Лекция № 3

ВИДЫ ПРОФЕССИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ ЧЕЛОВЕКА С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ И ИНФОРМАЦИОННЫХ РЕСУРСОВ

Некоторые виды информационной деятельности человека

Область деятельности	**Профессии**	**Технические средства**	**Информационные ресурсы**
Средства массовой информации	Журналисты	Телевидение, Радио, Телекоммуникации, Компьютеры, Компьютерные сети	Интернет, Электронная почта, Библиотеки, Архивы
Почта, телеграф, телефония	Служащие, Инженеры	Традиционный транспорт, Телеграф, Телефонные сети, Компьютерные сети	БД
Наука	Ученые	Телекоммуникации, Компьютеры, Компьютерные сети	Библиотеки, Архивы, БД, БЗ, Экспертные системы, Интернет
Техника	Инженеры	Телекоммуникации, Компьютеры, Компьютерные сети	Библиотеки, Патенты, БД, БЗ, Экспертные системы, Интернет

Некоторые виды информационной деятельности человека (продолжение)

Область деятельности	**Профессии**	**Технические средства**	**Информационные ресурсы**
Управление	Менеджеры	Информационные системы, Телекоммуникации, Компьютеры, Компьютерные сети	БД, БЗ, Экспертные системы
Образование	Преподаватели	Информационные системы, Телекоммуникации, Компьютеры, Компьютерные сети	Библиотеки, Интернет
Искусство	Писатели, Художники, Музыканты, дизайнеры	Компьютеры, устройства ввода/вывода и отображения информации, Аудио- и видеосистемы, системы мультимедиа, Телекоммуникации, Компьютерные сети	Библиотеки, Музеи, Интернет

Профессия	**Направление деятельности**
Математик, Системный программист	Прикладная математика и информатика, компьютерная безопасность. Математическое обеспечение и администрирование информационных систем
Информатик (область применения)	Прикладная информатика (по областям)
Специалист по защите информации	Организация и технология защиты информации, защита объектов информации
Инженер	Вычислительная техника, телекоммуникации, информационные системы.

Правовое регулирование в информационной сфере

В Российской Федерации существует ряд законов в этой области.

- Закон «О правовой охране программ для ЭВМ и баз данных» регламентирует юридические вопросы, связанные с авторскими правами на программные продукты и базы данных.
- Закон «Об информации, информатизации и защите информации» позволяет защищать информационные ресурсы (личные и общественные) от искажения, порчи, уничтожения. (статья 11)

В Уголовном кодексе РФ имеется раздел «Преступления в сфере компьютерной информации». Он предусматривает наказания за:

- неправомерный доступ к компьютерной информации;
- создание, использование и распространение вредоносных программ для ЭВМ;
- умышленное нарушение правил эксплуатации ЭВМ и их сетей.

Информационная безопасность- совокупность мер по защите информационной среды общества и человека.

Информационные угрозы безопасности информации можно разделить на:

- *преднамеренные* (хищение информации, компьютерные вирусы, физическое воздействие на аппаратуру)
- *случайные* (ошибки пользователя, ошибки профессионалов, отказы и сбои аппаратуры, форс-мажорные обстоятельства).

Политика безопасности — это совокупность технических, программных и организационных мер, направленных на защиту информации в компьютерной сети.

К *традиционным методам защиты* от преднамеренных информационных угроз относятся:

- ограничение доступа к информации,
- шифрование (криптография) информации,
- контроль доступа к аппаратуре,
- законодательные меры.

Ограничение доступа к информации осуществляется на двух уровнях:

- на *уровне среды обитания человека* (путем создания искусственной преграды вокруг объекта защиты: выдачи допущенным лицам специальных пропусков, установки охранной сигнализации или систем видеонаблюдения)
- *на уровне защиты компьютерных систем* (например, с помощью разделения информации, циркулирующей в компьютерной системе, на части и организации доступа к ней лиц в соответствии с их функциональными обязанностями (пароль).

Шифрование (криптография) информации заключается в преобразовании (кодировании) слов, букв, слогов, цифр с помощью специальных алгоритмов.

Для ознакомления с шифрованной информацией нужен обратный процесс — декодирование.

Контроль доступа к аппаратуре означает, что вся аппаратура закрыта и в местах доступа к ней установлены датчики, которые срабатывают при вскрытии аппаратуры.

Подобные меры позволяют избежать, например, подключения посторонних устройств, изменения режимов работы компьютерной системы, загрузки посторонних программ и т. п.

Законодательные меры заключаются в исполнении существующих в стране законов, постановлений, инструкций, регулирующих юридическую ответственность должностных лиц – пользователей и обслуживающего персонала за утечку, потерю или модификацию доверенной им информации.

Вопросы

1. Дайте определение информационной деятельности человека.
2. Какие виды информационной деятельности вы знаете?
3. Какие виды профессиональной информационной деятельности вы можете назвать?
4. Что такое информационная безопасность?
5. Перечислите традиционные методы защиты информации.
6. На каких уровнях осуществляется ограничение доступа к информации?
7. В чем заключается шифрование информации?
8. Что обозначает контроль доступа к аппаратуре?
9. В чем заключаются законодательные меры?
10. Что такое политика безопасности?