Обучающий курс по информационной безопасности для персонала компаний, организаций и учреждений

Об этом курсе

1. Введение
   1. Актуальность проблемы Информационной безопасности
   2. Основные понятия
   3. Основные принципы ИБ
   4. Тест
2. Блок Угроз
   1. По аспекту информационной безопасности, на который направлены угрозы:
      1. Угрозы конфиденциальности
      2. Угрозы [целостности](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8)
      3. Угрозы доступности
   2. По природе возникновения:
      1. Естественные
      2. Искусственные
         1. Непреднамеренные (случайные) угрозы
         2. Преднамеренные (умышленные) угрозы
   3. Тест
3. Наиболее распространение угрозы, которым может быть подвергнут персонал
   * 1. Фишинг и Социальная инженерия
     2. Вредоносное По
     3. Вербовка
     4. Слабая парольная система
     5. Тест
4. Важные правила цифровой гигиены
5. Итог
   1. Итоговый Тест

Оглавление

[Об этом курсе 2](#_Toc40952908)

[Глава 1: Введение 3](#_Toc40952909)

[Актуальность проблемы информационной безопасности 5](#_Toc40952910)

[Основные понятия 7](#_Toc40952911)

[Основные принципы ИБ 11](#_Toc40952912)

[Тест по итогам 1 главы 14](#_Toc40952913)

[Глава 2: Угрозы 16](#_Toc40952914)

[По аспекту информационной безопасности, на который направлены угрозы 16](#_Toc40952915)

[По природе возникновения 20](#_Toc40952916)

[Тест по 2 главе 23](#_Toc40952917)

[Глава 3: Наиболее распространение угрозы, которым может быть подвергнут персонал 26](#_Toc40952918)

[Фишинг и Социальная инженерия 26](#_Toc40952919)

[Вредоносное ПО 29](#_Toc40952920)

[Слабая парольная система 32](#_Toc40952921)

[Тест по 3 главе 36](#_Toc40952922)

[Глава 4: Важные правила цифровой гигиены 38](#_Toc40952923)

[Цифровая гигиена 38](#_Toc40952924)

[Глава 5: Подведение итогов курса 41](#_Toc40952925)

[Тест по итогам всего курса 41](#_Toc40952926)

# Об этом курсе

Целью курса является ознакомление слушателей с основными понятиями защиты информации, основными принципами построения систем защиты информации, базовым набором угроз, с которыми чаще всего сталкиваются рядовые пользователи, а также основными категориями мер защиты информации, их возможностями с точки зрения защиты информации, сильными и слабыми сторонами.

В процессе освоения курса слушатели получат базовые знания в сфере защиты информации, узнают о наиболее распространенных угрозах, которым может быть подвергнут персонал, а также о важнейших правилах цифровой гигиены. Курс направлен развитие критического мышления по отношению к информации, а также на понимание о важности информационной безопасности и данных, которые распростятся в компании.

Для освоения материала курса будут полезны знания из общего курса информационных технологий, а так основы работы с ПК. Их наличие позволит понять принципы различных угроз безопасности данных, а также терминологию, используемую в сфере информационной безопасности.

В качестве эксперта в курсе участвует Никитин Виктор Николаевич, доцент кафедры Информационные технологии и система, а так же директор ДВУНЦ (Дальневосточный Учебно-научный центр по информационной безопасности), который в настоящее время занимает одну из лидирующих позиций на территории Хабаровского края и Дальневосточного федерального округа в области услуг по обеспечению информационной безопасности объектов информатизации и автоматизированных систем, а также в области обучения, переподготовки и повышения квалификации специалистов по защите персональных данных, конфиденциальной информации и государственной тайны.

# Глава 1: Введение

Современный этап общемирового развития характеризуется возрастающей ролью информационной сферы. Превращаясь в системообразующий фактор жизни общества, она все более активно влияет на состояние политической, экономической, оборонной, личной, имущественной и других составляющих различных сфер общества. Бурное развитие средств вычислительной техники открыло перед человечеством небывалые возможности по автоматизации умственного труда и привело к созданию большого числа разного рода автоматизированных информационных и управляющих систем, к возникновению принципиально новых, так называемых, информационных технологий. В настоящее время информационные технологии существенно меняют не только структуру отношений, но и образ жизни людей, их мышление. Они становятся действенным фактором развития личности и общества. В то же время широкое распространение некоторых информационных технологий сопровождается появлением ряда новых угроз связанных с потерей данных. Неправомерное искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляющих системах наносят серьезный материальный и моральный урон многим субъектам (государству, юридическим и физическим лицам), участвующим в процессах автоматизированного информационного взаимодействия. Достижения науки и техники не только позволили упростить нашу жизнь, но и значительно расширили поле преступлений. Теперь правонарушитель, имея доступ к сети Интернет, способен нанести ущерб пользователям, корпорациям и целым государствам. Главным способом чувствовать себя защищенно в мире, полностью подвергшемся тотальной информатизации, обезопасить свои данные от утечки является информационная безопасность. В соответствии с доктриной информационной безопасности РФ под термином «информационная безопасность» понимается состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина.

## **Актуальность проблемы информационной безопасности**

Здравствуйте, в данном уроке мы рассмотрим актуальность проблемы информационной безопасности, ответим на вопросы почему нужна защита информации. Рассмотрим новый подход к обработке информации и как глобальная информатизация повлияла на работу компаний.

Острота проблемы обеспечения безопасности субъектов информационных отношений, защиты их законных интересов при использовании информационных и управляющих систем, хранящейся и обрабатываемой в них информации все более возрастает. Этому есть целый ряд объективных причин. Прежде всего — это расширение сферы применения средств вычислительной техники и возросший уровень доверия к автоматизированным системам управления и обработки информации. Компьютерным системам доверяют самую ответственную работу, от качества выполнения которой зависит жизнь и благосостояние многих людей. ЭВМ управляют технологическими процессами на предприятиях и атомных электростанциях, управляют движением самолетов и поездов, выполняют финансовые операции, обрабатывают секретную и конфиденциальную информацию.

Изменился подход и к самому понятию "информация". Этот термин все чаще используется для обозначения особого товара, стоимость которого зачастую превосходит стоимость вычислительной системы, в рамках которой он существует. Осуществляется переход к рыночным отношениям в области создания и предоставления информационных услуг, с присущей этим отношениям конкуренцией и промышленным шпионажем. Проблема защиты вычислительных систем становится еще более серьезной и в связи с развитием и распространением вычислительных сетей, территориально распределенных систем и систем с удаленным доступом к совместно используемым ресурсам. Доступность средств вычислительной техники и прежде всего персональных ЭВМ привела к распространению компьютерной грамотности в широких слоях населения, что закономерно, привело к увеличению числа попыток неправомерного вмешательства в работу государственных и коммерческих автоматизированных систем как со злым умыслом, так и чисто "из спортивного интереса". К сожалению, многие из этих попыток имеют успех и наносят значительный урон всем заинтересованным субъектам информационных отношений. Еще одним весомым аргументом в пользу усиления внимания к вопросам безопасности вычислительных систем является бурное развитие и широкое распространение так называемых компьютерных вирусов, способных скрытно существовать в системе и совершать потенциально любые несанкционированные действия. Особую опасность для компьютерных систем представляют злоумышленники, специалисты - профессионалы в области вычислительной техники и программирования, досконально знающие все достоинства и слабые места вычислительных систем и располагающие подробнейшей документацией и самыми совершенными инструментальными и технологическими средствами для анализа и взлома механизмов защиты.

Все вышеперечисленные причины дают, что информационная безопасность крайне важная сфера, а роль обычного пользователя велика. Действия сотрудника колоссально влияют на состояние защищенности системы от злоумышленника.

Актуальность проблемы защиты информационных технологий в современных условиях определяется следующими основными факторами:

* обострением противоречий между объективно существующими потребностями общества в расширении свободного обмена информацией и чрезмерными или наоборот недостаточными ограничениями на ее распространение и использование;
* расширением сферы использования ЭВМ, многообразием и повсеместным распространением информационно-управляющих систем, высокими темпами увеличения парка средств вычислительной техники и связи;
* повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических областях деятельности;
* вовлечением в процесс информационного взаимодействия все большего числа людей и организаций, резким возрастанием их информационных потребностей, наличием интенсивного обмена информацией между участниками этого процесса;
* концентрацией больших объемов информации различного назначения и принадлежности на электронных носителях;
* количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам;
* отношением к информации, как к товару, переходом к рыночным отношениям в области предоставления информационных услуг с присущей им конкуренцией и промышленным шпионажем;
* многообразием видов угроз и возникновением новых возможных каналов несанкционированного доступа к информации;
* ростом числа квалифицированных пользователей вычислительной техники и возможностей по созданию ими нежелательных программно-математических воздействий на системы обработки информации;
* увеличением потерь (ущерба) от уничтожения, фальсификации, разглашения или незаконного тиражирования информации (возрастанием уязвимости различных затрагиваемых субъектов);
* развитием рыночных отношений (в области разработки, поставки, обслуживания вычислительной техники, разработки программных средств, в том числе средств защиты).

## **Основные понятия информационной безопасности**

Здравствуйте, в данном уроке мы определим основные понятия, связанные с информационной безопасностью и информационными отношениями. Изучим, что такое субъекты и объекты информационных отношений и как они связаны с защитой информации.

**Информация и информационные отношения. Субъекты информационных отношений, их безопасность**

**Под *информацией***будем понимать сведения о фактах, событиях, процессах и явлениях, о состоянии объектов (их свойствах, характеристиках) в некоторой предметной области, необходимые для оптимизации принимаемых решений в процессе управления данными объектами.

Информация может существовать в различных формах в виде совокупностей некоторых знаков (символов, сигналов и т.п.) на носителях различных типов. В связи с бурным процессом информатизации общества все большие объемы информации накапливаются, хранятся и обрабатываются в автоматизированных системах, построенных на основе современных средств вычислительной техники и связи. В дальнейшем будут рассматриваться только те формы представления информации, которые используются при ее автоматизированной обработке.

**Под автоматизированной системой** (АС) обработки информации будем понимать организационно-техническую систему, представляющую собой совокупность следующих взаимосвязанных компонентов:

• технических средств обработки и передачи данных (средств вычислительной техники и связи);

• методов и алгоритмов обработки в виде соответствующего программного обеспечения;

• информации (массивов, наборов, баз данных) на различных носителях;

• обслуживающего персонала и пользователей системы, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки информации (данных) с целью удовлетворения информационных потребностей субъектов информационных отношений.

Под обработкой информации в АС будем понимать любую совокупность операций (прием, накопление, хранение, преобразование, отображение, передача и т.п.), осуществляемых над информацией (сведениями, данными) с использованием средств АС.

В дальнейшем *субъектами*будем называть:

• *государство*(в целом или отдельные его органы и организации);

• общественные или коммерческие организации (объединения) и предприятия *(юридических лиц);*

*•*отдельных граждан *(физических лиц).*

В процессе своей деятельности субъекты могут находиться друг с другом в разного рода отношениях, в том числе, касающихся вопросов получения, хранения, обработки, распространения и использования определенной информации. Такие отношения между субъектами будем называть *информационными отношениями,*а самих участвующих в них субъектов - *субъектами информационных отношений.*

Для обеспечения законных прав и удовлетворения интересов сотрудников необходимо постоянно поддерживать следующие свойства информации и систем ее обработки:

• доступность информации - такое свойство системы (инфраструктуры, средств и технологии обработки, в которой циркулирует информация), которое характеризует ее способность обеспечивать своевременный доступ персонала к интересующей их информации и соответствующим автоматизированным службам (готовность к обслуживанию поступающих от субъектов) запросов всегда, когда в обращении к ним возникает необходимость;

• целостность информации - такое свойство информации, которое заключается в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Точнее говоря, персонал интересует обеспечение более широкого свойства - достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, то есть ее не искаженности. Однако, мы ограничимся только рассмотрением вопросов обеспечения целостности информации, так как вопросы адекватности отображения выходят далеко за рамки проблемы информационной безопасности;

• конфиденциальность информации - такую субъективно определяемую (приписываемую) характеристику (свойство) информации, которая указывает на необходимость введения ограничений на круг сотрудников, имеющих доступ к данной информации, и обеспечиваемую способностью системы (инфраструктуры) сохранять указанную информацию в тайне от персонала, не имеющего прав на доступ к ней. Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты законных интересов других субъектов информационных отношений.

Следовательно, термин «безопасность информации» нужно понимать как защищенность информации от нежелательного для соответствующих субъектов информационных отношений ее разглашения (нарушения конфиденциальности), искажения или утраты (нарушения целостности, фальсификации) или снижения степени доступности информации, а также незаконного ее тиражирования (неправомерного использования).

Под «**безопасностью автоматизированной системы**» (системы обработки информации, компьютерной системы) следует понимать защищенность всех ее компонентов (технических средств, программного обеспечения, данных, пользователей и персонала) от разного рода нежелательных для соответствующих субъектов воздействий.

Безопасность любого компонента (ресурса) АС складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности.

* конфиденциальность компонента (ресурса) АС заключается в том, что он доступен только тем субъектам (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия;
* целостность компонента (ресурса) АС предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени;
* доступность компонента (ресурса) АС означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы.

Так что же в итоге такое информационная безопасность? Информационная безопасность – это свойство информации сохранять конфиденциальность, целостность и доступность.

**Основные принципы ИБ**

Здравствуйте, в этой лекции мы подробно рассмотрим основные принципы информационной безопасности, их детальное устройство, а также поближе познакомился с определением каждого из них.

Полноценная информационная безопасность базируется на нескольких основополагающих принципах:



*Рис 1. Основные принципы информационной безопасности*

А теперь рассмотрим вышеуказанные принципы защиты информации более подробно:

1. **Простота использования информационной системы**. Данный принцип информационной безопасности заключается в том, что для минимизации ошибок следует обеспечить простоту использования информационной системы. Во время эксплуатации информационной системы (далее ИС) пользователи и администраторы совершают непреднамеренные ошибки, некоторые из которых могут вести к невыполнению требований политик безопасности и снижению уровня информационной безопасности. Чем более сложны, запутанны и непонятны для пользователей и администраторов совершаемые ими операции, тем больше они делают ошибок. Простота использования ИС является необходимым условием для снижения числа ошибочных действий. При этом следует помнить, что данный принцип информационной безопасности не означает простоту архитектуры и снижение функциональности ИС.

2. **Контроль над всеми операциями**. Этот принцип подразумевает непрерывный контроль состояния информационной безопасности и всех событий, влияющих на защиту информации. Необходим контроль доступа к любому объекту ИС с возможностью блокирования нежелательных действий, а также быстрого восстановления нормальных и работоспособных параметров информационной системы, что непременно приводит к высокому уровню защиты системы.

3. **Запрещено всё, что не разрешено**. Этот принцип информационной безопасности заключается в том, что доступ к какому-либо объекту ИС должен предоставляться только при наличии соответствующего правила, отраженного, например, в регламенте бизнес-процесса или настройках защитного программного обеспечения. При этом основной функцией системы ИБ является разрешение, а не запрещение каких-либо действий. Данный принцип позволяет допускать только известные безопасные действия, а не заниматься распознаванием любой угрозы, что очень ресурсоёмко, невозможно в полной мере и не обеспечивает достаточный уровень ИБ.

4. **Открытая архитектура ИС**. Этот принцип информационной безопасности состоит в том, что безопасность не должна обеспечиваться через неясность. Попытки защитить информационную систему от компьютерных угроз путем усложнения, запутывания и скрытия слабых мест ИС, оказываются в конечном итоге несостоятельными и только отсрочивают успешную хакерскую, вирусную или инсайдерскую атаку.

5. **Разграничение доступа**. Данный принцип информационной безопасности заключается в том, что каждому пользователю предоставляется доступ к информации и её носителям в соответствии с его полномочиями. При этом исключена возможность превышения полномочий. Каждой роли/должности/группе пользователей можно назначить свои права на выполнение действий (чтение/изменение/удаление) над определёнными объектами ИС.

6. **Минимальные привилегии**. Принцип минимальных привилегий состоит в выделении пользователю наименьших прав и доступа к минимуму необходимых функциональных возможностей программ. Такие ограничения, тем не менее, не должны мешать выполнению работы.

7. **Достаточная стойкость**. Этот принцип информационной безопасности выражается в том, что потенциальные злоумышленники должны встречать препятствия в виде достаточно сложных вычислительных задач. Например, необходимо, чтобы взлом паролей доступа требовал от хакеров неадекватно больших промежутков времени и/или вычислительных мощностей.

8. **Минимум идентичных процедур**. Этот принцип информационной безопасности состоит в том, что в системе ИБ не должно быть общих для нескольких пользователей процедур, таких как ввод одного и того же пароля. В этом случае масштаб возможной хакерской атаки будет меньше.

## **Тест по итогам 1 главы**

\*-верный ответ

1. **Отметьте факторы, которыми определяется актуальность информационной безопасности в компании, организации и учреждении. (Не менее двух)**
2. обострением противоречий между объективно существующими потребностями общества в расширении свободного обмена информацией и чрезмерными или наоборот недостаточными ограничениями на ее распространение и использование;\*
3. огромным желанием генерального директора что-то защитить;
4. увеличением потерь (ущерба) от уничтожения, фальсификации, разглашения или незаконного тиражирования информации (возрастанием уязвимости различных затрагиваемых субъектов);\*
5. снижением уровня доверия к автоматизированным системам управления и обработки информации, использованием большего числа бумажных носителей;
6. **Выберите определение автоматизированной системы**
   1. Комплекс упорядоченной относительно постоянной информации на носителе данных, описывающей параметры и характеристики заданной области применения, и соответствующей документации, предназначенный для поставки пользователю.
   2. Совокупность работ от формирования исходных требований к системе до ввода в действие
   3. система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.\*
   4. Устройство, предназначенное для ввода сигналов с объекта и вывода сигналов на объект
7. **Безопасность любого компонента (ресурса) АС складывается из обеспечения трех его характеристик. Выберите данные характеристики:**
   1. целостность, ясность, защищенность;
   2. защищенность, секретность, безопасность;
   3. конфиденциальность, ясность, доступность;
   4. конфиденциальность, целостность, доступность.\*
8. **Что из этого НЕ является основополагающим принципом информационной безопасности?**
   1. контроль над всеми операциями;
   2. минимум идентичных процедур;
   3. запрещено всё, что не разрешено;
   4. максимум привилегии пользователям;\*

# Глава 2: Угрозы

Здравствуйте и добро пожаловать во вторую главу нашего обучающего курса по информационной безопасности для персонала компании, в этой главы мы подробно рассмотрим понятие угрозы защиты информации, пройдемся по классификации угроз, а также по наиболее распространённым типам, с которыми сотрудники сталкиваются чаще всего.

Давайте познакомимся с определениями основных терминов, требуемых для понимая данной главы:

**Под угрозой** понимают потенциально возможное событие, процесс или явление, которое может (воздействуя на что-либо) привести к нанесению ущерба чьим-либо интересам.

**Угрозой интересам субъектов информационных отношений**мы будем называть потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию, ее носители и процессы обработки может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.

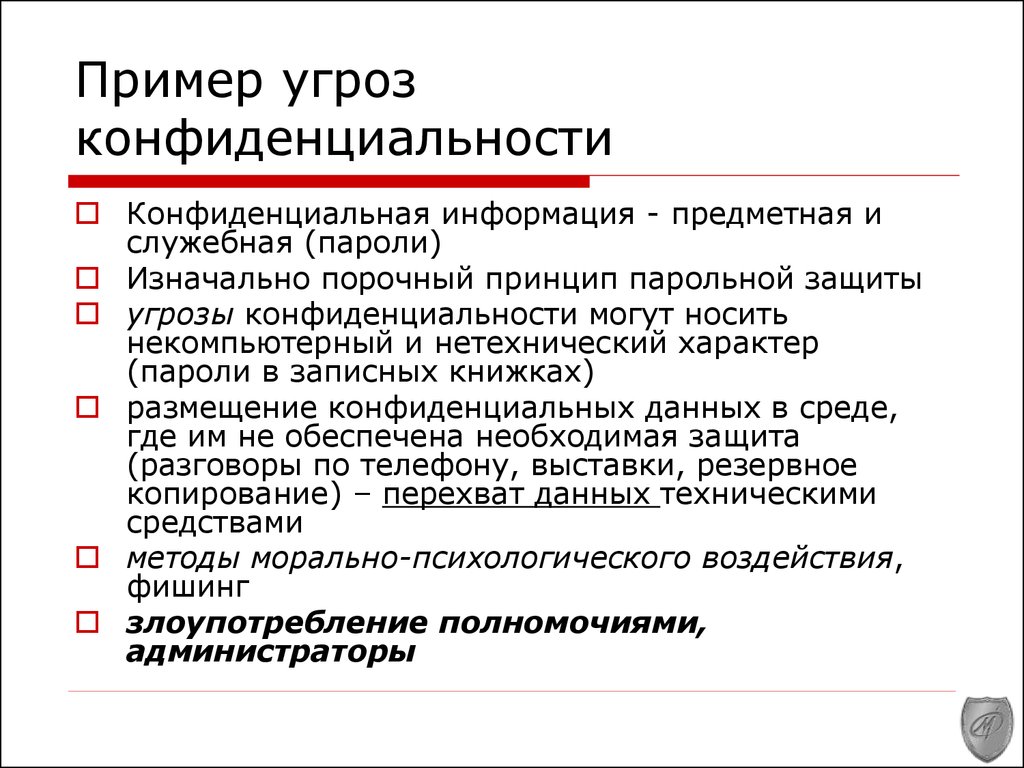
**Нарушением безопасности**(просто нарушением или атакой) принято называть реализацию угрозы безопасности. В силу особенностей современных АС, перечисленных выше, существует значительное число различных видов угроз безопасности субъектов информационных отношений. Следует иметь ввиду, что научно-технический прогресс может привести к появлению принципиально новых видов угроз и что изощренный ум злоумышленника способен придумать новые пути и способы преодоления систем безопасности, НСД к данным и дезорганизации работы АС.

## **По аспекту информационной безопасности, на который направлены угрозы**

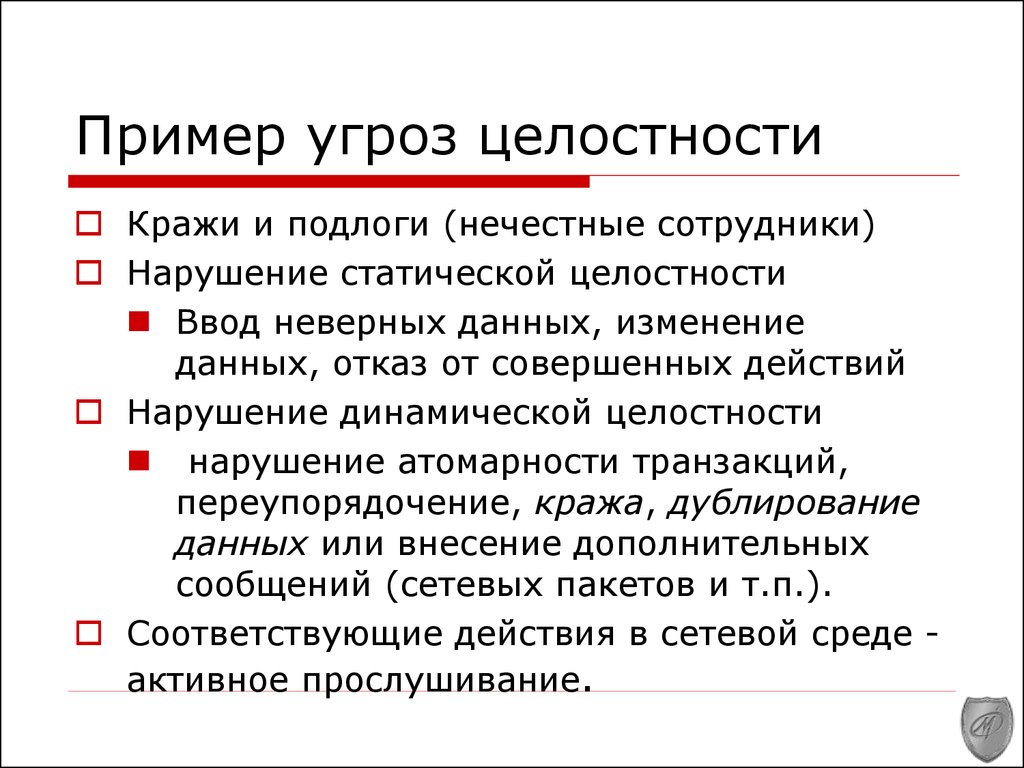
Здравствуйте, в данном уроке мы познакомился с угрозами, направленными на аспекты информационной безопасности. Данные против которого угрозы направлены в первую очередь на нарушение фундаментальных характеристик определения информационной безопасности.

**Угрозы конфиденциальности** (неправомерный доступ к информации). Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место, когда получен доступ к некоторой информации ограниченного доступа, хранящейся в вычислительной системе или передаваемой от одной системы к другой. В связи с угрозой нарушения конфиденциальности, используется термин «утечка». Подобные угрозы могут возникать вследствие «человеческого фактора» (например, случайное делегировании тому или иному пользователю привилегий другого пользователя), сбоев работе программных и аппаратных средств.

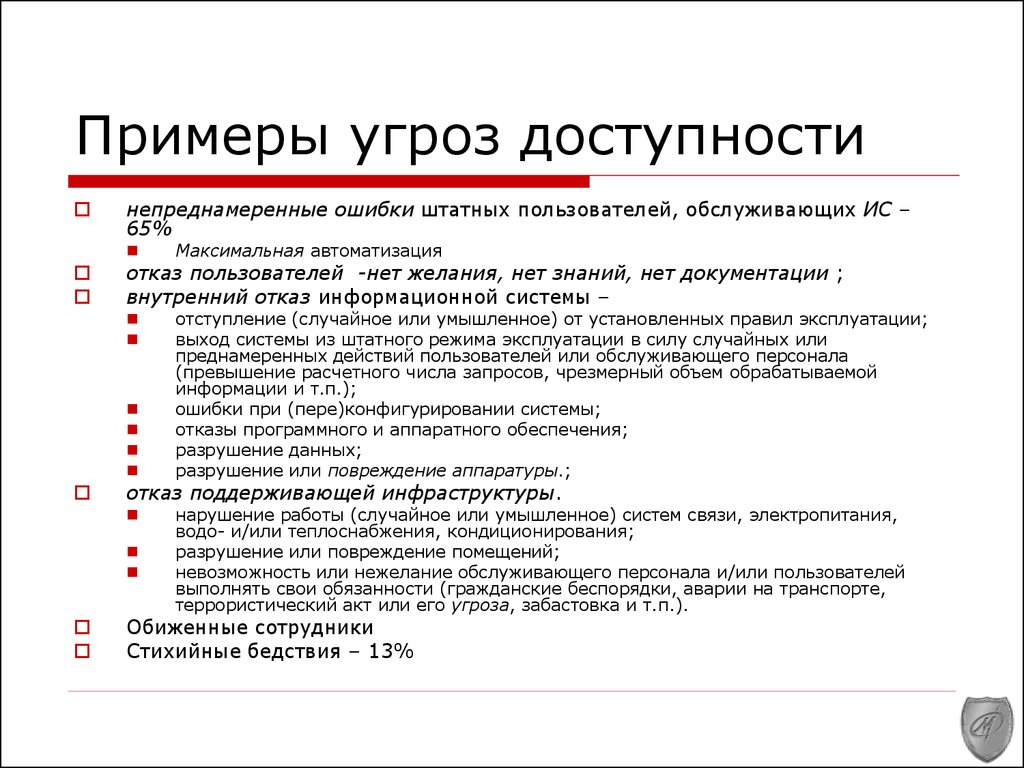
К информации ограниченного доступа относится государственная тайна и конфиденциальная информация (коммерческая тайна, персональные данные, профессиональные виды тайна: врачебная, адвокатская, банковская, служебная, нотариальная, тайна страхования, следствия и судопроизводства, переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений (тайна связи), сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации).



**Угрозы целостности** (неправомерное изменение данных). Угрозы нарушения целостности — это угрозы, связанные с вероятностью модификации той или иной информации, хранящейся в информационной системе. Нарушение целостности может быть вызвано различными факторами — от умышленных действий персонала до выхода из строя оборудования.



**Угрозы доступности** (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы). Нарушение доступности представляет собой создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных бизнес-целей.



## **По природе возникновения**

Здравствуйте, в этой лекции мы рассмотрим угрозы безопасности по природе их возникновения. Здесь мы будет изучать только самые основные из всех существующих угроз защиты информации.

Все множество потенциальных угроз по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные).



*Рис. Классификация угроз по источникам и мотивации*

**Естественные угрозы** — это угрозы, вызванные воздействиями на АС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

**Искусственные угрозы** — это угрозы АС, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

• непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании, АС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;

• преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).

Источники угроз по отношению к АС могут быть **внешними** или **внутренними** (компоненты самой АС - ее аппаратура, программы, персонал, конечные пользователи).

**Основные непреднамеренные искусственные угрозы**

Основные непреднамеренные искусственные угрозы АС (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

1. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
2. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
3. неумышленная порча носителей информации;
4. запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
5. заражение компьютера вирусами;
6. неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
7. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
8. игнорирование организационных ограничений (установленных правил) при работе в системе;
9. вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);
10. пересылка данных по ошибочному адресу абонента (устройства);
11. ввод ошибочных данных и неумышленное повреждение каналов связи.

**Основные преднамеренные искусственные угрозы**

Основные возможные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

1. физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);
2. действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);
3. внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);
4. вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
5. применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;
6. хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ)
7. несанкционированное копирование носителей информации;
8. незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путём имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя ("маскарад");
9. незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

Следует заметить, что чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

**Тест по 2 главе**

\*-верный ответ

1. **Дайте определение угрозы в информационной безопасности**
   1. потенциально возможное событие, процесс или явление, которое может (воздействуя на что-либо) привести к нанесению ущерба чьим-либо интересам\*
   2. что-то зловещие
   3. запугивание, причинить кому-нибудь зло
   4. доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.
2. **По аспекту информационной безопасности, на который направлены угрозы подразделяются на (выберите не меньше двух):**
   1. угрозы конфиденциальности\*
   2. угрозы целостности\*
   3. угрозы защищенности
   4. угрозы доступности\*
   5. угрозы потери контроля
   6. угрозы сохранности
3. **Выберите верный пример угрозы конфиденциальности**
   1. изменение конфиденциальных данных
   2. размещение данных в среде, где им не обеспечен должный уровень защиты\*
   3. невозможность работать с системой, так как нет соответствующей подготовки
   4. выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала
4. **Что из перечисленного ниже относится к непреднамеренным искусственным угрозам (выберите не меньше двух)??**
   1. игнорирование организационных ограничений (установленных правил) при работе в системе\*
   2. заражение компьютера вирусами
   3. неправомерное отключение оборудования или изменение режимов работы устройств и программ\*
   4. несанкционированное копирование носителей информации\*
5. **Что может выступать в качестве объекта защиты??**
   * 1. автономный компьютер, сервер, сетевое оборудование\*
     2. ПК, коммуникатор, терминатор
     3. сетевые адаптеры, концентраторы, маршрутизаторы
6. **Источники угроз по отношению к АС могут быть?**
   1. активными и пассивными
   2. внутренними и внешними\*
   3. локальными и удаленными
7. **Что из перечисленного ниже относится к преднамеренным искусственным угрозам (выберите не меньше двух)??**
   1. вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
   2. применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;
   3. несанкционированное копирование носителей информации;
   4. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы

# Глава 3: Наиболее распространение угрозы, которым может быть подвергнут персонал

Здравствуйте, в данном блоке лекций мы подробно рассмотрим наиболее распространение угрозы защиты информации актуальные для сотрудников компании. В данной занятии вы изучите основные шаблоны и паттерны, которыми пользуются злоумышленники для того, чтобы добыть защищенные данные компании.

### **Фишинг и Социальная инженерия**

Социальная инженерия – метод получения необходимого доступа к информации, основанный на особенностях психологии людей. Основной целью социальной инженерии является получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам.

В 2018 году компания Positive Technologies провела исследования, в котором организациям было направлено 3332 писем, содержащих ссылки на веб-ресурсы, формы для ввода паролей и приложенные файлы.

Ожидаемо наиболее успешным оказался метод социальной инженерии с применением фишинговой ссылки: 27% сотрудников перешли по ссылке.

Пользователи невнимательно читают адрес ссылки или же просто, не глядя, кликают на него и переходят на поддельный ресурс. Когда же пользователю предлагается скачать файл, а затем запустить его, то с каждым дополнительным действием у него начинают закрадываться подозрения. Поэтому лишь 7% сотрудников оказались невнимательными и попались на удочку.

Исследование показало, что на психологию сотрудника влияет даже тема письма. Предсказуемо страх увольнения или сокращения — достаточно мощный фактор, чтобы забыть о правилах информационной безопасности: почти 40% тестовых фишинговых писем с такой темой побуждали пользователей совершить потенциально опасное действие.

Злоумышленники так же используют телефонные звонки в качестве средства добычи конфиденциальной информации, 44% сотрудников в результате телефонного взаимодействия выдавали свои пароли, рассказывали об установленном ПО, переходили по требуемой ссылке.

Преступники не пренебрегают поиском сотрудников компаний в социальных сетях. Атака на профиль в социальной сети может быть достаточно эффективной. Например, можно заразить вредоносным ПО устройство сотрудника, с которого он впоследствии подключается к внутренней сети компании или проверяет корпоративную почту. Недостаточно осведомленные в вопросах ИБ пользователи могут обсуждать в социальных сетях рабочие вопросы, обмениваться конфиденциальными документами, которые представляют высокую ценность для нарушителя. В отдельных случаях сотрудники могут использовать одинаковые пароли для доступа к социальной и корпоративной сети либо незначительно изменять пароль, добавляя отдельные символы. Все полученные данные могут быть использованы преступниками при развитии атаки на инфраструктуру компании.

Так же сейчас все набирает популярность технология Deepfake с помощью которой злоумышленники могут синтезировать голос, любого человека. Исходя из этого, в будущем сотрудникам придется строго следовать всем нормативным документам по защите информации, а не доверять голосу начальника в телефонной трубке.



**Советы по защите**

1. Всегда внимательно проверяйте ссылку, по которой собираетесь кликнуть: не перепутаны ли буквы в названии сайта. Если с написанием что-то не так, это верный признак, что мошенники подсовывают вам поддельную страницу.
2. Перед тем как вводить логин и пароль, нужно проверить, защищено ли соединение. Если перед адресом сайта вы увидите префикс https (где «s» означает secure — безопасное), то все в порядке.
3. Даже если письмо или сообщение со ссылкой пришло от лучшего друга, все равно нужно помнить, что его тоже могли обмануть или взломать. Поэтому ведите себя не менее осторожно, чем при обращении со ссылками, пришедшими из неизвестного источника.
4. То же самое касается писем, отправленных из официальных инстанций и организаций: банков, налоговой, онлайн-магазинов, бюро путешествий, авиакомпаний и так далее. Даже с вашей работы. Не так уж трудно подделать официальное письмо настолько достоверно, что от реального
5. Иногда фальшивые письма и фальшивые сайты во всем повторяют дизайн настоящих. Качество подделки зависит от того, насколько хорошо преступники выполнили «домашнюю работу». А вот гиперссылки, скорее всего, будут неправильные — или с ошибками, или вообще будут ссылаться не туда. По этим признакам можно отличить фишинговое письмо от настоящего.
6. Вместо того чтобы кликать по ссылке, гораздо надежнее ввести адрес вручную в новом окне браузера. Следуя этому сценарию, вы не упустите шанс принять участие в акции или получить извещение из налоговой (если акция или извещение действительно есть) — и не попадетесь на удочку фишеров.
7. Обнаружив фишинговую операцию, крайне желательно сообщить о ней в отдел безопасности вашей компании. Так вы поможете вовремя остановить мошенников.
8. Файл, присланный вашим коллегой в мессенджере, с тем же успехом может оказаться трояном-шпионом или даже трояном-вымогателем, как и вложения к письмам и сообщениям. Будьте бдительны!

### **Вредоносное ПО**

Вредоносным считается любое программное обеспечение, которое пытается заразить компьютер или мобильное устройство. Злоумышленники используют его для самых разных целей, включая получение личных данных и паролей, похищение денежных средств, блокировку доступа к устройству для его владельца. Защититься от вредоносного ПО можно при помощи программного обеспечения, нацеленного на борьбу с этой угрозой.

**Что такое вредоносное ПО?**

Вредоносное программное обеспечение (или вредоносное ПО) – это собирательный термин, обозначающий вредоносную программу или код, который может причинить ущерб компьютерной системе. Вредоносное ПО умышленно создается враждебным, назойливым и агрессивным. Оно стремится проникнуть в систему, нанести урон, частично перехватить контроль над некоторыми процессами или вовсе вывести из строя компьютеры, компьютерные системы, сети, планшетные и мобильные устройства. Как и человеческий вирус гриппа, оно мешает нормальной работе.

Цель вредоносного ПО – получение незаконной прибыли за Ваш счет. Несмотря на то, что вредоносное ПО не может повредить аппаратное обеспечение системы или сетевое оборудование, оно может похитить, зашифровать или удалить Ваши данные, изменить функции компьютера или перехватить контроль над ними. Кроме того, оно может без Вашего ведома следить за активностью компьютера.

**Как понять, что система заражена вредоносным ПО?**

Вредоносное ПО может проявлять себя множеством способов. Вот лишь некоторые наиболее распространенные признаки, которые указывают на наличие вредоносного ПО в Вашей системе:

* Компьютер начинает работать медленно. Одно из основных последствий проникновения вредоносного ПО в операционную систему – снижение скорости ее работы независимо от того, просматриваете ли Вы веб-страницы или используете локальные приложения.
* На экране начинает периодически появляться навязчивая реклама. Неожиданные всплывающие рекламные сообщения являются типичным признаком заражения компьютера вредоносным ПО. Поэтому важно помнить: если на экране внезапно появляется сообщение «ПОЗДРАВЛЯЕМ! ВЫ ВЫИГРАЛИ МИЛЛИОН» не нажимайте на него! Какой бы приз не обещала реклама, заплатить все равно придется Вам, причем заплатить много.
* Компьютер часто выдает сбои, «зависает» или отображает «синий экран смерти», который в системах Windows свидетельствует о наличии критической ошибки.
* Вы замечаете, что по непонятным причинам уменьшилось количество свободного места на диске. Возможно, винить в этом следует разросшееся вредоносное ПО, которое скрывается где-то на жестком диске.
* Интенсивность использования системных ресурсов чрезмерно высока, а охлаждающий вентилятор компьютера постоянно работает на полной скорости. Это верный признак того, что вредоносное ПО использует системные ресурсы в фоновом режиме.
* В браузере внезапно появляются новые панели инструментов, расширения или плагины.
* Антивирусная программа перестает работать, Вам не удается ее обновить, так что Вы остаетесь беззащитными перед лицом коварного вредоносного ПО, отключившего ее.

И даже если система как будто в порядке, это еще не повод для самоуспокоения, поскольку отсутствие новостей – далеко не всегда хорошая новость. Опасное вредоносное ПО может спрятаться в недрах компьютера и делать свое грязное дело, не привлекая внимания: похищать пароли, файлы с конфиденциальными данными или использовать Ваш ПК для заражения других компьютеров.

Коварные планы вредоносного ПО не были бы столь успешны без самой важной составляющей – ***Вас***. Они используют Вашу доверчивость, Вашу привычку открывать сообщения электронной почты и переходить к вложениям, которые только выглядят безобидными, они эксплуатируют Ваше желание скорей нажать на ссылку и установить программу, источнику которой на самом деле нельзя доверять. Важно понимать, что мы ни в коем случае не хотим пристыдить Вас, поскольку злоумышленники могут обхитрить даже самых опытных пользователей и заставить их установить вредоносное ПО.

Даже если Вы устанавливаете программу из надежного источника, Вы можете не обратить внимание на то, что она запрашивает разрешение на установку еще одного приложения, которое Вы не собирались устанавливать. Эта дополнительная программа часто замаскирована под важный компонент, которым она часто не является.



**Советы по защите**

Чтобы предотвратить заражение вирусами и атаки троянских коней, необходимо выполнять некоторые рекомендации:

1. Не запускайте программы, полученные из Интернета или в виде вложения в сообщение электронной почты без проверки на наличие в них вируса.
2. Необходимо проверять все внешние диски на наличие вирусов, прежде чем копировать или открывать содержащиеся на них файлы или выполнять загрузку компьютера с таких дисков.
3. Необходимо установить антивирусную программу и регулярно пользоваться ею для проверки компьютеров. Оперативно пополняйте базу данных антивирусной программы набором файлов сигнатур вирусов, как только появляются новые сигнатуры.
4. Необходимо регулярно сканировать жесткие диски в поисках вирусов. Сканирование обычно выполняется автоматически при каждом включении ПК и при размещении внешнего диска в считывающем устройстве. При сканировании антивирусная программа ищет вирус путем сравнения кода программ с кодами известных ей вирусов, хранящихся в базе данных.
5. создавать надежные пароли, чтобы вирусы не могли легко подобрать пароль и получить разрешения администратора. Регулярное архивирование файлов позволит минимизировать ущерб от вирусной атаки
6. Основным средством защиты информации – это резервное копирование ценных данных, которые хранятся на жестких дисках

### **Слабая парольная система**

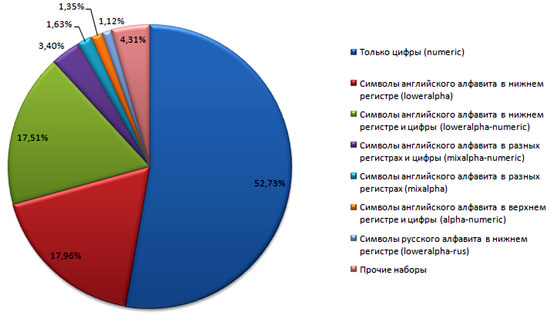
Наиболее распространенные уязвимости в системах компаний связаны с недостатками парольной политики (82%) и слабой защитой от атак, направленных на подбор учетных данных пользователей (82%), говорится в исследовании организации Positive Technologies, анализирующую уровень информационной безопасности в различных компаниях России и СНГ. Согласно сообщению, во многих системах также присутствует раскрытие информации о версиях используемого программного обеспечения (73%), что облегчает планирование атак на уязвимую систему.

Как сообщил Digit.ru Сергей Гордейчик, заместитель генерального директора Positive Technologies, «В поисках компромисса между защищенностью и удобством, часто выбор делается в пользу последнего, поскольку пользователи не всегда в состоянии запоминать и использовать сложные пароли. В целом, мы считаем, что аутентификация по паролю уже не соответствует современным требованиям безопасности. Во всех исследованных компанией системах те или иные ограничения на выбор пароля пользователя присутствовали, но каких-то требований не хватало. В каждой пятой системе, минимальная длина пароля составляла 6 символов — несколько лет назад этого было бы достаточно, но в современных условиях пароль такой длины может быть подобран достаточно быстро. Лучше, чтобы длина пароля составляла как минимум 8 символов.

**Суммарная статистика**

Суммарная статистика по используемым наборам символов в паролях приведена в Табл. 2 и на Рис. 1.

|  |  |
| --- | --- |
| **Набор символов** | **Доля, %** |
| Только цифры (numeric) | 52,73% |
| Символы английского алфавита в нижнем регистре | 17,96% |
| Символы английского алфавита в нижнем регистре и цифры | 17,51% |
| Символы английского алфавита в разных регистрах и цифры | 3,4% |
| Символы английского алфавита в разных регистрах | 1,63% |
| Символы английского алфавита в верхнем регистре и цифры | 1,35% |
| Символы русского алфавита в нижнем регистре | 1,12% |



*Рисунок . Суммарная статистика по используемым наборам символов в паролях*

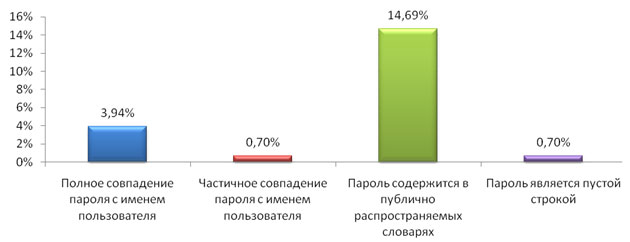
Наиболее распространенными паролями у российских пользователей являются цифровые пароли, на долю которых приходится около 53% от числа всех проанализированных паролей. Вторым по популярности набором используемых символов в своих паролях является набор из символов английского алфавита в нижнем регистре, на долю которого приходится до 18% от числа всех проанализированных паролей. С небольшим отрывом по популярности следуют аналогичные предыдущему набору символов пароли, состоящие из символов английского алфавита в нижнем регистре, но с усложнением пароля за счет использования в нем цифр. Пароли, состоящие из символов английского алфавита в нижнем регистре и цифр, встретились в 17% от числа всех проанализированных паролей.

Таким образом, около 88% паролей, используемых сотрудниками российских компаний – это пароли, содержащие в себе либо цифры, либо символы английского алфавита в нижнем регистре, либо и то и другое.

Если же рассматривать наиболее «слабые пароли», то будут получены данные, представленные в Табл. 4 и на Рис. 3.

*Таблица 4. Суммарная статистика по паролям низкой стойкости*

|  |  |
| --- | --- |
| **Причина низкой стойкости** | **Доля, %** |
| Полное совпадение пароля с именем пользователя | 3,94% |
| Частичное совпадение пароля с именем пользователя | 0,7% |
| Пароль содержится в публично распространяемых словарях | 14,69% |
| Пароль является пустой строкой | 0,7% |

  
*Рисунок 3. Суммарная статистика по паролям низкой стойкости*

Таким образом, до 4% от числа всех проанализированных паролей полностью совпадают с используемым логином, а около 15% содержатся в публично распространяемых словарях [5,6]. Подобная ситуация в значительной степени упрощает процесс реализации несанкционированного доступа злоумышленнику, действующему удаленно.

**Советы по защите**

* Длина пароля должна быть не менее 8 символов
* В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, \*, % и т.п.)
* Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.)
* При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-x позициях
* Личный пароль пользователь не имеет права сообщать никому
* Периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев

## **Тест по 3 главе**

\*-верный ответ

**В каких файлах, скаченных из интернета, могут быть вирусы?? (Несколько ответов)??**

1. В архивах\*
2. В видеофайлах\*
3. В документах\*
4. Ни в каких

**Кому разрешено сообщать свой пароль в случае необходимости??**

1. Непосредственно руководителю по его распоряжению
2. Специалисту отдела безопасности
3. ИТ специалисту для настройки компьютера
4. Сотруднику, замещающему вас на время отпуска
5. Никому\*

**Какой почтой разрешено пользоваться для переписки с внешними адресатами?**

1. только корпоративной\*
2. корпоративной почтой и сторонними почтовыми серверами
3. только сторонними почтовыми серверами (Yandex, Mail, Google)

**Что такое социальная инженерия?**

1. метод получения необходимого доступа к информации, основанный на особенностях психологии людей.\*
2. вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.
3. метод обхода систем информационной безопасности
4. любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ.

**Какова должна быть рекомендуемая длина пароля??**

1. 5 символов
2. не менее 8 символов\*
3. не имеет значения
4. более 12 символов

# Глава 4: Важные правила цифровой гигиены

Здравствуйте и добро пожаловать в четвертую главу нашего обучающего курса по информационной безопасности для персонала компании, в этой главы мы собрали для вас все важнейшие правила цифрой гигиены, которые помогут вам не только защитить данные вашей организации, но и не быть обманутыми злоумышленниками в повседневной жизни.

Жизнь в последнее время все стремительно уходит в онлайн. Существенную часть своей жизни современный человек проводит в интернете, а значит без базовых знаний в области кибербезопасности им не обойтись.

## **Цифровая гигиена**

В данном уроке мы собрали для вас наиболее нужны правила поведения в Интернете и все быстроразвивающимся онлайн пространстве.

В цифровом пространстве есть свои правила гигиены. К использованию интернета и потреблению информации стоит относиться так же, как к потреблению в физическом мире.

Вот 11 базовых приемов информационной безопасности, о которых нужно знать всем:

* 1. Ограничивайте к себе доступ ненужной и несущественной информацией. Не забывайте вовремя отписываться от неактуальных предложений, отправлять в спам ненужные письма и сообщения.
  2. Следите за общей безопасностью цифровых данных. Следите за надежностью паролей и сохранностью резервные копии данных и постоянно проверяйте свои баланс после покупок через интернет.
  3. Необходимо создавать сложные пароли, которые мы можете запомнить.

Лайфхак: Сложный пароль – не обязательно длинный пароль. Сложный пароль может состоять из 7-8 символов. Вот пример паролей: простой – sasha1987; сложный – $asha\_19B7

* 1. Не храните в «виртуальном облаке» сканы паспорта или другого важного документа

Подсказка: Если Вам необходимы цифровые копии документов, лучше храните их на флеш-карте, которая будет на брелоке с ключами или вовсе рядом со стационарным компьютером, с которого Вы обычно отправляете сканы документов.

* 1. Чистите почтовый ящик минимум 1 раз в год, удаляя старые письма.
  2. Не делитесь слишком личной информацией в социальных сетях.

Пояснение: Всему миру не нужно знать кличку Вашего домашнего животного, так как это может быть секретным вопросом от Вашей же почты.

* 1. Секретные вопросы лучше придумывать такие, на которые точно никто кроме Вас не знает ответа.

Лайфхак: вместо почтового индекса родителей или девичьей фамилии матери придумать секретный вопрос вроде «Имя первой любви?»

* 1. В банковских приложениях лучше регулярно проверять историю финансовых операций, а лучше вообще хранить на основной банковской карте минимальную сумму используя для основной суммы дополнительный счет, который легко открыть в большинстве банковских клиентов.

Пояснение: Если Вы расплачиваетесь банковской картой в мобильных приложениях или сети интернет, приложения могут подключить Вам автоплатеж, а Вы этого даже не заметите.

* 1. Не делайте отпечаток нескольких пальцев для входа в смартфон.

Пояснение: Пока Вы спите мошенник может вытянуть даже телефон из вашей сумки в автобусе или вагоне поезда и, если у Вас отсканировано больше 1 пальца для разблокирования доступа к телефону, Вы лишь облегчите злоумышленникам задачу.

* 1. Не подключайтесь к общественным WI-FI без острой необходимости и не оставляйте даже стационарный компьютер вечно подключенным к домашнему Wi-Fi, если не взаимодействуете с мировой паутиной в этот момент.
  2. Не храните все данные в одном мобильном телефоне

Пояснение: Большинство пользователей используют свой смартфон лишь на 30-40 % от всех его возможностей. Даже, разграничив свои потребности на два телефона (по одному вы ведете переговоры, и он может быть самым простым, а второй будет для использования навигатора, приложений для общения и знакомств) Вы не дадите возможности тому же Google формировать для Вас тематическую рекламу. Помните – приложения могут прослушивать телефонный разговор или даже ловить поток речи, в котором Вы обсуждаете чем кормить кошку или, что планируете поехать в отпуск.

# Глава 5: Подведение итогов курса

Здравствуйте и добро пожаловать в пятую и итоговую главу нашего обучающего курса по информационной безопасности для персонала компании. В данной главе мы с вами пройдем итоговый тест по всему курсу. Закрепим и повторим весь пройденный материал с помощью заданий и вопросов.

Спасибо вам за прохождение данного курса, наша команда рада помочь вам в поиске новых знаний и умений, а также мы все стремимся к тому, чтобы процент компаний, в которых данные были украдены из-за незнания сотрудников уменьшалось с каждым годом.

## **Тест по итогам всего курса 18 вопросов**

\*правильные ответы

**К коммерческой тайне относятся…**

* Информация о перегревах с контрагентами\*
* налоговая отчётность
* перечень лиц, имеющих право действовать без пропуска
* сведения о продажах\*
* учредительные документы компании

**В каких файлах, скаченных из интернета, могут быть вирусы?**

* В архивах\*
* В видеофайлах\*
* В документах\*
* Ни в каких

**Что такое информационная безопасность?**

* это свойство информации сохранять конфиденциальность, целостность и доступность\*
* это свойство автоматизированной системы быть защищенной от злоумышленника
* Комплекс упорядоченной относительно постоянной информации на носителе данных, описывающей параметры и характеристики заданной области применения, и соответствующей документации, предназначенный для поставки пользователю
* Ни один из вариантов

**В каком случае разрешено работать за компьютером под чужим логином и паролем?**

* После получения разрешения от владельца используемого логина и пароля
* После согласования с непосредственным руководством
* после получения разрешения от Отдела информационной безопасности
* Ни в каком\*

**В каком случае с рабочего компьютера разрешено пользоваться социальными сетями?**

* Ни в каком\*
* Если переписка в соц. сети ведется на тему работы
* Если пользоваться не русскоязычными социальными сетям
* Если пользоваться русскоязычными социальными сетями

**Как заблокировать компьютер?**

* Нажать клавиши Alt+F4
* Нажать клавиши Ctrl + Esc
* Нажать клавиши Windows + L\*
* Отключить монитор
* Нажать на кнопку питания на компьютере

**Что нужно сделать, если на экране вашего компьютера появился баннер с требованием заплатить деньги?**

* Обратиться к системному администратору\*
* Перезагрузить компьютер
* Заплатить деньги
* Написать письмо злоумышленникам с целью разблокировки компьютера

**Пароль – это информация?**

* Да\*
* Только в том случае, если записан на бумаге
* нет

**Выберите из предложенных верные принципы информационной безопасности**

* Простота использования\*
* Открытая архитектура ИС\*
* Разграничение доступа\*
* Работоспособность ИС

**Какие из перечисленных паролей сложные?**

* $kbn\*1U3\*
* Ys99%L7F4\*
* Dsjm83
* 09Qwerty
* Ш,Фь-Ыгзук89\*

**Что нужно сделать, чтобы установить программу на компьютер?**

* Обратиться в ИТ отдел\*
* Скачать программу из интернета, при возникновении проблем с установкой – обратиться в отдел ИТ
* Установить с флешки программу, заранее скаченную дома

**Представьте ситуацию: вы нашли флешку в коридоре. Что с ней необходимо сделать?**

* Передать специалисту ИТ\*
* Передать непосредственному руководителю
* Открыть флешку на компьютере, что бы по содержимому определить владельца
* Отформатировать флешку на компьютере

**От каких отправителе разрешено открыть вложения, покрепленные к письму?**

* От сотрудников компании\*
* От внешнего отправителя, с которым вы вели переписки и вложение ожидалось\*
* От внешнего отправителя, с которым вы вели переписку, но вложение не ожидалось
* От общеизвестной компании, с которой вы не вели переписку (МТС, Сбербанк, Магафон)

**По природе возникновения угрозы бывают?**

* + активными и пассивными
  + внутренними и внешними
  + локальными и удаленными
* естественными и искусственными\*

**Когда нужно блокировать компьютер?**

* Каждый раз, когда отходите от рабочего места\*
* Каждый раз, когда уходите из кабинета дольше чем на полчаса
* В конце рабочего дня
* Компьютер самостоятельно блокируется через 15 минут после прекращения работы, поэтому блокировать его не нужно

**Когда можно пользовать корпоративным интернетом в личных целях?**

* В любое время, если это не мешает работе
* Только в обеденный перерыв
* Никогда\*

**Вложения в письме с какими расширениями нельзя открывать?**

* .PS, .BAT, .EXE\*
* .XLSX, .DOCX, .JPG
* .PDF, .DOC, .TXT
* .COM, .JS, .VBS\*

**Как можно заразить компьютер вирусом?**

* Подключить к компьютеру мышку или клавиатуру
* Подключить к компьютеру флешку контрагента\*
* Открыть скаченный файл из интернета\*
* Пройти по ссылке, полученной от неизвестного отправителя\*