БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Деденко Михаил Михайлович
доцент, кандидат технических наук

Лекция № 7. Основы информационной безопасности

ПЛАН ЛЕКЦИИ:

1. Информационная безопасность.
2. Информационные опасности и угрозы.
3. Конфиденциальная информация и ее защита.
4. Опасности, возникающие при работе в информационной среде.

Вопрос № 1. Информационная безопасность

Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" трактует понятие ***информации*** как сведения (сообщения, данные) независимо от формы их представления.

Настоящий Федеральный закон регулирует отношения, возникающие при:

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

2) применении информационных технологий;

3) обеспечении защиты информации.

- Основным юридическим документом, регулирующим сферу информационной безопасности в России, является **Доктрина информационной безопасности Российской Федерации** (Указ Президента РФ от 5 декабря 2016 г. № 646), которая определяет информационную безопасность.
- ***Информационная безопасность Российской Федерации*** – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

- ***Интересы личности в информационной сфере*** заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.
- ***Интересы общества в информационной сфере*** заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.
- ***Интересы государства в информационной сфере*** заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности страны, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Составляющие национальных интересов Российской Федерации в информационной сфере

Первая составляющая включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Четвертая составляющая включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Основные средства и методы защиты информации

- ✔ Средства и методы защиты информации обычно делят на две большие группы: *организационные и технические*.
- ❖ ***Под организационными*** подразумеваются законодательные, административные и физические, а ***под техническими*** – аппаратные, программные и криптографические мероприятия, направленные на обеспечение защиты объектов, людей и информации.
- ❖ С целью организации защиты объектов используют ***системы охраны и безопасности объектов*** – это совокупность взаимодействующих радиоэлектронных приборов, устройств и электрооборудования, средств технической и инженерной защиты, специально подготовленного персонала, а также транспорта, выполняющих названную функцию.

Вопрос № 2. Информационные опасности и угрозы

Источники информационных опасностей и угроз

***Источниками внутренних угроз* являются:**

1) сотрудники организации;

2) программное обеспечение;

3) аппаратные средства.

❖ ***Внутренние угрозы могут проявляться в следующих формах:***

- ошибки пользователей и системных администраторов;
- нарушения сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации;
- ошибки в работе программного обеспечения;
- отказы и сбои в работе компьютерного оборудования.

Источники информационных опасностей и угроз

К внешним источникам угроз относятся:

1) компьютерные вирусы и вредоносные программы;

2) организации и отдельные лица;

3) стихийные бедствия.

❖ ***Формами проявления внешних угроз являются:***

- заражение компьютеров вирусами или вредоносными программами;
- несанкционированный доступ к корпоративной информации;
- информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб;
- действия государственных структур и служб, сопровождающиеся сбором, модификацией, изъятием и уничтожением информации;
- аварии, пожары, техногенные катастрофы, стихийные бедствия.

Классификация угроз по способам воздействия на объекты информационной безопасности

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации: информационные, программные, физические, радиоэлектронные и организационно-правовые.

- ***К информационным угрозам относятся:***

- несанкционированный доступ к информационным ресурсам;
- незаконное копирование данных в информационных системах;
- хищение информации из библиотек, архивов, банков и баз данных;
- нарушение технологии обработки информации;
- противозаконный сбор и использование информации;
- использование информационного оружия.

- ***К программным угрозам относятся:***

- использование ошибок в программном обеспечении;
- компьютерные вирусы и вредоносные программы;
- установка «закладных» устройств.

Классификация угроз по способам воздействия на объекты информационной безопасности

- ***К физическим угрозам относятся:***
  - уничтожение или разрушение средств обработки информации и связи;
  - хищение носителей информации;
  - хищение программных или аппаратных ключей и средств криптографической защиты данных;
  - воздействие на персонал.
- ***К радиоэлектронным угрозам относятся:***
  - внедрение электронных устройств перехвата информации в технические средства и помещения;
  - перехват, расшифровка, подмена и уничтожение информации в каналах связи.
- ***К организационно-правовым угрозам относятся:***
  - нарушение требований законодательства и задержка в принятии необходимых нормативно-правовых решений в информационной сфере;
  - закупки несовершенных или устаревших информационных технологий и средств информатизации.

Меры защиты субъектов информационных отношений

Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

1. ***Законодательный уровень*** (законы, нормативные акты, стандарты и т.п.).
2. ***Административный уровень*** (действия общего характера, предпринимаемые руководством организации.
3. ***Процедурный уровень*** (конкретные меры безопасности, ориентированные на людей).

Меры данного уровня включают в себя:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов систем обработки данных;
- мероприятия по разработке правил доступа пользователей к ресурсам системы;
- мероприятия, осуществляемые при подборе и подготовке персонала, обслуживающего систему;
- организацию охраны и режима допуска к системе;
- организацию учета, хранения, использования и уничтожения документов и носителей информации;
- распределение реквизитов разграничения доступа;
- организацию явного и скрытого контроля за работой пользователей;
- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения.

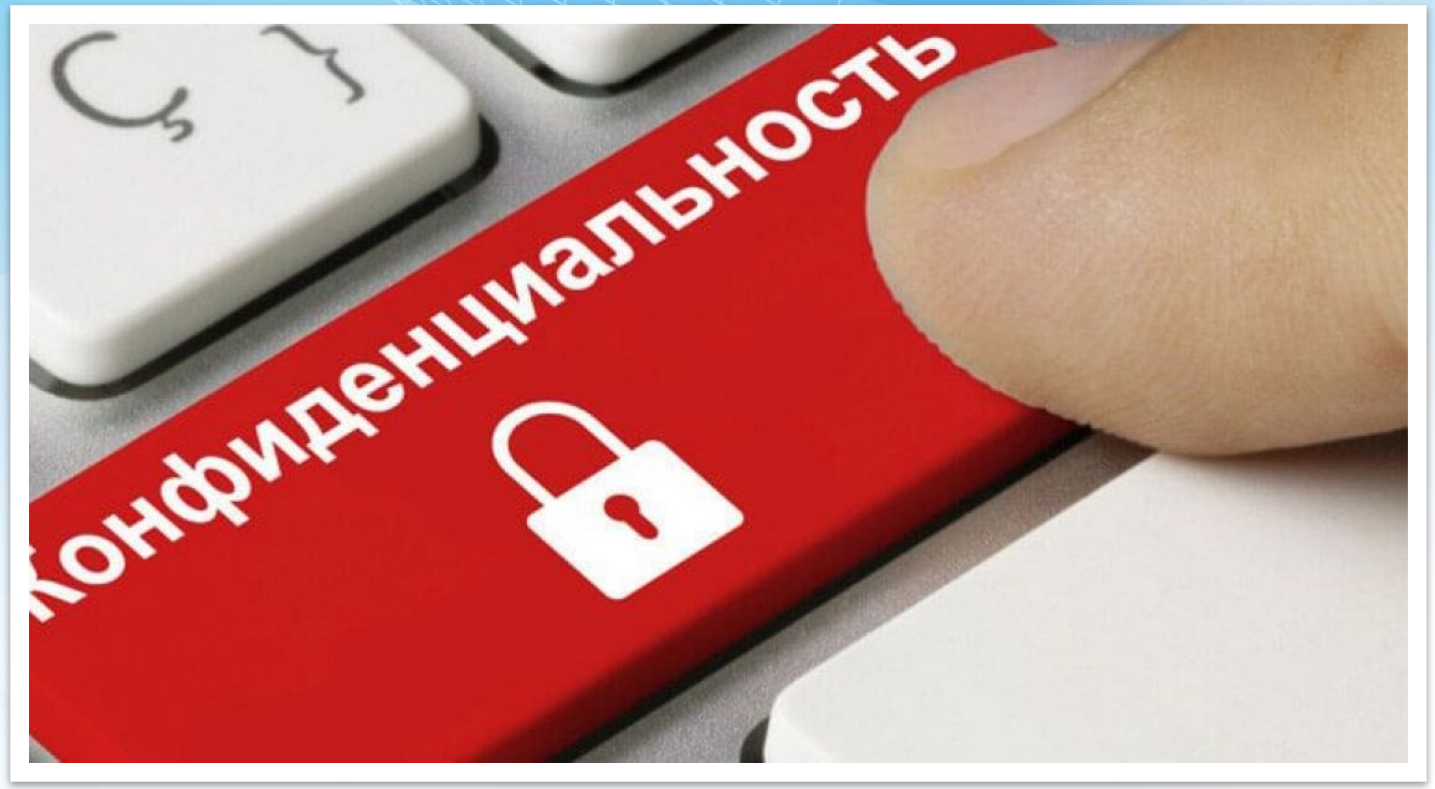
Меры защиты субъектов информационных отношений

Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

4. ***Программно-технический уровень*** (технические меры). Меры защиты этого уровня основаны на использовании специальных программ и аппаратуры и выполняют (самостоятельно или в комплексе с другими средствами) функции защиты:

- идентификацию и аутентификацию пользователей;
- ограничение доступа к ресурсам;
- регистрацию событий;
- проверку отсутствия вредоносных программ;
- программную защиту передаваемой информации и каналов связи;
- защиту системы от наличия и появления нежелательной информации;
- создание физических препятствий на путях проникновения нарушителей;
- мониторинг и сигнализацию соблюдения правильности работы системы;
- создание резервных копий ценной информации.

Вопрос № 3. Конфиденциальная информация и ее защита



Конфиденциальная информация — информация, доступ к которой ограничивается в соответствии с законодательством страны и уровнем доступа к информационному ресурсу.

Развернутая классификация конфиденциальной информации приводится в перечне сведений конфиденциального характера, установленном Указом Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

Согласно данному указу, к сведениям конфиденциального характера относятся:

- персональные данные;
- коммерческая тайна;
- служебная тайна;
- сведения, составляющие тайну следствия и судопроизводства;
- профессиональная тайна;
- сведения о сущности изобретения (полезной модели или промышленного образца до официальной публикации информации о них);
- сведения, содержащиеся в личных делах осужденных.

Персональные данные

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» регулируются отношения, связанные с обработкой персональных данных с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств.

Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

- Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
- Следует отметить, что в Федеральном законе установлены правила обработки персональных данных в общедоступных источниках персональных данных.

Коммерческая тайна

Федеральным законом от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» регулируются отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

Коммерческая тайна — режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Перечень сведений, которые не могут составлять коммерческую тайну:

- учредительные документы (решение о создании предприятия или договор учредителей) и Устав;
- документы, дающие право заниматься предпринимательской деятельностью;
- сведения по установленным формам отчетности о финансово — хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РСФСР;
- документы о платежеспособности;
- сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;
- документы об уплате налогов и обязательных платежах;
- сведения о загрязнении окружающей среды.

Служебная тайна

- Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» определяет, что к ***служебной информации ограниченного распространения*** относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами.

К ***основным объектам служебной тайны*** можно отнести такие виды информации, как:

1) служебная информация о деятельности федеральных государственных органов, доступ к которой ограничен законом в целях защиты государственных интересов:
   - *военная тайна*;
   - *тайна следствия;*
   - *судебная тайна;*

2) охраноспособная конфиденциальная информация:
   - *коммерческая тайна;*
   - *банковская тайна;*
   - *профессиональная тайна;*
   - *конфиденциальная информация о частной жизни лица.*

Профессиональная тайна

Профессиональная тайна — защищаемая по закону информация, доверенная или ставшая известной лицу исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица, доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

Информация может считаться профессиональной тайной, если она отвечает следующим требованиям:

- доверена или стала известна лицу лишь в силу исполнения им своих профессиональных обязанностей;
- лицо, которому доверена информация, не состоит на государственной или муниципальной службе (в противном случае информация считается служебной тайной);
- запрет на распространение доверенной или ставшей известной информации, которое может нанести ущерб правам и законным интересам доверителя, установлен федеральным законом;
- информация не относится к сведениям, составляющим государственную и коммерческую тайну.

Виды профессиональной тайны:

Врачебная тайна — сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении (ст. 13 Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»).

Тайна связи. На территории РФ гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи (ст. 63 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»).

Нотариальная тайна. Нотариусу при исполнении служебных обязанностей, лицу, замещающему временно отсутствующего нотариуса, а также лицам, работающим в нотариальной конторе, запрещается разглашать сведения, оглашать документы, которые стали им известны в связи с совершением нотариальных действий, в том числе и после сложения полномочий или увольнения (ст. 5 Основ законодательства Российской Федерации о нотариате» от 11 февраля 1993 г. № 4462-1).

Адвокатская тайна — любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю (ст. 8 Федерального закона от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»).

Виды профессиональной тайны:

Тайна усыновления. Судьи, вынесшие решение об усыновлении ребенка, или должностные лица, осуществившие государственную регистрацию усыновления, а также лица, иным образом осведомленные об усыновлении, обязаны сохранять тайну усыновления ребенка (ст. 139 Семейного кодекса Российской Федерации от 29 декабря 1995 г. № 223-ФЗ).

Тайна страхования. Страховщик не вправе разглашать полученные им в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и характера нарушения несет ответственность в соответствии с правилами, предусмотренными ст. 139 или 150 Гражданского кодекса Российской Федерации (часть вторая от 26 января 1996 г. № 14-ФЗ (ст. 946)).

Тайна исповеди — сведения, доверенные гражданином священнослужителю на исповеди. Священнослужитель не может быть привлечен к ответственности за отказ от дачи показаний по обстоятельствам, которые стали известны ему из исповеди (ст. 3 Федерального закона от 26 сентября 1997 г. № 125-ФЗ «О свободе совести и о религиозных объединениях»).

Банковская тайна. Кредитная организация, Банк России, организация, осуществляющая функции по обязательному страхованию вкладов, гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов (ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»).

Вопрос № 4. Опасности, возникающие при работе в информационной среде

При работе в локальных или глобальной сетях пользователи могут столкнуться со следующими угрозами:

- вредоносное программное обеспечение;
- несанкционированный доступ к личным данным, информационным ресурсам и систем;
- интернет-мошенничество (например, с целью кражи денежных средств, либо кражи персональных данных);
- угрозы психическому здоровью пользователя.

Вредоносное программное обеспечение

Вредоносное программное обеспечение – любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам компьютера, к информационным ресурсам и их использованию в целях причинение вреда (нанесение ущерба) физическим или юридическим лицам.

Вредоносные программы могут создавать следующие виды ущерба:

- создание помех в работе системы;
- уменьшение ресурсов компьютера;
- выполнение несанкционированных действий с данными;
- дестабилизация работы пользователя с компьютером.

О наличии вредоносного программного обеспечения в системе пользователь может судить по следующим признакам:

- появление сообщений антивирусных средств о заражении или о предполагаемом заражении, "самопроизвольное" отключение антивирусных программных средств;
- явные проявления присутствия вируса, такие как: сообщения, выдаваемые на монитор или принтер, звуковые эффекты, неожиданный запуск программ, уничтожение файлов и другие аналогичные действия, однозначно указывающие на наличие вируса в системе;
- неявные проявления заражения, которые могут быть вызваны и другими причинами, например, сбоями или отказами аппаратных и программных средств компьютерной системы – увеличение времени обработки той или иной информации, необоснованное уменьшение свободного объёма на дисковых носителях, отказ выполнять программы-сканеры вирусной активности, "зависания" системы и т.п.;
- рассылка писем, которые пользователем не отправлялись, по электронной почте.

Вредоносные программы включают следующие категории:

- компьютерные вирусы и черви;

- троянские программы;

- подозрительные упаковщики и вредоносные утилиты.

Компьютерные вирусы – это небольшие исполняемые или интерпретируемые программы, обладающие свойством несанкционированного пользователем распространения и самовоспроизведения в компьютерах или компьютерных сетях.

Черви считаются подклассом вирусов, но обладают характерными особенностями. Червь размножается (воспроизводит себя), не заражая другие файлы.

Троянские программы внешне выглядят как легальный программный продукт, но при запуске осуществляют несанкционированные пользователем действия, направленные на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей.

Подозрительные упаковщики часто сжимаются специфичными способами упаковки, включая использование многократных упаковщиков и совмещая упаковку с шифрованием содержимого файла для того, чтобы при распаковке усложнить анализ файла эвристическими методами.

Вредоносные утилиты разработаны для автоматизации создания других вирусов, червей или троянских программ, организации атак на удаленные серверы, взлома компьютеров и т.п.

Несанкционированный доступ к личным данным, информационным ресурсам и систем

Несанкционированный доступ — 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.

Способы несанкционированного доступа:

1. Взлом информационных ресурсов (корпоративных сетей, вебсайтов, облачных сервисов, отдельных компьютеров и мобильных устройств).

2. Перехват сообщений. Подразумеваются любые отправленные послания, включая электронную почту, мессенджеры, SMS и прочее.

3. Сбор данных. Может производиться законными способами, но преследовать противоправную цель.

4. Шантаж, вымогательство, дача взятки.

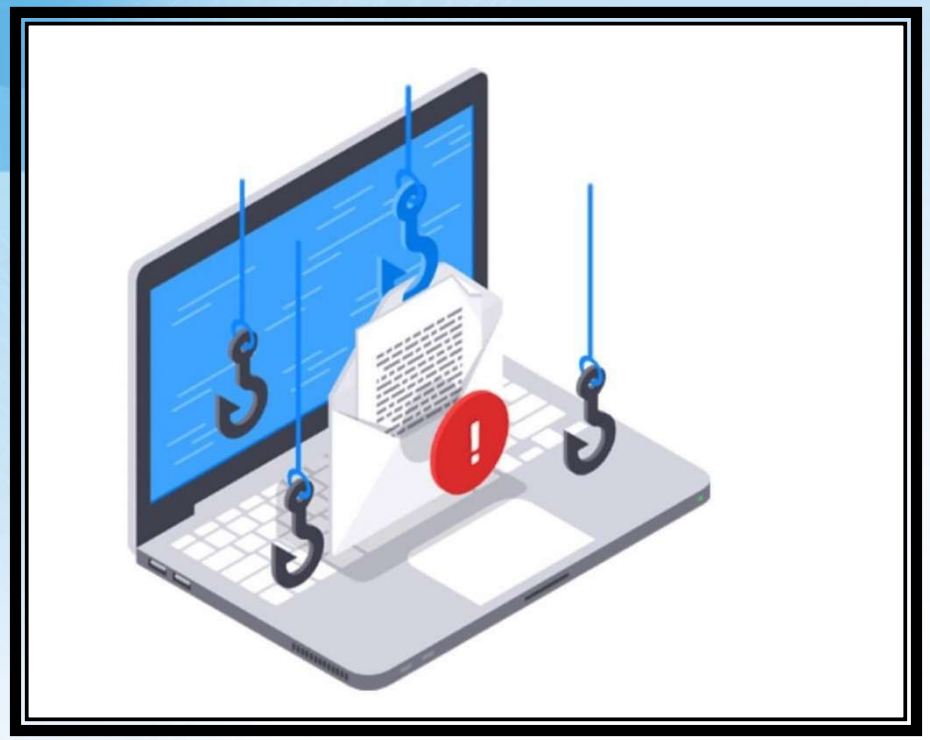
5. Похищение информации.

Интернет-мошенничество

Развитие вредоносных программ позволяет мошенникам использовать Интернет для получения личной информации пользователя, например, фамилию, имя, отчество, пароли к социальным сетям, паспортные данные, реквизиты банковской карты и другие сведения.

Хищение данных пользователей происходит следующими способами:

1. *Фишинговые сообщения* – к пользователю сети Интернет могут прийти письма от мошенников под видом официальных писем из банка или из других официальных учреждений.
2. *Поддельные сайты* – преступники могут создать «клон» официального сайта нужной вам организации.



Угрозы психическому здоровью пользователя

Неконтролируемое, необдуманное и чрезмерное использование Интернета, может представлять разнонаправленные угрозы для психического здоровья пользователя:

- информационная перегрузка, воздействующая на психику;
- изоляция от реальности;
- депрессивное состояние.

❖ Основной проблемой обеспечения психологической безопасности стала проблема информационной (когнитивной) перегрузки.

❖ Второй существенной проблемой является бесконтрольное распространение в сети информации, пропагандирующей насилие и жестокость.

Для уменьшения риска психическому здоровью при работе в сети интернет необходимо применять следующие меры:

- ограничение времени, проведенного в Интернете;
- если вы вынуждены работать в Интернете, не позволяйте себе отвлекаться на сторонние сайты.
- не смотрите и не читайте шокирующий контент, он не несет никакой смысловой информации, но психика на него реагирует остро, хотя этот процесс и не заметен для вас.

Задание на самостоятельную работу

1. Изучить конспект лекции, быть готовым к опросу.

2. Подготовьте сообщение (доклад):

2.1. Виды опасностей в информационной сфере, их причины и последствия.

2.2. Риски и угрозы информационного терроризма.

2.3. Меры противодействия криминальным опасностям в информационной среде.

2.4. Информационная война.

Рекомендуемая литература

1. Резчиков Е.А. Безопасность жизнедеятельности : учебник для вузов / Е. А. Резчиков, А. В. Рязанцева. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 639 с. — (Высшее образование). — ISBN 978-5-534-12794-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/468920 (дата обращения: 01.06.2021).
2. Резчиков Е.А. Безопасность жизнедеятельности : учебник для вузов / Е. А. Резчиков, А. В. Рязанцева. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 639 с. — (Высшее образование). — ISBN 978-5-534-12794-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/468920 .
3. Погодаева М.В. Безопасность жизнедеятельности [Электронный ресурс] : учеб. пособие / М. В. Погодаева, М. М. Деденко. - ЭВК. - Иркутск : Изд-во Ин-та географии им. В. Б. Сочавы СО РАН, 2020. - 93 с. - Режим доступа: ЭЧЗ "Библиотех". - Неогранич. доступ.