АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ЧЕЧЕНСКИЙ ГУМАНИТАРНО-ТЕХНИЧЕСКИЙ ТЕХНИКУМ»

План открытого практического урока

ПРОВЕРЕНО
Зам.директора по учебной работе
_____ Р.Д.Вахарбиева
«08» ____04____ 2022г.

Специальность:09.01.03.Делопроизводитель;
Наименование дисциплины: Технологии создания и обработки цифровой мультимедийной информации
Группа МОЦИ 20/9(1)
Дата 08.04.2022.
Преподаватель: Белхароев А.Л
Приглашенные представители администрации -специалист – практик Исмаилов Х.А

План – конспект открытого учебного занятия

Тема занятия: Виды, методы и средства защиты информации в информационных системах и информационных технологиях управления.

Курс:3 **, специальность:**09.01.03**, группа:**МОЦИ 20 (9)

Дата проведения:

Цель учебного занятия: формирование представлений о видах, методах и средствах защиты информации в ИС и МОЦИ

Задачи:

– *образовательные:* сформировать представление у студентов о понятии «средства защиты информации», познакомить с видами и методами защиты информации;

– *развивающие:* развитие умений выделять главное, существенное, обобщать имеющиеся факты, формирование логического мышления, внимания, интереса к предмету; развитие взаимопомощи, речи, умения выслушивать друг друга;

– *воспитательные:* воспитание ответственного отношения к соблюдению этических и правовых норм информационной деятельности, воспитание культуры общения, работа над повышением грамотности устной речи.

Используемые образовательные технологии: технология активного обучения, технология проблемного обучения, ИКТ

Форма занятия: урок

Тип занятия: комбинированное.

Формируемые компетенции: ПК1.1 ОК1-9

Оборудование и наглядные пособия: компьютерный класс, мультимедийный проектор, видеофильм, презентация.

Структурные элементы урока:

1. Организационный момент (5 мин)
2. Актуализация и проверка знаний: фронтальный опрос (10 мин)
3. Изложение нового материала (40 мин)
4. Первичное закрепление знаний, выполнение практической работы (15 мин)
5. Рефлексия (вопросы студентам) (5 мин)
6. Домашнее задание (3 мин)
7. Итог занятия (2 мин) **Организационный момент**

Приветствие, проверка присутствующих, тема и цель занятия

1. **Проверка домашнего задания**

1.Какова роль информации в современном обществе?

2.Дайте определение информационной безопасности

3.Объясните термин «угроза безопасности информации»?

4.Какие виды информационных угроз вам известны?.

5.Какие примеры несанкционированного и непреднамеренного воздействия на информацию вы можете привести?

3. **Изложение нового материала**

Просмотр видеофильма «Новые угрозы. Новые методы защиты информации»

Обсуждение проблем безопасности, затронутых в видеоматериале. Формирование понятия «комплексная защита информации». Переход к изучению нового материала.

Политика безопасности

.

В условиях использования АИТ под безопасностью понимается состояние защищенности ИС от внутренних и внешних угроз

Показатель защищенности – характеристика средств системы, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню и глубине в зависимости от класса защищенности

Современные методы и средства защиты информации

Технологии защиты данных основываются на применении современных методов, которые предотвращают утечку информации и ее потерю. Сегодня используется шесть основных способов защиты: **Препятствия; Управление; Маскировка (шифрование); Регламентация; Принуждение; Побуждение;**

Все перечисленные методы нацелены на построение эффективной технологии защиты информации, при которой исключены потери по причине халатности и успешно отражаются разные виды угроз.

Препятствие - способ физической защиты информационных систем, благодаря которому злоумышленники не имеют возможность попасть на охраняемую территорию.

Управление — способы защиты информации, при которых осуществляется управление над всеми компонентами информационной системы.

Маскировка — способы защиты информации, предусматривающие преобразование данных в форму, не пригодную для восприятия посторонними лицами. Для расшифровки требуется знание принципа.

Регламентация — важнейший метод защиты информационных систем, предполагающий введение особых инструкций, согласно которым должны осуществляться все манипуляции с охраняемыми данными.

Принуждение — методы защиты информации, тесно связанные с регламентацией, предполагающие введение комплекса мер, при которых работники вынуждены выполнять установленные правила.

Если используются способы воздействия на работников, при которых они выполняют инструкции по этическим и личностным соображениям, то речь идет о **побуждении**.

Физические средства защиты информации

Физические средства Физические средства защиты информации предотвращают доступ посторонних лиц на охраняемую территорию. Основным и наиболее старым средством физического препятствия является установка прочных дверей, надежных замков, решеток на окна. Для усиления защиты информации используются пропускные пункты, на которых контроль доступа осуществляют люди (охранники) или специальные системы. С целью предотвращения потерь информации также целесообразна установка противопожарной системы. Физические средства используются для охраны данных как на бумажных, так и на электронных носителях.

Примеры физических средств: замки на дверях, решетки на окнах, средства электронной охранной сигнализации и т.п.

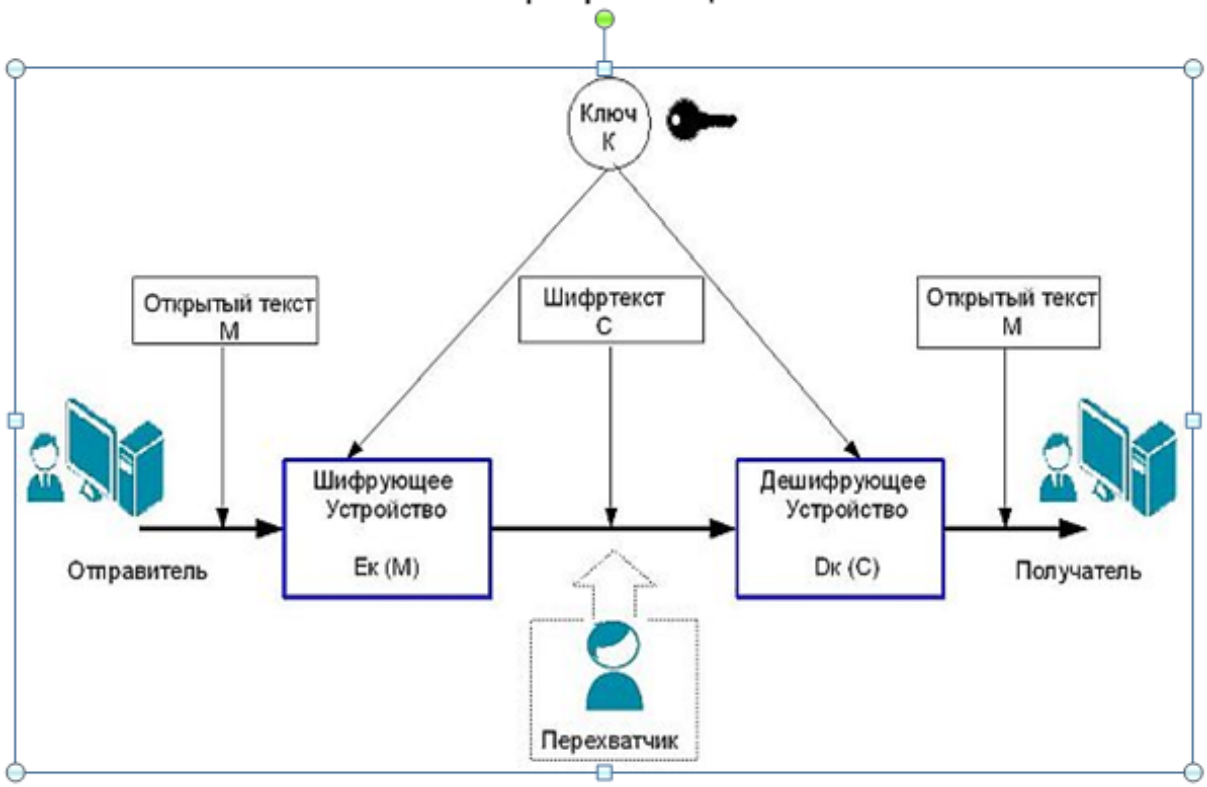
Аппаратные средства защиты информации

Аппаратные средства — устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу. Такие средства принадлежат к наиболее защищенной части системы. С их помощью могут быть реализованы любые концепции защиты, но стоимость реализации оказывается на порядок выше по сравнению с аналогичными по назначению программными средствами. При наличии выбора предпочтение следует отдавать аппаратным средствам защиты, так как они исключают любое вмешательство в их работу непосредственно из сети. Преимуществом аппаратных средств является их большая производительность по сравнению с программными средствами защиты (особенно в случае их использования в устройствах криптографической защиты).

Программные средства защиты информации

Криптографические методы защиты

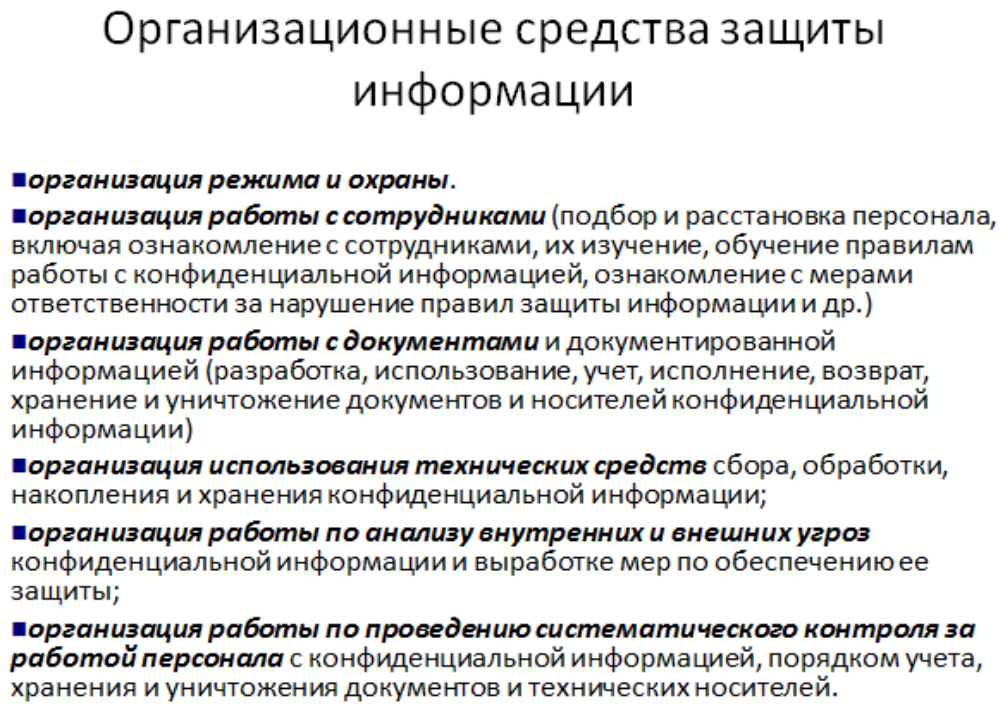
Криптографические средства защиты информации



Криптографические средства – это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

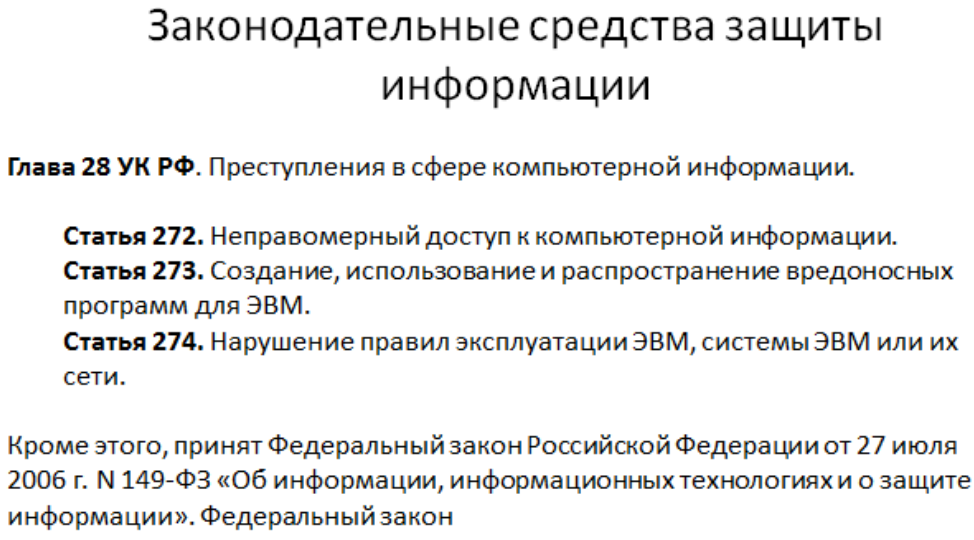
Потребности современной практической информатики привели к возникновению нетрадиционных задач защиты электронной информации, одной из которых является аутентификация электронной информации в условиях, когда обменивающиеся информацией стороны не доверяют друг другу. Эта проблема связана с созданием систем электронной цифровой подписи.

Организационные средства защиты информации



Организационные средства сопряжены с несколькими методами защиты: регламентацией, управлением, принуждением. К организационным средствам относится разработка должностных инструкций, беседы с работниками, комплекс мер наказания и поощрения. При эффективном использовании организационных средств работники предприятия хорошо осведомлены о технологии работы с охраняемыми сведениями, четко выполняют свои обязанности и несут ответственность за предоставление недостоверной информации, утечку или потерю данных.

Законодательные средства информации



Законодательные средства — комплекс нормативно-правовых актов, регулирующих деятельность людей, имеющих доступ к охраняемым сведениям и определяющих меру ответственности за утрату или кражу секретной информации.

Законодательная база в сфере информационной безопасности включает пакет Федеральных законов, Указов Президента РФ, постановлений Правительства РФ, межведомственных руководящих документов и стандартов.

Основополагающими документами по информационной безопасности в РФ являются Конституция РФ и Концепция национальной безопасности.

Закон РФ «Об информации, информатизации и защите информации» от 20 февраля 1995 года № 24-ФЗ — является одним из основных базовых законов в области защиты информации, который регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации на основе сбора, накопления, хранения, распространения и предоставления потребителям документированной информации, а также при создании и использовании информационных технологий, при защите информации и прав субъектов, участвующих в информационных процессах и информатизации.

Психологические средства — комплекс мер для создания личной заинтересованности работников в сохранности и подлинности информации. Для создания личной заинтересованности персонала руководители используют разные виды поощрений. К психологическим средствам относится и построение корпоративной культуры, при которой каждый работник чувствует себя важной частью системы и заинтересован в успехе предприятия.

4 **Первичное закрепление знаний, выполнение практической работы «Защита текстового документа»**

Цель работы – познакомиться с функциональными возможностями MS Word по защите информации**;** создать схему в текстовом документе MS Word схему «Фишбоун» по приведенному алгоритму (см. Приложение).

Ход работы:

1. Запустить MS Word.
2. Средствами MS Word (вкладка *Вставка, Фигуры*) построить «Фишбоун».
3. Открыть вкладку Рецензирование в разделе **Защита** щелкните **Разрешения (см. Таблицу 1)** и выберите **Ограниченный доступ**.
4. В полях **Чтение**, **Изменение** или **Полный доступ** введите адрес электронной почты или имя пользователя или группы, которой нужно назначить уровень доступа.
5. Если вы хотите найти адрес или имя в адресной книге, нажмите кнопку  .
6. Если вы хотите назначить уровень доступа всем контактам в вашей адресной книге, нажмите кнопку **Добавить всех**  .
7. После назначения уровней разрешений нажмите кнопку **ОК**.
8. Появится панель с сообщением о том, что это документ с управлением правами.
9. Установите пароль для вашего документа.

Таблица 1

Уровень разрешений	**Разрешает**
Чтение	Чтение
Изменение	Чтение, редактирование, копирование, сохранение изменений
Полный доступ	Чтение, редактирование, копирование, сохранение изменений, печать, установка срока действия контента, предоставление разрешений пользователям, доступ к контенту с помощью программных средств

5. **Домашнее задание** Разработать политику безопасности для защиты информации на домашнем ПК

6. Рефлексия (вопросы студентам)

Важна ли защита информации в современном мире? Можем ли мы обеспечить полную защиту информации? А может ли мы сделать все максимально возможное для защиты информации?

7. Итог занятия