1 курс

ПЛАН – КОНСПЕКТ
проведения лекционного занятия по дисциплине
«Информатика»

Раздел 1. «Информация и информационная деятельность человека.»

Тема № 1.9: «Информационная безопасность и тренды в развитии цифровых технологий; риски и прогнозы использования цифровых технологий при решении профессиональных задач.»

часть 1

Рязань 2023

Лекционное занятие (часть 1)
по Теме № 1.9. «Информационная безопасность и тренды в развитии цифровых технологий; риски и прогнозы использования цифровых технологий при решении профессиональных задач.»

Цель занятия: изучить со студентами основные сведения об информационной безопасности, защите информации, тренды в развитии цифровых технологий; риски и прогнозы использования цифровых технологий при решении профессиональных задач.

Вид занятия: классно-групповое, комбинированное (по проверке знаний, умений по пройденному материалу, по изучению и первичному закреплению нового материала).

Метод проведения занятия: доведение теоретических сведений.
Время проведения: 2 ч (90 мин.)

Основные вопросы:

1. Информационная безопасность. Защита информации от несанкционированного доступа.
2. Требования к выбору пароля.
3. Электронная подпись.
4. Основные положения Доктрины информационной безопасности Российской Федерации.
5. Компьютерные вирусы: методы распространения, профилактика заражения.
6. Защита информации от компьютерных вирусов.
7. Тренды в развитии цифровых технологий.
8. Риски и прогнозы развития цифровых технологий при решении профессиональных задач.
9. Применение облачных технологий на Российских железных дорогах.
10. Применение цифровых технологий при эксплуатации путевого хозяйства Российских железных дорог.

Литература:

1. [2 учебник раздела «Основной учебной литературы» рабочей программы изучения дисциплины]: Гаврилов, М. В. Информатика. Базовый уровень. 10—11 классы : учебник для среднего общего образования / М. В. Гаврилов, В. А. Климов. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 352 с. — (Общеобразовательный цикл). — ISBN 978-5-534-16226-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530644, главы 11-12.

Примерный расчет времени:

1. Вступительная часть – 20 мин.

2. Основная часть – 60 мин.
3. Заключительная часть – 10 мин.

Вступительная часть:

Занятие начать с объявления темы занятия, основных рассматриваемых вопросов, времени изучения темы (нового материала), закрепления на практике полученных знаний, перечисления литературы.

Основная часть (теоретическая):

Первый вопрос: Информационная безопасность. Защита информации от несанкционированного доступа.

Информационная безопасность.

Если компания хранит бухгалтерскую информацию, клиентскую базу, анкеты сотрудников или корпоративные тайны, то важно, чтобы эти данные не попали не в те руки, то есть были защищены. Защитой данных занимается информационная безопасность.

Информационная безопасность — это различные меры по защите информации от посторонних лиц. В доцифровую эпоху для защиты информации люди запирали важные документы в сейфы, нанимали охранников и шифровали свои сообщения на бумаге.

Сейчас чаще защищают не бумажную, а цифровую информацию, но меры, по сути, остались теми же: специалисты по информационной безопасности создают защищенные пространства (виртуальные «сейфы»), устанавливают защитное ПО вроде антивирусов («нанимают охранников») и используют криптографические методы для шифрования цифровой информации.

Однако цифровую информацию тоже нужно защищать не только виртуально, но и физически. Антивирус не поможет, если посторонний похитит сам сервер с важными данными. Поэтому их ставят в охраняемые помещения.

За что отвечает информационная безопасность?

Она отвечает за три вещи: конфиденциальность, целостность и доступность информации. В концепции информационной безопасности их называют принципами информационной безопасности.

Конфиденциальность означает, что доступ к информации есть только у того, кто имеет на это право. Например, ваш пароль от электронной почты знаете только вы, и только вы можете читать свои письма. Если кто-то узнает пароль

или другим способом получит доступ в почтовый ящик, конфиденциальность будет нарушена.

Целостность означает, что информация сохраняется в полном объеме и не изменяется без ведома владельца. Например, на вашей электронной почте хранятся письма. Если злоумышленник удалит некоторые или изменит текст отдельных писем, то это нарушит целостность.

Доступность означает, что тот, кто имеет право на доступ к информации, может ее получить. Например, вы в любой момент можете войти в свою электронную почту. Если хакеры атакуют серверы, почта будет недоступна, это нарушит доступность.

Какая бывает информация и как ее защищают.

Информация бывает общедоступная и конфиденциальная. К общедоступной имеет доступ любой человек, к конфиденциальной — только отдельные лица.

Может показаться, что защищать общедоступную информацию не надо. Но на общедоступную информацию не распространяется только принцип конфиденциальности — она должна оставаться целостностной и доступной. Поэтому информационная безопасность занимается и общедоступной информацией.

Например, возьмем интернет-магазин. Карточки товаров, статьи в блоге, контакты продавца — все это общедоступная информация, ее может просматривать любой. Но интернет-магазин все равно нужно защищать, чтобы никто не нарушил его работу, например, не изменил важную информацию в карточках товаров или не «уронил» его сайт.

Главная задача информационной безопасности в IT и не только — защита конфиденциальной информации. Если доступ к ней получит посторонний, это приведет к неприятным последствиям: краже денег, потере прибыли компании, нарушению конституционных прав человека и другим неприятностям.

Информация бывает общедоступная и конфиденциальная. К общедоступной имеет доступ любой человек, к конфиденциальной — только отдельные лица.

Основные виды конфиденциальной информации.

Персональные данные**.** Информация о конкретном человеке: ФИО, паспортные данные, номер телефона, физиологические особенности, семейное положение и другие данные. В России действует 152-ФЗ — закон, который обязывает охранять эту информацию. Мы подробно рассказывали об этом в статье «Как выполнить 152-ФЗ о защите персональных данных и что с вами будет, если его не соблюдать».

Тот, кто работает с персональными данными, обязан защищать их и не передавать третьим лицам. Информация о клиентах и сотрудниках относится как раз к персональным данным.

Коммерческая тайна. Внутренняя информация о работе компании: технологиях, методах управления, клиентской базе. Если эти данные станут известны посторонним, компания может потерять прибыль.

Компания сама решает, что считать коммерческой тайной, а что выставлять на всеобщее обозрение. При этом не вся информация может быть коммерческой тайной — например, нельзя скрывать имена учредителей юрлица, условия труда или факты нарушения законов. Подробнее о коммерческой тайне рассказывает закон 98-ФЗ.

Профессиональная тайна. Сюда относятся врачебная, нотариальная, адвокатская и другие виды тайны, относящиеся к профессиональной деятельности. С ней связано сразу несколько законов.

Служебная тайна. Информация, которая известна отдельным службам, например, налоговой или ЗАГСу. Эти данные обычно хранят государственные органы, они отвечают за их защиту и предоставляют только по запросу.

Государственная тайна. Сюда относят военные сведения, данные разведки, информацию о состоянии экономики, науки и техники государства, его внешней политики. Эти данные самые конфиденциальные — к безопасности информационных систем, в которых хранится такая информация, предъявляют самые строгие требования.

Если ваша компания хранит персональные данные, коммерческую или профессиональную тайну, то эти данные нужно защищать особым образом. Для этого необходимо ограничить доступ к ней посторонним лицам — установить уровни доступа и пароли, поставить защитное ПО, настроить шифрование.

Кратко об информационной безопасности и защите информации.

1. Информационная безопасность отвечает за защиту данных и обеспечивает их конфиденциальность, целостность и доступность.

2. Конфиденциальность означает, что доступ к данным есть только у тех, кто имеет на это право.

3. Целостность означает, что данные хранятся в неизменном виде и остаются достоверными.

4. Доступность означает, что человек, у которого есть право на доступ к информации, может ее получить.

5. Информационная безопасность защищает и конфиденциальные, и общедоступные данные. Общедоступным она обеспечивает целостность и доступность, конфиденциальным — еще и нужный уровень секретности.

6. К конфиденциальной информации относятся персональные данные, коммерческая, профессиональная, служебная и государственная тайны.

Основные определения по информационной безопасности.

Объекты защиты.

Основными объектами защиты при обеспечении информационной безопасности являются:

– все виды информационных ресурсов. Информационные ресурсы (документированная информация);

–информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать;

–права граждан, юридических лиц и государства на получение, распространение и использование информации;

–система формирования, распространения и использования информации (информационные системы и технологии, библиотеки, архивы, персонал, –нормативные документы и т.д.);

–система формирования общественного сознания (СМИ, социальные институты и т.д.).

ФЗ "Об информации, информационных технологиях и о защите информации".

В Российском законодательстве базовым законом в области защиты информации является ФЗ "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года номер 149-ФЗ. Поэтому основные понятия и решения, закрепленные в законе, требуют пристального рассмотрения.

Закон регулирует отношения, возникающие при:

• осуществлении права на поиск, получение, передачу, производство и распространение информации;

• применении информационных технологий;

• обеспечении защиты информации. Закон дает основные определения в области защиты информации.

Приведем некоторые из них:

• информация – сведения (сообщения, данные) независимо от формы их представления;

• информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

• информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

• обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

• оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

• конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

В вышеназванном ФЗ дается следующее определение защите информации - представляет собой принятие правовых, организационных и технических мер, направленных на:
1. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2. соблюдение конфиденциальности информации ограниченного доступа; 3. реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:
1. предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
2. своевременное обнаружение фактов несанкционированного доступа к информации;
3. предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
4. недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
5. возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
6. постоянный контроль за обеспечением уровня защищенности информации.

Защита информации от несанкционированного доступа.

Основные положения концепции защиты средств вычислительной техники от несанкционированного доступа к информации.

Защита информации от несанкционированного доступа в государственных и коммерческих структурах организована на основе системы законодательных и нормативно-правовых документов. Комплекс руководящих документов, регламентирующих вопросы защиты информации от НСД разработан Гостехкомиссией РФ, которая является основной организацией курирующей это направление защиты информации.

Комплекс руководящих документов по защите от НСД включает:

1) Концепцию защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (утверждена решением

Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.)

2) Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники

3) Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации

4) Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации

5) Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации

6) Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.

Защита от несанкционированного доступа. Термины и определения.

Известны такие направления исследования проблемы безопасности информации, как радиотехническое, побочные электромагнитные излучения и наводки, акустическое, НСД и другие.

Несанкционированный доступ (НСД) определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС.

Под **штатными средствами** понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

Определение НСД в руководящих документах Гостехкомиссии РФ отличается по содержанию от определения НСД по ГОСТ Р 50922-96 «Защита информации. Основные термины и определения», в котором акцент на использование штатных средств при осуществлении НСД не делается.

Защита СВТ и АС основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от НСД к информации.

Защита СВТ обеспечивается комплексом программно-технических средств. Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

В качестве **нарушителя** рассматривается субъект, имеющий доступ к работе со штатными средствами АС и СВТ как части АС. Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяется четыре уровня этих возможностей. Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС - запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

В своем уровне нарушитель является специалистом высшей квалификации, знает все об АС и, в частности, о системе и средствах ее защиты.

К основным способам НСД относятся:

1) непосредственное обращение к объектам доступа. Появление этого способа НСД возможно при выборе неправильной политики информационной безопасности, когда остаются возможности непосредственного обращения

субъектов к объектам доступа без посредничества механизмов защиты. Например, если в таблице разграничения доступа не ограничены права пользователя по доступу к файлам и каталогам;

2) создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты. Этот способ НСД появляется, если используемые программные и технические средства не проверены на отсутствие недекларированных возможностей или в АС имеются инструментальные средства для создания программ. В этом случае имеющиеся или специально созданные пользователем средства могут иметь возможность обращаться к объектам защиты в обход механизмов защиты, используя низкоуровневые команды;

3) модификация средств защиты, позволяющая осуществить НСД. Модификация средств защиты возможна при наличии в них конструктивных дефектов, например, «люков» в программных средствах, не удаленных после отладки программы;

4) внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.

Внедрение программных или программно-аппаратных закладок, как правило, производится на этапе разработки и создания средств СВТ. Чаще всего, в программные средства включаются программные закладки типа «троянского коня», которые способны на несанкционированные действия, например, перехват пароля пользователя и передачу его по сети создателю закладки.

Обеспечение защиты СВТ и АС осуществляется:

1) системой разграничения доступа (СРД) субъектов к объектам доступа;

2) обеспечивающими средствами для СРД.

Методы защиты от несанкционированного доступа.

Методы защиты компьютеров от несанкционированного доступа делятся на программно-аппаратные и технические. Первые отсекают неавторизованных пользователей, вторые предназначены для исключения физического проникновения посторонних людей в помещения компании.

Создавая систему защиты информации (СЗИ) в организации, следует учитывать, насколько велика ценность внутренних данных в глазах злоумышленников.

Для грамотной защиты от несанкционированного доступа важно сделать следующее:

- отсортировать и разбить информацию на классы, определить уровни допуска к данным для пользователей;

- оценить возможности передачи информации между пользователями (установить связь сотрудников друг с другом).

В результате этих мероприятий появляется определенная иерархия информации в компании. Это дает возможность разграничения доступа к сведениям для сотрудников в зависимости от рода их деятельности.

Аудит доступа к данным должен входить в функционал средств информационной безопасности. Помимо этого, программы, которые компания решила использовать, должны включать следующие опции:

- аутентификация и идентификация при входе в систему;
- контроль допуска к информации для пользователей разных уровней;
- обнаружение и регистрация попыток НСД;
- контроль работоспособности используемых систем защиты информации;
- обеспечение безопасности во время профилактических или ремонтных работ.

Идентификация и аутентификация пользователей.

Для выполнения этих процедур необходимы технические средства, с помощью которых производится двухступенчатое определение личности и подлинности полномочий пользователя. Необходимо учитывать, что в ходе идентификации необязательно устанавливается личность. Возможно принятие любого другого идентификатора, установленного службой безопасности.

После этого следует аутентификация – пользователь вводит пароль или подтверждает доступ к системе с помощью биометрических показателей (сетчатка глаза, отпечаток пальца, форма кисти и т. п.). Кроме этого, используют аутентификацию с помощью USB-токенов или смарт-карт. Этот вариант слабее, так как нет полной гарантии сохранности или подлинности таких элементов.

Защита данных на ПК.

Для защиты информации, хранящейся на жестких дисках компьютеров, используются многоступенчатые средства шифрования и авторизации. При загрузке операционной системы используется сложный пароль, который невозможно подобрать обычными методами. Возможность входа в систему пользователя со стороны исключается путем шифрования данных в BIOS и использования паролей для входа в разделы диска.

Для особо важных устройств следует использовать модуль доверенной загрузки. Это аппаратный контроллер, который устанавливается на материнскую плату компьютера. Он работает только с доверенными пользователями и блокирует устройство при попытках включения в отсутствие владельца.

Также применяются криптографические методы шифрования данных, превращающие текст «вне системы» в ничего не значащий набор символов.

Эти мероприятия обеспечивают защиту сведений и позволяют сохранить их в неприкосновенности.

Определение уровней защиты.

С методической точки зрения процесс защиты информации можно разделить на четыре этапа:

- предотвращение – профилактические меры, ограничение доступа посторонних лиц;
- обнаружение – комплекс действий, предпринимаемых для выявления злоупотреблений;
- ограничение – механизм снижения потерь, если предыдущие меры злоумышленникам удалось обойти;
- восстановление – реконструкция информационных массивов, которая производится по одобренной и проверенной методике.

Каждый этап требует использования собственных средств защиты информации, проведения специальных мероприятий. Необходимо учитывать, что приведенное разделение условно. Одни и те же действия могут быть отнесены к разным уровням.

Стандартность архитектурных принципов построения, оборудования и программного обеспечения персональных компьютеров, мобильность программного обеспечения определяют сравнительно легкий доступ к информации, находящейся в персональном компьютере.

Несанкционированный доступ к информации персонального компьютера - незапланированное ознакомление, обработка, копирование, применение различных вирусов, модификация или уничтожение информации в нарушение правил доступа.

Под защитой информации понимают создание организованной совокупности средств, методов и мероприятий, предназначенных для предупреждения искажения, уничтожения или несанкционированного использования защищаемой информации. К ним относятся аппаратные и программные средства, криптографическое закрытие информации, физические меры, организационные мероприятия и законодательные меры. Один из методов защиты - парольная идентификация, ограничивающая доступ несанкционированного пользователя.

Включение защиты в программу связано с разработкой программ с запросом информации, т.е. требующих для своей работы ввода дополнительной информации, такой как пароли или номера ключей. Однако такая проверка доступа к программам или системам не должна существенно сказываться на быстродействии программы или требовать от пользователя сложных дополнительных действий.

Второй вопрос: Требования к выбору пароля.

Каждый пользователь компьютера или мобильных устройств сталкивался с необходимостью создания пароля для защиты своих учетных данных (учетная запись устройства, аккаунты электронной почты, интернет банкинга или социальной сети). Однако немногие относятся к созданию надежных паролей с должной аккуратностью.

Прежде всего надежный пароль — это пароль, обладающий следующими качествами:

Сложность. К созданию пароля необходимо подойти ответственно вне зависимости от вида и важности ресурса, где он будет использоваться. При создании сложного пароля стоит придерживаться следующих правил:

- Длина пароля. Пароль должен содержать не менее 8 символов, а лучше – 10 и более.
- Наличие цифр и букв верхнего и нижнего регистров, идущих не подряд – AAaaBBbb.
- Наличие специальных знаков – «@», «$», «&» и т.д. (если допустимо их присутствие).

Несмотря на то что многие ресурсы при регистрации принудительно заставляют, придумать сложный пароль (требуя определенную длину пароля, наличие цифр и букв, а также специальных символов), пользователи зачастую просто стараются выполнить эти требования, не задумываясь о надежности такого пароля. В результате получается что-то похожее на – p@ssword1234.

Использование паролей типа «qwerty1234», «abcd12345», «p@ssword1234» не гарантирует надежную защиту данных, поскольку программы подбора паролей, которыми пользуются злоумышленники, в первую очередь проверяют именно такие пароли.

Надежный пароль не должен содержать имена, клички животных или названия городов, а также цифры даты рождения или номера телефонов. Пароль типа «M@sha1990» будет угадан программами по подбору паролей, т.к. содержит достаточно распространенную комбинацию букв.

Уникальность. Для каждого ресурса необходимо иметь свой пароль. Это обусловлено необходимостью защиты всех остальных пользовательских ресурсов при компрометации пароля одного ресурса.

Пароль должен быть известен только пользователю, иначе никакой надежной защиты уже быть не может. Нежелательно записывать пароли на бумаге и тем более держать эти записи рядом с компьютером в открытом доступе для всех. Кроме того, не рекомендуется вводить свои пароли на сайтах

по проверке надежности паролей, так как они могут оказаться ловушками для паролей.

Как выбирать (создавать) надежные пароли:

1. Генерация пароля с помощью специализированных программ.

Тем пользователям, кому сложно придумать надежный пароль самостоятельно, можно порекомендовать воспользоваться сервисами по генерации надежных паролей. При необходимости программа сгенерирует пароль необходимой длины, с наличием специальных символов и букв разных регистров, например – $y@85u!K1n3x.

Важным требованием является то, чтобы это была именно программа, установленная на устройстве, а не онлайн сервис. В противном случае, сгенерируемый пароль может быть известен не только пользователю, но и попасть в базы злоумышленников. К оффлайн сервисам можно отнести: ViPNet Password Generator, Random password generator, Drowssap.

2. Самостоятельное создание пароля с помощью своей методики.

Требования к надежному паролю:

1. Пароль должен быть секретным
2. Пароль должен быть длинным
3. Пароль должен быть трудно угадываемым
4. Пароль не должен представлять собой распространенные слова, имена, названия
5. Пароль должен быть сложным
6. Пароль должен регулярно меняться

Парольная идентификация.

Пароль - это код, используемый для получения доступа к системам или файлам, оснащенным парольной защитой.

Пароли обеспечивают сохранение целостности программного обеспечения в составе вычислительной системы, но для поддержания паролей требуется высокая дисциплинированность. При первой регистрации пользователя администратор определяет круг полномочий для получения и изменения информации или выполнения определенных управляющих действий в системе, руководствуясь его профессиональными обязанностями и должностными инструкциями. Затем пользователю прелагается ввести свой пароль согласно правилам, принятым в данной системе. Метод паролей требует, чтобы вводимый пользователем пароль (строка символов) сравнивался с тем, который хранится в вычислительной системе для данного пользователя. Если пароль верен, система должна вывести на экран терминала дату и время последнего входа в систему этого пользователя. Затем пользователю предоставляется возможность пользоваться всей информацией, доступ к которой ему разрешен (пароли можно также использовать независимо от пользователя для защиты файлов, записей, полей данных внутри записей и т.д.).

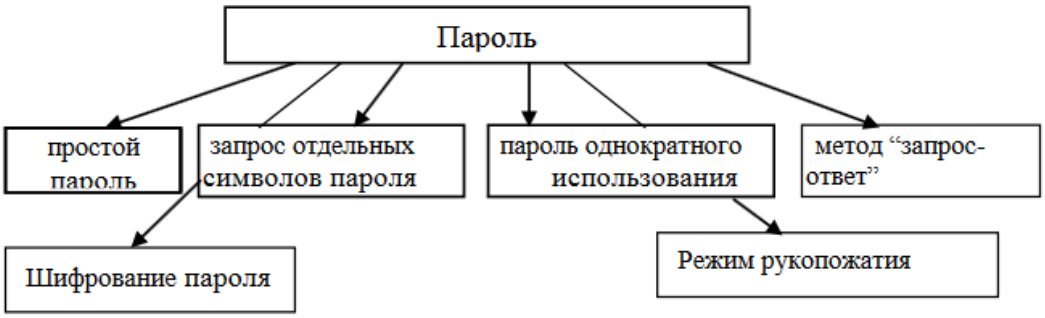

Рисунок 7.2 - Виды паролей

Простой пароль

Простой пароль - вводимая пользователем с клавиатуры строка символов. В схеме с простым паролем пользователю разрешается самому выбирать пароль таким образом, чтобы его было легко запомнить. Иногда в ряду символов пароля и в конце его оставляют пробелы. Отличие действительного пароля от кажущегося (без пробелов) повышает защищенность системы.

Подбор пароля путем простого перебора комбинаций предполагает перебор всех возможных сочетаний символов в пароле. Время, необходимое для разгадывания пароля методом простого перебора, является геометрической прогрессией от длины пароля, но есть различные кривые, зависящие от размера алфавита, на основе которого был создан пароль и от размера набора символов, по отношению к которым рассматриваются различные пароли.

Пароли однократного использования могут применяться также для установления подлинности подтверждения об отключении ЭВМ от обслуживания пользователя и подтверждения подлинности требования пользователя об отключении от ЭВМ. Всякий раз, когда получено требование пользователя об окончании работы, ЭВМ немедленно передает ему свой пароль однократного использования и прерывает связь. Если пользователь отключается и не получает истинного пароля от ЭВМ, ему следует принять меры предосторожности.

Третий вопрос: Электронная подпись.

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию[5].

ЭП представляет собой комбинацию символов, которая формируется в результате математического преобразования исходного документа при помощи специального программного обеспечения. ЭП добавляется к исходному документу при пересылке, и любое изменение исходного документа делает эту ЭП недействительной. Таким образом, ЭП безошибочно указывает на подлинность и авторство, не переносится с одного документа на другой документ, защищает подписанный документ от подделки, а также от изменения или искажения информации.

ЭП основана на асимметричном криптографическом алгоритме
Особенностью такого алгоритма является то, что используются два разны
ключа: один ключ для зашифрования информации, а второй, который спе
циальным образом получен из первого и отличен от него, – для ее расшиф
рования.

Ключ электронной подписи – уникальная последовательность сим
волов, предназначенная для создания электронной подписи.

Первый ключ является секретным – закрытым (личным) ключом, о
известен только лицу, подписывающему документ. Второй ключ несекрет
ный – открытый ключ, он может быть известен любому получателю элек
тронного документа.

Открытый ключ публикуется на сайте удостоверяющего центра, услугами которого пользуется владелец ключа, а закрытый ключ он хранит со всеми возможными мерами предосторожности.

УЦ является системой управления ключами в рамках криптографической системы на основе инфраструктуры открытых ключей (закрытый ключ известен только его владельцу).

УЦ создает сертификат открытого ключа и таким образом удостоверяет этот ключ.

УЦ подтверждает или опровергает принадлежность открытого ключа лицу, которое владеет соответствующим закрытым ключом. Удостоверяющий центр – это организация, которая выпускает сертификаты ключей проверки ЭП и отвечает за управление криптографическими ключами пользователей. Открытые ключи и другая информация о пользователях хранится удостоверяющими центрами в виде цифровых сертификатов.

Сертификат – это электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи[6].

Выдавая сертификат, УЦ удостоверяет подлинность связи между открытым ключом пользователя УЦ и информацией, его идентифицирующей. И ключ, и сертификат хранятся в файлах. Для того, чтобы никто, кроме владельца подписи, не мог воспользоваться закрытым ключом, его обычно записывают на съемный носитель ключа (например, «Рутокен»). Для дополнительной защиты его снабжают PIN-кодом. Для создания электронной подписи необходимо ввести правильное значение PIN-кода. Сертификат содержит всю необходимую информацию для проверки электронной подписи. Данные сертификата открыты и публичны. Поэтому обычно

сертификаты хранятся в хранилище сертификатов операционной системы. И, конечно, все сертификаты всегда хранятся в УЦ[7].

Схема цифровой подписи - набор алгоритмов и протоколов, позволяющих построить информационное взаимодействие между двумя и более участниками таким образом, чтобы факт авторства переданного массива данных, «подписанного одним из участников», мог быть надежно подтвержден или опровергнут третьей стороной.

Любая схема цифровой подписи предполагает добавление к подписываемому массиву данных дополнительного кода - цифровой подписи, выработать которую может только автор сообщения, обладающий секретным ключом подписи, а все остальные могут лишь проверить соответствие этой подписи подписанным данным.

Процедура ЭЦП на базе асимметричного криптографического алгоритма включает в себя процедуры выработки и проверки подписи под данным

сообщением. Цифровая подпись, состоящая из двух целых чисел, вычисляется с помощью определенного набора правил.

ЭЦП обеспечивает:

Защиту от изменений документа. При любом случайном или преднамеренном изменении документа (или подписи) подпись станет недействительной, потому что вычислена она на основании исходного состояния документа и соответствует лишь ему.

Невозможность отказа от авторства. Так как создать корректную подпись можно лишь, зная закрытый ключ, а он известен только владельцу, то владелец не может отказаться от своей подписи под документом.

Четвёртый вопрос: Основные положения Доктрины информационной безопасности Российской Федерации.

Основные положения Доктрины информационной безопасности Российской Федерации представлены в приложении № 1 к данному план-конспекту.

Пятый вопрос: Компьютерные вирусы: методы распространения, профилактика заражения.

Шестой вопрос: Защита информации от компьютерных вирусов.

Сведения о видах компьютерных вирусов, антивирусных средствах защиты, антивирусных программах, представлены в приложении № 2 к данному план-конспекту.