защитить данные компании.

На выбор подходящих средств защиты информации влияют многие факторы, включая сферу деятельности компании, ее размер, техническую сторону, а также знания сотрудников в области информационной безопасности.