Государственное агентство по защите персональных данных при Кабинете Министров Кыргызской Республики

ТИПОВОЙ ПЕРЕЧЕНЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Оглавление

1. Общие положения 3

2. Классификация угроз безопасности персональных данных 11

3. Основные элементы канала реализации угроз безопасности персональных данных 14
   3.1. Источник угроз безопасности персональных данных 14
      3.1.1. Антропогенные источники угроз 14
      3.1.2. Техногенные источники угроз 16
      3.1.3. Стихийные источники угроз 17
   3.2. Среда распространения 17
   3.3. Носители информации 17

4. Классификация угроз 18

5. Угрозы утечки информации по техническим каналам 29
   5.1 Угрозы утечки акустической (речевой) информации 29
   5.2 Угрозы утечки визуальной информации 30
   5.3 Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок 31

6. Угрозы несанкционированного доступа к информации в информационной системе 34

7. Классификация уязвимостей программных систем 37
   7.1 Классификация угроз и атак 37
   7.2 Классификация вредоносных программ 37
      7.2.1 Как распространяется вредоносное программное обеспечение? 40
      7.2.2 Распространенные формы атак вредоносных программ 40
   7.3 Классификации и реестры уязвимостей 44
   7.4 Классификация дефектов 48

8.Актуальные угрозы безопасности информационных систем государственных органов, органов местного самоуправления, организаций и учреждений. 56

Приложение 1. Виды и мотивация нарушителей 60

Приложение 2. Виды программ-вымогателей 63

Приложение 3. Классификация распространенных троянских типов приложений 64

Приложение 4. Категории DoS и DDoS-трафика

Приложение 5. Классификация и цели DDoS-атак по уровням OSI 70

Приложение 6. Уязвимости отдельных протоколов стека протоколов TCP/IP, на базе которого функционируют глобальные сети общего пользования 73

Приложение 7. Примерный список источников, полезных при рассмотрении вопросов защиты персональных данных и кибербезопасности 75

1. Общие положения

1. Настоящий «Типовой перечень угроз безопасности персональных данных при обработке персональных данных в информационных системах» (далее – Типовой перечень) разработан в соответствии с Законами Кыргызской Республики «Об информации персонального характера», «Об электронном управлении», «Об электронной подписи», Постановлением Правительства Кыргызской Республики от 21 ноября 2017 года № 760, Постановлением Правительства Кыргызской Республики от 21 ноября 2017 года № 762 и Постановлением Кабинета Министров Кыргызской Республики «О Государственном агентстве по защите персональных данных при Кабинете Министров Кыргызской Республики» от 22 декабря 2021 года № 325.

2. Типовой перечень содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических и юридических лиц, а также действиями преступных организаций, создающих условия (предпосылки) для нарушения безопасности персональных данных, которые ведут к ущербу важных интересов личности, общества и государства. В настоящем Типовом перечне под “информационными системами персональных данных” понимаются информационные системы, в которых хранятся или обрабатываются персональные данные, и далее по тексту используется словосочетание “информационные системы”.

3. Учитывая особенности обработки персональных данных в Кыргызской Республике в государственных органах, органах местного самоуправления, в частных и государственных организациях и учреждениях, а также категорию и объем обрабатываемых в информационных системах, основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

4. Типовой перечень содержит единые исходные данные по угрозам безопасности персональных данных, обрабатываемых в информационных системах, связанные с:

- перехватом (съемом) персональных данных по техническим каналам с целью их копирования или неправомерного использования, или распространения;
- несанкционированным, в том числе случайным, доступом в информационную систему с целью сбора, записи, хранения, актуализации, группировки, блокирования, стирания и разрушения, а также неправомерного использования или распространения персональных данных или деструктивных воздействий на элементы информационной системы и обрабатываемых в них персональных данных с использованием программных и программно-аппаратных

средств с целью уничтожения или блокирования персональных данных.

5. К основным типам источников угроз безопасности информации относятся:

- антропогенные источники (антропогенные угрозы);
- техногенные источники (техногенные угрозы);
- стихийные источники (угрозы стихийных бедствий и иных природных явлений).

6. Основными видами угроз безопасности персональных данных в информационных системах являются:

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к информационным ресурсам информационной системы, включая ее пользователей, в том числе с использованием внутренних сетей связи;
- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к информационным системам, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;
- угрозы, возникновение которых напрямую зависит от свойств техники и программного обеспечения, используемого в информационных системах;
- угрозы, возникающие в результате внедрения аппаратных закладок и вредоносных программ;
- угрозы, направленные на нарушение нормальной работы технических средств и средств связи, используемых в информационных системах;
- угрозы, связанные с недостаточной квалификацией персонала, обслуживающего информационные системы.

7. Настоящий Типовой перечень применяется совместно с Требованиями к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных, утвержденными постановлением Правительства Кыргызской Республики от 21 ноября 2017 года № 760, Методикой определения угроз безопасности в информационных системах персональных данных, утверждаемой уполномоченным государственным органом по персональным данным. Также использоваться актуальные базы угроз, формируемые международными ведущими организациями в области кибербезопасности.

8. Типовой перечень является методическим документом и

предназначен для государственных и муниципальных органов, юридических и (или) физических лиц (далее – держатели или обладатели персональных данных), организующих и (или) осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных, заказчиков и разработчиков информационной системы и ее подсистем. С применением настоящего Типового перечня решаются следующие задачи:

- разработка отраслевых перечней угроз безопасности персональных данных в конкретных информационных системах с учетом их назначения, условий и особенностей функционирования;
- анализ защищенности информационной системы от угроз безопасности персональных данных в ходе организации и выполнения работ по обеспечению безопасности персональных данных;
- разработка системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационной системы;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства информационной системы, в результате которого может быть нарушено их функционирование;
- контроль обеспечения уровня защищенности персональных данных.

9. В Типовом перечне дано обобщенное описание информационной системы как объекта защиты, возможных источников угрозы безопасности персональных данных, основных классов уязвимостей информационной системы, возможных видов деструктивных воздействий на персональные данные, а также основных способов их реализации. Угрозы безопасности персональных данных, обрабатываемых в информационных системах, содержащиеся в настоящем Типовом перечне, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в информационных системах. Внесение изменений в Типовой перечень осуществляется Уполномоченным государственным органом по защите персональных данных Кыргызской Республики.

10. Для целей настоящего Типового перечня используются и применяются следующие основные термины и определения:

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Атака – попытка уничтожения, раскрытия, внесения изменений, вывода из строя, хищения или получения несанкционированного доступа к активу.

Актив – некоторая сущность, ценная для личности, организации или государства.

Бот, робот – компьютерная программа, используемая для автоматизированного выполнения особых функций и решения специфических задач. Термин часто используется для программ, которые автоматизируют задачи, обычно исполняемые на сервере, например, для отправки или сортировки электронной почты. Бот может представлять собой программу, которая выступает агентом пользователя или другой программы, либо же симулирует деятельность пользователя.

Ботнет – дистанционно управляемые компьютерные программы, представляющие собой, как правило, набор вредоносных ботов, которые находятся на зараженных компьютерах сети и запускаются в работу автономно или автоматизировано.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах.

Блокирование персональных данных – временное прекращение передачи, уточнения, использования и уничтожения персональных данных.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы с целью компрометации финансовых данных, медицинских записей, электронных писем, паролей и т.д..

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы.

Держатель (обладатель) массива персональных данных – органы государственной власти, органы местного самоуправления и юридические лица, на которые возложены полномочия определять цели, категории персональных данных и контролировать сбор, хранение, обработку и использование персональных данных в соответствии с законодательством Кыргызской Республики.

Доступ в операционную среду компьютера (информационной системы) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации –возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый,вносимый или подключаемый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация персонального характера (персональные данные) - зафиксированная информация на материальном носителе о конкретном человеке, отождествленная с конкретным человеком или которая может быть отождествлена с конкретным человеком, позволяющая идентифицировать этого человека прямо или косвенно, посредством ссылки на один или несколько факторов, специфичных для его биологической, экономической, культурной, гражданской или социальной идентичности.

Информативный сигнал – электрические и оптические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных – совокупность, содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации.

Источник угрозы безопасности информации – субъект доступа, материальный и не материальный объект или физическое явление, являющееся причиной возникновения угрозы безопасности информации.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей обработчика и посторонних транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения обработчиком или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – это программный (защитное решение) или аппаратный (физическое оборудование) элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

Нарушитель безопасности персональных данных – физическое / юридическое лицо или преступная организация, случайно или преднамеренно совершающие действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Нежелательный контент – это не только вредоносный код, потенциально опасные программы и спам (т.е. то, что непосредственно создано для уничтожения или кражи информации), но и сайты, запрещенные законодательством, а также нежелательные ресурсы с информацией, не соответствующей возрасту потребителя.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование,

распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Обработчик – физическое или юридическое лицо, определяемое держателем (обладателем) персональных данных, которое осуществляет обработку персональных данных на основании заключенного с ним договора.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы – лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Прикладное программное обеспечение – программное обеспечение, используемое конечными пользователями для решения своих конкретных, прикладных задач, и не выполняющее функций программного обеспечения, которое сам компьютер использует для служебных, технологических целей без участия конечного пользователя

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником. Среда распространения, может быть, как однородной (например, только воздушной), так и неоднородной за счет перехода сигнала из одной среды в другую (например, в результате акустоэлектрических или виброакустических преобразований)

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Субъект персональных данных - физическое лицо, к которому относятся соответствующие персональные данные.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Технические средства информационной системы – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – дефект программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использована для реализации угроз безопасности информации.

Фарминг – возможность неправомерного ознакомления нарушителем с защищаемой информацией (в т.ч. идентификации/аутентификации) пользователя путём скрытого перенаправления пользователя на поддельный сайт (выглядящий одинаково с оригинальным), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию.

Фишинг – возможность неправомерного ознакомления нарушителем с защищаемой информацией (в т.ч. идентификации/аутентификации) пользователя путем убеждения его с помощью методов социальной инженерии (в т.ч. посылкой целевых писем (т.н. spear-phishing attack), с помощью звонков с вопросом об открытии вложения письма, имитацией рекламных предложений (fake offers) или различных приложений (fake apps)) зайти на поддельный сайт (похожий на оригинальный), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию или открыть зараженное вложение в письме.

Кибersталкинг – систематическое преследование человека, группы лиц или компании, их запугивание и/или домогательство с использованием интернета и других электронных средств коммуникации.

Хакер - лицо, совершающее различные незаконные действия в сфере информационных технологий: несанкционированное проникновение в чужие компьютерные сети и получение из них информации, незаконные снятие защиты с программных продуктов и их копирование, создание и распространения компьютерных вирусов и т. п.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только управомоченными субъектами.

2. Классификация угроз безопасности персональных данных

11. Состав и содержание угрозы безопасности персональных данных определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным. Совокупность таких условий и факторов формируется с учетом характеристик информационной системы, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы.

12. К характеристикам информационной системы, обусловливающим возникновение угроз безопасности персональных данных, можно отнести категорию и объем обрабатываемых в информационных системах, актуальности угроз, возможности нанесения ущерба, продолжительности обработки персональных данных, структуру

информационных систем, наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена, характеристики подсистемы безопасности персональных данных, обрабатываемых в информационных системах, режимы обработки персональных данных, режимы разграничения прав доступа пользователей информационной системы, местонахождение и условия размещения технических средств информационных систем.

13. Основными элементами информационной системы являются:

1) персональные данные, содержащиеся в базах данных, как совокупность информации и ее носителей, используемых в информационной системе;
2) информационные технологии, применяемые при обработке персональных данных;
3) технические средства, осуществляющие обработку персональных данных (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации);
4) программные средства (операционные системы, системы управления базами данных и т.п.);
5) средства защиты информации;
6) вспомогательные технические средства и системы – технические средства и системы, их коммуникации, не предназначенные для обработки персональных данных, но размещенные в помещениях (далее – служебные помещения), в которых расположены информационные системы, их технические средства (различного рода телефонные средства и системы, средства вычислительной техники, средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, контрольно-измерительная аппаратура, средства и системы кондиционирования, средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения, средства электронной оргтехники, средства и системы электрочасофикации).

14. Свойства среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической среды, в которой распространяются персональные данные, и определяются при оценке возможности реализации угроз безопасности

персональных данных.

15. Возможности источников угроз безопасности персональных данных обусловлены совокупностью способов несанкционированного и (или) случайного доступа к персональным данным, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) персональных данных.

16. Угроза безопасности персональных данных реализуется в результате образования канала реализации угроз безопасности персональных данных между источником угрозы и носителем (источником) персональных данных, что создает условия для нарушения безопасности персональных данных (несанкционированный или случайный доступ).

3. Основные элементы канала реализации угроз безопасности персональных данных

17. Основными элементами канала реализации угроз безопасности персональных данных (рис. 1) являются:

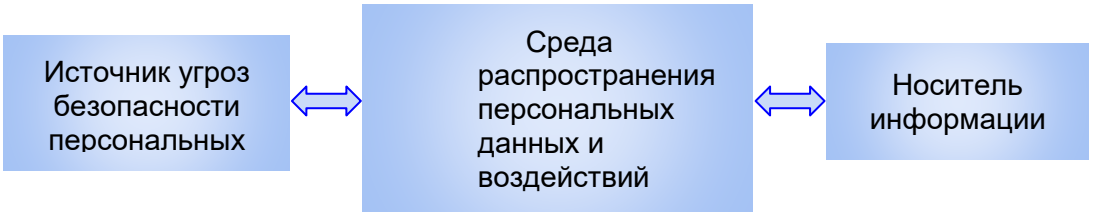

Рис. 1. Обобщенная схема канала реализации угроз безопасности персональных данных

3.1. Источник угроз безопасности персональных данных

18. Все источники угроз безопасности информации можно разделить на три основные группы:

- обусловленные действиями субъекта (антропогенные);
- обусловленные техническими средствами (техногенные);
- обусловленные стихийными источниками (стихийные).

19. Источники угроз могут находиться как внутри защищаемой организации – внутренние источники, так и вне ее – внешние источники.

3.1.1. Антропогенные источники угроз

20. Личность (субъектов может быть несколько), которая имеет возможность совершать операции с конфиденциальной информацией. Доступ может быть как санкционированным, так и несанкционированным. Другими словами, нарушение режима конфиденциальности может быть вызвано как спланированными операциями злоумышленников, так и неопытностью сотрудников. Пользователь должен иметь базовые компетенции в области информационной безопасности, вредоносном программном обеспечении, чтобы своими действиями не нанести ущерб организации и самому себе. Такие инциденты, как потеря или утечка информации, могут также быть обусловлены целенаправленными действиями сотрудников организации, которые заинтересованы в получении прибыли в обмен на данные юрлица, в которой они работают или работали.

21. Основными источниками угроз являются отдельные злоумышленники («хакеры»), группы киберпреступников и иностранные спецслужбы (киберподразделения), которые применяют весь арсенал

доступных кибер средств. Чтобы преодолеть информационную, техническую и физическую защиту и получить доступ к нужной информации, они используют слабые места и ошибки в работе программного обеспечения и веб-приложений, изъяны в конфигурациях средств защиты информации и настройках прав доступа, прибегают к взлому каналов связи и использованию клавиатурных шпионов (закладок).

22. Группы источников угроз персональных данных:

- внутренние – штатные сотрудники, в частности, работники отделов в области информационных технологий, кадровой службы, техперсонал или представители службы безопасности организации. В процессе своей деятельности они могут подвергать средства защиты персональных данных опасности из-за некомпетентности и ошибочных действий, применения неучтенного программного обеспечения, изменения и уничтожения компонентов программ, предоставления доступа неуполномоченным лицам или игнорирования правил хранения персональных данных. Причиной утечки может стать также самовольное изменение параметров системы защиты и сокрытие фактов потери информации, находящейся в ограниченном доступе (паролей, ключей и т.д.).
- внешние – поставщики услуг, работники контролирующих государственных органов и аварийных служб, а также хакеры, представители конкурирующих организаций. Их действия могут быть преднамеренными, то есть направленными на получение сведений, или не специальными, например, если утечка происходит в результате технического сбоя или составления проекта информационной системы с нарушением требований информационной безопасности .

№	**Внутренние**	**Внешние**
1	Штатный персонал: - привилегированный (ИТ, ИБ, разработчики); - непривилегированный (другие пользователи)	Зарубежные спецслужбы или организации (в том числе террористические), а также криминальные группировки
2	Представители службы защиты информации (администраторы)	Преступники и хакеры (хакеры-одиночки и хакерские группы)
3	Вспомогательный персонал (уборщики, охрана)	Недобросовестные партнеры

4	Технический персонал (жизнеобеспечение, эксплуатация)	Технический персонал поставщиков телекоммуникационных услуг
5		Представители надзорных организаций и аварийных служб
6	Представители силовых структур страны	Представители силовых структур других государств

3.1.2. Техногенные источники угроз

23. Эти источники обусловлены применяемыми техническими средствами и бывают двух разновидностей:

- внутренние – это аппаратные закладки, вирусы и прочие вредоносные программы, системы охраны и сигнализации, нелицензионное программное обеспечение и оборудование, задействованное в процессе обработки персональных данных;
- внешние – составляющие инфраструктурного назначения, например, линии телефонной и интернет-связи, системы отопления, канализации, водоснабжения, газоснабжения.

№	Внутренние	Внешние
1	Технические средства обработки информации (компьютерная и иная техника)	Средства связи
2	Программные средства обработки информации не соответствующие государственным и/или международным стандартам	Сети инженерных коммуникаций (водоснабжения, канализации)
3	Вспомогательные средства (охраны, сигнализации, телефонии)	Транспорт
4	Другие технические средства, применяемые в учреждении	

3.1.3. Стихийные источники угроз

24. Наиболее сложно прогнозируемые ввиду огромного разнообразия, причин возникновения и способов проявления. Преимущественно это те факторы, на которые оператор никаким образом не способен повлиять:

- наводнения и сели;
- пожары;
- ураганы;
- гроза, град, снегопад;
- оползни;
- землетрясения;
- военные и политические конфликты;
- акты гражданского неповиновения;
- магнитные бури;
- различные непредвиденные обстоятельства;
- другие форс-мажорные обстоятельства.

3.2. Среда распространения

25. Угрозы безопасности могут быть реализованы тремя путями:

- через технические каналы утечки;
- путем непосредственного доступа;
- шантажа, подкупа, запугивания и жажды личной наживы персонала.

3.3. Носители информации

26. Носители персональных данных могут содержать информацию, представленную в следующих видах:

1) акустическая (речевая) информация, содержащаяся непосредственно в произносимой речи пользователя информационной системы при осуществлении им функции голосового ввода персональных данных в информационную систему, либо воспроизводимая акустическими средствами информационной системы (если такие функции предусмотрены технологией обработки персональных данных), а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;
2) Визуальная информация, представленная в виде текста, видео и изображений различных устройств отображения информации;

3) информация, обрабатываемая (циркулирующая) в информационных системах, в виде электрических, электромагнитных, оптических сигналов;
4) информация, обрабатываемая в информационных системах, представленная в виде бит, байт, файлов и других логических структур.

4. Классификация угроз

27. В целях формирования перечня угроз безопасности персональных данных при их обработке в информационных системах и разработке на их основе отраслевых перечней применительно к конкретному виду информационной системы угрозы классифицируются в соответствии со следующими признаками:

1) по цели реализации угрозы;
2) по виду защищаемой от угроз безопасности персональных данных информации, содержащей персональные данные;
3) по видам возможных источников угроз безопасности персональных данных;
4) по типу информационной системы, на которую направлена реализация угроз безопасности персональных данных;
5) по способу реализации угроз безопасности персональных данных;
6) по виду нарушаемого свойства информации (несанкционированных действиях, осуществляемых с персональными данными);
7) по используемой уязвимости;
8) по объекту воздействия.

28. Рассмотрение каждой классификации угроз по признакам:

1) По **цели реализации угрозы.** Реализация той или иной угрозы безопасности может преследовать следующие цели:

- нарушение конфиденциальной информации;
- нарушение целостности информации;
- нарушение (частичное или полное) работоспособности

2) По **виду** информации, защищаемой от угроз безопасности персональных данных, угрозы делятся на (рис. 2):

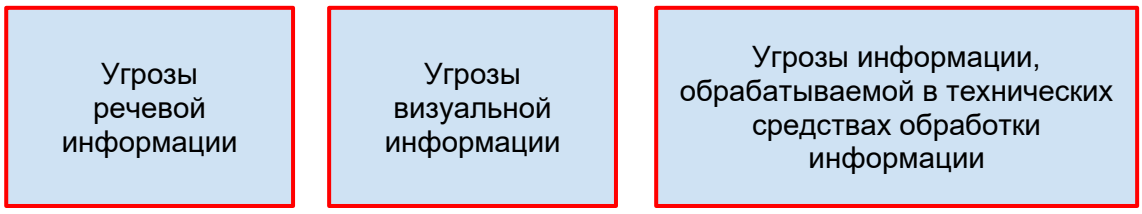

Рис. 2. Виды информации, защищаемой от угроз безопасности персональных данных

3) **Виды возможных источников угроз безопасности персональных данных.** По видам возможных источников угроз безопасности персональных данных выделяются следующие классы угроз (рис. 3):

- угрозы, создаваемые нарушителем;
- аппаратные закладки;
- вредоносные программы.

По наличию права постоянного или разового доступа в контролируемую зону информационной системы нарушители подразделяются на два типа:

- внутренний нарушитель – реализующий угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к информационной системе, включая пользователей информационных систем, реализующих угрозы непосредственно в информационной системе;
- внешний нарушитель – реализующий угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к информационной системе, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Виды и угрозы нарушителя можно найти в Приложении 1.

Рис. 3. Виды возможных источников угроз безопасности персональных данных

4) **Типы информационной системы, на которые направлена реализация угроз безопасности персональных данных.**

По типу информационной системы выделяются следующие классы угроз (рис. 4):

- угрозы безопасности персональных данных, обрабатываемых в информационных системах на базе автономного автоматизированного рабочего места;
- угрозы безопасности персональных данных, обрабатываемых в информационных системах на базе автоматизированного рабочего места, подключенного к сети общего пользования (к сети международного информационного обмена);
- угрозы безопасности персональных данных, обрабатываемых в информационных систем на базе локальных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);
- угрозы безопасности персональных данных, обрабатываемых в информационных системах на базе локальных информационных систем

с подключением к сети общего пользования (к сети международного информационного обмена);

- угрозы безопасности персональных данных, обрабатываемых в информационных систем на базе распределенных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);
- угрозы безопасности персональных данных, обрабатываемых в информационных системах на базе распределенных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена).

Рис. 4. Угрозы безопасности персональных данных, обрабатываемых в информационных системах

5) **Способы реализации угроз безопасности персональных данных;**

По способам реализации выделяются следующие классы угроз:

- угрозы, связанные с доступом к персональным данным (в том числе угрозы внедрения вредоносных программ) (рис. 5);
- угрозы утечки по техническим каналам утечки информации (рис. 6);
- угрозы специальных воздействий на информационные системы (рис. 7);

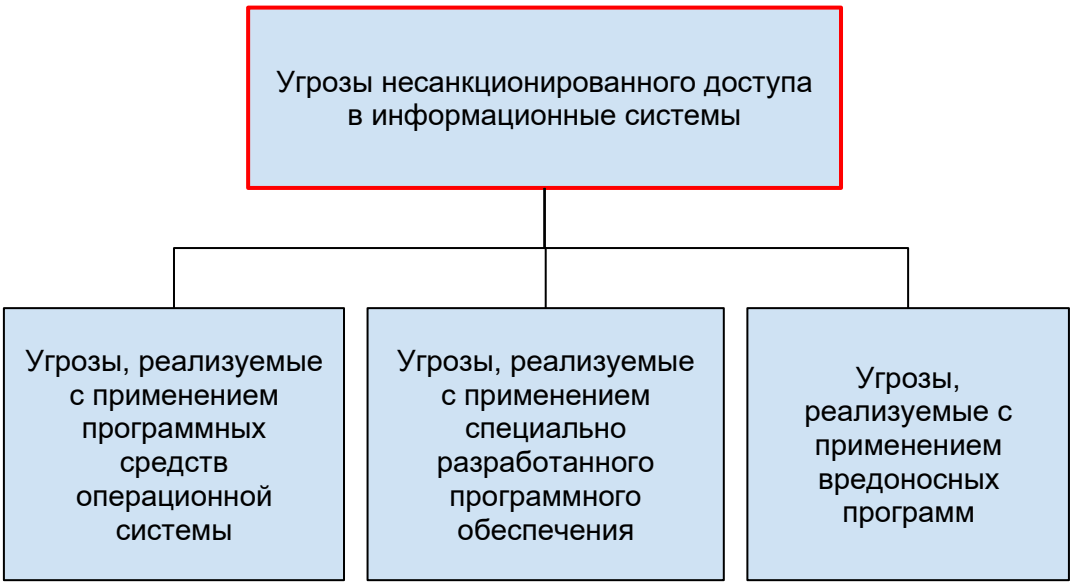

Рис. 5. Угрозы, связанные с несанкционированным доступом к персональным данным

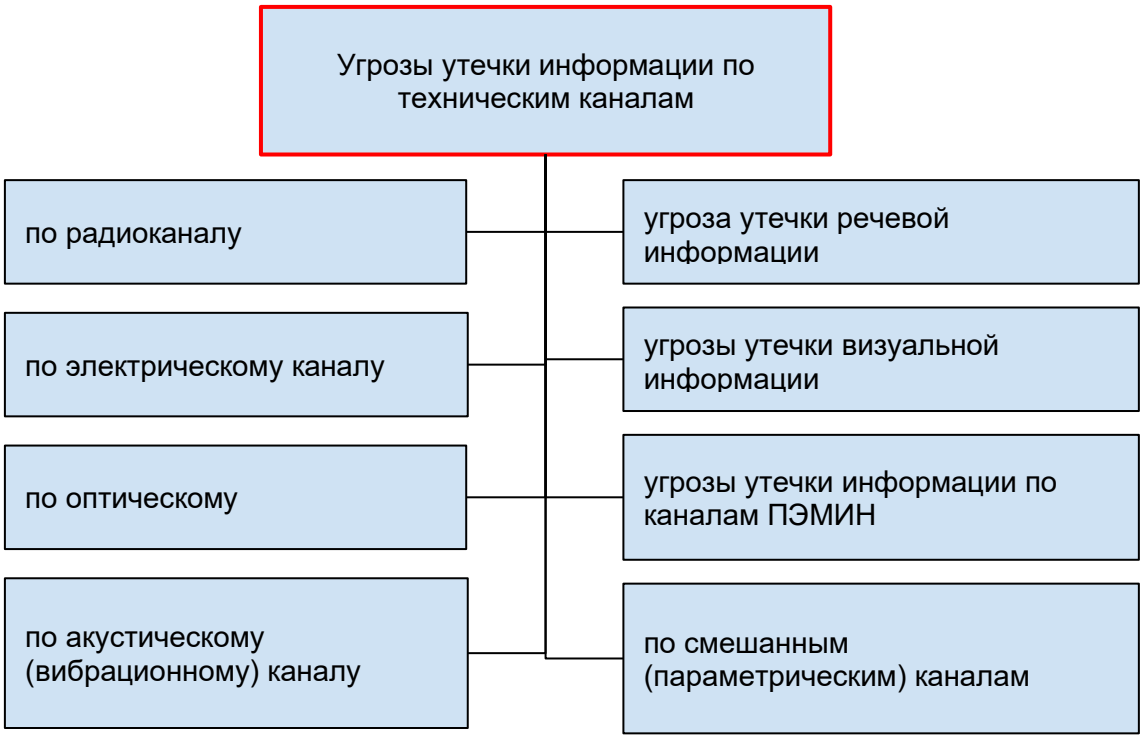

Рис. 6. Угрозы утечки по техническим каналам утечки информации

Рис. 7. Угрозы специальных воздействий на информационные системы

6) По **возможностям реализации атак** угрозы делятся:

- на угрозы, реализуемые в информационных системах при их подключении к сетям связи общего пользования;
- на угрозы, реализуемые в информационных системах при их подключении к сетям международного информационного обмена;
- на угрозы, реализуемые в информационных системах, не имеющих подключений к сетям связи общего пользования и сетям международного информационного обмена.

7) По **видам нарушаемого свойства информации (видам несанкционированных действий, осуществляемых с персональными данными)** выделяются следующие классы угроз (рис. 8):

- угрозы, приводящие к нарушению конфиденциальности персональных данных (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;
- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение персональных данных или их уничтожение;
- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы информационной системы, в результате которого осуществляется блокирование персональных данных.

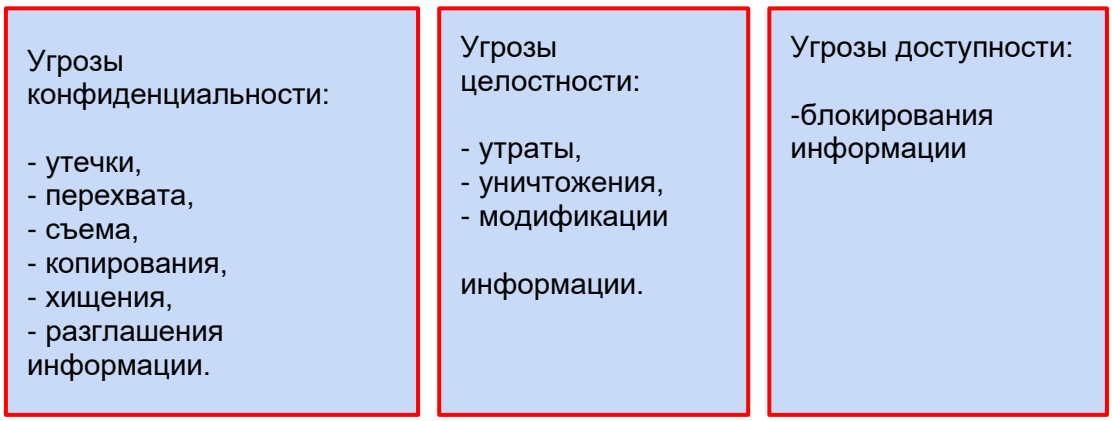

Рис. 8. Угрозы по видам нарушаемого свойства информации

8) По **используемой уязвимости** выделяются следующие классы угроз (рис. 9):

- угрозы, реализуемые с использованием уязвимости системного программного обеспечения;
- угрозы, реализуемые с использованием уязвимости прикладного программного обеспечения;
- угрозы, возникающие в результате использования уязвимости, вызванной наличием в автоматизированных систем программной закладки;
- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;
- угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации технической защиты информации от несанкционированного доступа;
- угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;

- угрозы, реализуемые с использованием уязвимостей средств защиты информации.

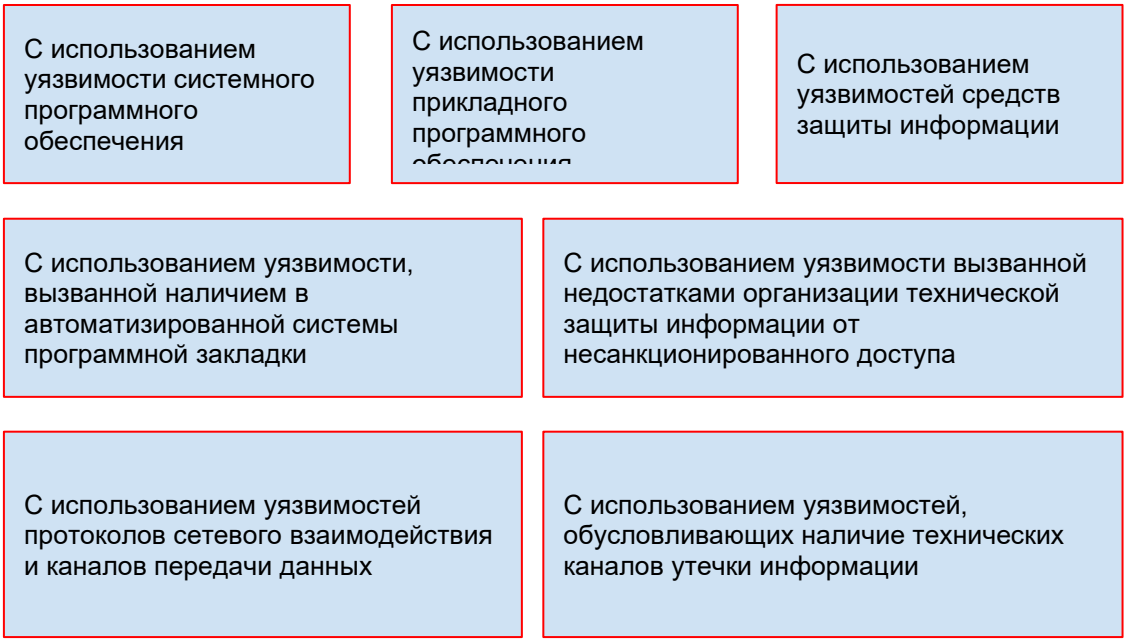

Рис. 9. Угрозы по используемой уязвимости

9) **По объекту воздействия** выделяются следующие классы угроз:

- угрозы безопасности персональных данных, обрабатываемых на автоматизированных рабочих местах (рис. 10);
- угрозы безопасности персональных данных, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.) (рис. 11);
- угрозы безопасности персональных данных, передаваемых по сетям связи (рис. 12);
- угрозы прикладным программам, с помощью которых обрабатываются персональные данные;
- угрозы системному программному обеспечению, обеспечивающему функционирование информационной системы.

Рис. 10. Угрозы безопасности персональных данных, обрабатываемых на автоматизированных рабочих местах

Рис. 11. Угрозы безопасности персональных данных, обрабатываемых в выделенных технических средствах обработки

Рис. 12. Угрозы безопасности персональных данных, передаваемых по сетям связи

29. Реализация одной из угроз безопасности персональных данных перечисленных классов или их совокупности может привести к следующим типам последствий для субъектов персональных данных:

- значительным негативным последствиям для субъектов персональных данных;
- негативным последствиям для субъектов персональных данных;
- незначительным негативным последствиям для субъектов персональных данных.

30. **Основные группы угроз.** В зависимости от различных способов классификации все возможные угрозы информационных систем можно разделить на следующие основные подгруппы.

- нежелательный контент;
- несанкционированный доступ;
- утечки информации;
- потеря данных;
- мошенничество;
- кибервойны.

5. Угрозы утечки информации по техническим каналам

31. Основными элементами описания угроз утечки информации по техническим каналам являются: источник угрозы, среда (путь) распространения информативного сигнала и носитель защищаемой информации.

32. Источниками угроз утечки информации по техническим каналам являются физические лица, а также организации (в том числе, конкурирующие или террористические), криминальные группировки, осуществляющие перехват (съем) информации с использованием технических средств ее регистрации, приема или фотографирования.

33. При обработке персональных данных в информационных системах за счет реализации технических каналов утечки информации возможно возникновение следующих угроз безопасности персональных данных:

- угроз утечки акустической (речевой) информации;
- угроз утечки визуальной информации;
- угроз утечки информации по каналам побочных электромагнитных излучений и наводок.

5.1 Угрозы утечки акустической (речевой) информации

34. Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя информационной системы, при обработке персональных данных в информационных системах, обусловлено наличием функций голосового ввода персональных данных в информационных системах или функций воспроизведения персональных данных акустическими средствами информационной системы.

35. Перехват акустической (речевой) информации в данных случаях возможен с использованием аппаратуры, регистрирующей акустические (в воздухе) и виброакустические (в упругих средах) волны, а также электромагнитные (в том числе оптические) излучения и электрические сигналы, модулированные информативным акустическим сигналом, возникающие за счет преобразований в технических средствах обработки персональных данных, вспомогательных технических средствах и системах, и строительных конструкциях и инженерно-технических коммуникациях под воздействием акустических волн.

36. Кроме этого, перехват акустической (речевой) информации возможен с использованием специальных электронных устройств съема речевой информации, внедренных в технические средства обработки персональных данных, вспомогательных технических средствах и системах

и помещения или подключенных к каналам связи.

37. Перехват акустической (речевой) информации может вестись:

- стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;
- портативной носимой аппаратурой, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;
- портативной носимой аппаратурой – физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них;
- автономной автоматической аппаратурой, скрытно устанавливаемой физическими лицами непосредственно в служебных помещениях или в непосредственной близости от них.

5.2 Угрозы утечки визуальной информации

38. Угрозы утечки визуальной информации реализуются за счет просмотра персональных данных с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы.

39. Просмотр (регистрация) персональных данных также возможен с использованием специальных электронных устройств съема, внедренных в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений.

40. Необходимым условием осуществления просмотра (регистрации) персональных данных является наличие визуального контакта между средством наблюдения и держателем / обработчиком персональных данных.

41. Перехват персональных данных может вестись:

- стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;
- портативной носимой аппаратурой, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;
- портативной носимой аппаратурой – физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них.

42. Перехват (просмотр) персональных данных может

осуществляться посторонними лицами путем их непосредственного наблюдения в служебных помещениях либо с расстояния прямой видимости из-за пределов информационной системы с использованием оптических (оптико электронных) средств.

5.3 Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок

43. Возникновение угрозы персональных данных по каналам побочных электромагнитных излучений и наводок возможно за счет перехвата техническими средствами побочных (не связанных с прямым функциональным значением элементов информационной системы) информативных электромагнитных полей и электрических сигналов, возникающих при обработке персональных данных техническими средствами информационной системы.

44. Генерация информации, содержащей персональные данные и циркулирующей в технических средствах информационной системы в виде электрических информативных сигналов, обработка и передача указанных сигналов в электрических цепях технических средств информационной системы сопровождается побочными электромагнитными излучениями, которые могут распространяться за пределы служебных помещений в зависимости от мощности излучений и размеров информационной системы.

45. Регистрация побочных электромагнитных излучений и наводок осуществляется с целью перехвата информации, циркулирующей в технических средствах, обрабатывающих персональные данные(в средствах вычислительной техники, информационно-вычислительных комплексах и сетях, средствах и системах передачи, приема и обработки персональных данных, в том числе в средствах и системах звукозаписи, звукоусиления, звуковоспроизведения, переговорных и телевизионных устройствах, средствах изготовления, тиражирования документов и других технических средствах обработки речевой, графической, видео- и буквенно-цифровой информации).

46. Для регистрации побочных электромагнитных излучений и наводок используется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информации.

47. Кроме этого, перехват побочных электромагнитных излучений и наводок возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки персональных данных.

48. Регистрация побочных электромагнитных излучений и наводок может вестись с использованием аппаратуры следующих видов:

- стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;

- портативной возимой аппаратуры, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;
- портативной носимой аппаратурой – физическими лицами в непосредственной близости от информационной системы;
- автономной автоматической аппаратурой, скрытно устанавливаемой физическими лицами в непосредственной близости от информационной системы.

49. Каналы утечки информации, обусловленные наводками, образуются за счет соединительных линий технических средств информационных систем и вспомогательные технические средства и системы и посторонних проводников (в том числе цепей электропитания и заземления).

50. Наводки электромагнитных излучений технических средств информационной системы возникают при излучении элементами технических средств информационной системы информативных сигналов при наличии емкостной, индуктивной или гальванической связей соединительных линий технических средств информационной системы, линий вспомогательных технических средств и систем и посторонних проводников. В результате на случайных антеннах (цепях вспомогательных технических средств и систем или посторонних проводниках) наводится информативный сигнал.

51. Прохождение информативных сигналов в цепи электропитания возможно при наличии емкостной, индуктивной или гальванической связи источника информативных сигналов в составе технических средств информационных систем и цепей питания.

52. Прохождение информативных сигналов в цепи заземления обусловлено наличием емкостной, индуктивной или гальванической связи источника информативных сигналов в составе аппаратуры технических средств приема, обработки, хранения и передачи информации и цепей заземления.

53. Для съема информации с проводных линий могут использоваться:

- средства съема сигналов, содержащих защищаемую информацию, с цепей технических средств информационных систем и вспомогательных технических средств и систем, линий связи и передачи данных, выходящих за пределы служебных помещений (эквиваленты сети, токовые трансформаторы, пробники);
- средства съема наведенных информативных сигналов с цепей электропитания;
- средства съема наведенных информативных сигналов с шин заземления;

- средства съема наведенных информативных сигналов с проводящих инженерных коммуникаций.

54. Для волоконно-оптической системы передачи данных угрозой утечки информации является утечка оптического излучения, содержащего защищаемую информацию, с боковой поверхности оптического волокна.

55. В каналах сотовой связи, спутниковых и беспроводных сетей передачи данных характерно применение специализированных систем и средств контроля и перехвата информации, ориентированных на используемые в них информационные технологии, в том числе средств:

- перехвата сообщений и сотовой связи;
- перехвата информации в каналах передачи данных вычислительных сетей.

6. Угрозы несанкционированного доступа к информации в информационной системе

56. Угрозы несанкционированного доступа (НСД) в информационную систему с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного, доступа, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированное распространение), целостности (уничтожение, изменение) и доступности (блокирование) персональных данных, и включают в себя:

- угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);
- угрозы создания нештатных режимов работы программных (программно- аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
- угрозы внедрения вредоносных программ (программно-математического воздействия).

57. Кроме этого, возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для несанкционированного доступа в операционную среду компьютера, в том числе путем формирования нетрадиционных информационных каналов доступа.

58. Угрозы доступа (проникновения) в операционную среду информационной системы с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и программно-аппаратных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

59. Эти угрозы реализуются относительно информационной системы как на базе автоматизированного рабочего места, не включенного в сети связи общего пользования, так и применительно ко всем информационным системам, имеющим подключение к сетям связи общего пользования и сетям международного информационного обмена.

60. Описание угроз доступа (проникновения) в операционную среду компьютера формально может быть представлено следующим образом:

угроза НСД в информационной системе: = <источник угрозы>, <уязвимость в информационной системе>, <способ реализации угрозы>, <объект воздействия (программа, протокол, данные и др.)>, <деструктивное действие или несанкционированный доступ>.

61. Угрозы создания нештатных режимов работы программных (программно- аппаратных) средств – это угрозы «Отказа в обслуживании». Как правило, данные угрозы рассматриваются применительно к информационной системе на базе локальных и распределенных информационных систем вне зависимости от подключения информационного обмена. Их реализация обусловлена тем, что при разработке системного или прикладного программного обеспечения не учитывается возможность преднамеренных действий по целенаправленному изменению:

- содержания служебной информации в пакетах сообщений, передаваемых по сети;
- условий обработки данных (например, игнорирование ограничений на длину пакета сообщения);
- форматов представления данных (с несоответствием измененных форматов, установленных для обработки по протоколам сетевого взаимодействия);
- программного обеспечения обработки данных.

62. В результате реализации угроз «Отказа в обслуживании» могут возникнуть следующие последствия:

- переполнение буферов;
- блокирование процедур обработки;
- «зацикливание» процедур обработки;
- «зависание» компьютера;
- отбрасывание пакетов сообщений и др.

Описание таких угроз формально может быть представлено следующим образом:

угроза «Отказа в обслуживании»: = <источник угрозы>, <уязвимость в информационной системе>, <способ реализации угрозы>, <объект воздействия >, <непосредственный результат реализации угрозы (переполнение буфера, блокирование процедуры обработки, «зацикливание» обработки и т.п.)>.

63. Угрозы внедрения вредоносных программ нецелесообразно описывать с той же детальностью, что и вышеуказанные угрозы. Это обусловлено тем, что, во-первых, количество вредоносных программ сегодня уже значительно превышает сто тысяч. Во-вторых, при организации

защиты информации на практике, как правило, достаточно лишь знать класс вредоносной программы, способы и последствия от ее внедрения. В связи с этим угрозы программно-математического воздействия формально могут быть представлены следующим образом:

> *Угроза воздействия вредоносных программ в информационной системе: = <класс вредоносной программы (с указанием среды обитания: файловые, загрузочные и сетевые)>, <источник угрозы (носитель вредоносной программы)>, <способ инфицирования>, <объект воздействия (загрузочный сектор, файл и т.п.)>, <описание возможных деструктивных действий>,<дополнительная информация об угрозе (резидентность, скорость распространения, полиморфичность и др.)>.*

7. Классификация уязвимостей программных систем

64. В настоящее время можно встретить ряд как простых, так и сложных иерархических классификаций (таксономий) в области программной безопасности, которые можно разделить на следующие:

- классификации угроз и атак;
- классификации вредоносных программ;
- классификации и реестры уязвимостей;
- классификации дефектов.

7.1 Классификация угроз и атак

65. Данные классификации систематизируют различные виды искусственных и естественных, случайных или злонамеренных, внутренних и внешних угроз по различным параметрам. Классификации выделяют класс угроз, связанный с возможностью реализации нарушителем программных уязвимостей. При всем этом данные классификации являются основой для построения моделей угроз безопасности информации

7.2 Классификация вредоносных программ

66. Вредоносные программы можно разбить на группы, для определения вида программы, и запуска алгоритмов борьбы с установленным видом вредоносной программы. Классы вредоносных программ указаны на рис. 13. В Таблице 1 дается название, определение и реализация вредоносных программ.

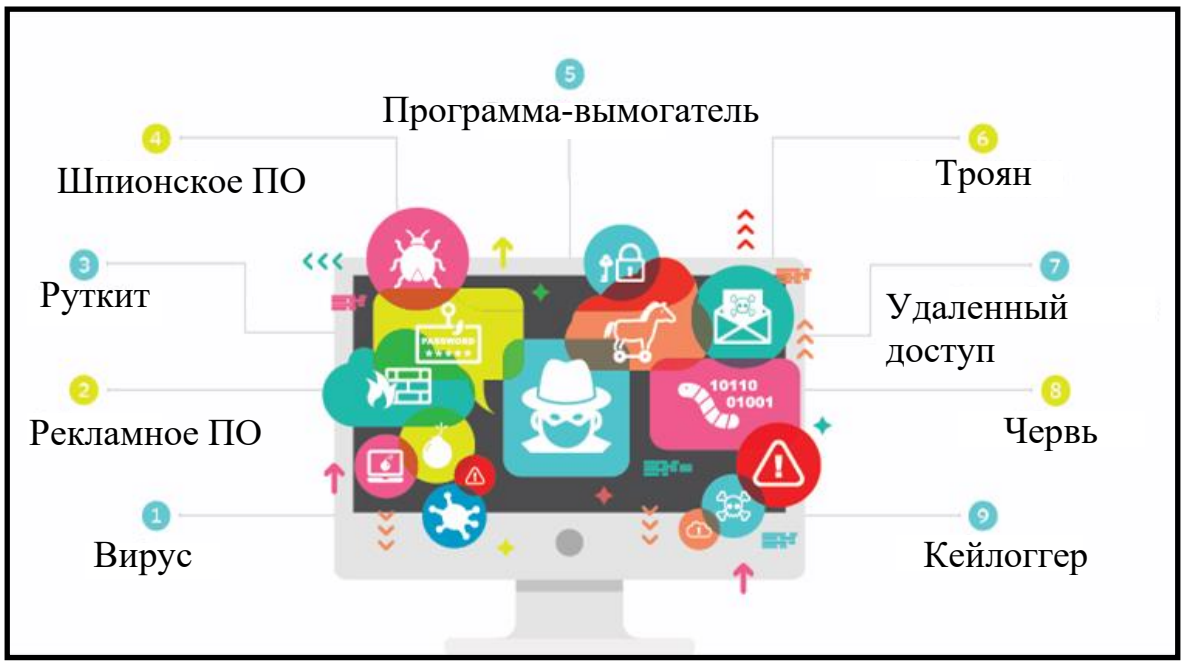

Рисунок 13. Классы вредоносных программ

Таблица 1. Определение и реализация вредоносных программ

№	Название	Определение и реализация
1	Вирус	Самовоспроизводящийся программный код, который внедряется в установленные программы. Вирусы можно разделить по типу объектов, которые они заражают, по методам заражения и выбора жертв. Вирусы могут быть внедрены разными способами: от нажатия на вредоносную ссылку или файл в известном письме до заражения на вредоносном сайте. При этом вирус может выполнять множество разных задач, направленных в первую очередь на принесение вреда операционной системе. Вирусы имеют такие особенности, как: − способность к саморазмножению; − высокой скорости распространения; − избирательности поражаемых систем (каждый вирус поражает только определенные системы или однородные группы систем); − наличию в большинстве случаев определенного инкубационного периода; − способности «заражать» еще не зараженные системы; Среда обитания: − Сетевые - распространяются по компьютерной сети; − Файловые - внедряются в выполняемые файлы; − Загрузочные - внедряются в загрузочный сектор диска (Boot-сектор)
2	Рекламное программное обеспечение	Приложение, которое навязывает рекламу пользователю и/или собирает информацию о поведении пользователя в Интернет. Рекламное программное обеспечение является одним из наиболее известных типов вредоносных программ. Он показывает всплывающие окна и медийную рекламу. Также рекламные объявления ссылаются на сайты, с вредоносными файлами и ссылками. Рекламное программное обеспечение также может доставлять шпионское программное обеспечение, что делает устройства, на которых оно установлено, доступными для хакеров, фишеров и мошенников. Рекламное программное обеспечение может быть установлено с ведома пользователя либо без его согласия, а также может предлагаться пользователю в одном из пунктов лицензионных прав на использование нелицензированного или неофициального программного обеспечения.
3	Руткит	Средство сокрытия вредоносной деятельности. Руткит модифицирует операционную систему, чтобы создать бэкдор. Затем злоумышленники используют бэкдор для удаленного доступа к компьютеру. Большинство руткитов используют уязвимости программного обеспечения для изменения системных файлов.

4	Шпионское программное обеспечение	Программа, установленная на компьютере, о наличии которой пользователь обычно не знает и которая получает доступ, отслеживает, собирает и передает личную информацию или шаблоны поведения пользователя. Шпионская программа позволяет ее владельцам отслеживать все формы связи на устройстве жертвы. Шпионские программы часто используются для проверки и отслеживания сообщений в конфиденциальной среде или в ходе расследования.
5	Программы-вымогатели	Программы-вымогатели устанавливаются на компьютер жертвы, шифруют файлы или блокируют доступ к операционной системе, а затем требуют выкуп за возврат этих данных пользователю или разблокирование доступа. Виды и примеры программ вымогателей приведены в Приложении 2.
6	Троянский конь, троян (троянская программа)	Широкий класс вредоносных объектов разнообразного назначения, которые обычно не имеют собственного механизма распространения (т.е. не могут заражать файлы или размножать свои копии через сеть). По своему действию является противоположностью вирусам и червям. Его предлагают загрузить под видом законного приложения, однако вместо заявленной функциональности он делает то, что нужно злоумышленникам. Трояны не самовоспроизводятся и не распространяются сами по себе. Однако с увеличением информации и файлов в Интернете трояна стало довольно легко подцепить. Виды и примеры троянских приложений приведены в Приложении 3.
7	Бэкдор	Бэкдор обходит обычную аутентификацию, используемую для доступа к системе. Целью бэкдора является предоставление злоумышленнику доступа к системе в будущем, даже если организация исправит первоначальную уязвимость, использованную для атаки на систему.
8	Червь	Вредоносные программы с самой разной функциональной нагрузкой, которые способны самостоятельно распространяться по компьютерным сетям. Черви являются в некотором роде вирусами, так как созданы на основе саморазмножающихся программ. Однако черви не могут заражать существующие файлы. Вместо этого червь поселяется в компьютер отдельным файлом и ищет уязвимости в Сети или системе для дальнейшего распространения себя. Черви также могут подразделяться по способу заражения (электронная почта, мессенджеры, обмен файлами и пр.). Некоторые черви существуют в виде сохраненных на жестком диске файлов, а некоторые поселяются лишь в оперативной памяти компьютера.
9	Кейлоггер	Регистраторы нажатий клавиш или системный мониторинг – это

		тип вредоносных программ, используемых для отслеживания и записи каждого нажатия клавиши на клавиатуре определенного компьютера. Кейлоггеры – Keylogger записывают все, что пользователь вводит в своей компьютерной системе, чтобы получить пароли и другую конфиденциальную информацию и отправить их источнику программы кейлоггинга.

7.2.1 Как распространяется вредоносное программное обеспечение?

67. Существует шесть распространенных способов распространения вредоносных программ:

1) Уязвимости: дефект безопасности в программном обеспечении позволяет вредоносным программам использовать его для получения несанкционированного доступа к компьютеру, оборудованию или сети.
2) Бэкдоры: преднамеренные или непреднамеренные бреши в программном обеспечении, оборудовании, сетях или системе безопасности.
3) Попутные загрузки: непреднамеренная загрузка программного обеспечения с ведома или без ведома конечного пользователя.
4) Однородность: если все системы работают под управлением одной и той же операционной системы и подключены к одной и той же сети, повышается риск успешного распространения червя на другие компьютеры.
5) Повышение привилегий: ситуация, когда злоумышленник получает расширенный доступ к компьютеру или сети, а затем использует его для организации атаки.
6) Смешанные угрозы: пакеты вредоносных программ, которые сочетают в себе характеристики нескольких типов вредоносных программ, что затрудняет их обнаружение и остановку, поскольку они могут использовать различные уязвимости.

7.2.2 Распространенные формы атак вредоносных программ

Таблица 2. Распространенные формы атаки

№	Атака	Реализация
1	Фишинговые и социальные инженерные атаки	Фишинг включает в себя отправку электронных писем, коротких сообщений, которые кажутся отправленными из надежных источников. Цель состоит в том, чтобы получить доступ к конфиденциальной информации или распространить

		вредоносное программное обеспечение.
2	Целевой фишинг	Целевой фишинг имеет тот же результат что и фишинг, но использует более сфокусированный подход. Эти атаки требуют дополнительных исследований отдельных лиц или целевых групп пользователей. Например, проведя небольшое онлайн-исследование, злоумышленник может определить адреса электронной почты жертвы или номер с сети оператора сотовой связи и отправить то, что кажется законным электронным письмом или сообщением, в том числе в виде СМС или в Мессенджер из надежного источника, которое содержит инструкцию или поля для заполнения, а также ссылку на загрузку файла (вредоносное программное обеспечение) или даже просьбу передать данные для входа в систему злоумышленнику.
3	Фарминг	Автоматическое перенаправление пользователей на фальшивые сайты с целью хищения конфиденциальной информации, например, паролей и доступов к банковским счетам, доступов в информационную систему обрабатывающую конфиденциальную информацию в том числе персональных данные. Фарминг имеет дело с инструкциями, с помощью которых компьютер пытается найти запрошенный пользователем веб-сайт, для того чтобы незаметно направить пользователя на «фальшивый» веб-сайт. Зачастую фишинговые веб-сайты трудно визуально отличить от подлинного веб-сайта. В отличие от фишинга, фарминг-атаки практически не требуют выполнения каких-либо действий со стороны потенциальной жертвы. При проведении фарминг-атак злоумышленники используют уязвимости в браузерах, операционных системах, а также программном обеспечении DNS-серверов.
4	Отказ в обслуживании - DoS и DDoS-атака	DoS (Denial-of-Service) – отказ в обслуживании. DDoS (Distributed Denial-of-Service) – распределенный отказ в обслуживании. DDoS-атака (от англ. Distributed Denial-of-Service) – это атака на компьютерную систему, цель которой – вызвать отказ от обслуживания пользователей (нарушение доступности). Технология проведения DDoS-атаки – большой поток запросов от различных пользователей к системе, вследствие чего система зависает и не может обслуживать все запросы. Чаще всего злоумышленники для DDoS-атак используют собственные ботнеты. Категории DoS и DDoS атак приведены в Приложении 4. Классификации и цели DDoS-атак по уровням OSI приведены в Приложении 5.
5	Агенты ботнетов	Ботнетом называется группа зараженных компьютеров, получающих команды от злоумышленника; за прием и

		исполнение этих команд отвечает соответствующая вредоносная программа. Такая сеть может насчитывать от нескольких единиц до миллионов компьютеров, а также, иных физических объектов, подключенных к интернету и обменивающихся данными, она также называется зомби-сетью.
6	Атака «человек посередине» (Man-in-the-middle attack) - MitM	Это атака, когда хакер внедряется между двумя законными хостами. Это кибер-эквивалент подслушивания частного разговора. На самом деле, атака подслушивания сама по себе является распространенным типом атаки. Но атака MitM идет еще дальше. Атака MitM имеет дополнительную злонамеренность, заключающуюся в том, что она маскируется под одного или обоих говорящих людей. Это означает, что он не просто перехватывает и прослушивает сообщения между клиентами и серверами. Он также может изменять сообщения и запросы на установку, которые кажутся исходящими из законного источника. Общеизвестно, что такие атаки трудно обнаружить, но есть превентивные меры, которые вы можете предпринять.
7	SQL-инъекции - Внедрение языка структурированных запросов	Внедрение языка структурированных запросов (SQL) – это когда вредоносный код вставляется в базу данных SQL. Для злоумышленника это может быть так же просто, как отправить вредоносный код в окно поиска веб-сайта. После запуска кода он может читать, изменять или удалять данные. Некоторые атаки SQL могут даже отключить базу данных и выдать команды операционной системе.
8	Эксплойты	Эксплойты – хакерские утилиты, предназначенные для эксплуатации уязвимостей в программном обеспечении
9	Межсайтовый скриптинг (XSS) - Cross-site Scripting	Тип уязвимости веб-сайта, при которой вредоносный скрипт внедряется в сайт или приложение, который затем устанавливает вредоносное ПО в браузер жертвы. Используя межсайтовый скриптинг, хакеры не нацеливаются на конкретных пользователей, а распространяют свой вредоносный код бесчисленному количеству случайных пользователей.
10	Брутфорс атака	Метод взлома учетных записей путем подбора паролей, который включает в себя угадывание и подбор имен пользователей и паролей для получения несанкционированного доступа к системе или конфиденциальным данным.
11	Спуфинг	Спуфинг - это технический прием выдачи себя за другое лицо, чтобы обмануть сеть или конкретного пользователя с целью вызвать доверие в надежность источника информации. К примеру, хакеры посредством email спуфинга могут ввести пользователя в заблуждение относительно подлинности

		отправителя и получить доступ к конфиденциальным данным. Или они могут попытаться применить технику спуфинга IP и DNS-запросов, чтобы обмануть сеть пользователя и переадресовать его на мошеннические сайты, маскирующиеся под настоящие, в результате чего компьютер пользователя будет заражен..
12	Тайная загрузка (Drive-by attack)	Заключается в распространении вредоносного ПО. Злоумышленники ищут незащищенные сайты и внедряют вредоносные скрипты в их HTTP- или PHP-код. Этот скрипт может установить вредоносное ПО напрямую на компьютер пользователя, посетившего сайт или создать IFRAME-форму, которая перенаправляет жертву на сайт, контролируемый злоумышленниками. Для успеха атаки жертве не нужно выполнять никаких действий: достаточно посетить зараженный ресурс. Тайная загрузка может использовать преимущества операционной системы, веб-браузера или приложения, которые имеют уязвимости (из-за отсутствия обновлений безопасности). Он может быть передан, когда пользователь просто просматривает электронную почту, всплывающее окно или веб-сайт.
13	Кибersталкинг	Информационное преследование жертвы: отслеживают ее местонахождение и действия в виртуальном и реальном мире. Установка GPS-устройств на машины жертв, установка шпионского программного обеспечения на мобильные и стационарные устройства субъектов персональных данных, а также навязчивая слежка за перемещениями объектов кибersталкинга посредством социальных сетей с целью запугать жертву или воздействовать на психику. Например, злоумышленник может выслеживать жертву через социальные сети, издеваться над ним, отправлять сообщения с угрозами или даже взломать почту и общаться с контактами жертвы, а также использовать персональные данные жертвы, чтобы создать поддельный профиль в социальных сетях или блог, в том числе для организации мероприятий по промышленному шпионажу или отмыванию преступных доходов и финансированию террористической деятельности.
14	Атака холодной загрузки (Cold boot attack)	Тип атаки по побочному каналу, при которой злоумышленник с физическим доступом к компьютеру выполняет дамп памяти (сохранение памяти) из оперативной памяти (RAM) компьютера, выполняя аппаратный сброс целевой машины. Атака основывается на свойстве остаточных данных для DRAM и SRAM для извлечения содержимого памяти, которое остается доступным для чтения в течение от секунд до минут после подачи питания. был удален. Злоумышленник, имеющий физический доступ к работающему компьютеру, обычно выполняет атаку с холодной загрузкой,

		перезагружая машину и загружая облегченную операционную систему со съемного диска для сброса содержимое предзагрузочной физической памяти в файл. Затем злоумышленник может проанализировать данные , выгруженные из памяти, чтобы найти конфиденциальные данные, такие как ключи, используя различные формы атак по поиску ключей. Поскольку атаки с «холодной загрузкой» нацелены на оперативную память, схемы полного шифрования диска, даже с установленным модулем доверенной платформы, неэффективны против этого вида атак. Это связано с тем, что проблема заключается в основном в аппаратном (небезопасная память), а не в программном.

7.3 Классификации и реестры уязвимостей

68. Появление потенциальных угроз безопасности связано с наличием уязвимостей в информационной системе.

69. Причинами возникновения уязвимостей в общем случае являются:

- ошибки при разработке программного обеспечения;
- преднамеренные изменения программного обеспечения с целью внесения уязвимостей;
- неправильные настройки программного обеспечения;
- несанкционированное внедрение вредоносных программ;
- неумышленные действия пользователей;
- сбои в работе программного и аппаратного обеспечения.

70. Уязвимости, как и угрозы, можно классифицировать по различным признакам:

- по типу программного обеспечения – системное или прикладное.
- по этапу жизненного цикла программного обеспечения, на котором возникла уязвимость – проектирование, эксплуатация и пр.
- по причине возникновения уязвимости, например, недостатки механизмов аутентификации сетевых протоколов.
- по характеру последствий от реализации атак – изменение прав доступа, подбор пароля, вывод из строя системы в целом и пр.

71. Наиболее часто используемые уязвимости относятся к протоколам сетевого взаимодействия и к операционным системам, в том числе к прикладному программному обеспечению.

72. Уязвимости операционной системы и прикладного программного обеспечения в частном случае могут представлять:

- функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;
- фрагменты кода программ (“дыры”), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;
- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

73. Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др. Так, например, протокол прикладного уровня FTP, широко используемый в Интернете, производит аутентификацию на базе открытого текста, тем самым позволяя перехватывать данные учетной записи. Краткая характеристика этих уязвимостей применительно к протоколам приведена в Приложении 6.

74. Данные об уязвимостях разрабатываемого и распространяемого прикладного программного обеспечения собираются, обобщаются и анализируются в базе данных MITRE CVE.

75. Реестры уязвимостей обусловлены потребностью в регулярном распространении бюллетеней и сводок о найденных уязвимостях для каждого типа и версии программных продуктов и сред. Такие реестры поддерживаются как крупными разработчиками программных обеспечений (например Adobe, Microsoft, RedHat), так и различными ассоциациями (US-CERT, Secunia, Open Security Foundation). Последние создали ряд реестров, группирующих в единой системе идентификаторов (например, CVE-ID) уязвимости программных обеспечений различных разработчиков.

76. Стандарт **Common Vulnerabilities and Exposures (CVE)**[1], разработанный американской некоммерческой исследовательской корпорацией MITRE Corporation в 1999 году, де-факто является на сегодняшний день основным стандартом в области унифицированного именования и регистрации обнаруженных уязвимостей программного обеспечения. Данный стандарт непосредственно определяет как формат идентификаторов и содержимого записей об отдельных обнаруженных

1 Более подробно см. http://cve.mitre.org.

уязвимостях, так и процесс резервирования идентификаторов для новых обнаруженных уязвимостей и пополнения соответствующих баз данных.

- CVE List – реестр уязвимостей MITRE Corporation;
- NVD (National Vulnerability Database) – база данных уязвимостей Национального института технологий и стандартов США.

77. **MITRE Att&ck** (Adversarial Tactics, Techniques & Common Knowledge – «тактики, техники и общеизвестные факты о злоумышленниках») – основанная на реальных наблюдениях база знаний организации MITRE, содержащая описание тактик, приемов и методов, используемых киберпреступниками.[2]

78. Информация в базе знаний MITRE Att&ck представлена в виде матриц, каждая из которых представляет собой таблицу, в которой заголовки столбцов соответствуют тактикам киберпреступников, то есть основным этапам кибератаки или подготовки к ней, а содержимое ячеек – методикам реализации этих тактик, или техникам. Так, если сбор данных согласно MITRE Att&ck – это тактика атаки, то способы сбора, например автоматический сбор или сбор данных со съемных носителей – это техники.

79. Матрицы MITRE Att&ck объединены в четыре группы:

- PRE-ATT&CK – тактики и техники, которые злоумышленники используют на этапе подготовки к кибератаке.
- Enterprise – тактики и техники, которые злоумышленники применяют в ходе атаки на предприятия. В этой группе доступна как сводная матрица, так и отдельные матрицы, содержащие тактики и техники кибератак на конкретные операционные системы и облачные сервисы.
- Mobile – тактики и техники, которые злоумышленники используют в ходе атаки на мобильные устройства под управлением iOS и Android.
- Att&ck for ICS – тактики и техники, которые используются в атаках на промышленные системы управления.

80. Матрица MITRE Att&ck содержит набор методов, используемых злоумышленниками для достижения конкретной цели. Эти цели классифицируются как тактика в матрице Att&ck. Цели представлены линейно от точки разведки до конечной цели эксфильтрации или «воздействия». Выделяют следующие тактики злоумышленников:

1) Первоначальный доступ: попытка проникнуть в сеть, т.е. целевой фишинг.
2) Выполнение: попытка запуска вредоносного кода, т.е. запуск инструмента удаленного доступа.

2 Ознакомиться с матрицами MITRE Att&ck для предприятия можно по адресу: https://attack.mitre.org/

3) Настойчивость: попытка удержать свои точки опоры, т.е. изменение конфигурации.
4) Повышение привилегий: попытка получить разрешения более высокого уровня, т. е. использование уязвимости для повышения уровня доступа.
5) Уклонение от защиты: попытка избежать обнаружения, т.е. использование доверенных процессов для сокрытия вредоносных программ.
6) Доступ к учетным данным: кража имен учетных записей и паролей, т.е. Кейлоггинг
7) Обнаружение: попытка выяснить ваше окружение, т.е. изучение того, что они могут контролировать.
8) Боковое перемещение: перемещение по вашей среде, т.е. Использование законных учетных данных для поворота через несколько систем.
9) Сбор: сбор данных, представляющих интерес для цели противника, т.е. Доступ к данным в облачном хранилище.
10) Эксфильтрация: Злоумышленник пытается украсть данные.
11) Командование и управление: взаимодействие со скомпрометированными системами для управления ими, т.е. имитация обычного веб-трафика для связи с сетью-жертвой.
12) Воздействие: манипулирование, прерывание или уничтожение систем и данных, т. е. шифрование данных с помощью программ-вымогателей.
13) Разведка: сбор информации для планирования будущих операций противника, т.е Информация о целевой организации.
14) Развитие ресурсов: создание ресурсов для поддержки операций, т.е. создание инфраструктуры управления и контроля.

81. В каждой тактике матрицы MITRE Att&ck есть приемы противника, которые описывают реальную деятельность, осуществляемую противником. У некоторых техник есть подтехники, которые более подробно объясняют, как противник выполняет конкретную технику.

82. **База OSVDB** была запущена в 2004 году. Одним из косвенных результатов деятельности коллектива исследователей, причастных к развитию базы OSVDB, стало основание в 2005 году организации Open Security Foundation. Ее целью является поиск уязвимостей и агрегация публично доступной информации об обнаруженных уязвимостях или сценариях их эксплуатации.

83. OSVDB на постоянной основе продолжается поддержка проекта (https://blog.osvdb.org). При этом сотрудничество организации Open Security Foundation и коммерческой компании Risk Based Security привело к

созданию каталога уязвимостей VulnDB, как коммерческой реинкарнации OSVDB.

84. По состоянию на 2018 год доступная по платной подписке в виде сервиса база VulnDB (https://vulndb.cyberriskanalytics.com/) содержит информацию о 176 тыс. обнаруженных уязвимостях (включая почти 60 тыс. записей об уязвимостях, отсутствующих в базах CVE List и NVD), а поддерживающие базу специалисты отслеживают появление новых уязвимостей для 19 тыс. современных программных продуктов и 2 тыс. популярных библиотечных компонентов.

85. Одной из основных организаций отвечающих за обеспечение информационной безопасности в ключевых системах информационной инфраструктуры, включая компьютерные сети органов государственной власти и компьютерные сети критичных объектов инфраструктуры и предприятий на территории СНГ, является российская Федеральная служба по техническому и экспортному контролю – ФСТЭК России.

86. Для обеспечения деятельности по сертификации средств защиты информации и обнаружения уязвимостей программного обеспечения, ФСТЭК России с 2014 года поддерживает собственный реестр известных угроз информационной безопасности и уязвимостей программного обеспечения – Банк данных угроз безопасности информации.

7.4 Классификация дефектов

87. Данный вид касается систематизации дефектов безопасности программного обеспечения при исследовании исходного кода программного обеспечения. В отличие от известных описанных уязвимостей (внесенных в реестры) дефекты представляют собой внутреннее свойство каждой реализации программного обеспечения или системы.

88. Большая часть дефектов возникает в процессе создания программного обеспечения. Это могут быть ошибки проектирования, ошибки кодирования программистов, ошибки, допущенные при сборке дистрибутива и интеграции различных версий компонентов программного обеспечения.

89. Некоторые таксономии включают понятие дефектов информационной системы, которые связаны с конфигурацией системы и вызваны либо ошибками администраторов (например, неверными настройками схемы аутентификации, несвоевременной установкой обновлений операционной системы или сетевых сервисов), либо ошибками операторов информационных систем(например, слабыми паролями в учетной записи, некорректным выключением компьютера).

90. В табл. 3. представлены популярные классификации в области безопасности программного обеспечения. Из табл. 3. видно, что в настоящее

время известно достаточно большое количество таксономий в области информационной безопасности, но в основном они ориентированы на конкретные задачи, будь то сетевые атаки, уязвимости операционных систем или некорректности программирования.

Таблица 3. Классификации в области безопасности программного обеспечения

Вид	**Примеры**	**Особенности**
Классификации вредоносного программного обеспечения	Mitre MAEC (Malware Attribute Enumeration and Characterization) – перечень и характеристики признаков вредоносного программного обеспечения	Язык для описания вредоносного программного обеспечения, учитывающий признаки поведения, тип атаки и т. п.
	Kaspersky Classification – классификация Лаборатории Касперского	Классификация вредоносного программного обеспечения по способам воздействия
	Symantec Classification – классификация фирмы Symantec	Классификация обнаруженного вредоносного программного обеспечения
Реестры и классификации уязвимостей программных систем	MITRE CVE (Common Vulnerabilities and Exposures) – общие уязвимости и «незащищенности»	База данных известных уязвимостей
	NVD (National Vulnerability Database) – национальная база уязвимостей США	База уязвимостей, использующая идентификаторы CVE
	OSVDB (Open Security Vulnerability Database) – база уязвимостей открытого доступа	База данных известных уязвимостей
	US-CERT Vulnerability Notes Database – база уязвимостей	Описание найденных уязвимостей и способов их обнаружения
	Бюллетени разработчиков: - Microsoft Bulletin ID - Secunia ID - VUPEN ID	Сводки найденных уязвимостей
	Таксономия Бишопа и Бейли	Устаревшая классификация уязвимостей Unix-систем
Классификации	OWASP Top Ten – 10 самых	Десять наиболее актуальных

угроз безопасности и компьютерных атак на ресурсы системы	распространенных угроз для веб-приложений	классов угроз, связанных с уязвимостями web-приложений за последний год
	MITRE CAPEC (Common Attack Pattern Enumeration and Classification) – перечень и классификация распространенных типов атак	Всесторонняя классификация типов атак
	Microsoft STRIDE Threat Model – модель угроз Microsoft	Описание пяти основных категорий уязвимостей
	WASC Threat Classification 2.0 – классификация угроз Консорциума безопасности web-приложений	Классификация изъянов, угроз web-безопасности, нацеленная на практическое применение
Классификации дефектов, внесенных в процессе разработки	MITRE CWE (Common Weaknesses Enumeration) – общая классификация дефектов программного обеспечения	Система классификации «изъянов» программного обеспечения
	Fortify Seven Pernicious Kingdoms – 7 разрушительных «царств» компании HP Fortify	Классификация дефектов программного обеспечения на 8 основных видов
	CWE/SANS Top 25 Most Dangerous Software Errors – 25 наиболее опасных ошибок в разработке программного обеспечения	25 наиболее распространенных и опасных ошибок, которые могут стать причиной уязвимости
	OWASP CLASP (OWASP Comprehensive, Lightweight, Application Security Process) – описание процесса безопасной разработки приложений	Принципы безопасности организации процесса разработки приложений
	DoD Software Fault Patterns – образцы программных ошибок Минобороны США	Система типов дефектов программного обеспечения, ассоциированная с CWE и разработанная с целью автоматизации их выявления
	Устаревшие классификации: - перечни RISOS/PA - таксономия Ландвера - таксономия Аслама - таксономия Макгоу - таксономия Вебера	Первые проекты по частичной каталогизации известных дефектов безопасности и их классификации

	- перечень PLOVER	
	MITRE Common Configuration Enumeration (CCE) – общий реестр конфигураций	Идентификация проблемных конфигураций системы, устанавливающая соответствие между различными источниками
Классификации дефектов, внесенных в процессе внедрения и эксплуатации	DPE (Security-Database Default Password Enumeration) – реестр паролей по умолчанию	База данных паролей по умолчанию для сетевых устройств, программного обеспечения и операционной системы, предназначенная для тестирования с целью выявления слабых конфигураций

91. Дерево предлагаемой классификации уязвимостей на основе причин их возникновения (дефектов) в общем виде представлено в Таблице 4. Классификация включает два типа и восемь классов.

Типы представляют собой:

- уязвимости, вызванные дефектами проектирования и программирования;
- уязвимости, вызванные дефектами конфигурирования и управления.

92. Восемь классов соответствуют наиболее применимым с точки зрения практики анализа кода международным таксономиям, а именно включают уязвимости, связанные со следующим:

1) обработкой и представлением данных;
2) внутренней структурой и зависимостями компонентов;
3) обработкой событий и состояний;
4) внутренними механизмами и ресурсами;
5) преднамеренным внедрением;
6) качеством проектирования и документированием;
7) конфигурациями;
8) окружением.

93. Элементы дерева классификации имеют вид абстрактных данных, то есть содержат необходимые свойства, отражающие различные связи и ссылки на международные источники и др. Для удобства восприятия ссылки на международные стандарты вынесены в Таблице 5.

94. В Таблице 4 предложены принципы таксономии,

ориентированной на дефекты кода и эксплуатации систем и комплексированной с международными таксономиями CWE и Fortify. К достоинству такого подхода следует отнести учет реальных причин уязвимостей, соответствие наиболее удобным международным практикам классификации и возможность исключения многократного дублирования отдельных позиций.

Таблица 4. Классификация уязвимостей на основе причин их возникновения

Класс	Класс	Группа	Вид
Тип 1. Уязвимости, вызванные дефектами кодирования и проектирования системы	Класс 1. Обработка и представление данных	Группа 1.1. Обработка входных и выходных данных	Вид 1.1.1. Проверка и представление ввода
			Вид 1.1.2. Некорректное кодирование и экранирование вывода
			Вид 1.1.3. Некорректная обработка синтаксически неверных структур
		Группа 1.2. Внутренние трансформации данных	Вид 1.2.1. Ошибки строк
			Вид 1.2.2. Ошибки типов
			Вид 1.2.3. Ошибки представления
			Вид 1.2.4. Числовые ошибки
			Вид 1.2.5. Проблемы структур данных
		Группа 1.3. Ошибки доступа к данным	Вид 1.3.1. Ошибки управления информацией
			Вид 1.3.2. Неверный доступ к индексируемому ресурсу
			Вид 1.3.3. Модификация постоянных данных
	Класс 2. Внутренняя структура и зависимости	Группа 2.1. Злоупотребление API	
		Группа 2.2. Инкапсуляция	

	Класс 3. Обработка событий и состояний	Группа 3.1. Время и внутреннее состояние	
		Группа 3.2. Проблемы с логикой функционирования	
		Группа 3.3. Проблемы с обработчиками	Вид 3.3.1. Обработка ошибок и внештатных ситуаций
	Класс 4. Ресурсы и внутренние механизмы системы	Группа 4.1. Механизмы безопасности	
		Группа 4.2. Ошибки каналов и путей	
		Группа 4.3. Ошибки инициализации и очистки	
		Группа 4.4. Проблемы ссылок и псевдонимов	Вид 4.4.1. Проблемы с указателями
		Группа 4.5. Ошибки свойственные определенному типу функционала	Вид 4.5.1. Пользовательский интерфейс
			Вид 4.5.2. Проблемы WEB
	Класс 5. Внедренные объекты (закладки)	Группа 5.1. Намеренное внедренные объекты	
		Группа 5.2. Внедренные ненамеренно объекты	
	Класс 6. Качество проектирования, реализации, документирования	Группа 6.1. Качество кода	
		Группа 6.2. Нарушение принципов проектирования безопасного ПО	
		Группа 6.3.	

		Неполная или некорректная документация	
Тип 2. Уязвимости, вызванные дефектами конфигурирования и управления системой и ее окружением	Класс 7. Конфигурация	Группа 7.1. Настройки механизмов безопасности	
		Группа 7.2. Настройки структуры и функционала	
		Группа 7.3. Закладки в настройках	
		Группа 7.4. Совместимость версий	
		Группа 7.5. Качество настроек	
	Класс 8. Окружение	Группа 8.1. Среда компиляции и выполнения программного кода	
		Группа 8.2. Прикладное программное обеспечение	
		Группа 8.3. Системное программное обеспечение (гипервизор, ОС, драйвера)	
		Группа 8.4. Аппаратное обеспечение	

Таблица 5. Соответствие международным стандартам

Класс, группа, вид	**Ссылка на международные стандарты**
Класс 1. Обработка и представление данных	Обработка данных (CWE-19)

Вид 1.1.1. Проверка и представление ввода	Некорректная проверка ввода (CWE-20), Проверка и представление ввода (Fortify-1)
Вид 1.1.2. Некорректное кодирование и экранирование вывода	Некорректное кодирование и экранирование вывода (CWE-116)
Вид 1.1.3. Некорректная обработка синтаксически неверных структур	Неправильная обработка синтаксически некорректных конструкций (CWE-228)
Вид 1.2.1. Ошибки строк	Ошибки строк (CWE-133)
Вид 1.2.2. Ошибки типов	Ошибки типов (CWE-136)
Вид 1.2.3. Ошибки представления	Ошибки представления (CWE-137)
Вид 1.2.4. Числовые ошибки	Числовые ошибки (CWE-189)
Вид 1.2.5. Проблемы структур данных	Проблемы структур данных (CWE-461)
Вид 1.3.1. Ошибки управления информацией	Ошибки управления информацией (CWE-199)
Вид 1.3.2. Неверный доступ к индексируемому ресурсу	Неверный доступ к индексируемому ресурсу («Ошибка диапазона») (CWE-118)
Вид 1.3.3. Модификация постоянных данных	Модификация предположительно постоянных данных – MAID (CWE-471)
Группа 2.1. Злоупотребление API	Злоупотребление API (CWE-227, Fortify-2)
Группа 2.2. Инкапсуляция	Недостаточная инкапсуляция (CWE-485), Инкапсуляция (Fortify-7)
Группа 3.1. Время и внутреннее состояние	Время и состояние (CWE-361, Fortify-3)
Группа 3.2. Проблемы с логикой функционирования	Проблемы поведения (CWE-438)
Группа 3.3. Проблемы с обработчиками	Обработчик ошибок (CWE-429)
Вид 3.3.1. Обработка ошибок и внештатных ситуаций	Обработка ошибок (CWE-388, Fortify-5)
Группа 4.1. Механизмы безопасности	Механизмы безопасности (CWE-254, Fortify-4)
Группа 4.2. Ошибки каналов и путей	Ошибки каналов и путей (CWE-417)
Группа 4.3. Ошибки инициализации и	Ошибки инициализации и очистки (CWE-

очистки	452)
Вид 4.4.1. Проблемы с указателями	Проблемы с указателями (CWE-465)
Вид 4.5.1. Пользовательский интерфейс	Ошибки пользовательского интерфейса (CWE-445)
Вид 4.5.2. Проблемы web	Проблемы web (CWE-442)
Группа 5.1. Намеренно внедренные объекты	Намеренно внедренные объекты (CWE-505)
Группа 5.2. Внедренные ненамеренно объекты	Внедренные ненамеренно объекты (CWE-518)
Группа 6.1. Качество кода	Индикатор плохого качества кода (CWE-398), Качество кода (Fortify-6)
Группа 6.2. Нарушение принципов проектирования безопасного ПО	Нарушение принципов проектирования безопасного ПО (CWE-657)
Класс 7. Конфигурация	Конфигурация (CWE-16)
Класс 8. Окружение	Окружение (CWE-2, Fortify-*)
Группа 8.1. Среда компиляции и выполнения программного кода	Байт-код/объектный модуль (CWE-503)

8.Актуальные угрозы безопасности информационных систем государственных органов, органов местного самоуправления, организаций и учреждений.

95.Государственные информационные системы (далее – ГИС) используемые государственными органами, органами местного самоуправления, а также государственными учреждениями и организациями, в том числе акционерными обществами, в которых имеется государственная доля, обрабатывающие персональные данные, отличаются следующими особенностями:

- использованием широкой номенклатуры (зачастую уникальных) технических средств получения, отображения и обработки информации;
- использованием специального (адаптированного под конкретную задачу) программного обеспечения;

- наличием значительного количества автоматизированных рабочих мест, участвующих в обработке персональных данных;
- построением ГИС на базе распределенной по территории Кыргызской Республики вычислительной сети со сложной архитектурой;
- наличием выходов в сети общего пользования и (или) сети международного информационного обмена, локальные вычислительные сети сторонних организаций;
- использованием разнообразной телекоммуникационной среды, принадлежащей различным операторам связи;
- широким применением средств защиты информации, сертифицированных средств криптографической защиты информации при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена;
- использованием аутсорсинга при создании и эксплуатации ГИС и ее элементов;
- сложностью дублирования больших массивов информации, содержащей персональные данные, на бумажных носителях и внешних накопителях информации;
- значительными негативными последствиями при реализации угроз безопасности ГИС;
- риском недостаточной квалификации пользователей и обслуживающего ГИС и средств защиты информации персонала;
- проблемами взаимодействия различных ГИС, вызванными несовершенством действующего законодательства и ведомственных инструкций.

96. Актуальными угрозами безопасности ГИС, обрабатывающих персональные данные учитывая положения, изложенные в настоящем разделе, помимо угроз, указанных в пункте 3 настоящего Типового перечня, признаются:

- угрозы аппаратно-программным средствам виртуализации (при их использовании в ГИС);
- угрозы обнаружения хостов;
- угрозы обнаружения открытых портов и идентификации привязанных к ним сетевых служб;
- угрозы неправомерных действий в каналах связи;
- угрозы межсайтового скриптинга;
- угрозы межсайтовой подделки запросов;

- угрозы использования альтернативных путей доступа к ресурсам;
- угрозы фишинга;
- угрозы фарминга;
- угрозы спама веб-сервера;
- угрозы доступа/перехвата/изменения HTTP cookies;
- угрозы "кражи" учетной записи доступа к сетевым сервисам;
- угрозы подмены субъекта сетевого доступа;
- угрозы подмены содержимого сетевых ресурсов;
- угрозы перехвата данных, передаваемых по вычислительной сети;
- угрозы передачи данных по скрытым каналам;
- угрозы несанкционированного доступа по каналам связи.

97.В зависимости от целей и содержания обработки персональных данных оператор может осуществлять обработку персональных данных в информационных системах различных типов.

- По структуре информационные системы подразделяются на автоматизированные рабочие места, локальные информационные системы и распределенные информационные системы.
- По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.
- По режиму обработки персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.
- По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

98.Информационные системы в зависимости от местонахождения их технических средств подразделяются на системы, все технические средства которых находятся в пределах Кыргызской Республики, и системы, технические средства которых частично или целиком находятся за пределами Кыргызской Республики.

99.В Приложении 7 представлен список источников, которые могут быть полезными при рассмотрении различных вопросов защиты персональных данных и кибербезопасности.

Список не преследует цели дать исчерпывающий перечень международных стандартов и технических отчетов по всем аспектам защиты персональных данных и кибербезопасности.

Приложение 1. Виды и мотивация нарушителей

№	Вид нарушителя	Тип нарушителя	Мотивация нарушителя
1	Специальные службы иностранных государств	внешний, внутренний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности органов государственной власти, организаций
2	Террористические, экстремистские группировки	внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной власти, организаций
3	Преступные группы (криминальные структуры)	внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
4	Внешние субъекты	внешний	Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
5	Конкурирующие организации	внешний	Получение конкурентных преимуществ. Причинение имущественного и/или репутационного ущерба путем обмана или злоупотребления доверием
6	Разработчики, производители, поставщики программных, технических и программно-технических средств	внешний	Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или

			неквалифицированные действия
7	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и других видов работ	внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
8	Лица, обеспечивающие функционирование информационных систем или обслуживание инфраструктуры оператора (охранники, уборщики и т.д.)	внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.
9	Пользователи информационной системы	внутренний	Причинение имущественного ущерба или репутационного путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия.
10	Администраторы информационной системы и администраторы безопасности	внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия
11	Бывшие работники (пользователи)	внешний	Причинение имущественного или репутационного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия.

Приложение 2. Виды программ-вымогателей

№	Название	Определение
1	Лже-антивирус (Scareware)	поддельное программное обеспечение безопасности, которое утверждает, что на компьютере установлено вредоносное программное обеспечение. Конечный пользователь получает всплывающее окно с требованием оплаты за удаление. Если платеж не произведен, всплывающие окна будут продолжать появляться, но файлы, как правило, безопасны. Настоящее анти вредоносное/антивирусное программное обеспечение уже отслеживает атаки вредоносного программного обеспечения. Это также не заставит вас платить за удаление инфекции.
2	Блокировщики экрана	Блокировщики экрана блокируют доступ к компьютеру. Программа-вымогатель заменяет экран входа в систему экраном с требованием оплаты. Часто на экране есть логотип какой-то организации или правоохранительного органа. Ни один правоохранительный орган не вытащит вас из вашего компьютера. Они также не будут требовать оплаты за незаконную деятельность. Они пойдут по соответствующим законным каналам.
3	Программа вымогатель-шифровальщик	шифрует ваши файлы и требует оплаты за их расшифровку. Это программа-вымогатель имеет самый высокий риск кибербезопасности. Трудно восстановить доступ к зашифрованным файлам. Единственный способ – заплатить выкуп или использовать инструмент для расшифровки. Даже если вы заплатите выкуп, нет никакой гарантии, что злоумышленник расшифрует ваши файлы.
4	Мобильные программы-вымогатели	Популярность мобильных устройств привела к появлению мобильных программ-вымогателей. Он часто нацелен на Android, поскольку позволяет устанавливать сторонние приложения. В отличие от операционной системы iPhone от Apple.

Приложение 3. Классификация распространенных троянских типов приложений

№	Название	Определение	Примеры
1	Бэкдор - BackDoor	Разновидность троянских программ, которые содержат функции удаленного управления. Эти трояны позволяют злоумышленникам дистанционно контролировать зараженные устройства и выполнять на них различные действия без согласия пользователей. В зависимости от функциональных особенностей конкретного бэкдора, хакер может установить и запустить на компьютере жертвы любое программное обеспечение, сохранять все нажатия клавиш, загружать и сохранять любые файлы, включать микрофон или камеру, то есть брать на себя контроль за компьютером и информацией жертвы.	ShadowPad, FinSpy, Tixanbot, Briba, Win32/Industroyer, Exaramel
2	Руткит	Средства сокрытия вредоносной деятельности. Руткит представляет собой особую часть вредоносных программ, разработанных специально, чтобы скрыть присутствие вредоносного кода и его действия от пользователя и установленного защитного программного обеспечения. Это возможно благодаря тесной интеграции руткита с операционной системой.	Stuxnet, Flame, Necurs, ZeroAccess, TDSS
3	Загрузчик, DownLoader и DownLoad	Программы, основная функция которых – загрузка, установка и запуск вредоносного, рекламного и другого ненужного программного обеспечения на атакуемых устройствах. Этот троян является небольшой частью кода, используемой для	Trojan.DownLoader34.3812, Trojan.DownLoad.57289

		дальнейшей загрузки и установки полной версии вредоносного программного обеспечения. После того как загрузчик попадает в систему путем сохранения вложения электронного письма или, например, при просмотре зараженной картинки, он соединяется с удаленным сервером и загружает весь вредонос.	
4	Кодировщик - Encoder	Класс троянских приложений-вымогателей (энкодеры, шифровальщики), которые шифруют файлы на атакованных устройствах и требуют выкуп за их расшифровку.	Trojan.Encoder.68, Linux.Encoder.1, Android.Encoder.3.origin
5	Winlock	Класс вредоносных программ-вымогателей, которые нарушают работу операционной системы Windows, блокируют компьютеры и вымогают у пользователей деньги за восстановление работоспособности устройств.	Trojan.Winlock.5490
6	MulDrop	Класс троянских приложений, которые скрывают в себе (часто в зашифрованном виде) другое вредоносное или нежелательное программное обеспечение. Используются для его распространения и установки в обход антивирусов и незаметно для пользователей.	Trojan.MulDrop13.32284, Android.MulDrop.924, Linux.MulDrop.14
7	Встраивание кода - Inject	Троянские программы, встраивающиеся вредоносный код в процессы других приложений.	Trojan.Inject2.62347
8	Кейлоггер - Keylogger	Программы-шпионы, отслеживающие нажатия клавиш на клавиатуре и перехватывающие вводимые символы.	Trojan.KeyLogger.20146
9	KillProc	Трояны, основная задача которых – завершение процессов других приложений. В зависимости от	Trojan.KillProc.12769

		семейства, версии, модификации и поставленной задачи могут атаковать самые разные процессы – как системные, так и пользовательские.	
10	Packed	Категория троянов, защищенных программными упаковщиками для снижения эффективности обнаружения их антивирусами. Без упаковщика у таких вредоносных приложений могут иметь иное наименование.	Trojan.Packed.1198, Android.Packed.15893, Linux.Packed.483
11	AVKill	Трояны, атакующие антивирусы. Они могут нарушать работу их отдельных компонентов, повреждать файлы или полностью удалять из системы.	Trojan.AVKill.2942
12	Fakealert	Программы, выдающие себя за настоящие антивирусы и другое защитное программное обеспечение. Они информируют о несуществующих угрозах, пугают пользователей и обманом заставляют их купить «полную версию», которая является пустышкой.	Trojan.Fakealert.23300, Android.Fakealert.11
13	Майнер	Программы, предназначенные для майнинга (добычи) различных криптовалют. Они используют вычислительные мощности заражаемых устройств, замедляя их работу, вызывая перегрев и перерасход электроэнергии.	Maze

Приложение 4. Категории DoS и DDoS-трафика

№	Название	Определение
1	Атаки на	Нападения реализуются путем отправки серверу

	переполнение канала	многочисленных эхо-запросов, которые потребляют ресурсы интернет-канала. Задача подобных атак – провести через сеть жертвы как можно больше ложного трафика, тем самым исчерпав всю емкость полосы пропускания. Успешность их проведения напрямую зависит от отправленного объема данных (Гбит/сек.).
1.1	DNS-флуд	Злоумышленник атакует DNS-сервер, который напрямую взаимодействует с жертвой. В результате веб-ресурс, на который было рассчитано нападение, продолжает функционировать внутри своей сети, но оказывается отрезанным от интернета. Атака часто используется, поскольку для перегрузки полосы пропускания среднестатистического DNS-сервера достаточно 10 тыс. запросов в секунду. Один персональный компьютер способен сгенерировать около 1 тыс. таких запросов. Поэтому хакеру потребуется всего 10 компьютеров для перегрузки и отключения одного DNS-сервера.
1.2	Ping-флуд	Сопровождается пересылкой многочисленных, но небольших по размеру ICMP-сообщений (эхо-запросов). Злоумышленник быстро отправляет пакеты, не дожидаясь обязательного ответа. В конце концов на целевом сервере возникает перегрузка по количеству запросов, инициирующая потери настоящих пакетов по всем протоколам.
1.3	UDP-флуд	Жертве отправляются большие пакеты через бес сеансовый протокол пользовательских дейтаграмм (UDP). Когда сервер фиксирует отсутствие приложения, отвечающего за порт, в ответ злоумышленнику отправляется пакет ICMP с сообщением «адресат недоступен». У протокола UDP отсутствуют средства защиты от перегрузок, поэтому этот тип атаки способен захватить весь полезный интернет-трафик сервера.
1.4	ICMP-флуд.	Протокол межсетевых управляющих сообщений (ICMP) используется в первую очередь для передачи сообщений об ошибках и не используется для передачи данных. ICMP-пакеты могут сопровождать TCP-пакеты при соединении с сервером. ICMP-флуд – метод DDoS атаки на 3-м уровне модели OSI, использующий ICMP-сообщения для перегрузки сетевого канала атакуемого.
1.5	MAC-флуд	MAC-флуд – редкий вид атаки, при котором атакующий посылает множественные пустые Ethernet-фреймы с различными MAC-адресами. Сетевые свитчи

		рассматривают каждый MAC-адрес в отдельности и, как следствие, резервируют ресурсы под каждый из них. Когда вся память на свитче использована, он либо перестает отвечать, либо выключается. На некоторых типах роутеров атака MAC-флудом может стать причиной удаления целых таблиц маршрутизации, таким образом нарушая работу целой сети.
2	Атаки, использующие уязвимость стека протоколов	Нападения на межсетевые экраны, файервол и другие сервисы, с целью ограничить количество допустимых соединений у жертвы по TCP протоколу.
2.1	SYN-флуд	Злоумышленник создает с сервером несколько деактивированных подключений по протоколу TCP. Со стороны хакера отправляются SYN-запросы для соединения с целевой сетью, а жертва, в свою очередь, отправляет ответный пакет SYN-ACK. Для окончания квитирования со стороны отправителя ожидается пакет ACK. Однако злоумышленник оставляет сессию полуоткрытой – не отправляет запрос или пересылает его на несуществующий адрес. Это происходит до тех пор, пока на сервере не сработает ограничение на максимальное число одновременных открытых подключений. В конечном результате система перестаёт принимать запросы на соединение от настоящих пользователей.
2.2	«Медленные запросы HTTP» - Slow HTTP POST	Атака «Медленные запросы HTTP» направлена на перегрузку веб-серверов с использованием уязвимости в HTTP протоколе. Во время начала нападения злоумышленник отправляет HTTP запрос с заголовком «Content-Length», который даёт информацию целевому веб-серверу о размере последующего пакета. Затем хакер отправляет само сообщение методом POST (отправка), но делает это с очень низкой скоростью, максимально растягивая продолжительность сессии. Таким образом, злоумышленник занимает ресурсы жертвы на длительное время, создавая проблемы при обработке запросов от настоящих пользователей.
2.3	«Пинг смерти» - Ping of Death / POD	Хакер посылает фрагменты модифицированных пакетов на один компьютер с помощью эхо-запроса (ping), который используется для проверки ответа от сетевого оборудования. При попытке собрать единый пакет из полученных фрагментов, происходит переполнение памяти, а следовательно, многочисленные сбои в системе.

3	Атака приложений	Нападения сопровождаются чрезмерным потреблением ресурсов у жертвы из-за стрессовой нагрузки служб и приложений на внешнем уровне. Во время атаки задача злоумышленника – запустить максимальное число процессов и транзакций на целевом сервере. Для перегрузки системы подобными атаками не нужно большого числа машин, что усложняет обнаружение и устранение нападений.
3.1	Slowloris (Slow HTTP GET)	Атака производится с помощью специальных программ, разработанных для нападения на интернет-сервисы, путем создания многочисленных «медленных сессий». Со стороны хакера, в рамках одного запроса, отправляется цепочка неполных HTTP-сессий, содержащих только заголовок без продолжения. Для обработки HTTP-заголовков сервер открывает и поддерживает массу подключений, блокирующих его основную работу. Метод Slowloris отличается от других типов атак тем, что для его реализации не требуется широкая полоса пропускания трафика.
3.2	Переполнение буфера (Buffer Overflow)	Самый распространённый метод DoS-атак. Он позволяет злоумышленнику получить доступ к системе или вызвать ошибку в программном обеспечении с помощью эксплойта, путем переполнения буфера программы. Эта уязвимость характерна для приложений, работающих без проверки длины входных данных.
3.3	HTTP-флуд	Основная задача атаки: запустить максимальное количество процессов, направленных на обработку запроса. Для нападения злоумышленник отправляет HTTP-серверу многочисленные поддельные запросы GET (получение данных) или POST (отправка данных) через ботнет. В результате исчерпывается лимит размера log-файла и система перестает отвечать на реальные запросы пользователей. Хакеры часто применяют HTTP-флуд, поскольку для его реализации требуется меньшая пропускная способность, чем для других видов атак.

Приложение 5. Классификация и цели DDoS-атак по уровням OSI

Интернет использует модель OSI. Всего в модели присутствует 7 уровней, которые охватывают все среды коммуникации: начиная с физической среды (1-й уровень) и заканчивая уровнем приложений (7-й уровень), на котором «общаются» между собой программы. DDoS-атаки возможны на каждом из семи уровней.

7	**7-й уровень OSI:**	**Прикладной**
	Тип данных	Данные
	Описание уровня	Начало создания пакетов данных. Присоединение и доступ к данным. Пользовательские протоколы, такие как FTP, SMTP, Telnet, RAS
	Протоколы	FTP, HTTP, POP3, SMTP и шлюзы, которые их используют
	Примеры технологий DoS	PDF GET запросы, HTTP GET, HTTP POST (формы веб-сайтов: логин, загрузка фото/видео, подтверждение обратной связи)
	Последствия DDoS-атаки	Нехватка ресурсов. Чрезмерное потребление системных ресурсов службами на атакуемом сервере.
6	**6-й уровень OSI:**	**Представительский**
	Тип данных	Данные
	Описание уровня	Трансляция данных от источника получателю
	Протоколы	Протоколы сжатия и кодирования данных (ASCII, EBCDIC)
	Примеры технологий DoS	Подложные SSL запросы: проверка шифрованных SSL пакетов очень ресурсоемкая, злоумышленники используют SSL для HTTP-атак на сервер жертвы
	Последствия DDoS-атаки	Атакуемые системы могут перестать принимать SSL соединения или автоматически перезагружаться
5	**5-й уровень OSI:**	**Сеансовый**
	Тип данных	Данные
	Описание уровня	Управление установкой и завершением соединения, синхронизацией сеансов связи в рамках операционной системы через сеть (например, когда вы выполняете вход/выход)
	Протоколы	Протоколы входа/выхода (RPC, PAP)

	Примеры технологий DoS	Атака на протокол Telnet использует слабые места программного обеспечения Telnet-сервера на свитче, делая сервер недоступным
	Последствия DDoS-атаки	Делает невозможным для администратора управление свитчем
4	**4-й уровень OSI:**	**Транспортный**
	Тип данных	Сегменты
	Описание уровня	Обеспечение безошибочной передачи информации между узлами, управление передачей сообщений с 1 по 3 уровень
	Протоколы	Протоколы TCP, UDP
	Примеры технологий DoS	SYN-флуд, Smurf-атака (атака ICMP-запросами с измененными адресами)
	Последствия DDoS-атаки	Достижение пределов по ширине канала или по количеству допустимых подключений, нарушение работы сетевого оборудования
3	**3-й уровень OSI:**	**Сетевой**
	Тип данных	Пакеты
	Описание уровня	Маршрутизация и передача информации между различными сетями
	Протоколы	Протоколы IP, ICMP, ARP, RIP и роутеры, которые их используют
	Примеры технологий DoS	ICMP-флуд – DDos-атаки на третьем уровне модели OSI, которые используют ICMP-сообщения для перегрузки пропускной способности целевой сети
	Последствия DDoS-атаки	Снижение пропускной способности атакуемой сети и возможная перегруженность брандмауэра
2	**2-й уровень OSI:**	**Канальный**
	Тип данных	Кадры
	Описание уровня	Установка и сопровождение передачи сообщений на физическом уровне
	Протоколы	Протоколы 802.3, 802.5, а также контроллеры, точки доступа и мосты, которые их используют
	Примеры технологий DoS	MAC-флуд – переполнение пакетами данных сетевых коммутаторов

	Последствия DDoS-атаки	Потоки данных от отправителя получателю блокируют работу всех портов
1	**1-й уровень OSI:**	**Физический**
	Тип данных	Биты
	Описание уровня	Передача двоичных данных
	Протоколы	Протоколы 100BaseT, 1000 Base-X, а также концентраторы, розетки и патч-панели, которые их используют
	Примеры технологий DoS	Физическое разрушение, физическое препятствие работе или управлению физическими сетевыми активами
	Последствия DDoS-атаки	Сетевое оборудование приходит в негодность и требует ремонта для возобновления работы

Приложение 6. Уязвимости отдельных протоколов стека протоколов TCP/IP, на базе которого функционируют глобальные сети общего пользования

Наименование протокола	Уровень стека протоколов	Наименование (характеристика) уязвимости	Содержание нарушения безопасности информации
FTP (File Transfer Protocol)- протокол передачи файлов по сети	Прикладной, представительный, сеансовый	1.Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) 2. Доступ по умолчанию 3. Наличие двух открытых портов	Возможность перехвата данных учетной записи (имен зарегистрированных пользователей, паролей). Получение удаленного доступа к хостам
telnet - протокол управления удаленным терминалом	Прикладной, представительный, сеансовый	Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде)	Возможность перехвата данных учетной записи пользователя. Получение удаленного доступа к хостам
UDP - протокол передачи данных без установления соединения	Транспортный	Отсутствие механизма предотвращения перегрузок буфера	Возможность реализации UDP-шторма. В результате обмена пакетами происходит существенное снижение производительности сервера.
ARP - протокол преобразования IP-адреса в физический адрес	Сетевой	Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде)	Возможность перехвата трафика пользователя злоумышленником.
OSPF/EIGRP/BGP - протоколы маршрутной информации	Транспортный	Отсутствие аутентификации управляющих сообщений об	Возможность перенаправления трафика через хост злоумышленника

		изменение маршрута	
TCP - протокол управления передачей	Транспортный	Отсутствие механизма проверки корректности заполнения служебных заголовков пакета	Существенное снижение скорости обмена и даже полный разрыв произвольных соединений по протоколу TCP
DNS - протокол установления соответствия мнемонических имен и сетевых адресов	Прикладной, представительный, сеансовый	Отсутствие средств проверки аутентификации полученных данных от источника	Фальсификация ответов DNS-сервера
IGMP - протокол передачи сообщений о маршрутизации	Сетевой	Отсутствие аутентификации сообщений об изменении параметров маршрута	Зависание систем Win 9x/NT/200
SMTP - протокол обеспечения сервиса доставки сообщений по электронной почте	Прикладной, представительный, сеансовый	Отсутствие поддержки аутентификации заголовков сообщений	Возможность подделывания сообщений электронной почты, а также адреса отправителя сообщения
SNMP - протокол установления маршрутизаторами в сетях	Прикладной, представительный, сеансовый	Отсутствие поддержки аутентификации заголовков сообщений	Возможность переполнения пропускной способности сети

Приложение 7. Примерный список источников, полезных при рассмотрении вопросов защиты персональных данных и кибербезопасности

Документы Международной Организации по Стандартизации (ISO) и Международной электротехнической комиссии (IEC)

Системы менеджмента информационной безопасности

- ISO/IEC 27000 «Information technology – Security techniques – Information security management systems – Overview and vocabulary» (аналог- ГОСТ РИСО/ МЭК. 27000. «Информационные технологии. Обеспечение безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»)
- ISO/IEC 27001 «Information technology – Security techniques – Information security management systems – Requirements» (аналог-ГОСТРИСО/МЭК 27001-2006. «Информационные технологии. Обеспечение безопасности. Системы менеджмента информационной безопасности. Требования »).
- ISO/IEC 27002 «Information technology – Security techniques – Code of practice for information security management» (Информационные технологии. Обеспечение безопасности.Практические правила менеджмента информационной безопасности).
- ISO/IEC 27003 «Information technology – Security techniques – Information security management system implementation guidance» (аналог-ГОСТРИСО/МЭК 27003. «Информационные технологии. Обеспечение безопасности. Руководство по внедрению системы менеджмента информационной безопасности.»).
- ISO/IEC 27010 «Information technology – Security techniques – Information security management for intersector communications» (Информационные технологии. Обеспечение безопасности. Руководство по менеджменту информационной безопасности при межведомственном взаимодействии.)

Менеджмент рисков

- ISO/IEC 27005 «Information technology – Security techniques – Information security risk management» (аналог - ГОСТ Р ИСО/МЭК 27005-2910. «Информационные технологии. Обеспечение безопасности. Менеджмент риска информационной безопасности»).

- ISO/IEC 16085 «Systems and software engineering – Life cycle processes – Risk management» (аналог - ГОСТ Р ИСО/МЭК 16085-2007. «Менеджмент риска. Применение в процессах жизненного цикла систем и программного обеспечения»).

Оценка безопасности IT-систем

- ISO/IEC 15408 «Information technology – Security techniques – Evaluation criteria for IT security» (аналог - ГОСТ Р ИСО/МЭК 15408-2008. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»).
- ISO/IEC 18045 «Information technology – Security techniques – Methodology for IT security evaluation» (аналог - ГОСТ Р ИСО/МЭК 18045-2008. «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»).
- ISO/IEC 19791 «Information technology – Security techniques – Security assessment of operational systems». (аналог - ГОСТ Р ИСО/МЭК 19791-2008. «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем»).

Обеспечение безопасности

- ISO/IEC 15443 «Information Technology–Security Techniques–A framework for IT Security assurance» (аналог - ГОСТ Р 54581-2001/ISO/IEC/TR 15443-2005 «Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ»).
- ISO/IEC 15026 «Systems and software engineering – Systems and software assurance» (Системная И программная инженерия. Гарантированность систем и программного обеспечения.)

Разработка и реализация

- ISO/IEC 12207 «Systems and software engineering – Software life cycle processes» (аналог-ГОСТРИСО/МЭК 12207-2010. «Системная и программная инженерия. Процессы жизненного цикла программных средств»).
- ISO/IEC 14764 «Software Engineering – Software Life Cycle Processes – Maintenance» (аналог-ГОСТ Р ИСО/МЭК 14764-2002. «Информационная технология. Сопровождение программных средств»).
- ISO/IEC 15288 «Systems and software engineering – System life cycle processes» (аналог-ГОСТ Р ИСО/МЭК 15288-2005. «Информационная

технология. Системная и программная инженерия. Процессы жизненного цикла систем»).

- ISO/IEC 23026 «Software Engineering – Recommended Practice for the Internet – Web Site Engineering, Web Site Management, and Web Site Life Cycle» (Разработк апрограммного обеспечения. Рекомендуемая практика для Интернета. Разработка веб-сайтов, администрирование веб-сайтов и жизненный цикл веб-сайтов.)
- ISO/IEC 42010 «Systems and software engineering – Architecture description» (Системная и программная инженерия. Описание архитектуры.)

Аутсорсинг и услуги третьих сторон

- ISO/IEC 14516 «Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services» (Информационные технологии. Методы защиты. Руководящие указания по использованию и менеджменту доверенных сервисов третьей стороны.)
- ISO/IEC 15945 «Information technology–Security techniques– Specification of TTP services to support the application of digital signatures» (аналоги– ДСТУ ISO/IEC TR 14516:2008 «Информационные технологии – Методы защиты – Руководящие указания по применению и управлению службами доверенной третьей стороны».)

Сетевая безопасность и безопасность приложений

- ISO/IEC 18028 «Information technology – Security techniques – IT network security» (аналог-ГОСТ Р ИСО/МЭК 18028-2008. «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Менеджмент сетевой безопасности».)
- ISO/IEC 18043 «Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems» (Информационные технологии. Методы защиты. Выбор, развертывание и эксплуатация систем обнаружения вторжений.)
- ISO/IEC 27033 «Information technology – Security techniques – Network security» (аналог-ГОСТ Р ИСО/МЭК 27033 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей».)
- ISO/IEC 27034 «Information technology – Security techniques – Guidelines for application security» (Информационные технологии. Методы обеспечения безопасности. Безопасность приложений.)

Непрерывность и менеджмент инцидентов

- ISO/IEC 18044 «Information technology – Security techniques – Information security incident management» (аналог- ГОСТ Р ИСО/МЭК ТО 18044. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»).
- ISO/IEC 24762 «Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services» (аналог-ГОСТ Р 53131-2008 (ИСО/МЭК ТО 24762:2008) «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий»).
- ISO/IEC 27031 «Information technology – Security techniques – Guidelines for ICT readiness for business continuity» (Информационные технологии. Методы обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса.)
- ISO/IEC 27035 «Information technology – Security techniques – Information security incident management» (Информационные технологии. Методы обеспечения безопасности. Менеджмент инцидентов информационной безопасности.)

Менеджмент идентификации, установления тождественности (Identity management)

- ISO/IEC 24760 «Information technology – Security techniques – A framework for identity management» (Информационные технологии. Методы обеспечения безопасности. Базовая модель менеджмента идентификации.)

Информационная неприкосновенность, информационный суверенитет личности (Privacy)

- ISO/IEC 29100 «Information technology – Security techniques – Privacy framework» (Информационные технологии. Методы обеспечения безопасности. Базовая модель обеспечения информационного суверенитета личности.)

Менеджмент активов ISO/IEC 19770 «Information technology – Software asset management». (Информационные технологии. Менеджмент программного обеспечения.)

Менеджмент услуг ISO/IEC 20000 «Information technology – Service management» (аналог-ГОСТ Р ИСО/МЭК 20000-1-2010. «Информационная технология. Менеджмент услуг»).

Документы Международного союза телекоммуникаций (ITU)

Кибербезопасность

- ITU-TX.1200 –X.1299 Series. Series X: Data Networks, Open System Communications and Security, Telecommunication Security – Cyberspace security. (Рекомендации МСЭ-Т. X.1200-X.1299. Серия X: «Сети передачи данных. Взаимодействие и безопасность открытых систем. Безопасность телекоммуникаций.» - Безопасность Киберпространства»).
- ITU-TX.1205. -SeriesX: DataNetworks, OpenSystemCommunicationsandSecurity, TelecommunicationSecurity– OverviewofCybersecurity. (Рекомендации МСЭ-Т. X.1205. Серия X: «Сети передачи данных. Взаимодействие и безопасность открытых систем. Безопасность телекоммуникаций. Общее представление о кибербезопасности»).

Менеджмент непрерывности бизнеса и менеджмент инцидентов

- ITU-T X.1206. Series X: Data Networks, Open System Communications and Security, Telecommunication Security – A vendor-neutral framework for automatic notification of security related information and dissemination of updates (Рекомендации МСЭ-Т. X.1206. Серия X: «Сети передачи данных. Взаимодействие и безопасность открытых систем. Безопасность телекоммуникаций. Независимый от производителя фреймворк автоматического распространения обновлений и рассылки информации, связанной с безопасностью»)

Нежелательные программные коды

- ITU-T X.1207. Series X: Data Networks, Open System Communications and Security, Telecommunication Security – Guidelines for Telecommunication Service Providers for Addressing the Risk of Spyware and Potentially Unwanted Software. (Рекомендации МСЭ-Т. X.1207. Серия X: «Сети передачи данных. Взаимодействие и безопасность открытых систем. Безопасность телекоммуникаций. Руководящие указания провайдерам телекоммуникационных услуг в отношении обращения с рисками шпионских программ и потенциально нежелательных программных кодов»).

Противодействие спаму

- ITU-T X.1231. Series X: Data Networks, Open System Communications and Security, Telecommunication Security – Technical strategies for countering spam. (Рекомендации МСЭ-Т. X.1231. Серия X: «Сети передачи данных. Взаимодействие и безопасность открытых систем. Безопасность телекоммуникаций. Технические методы противодействия спаму»).
- ITU-T X.1240. Series X: Data Networks, Open System Communications and Security, Telecommunication Security – Technologies involved in countering e-mail spam. (Рекомендации МСЭ-Т. X.1240. Серия X: «Сети передачи данных. Взаимодействие и безопасность открытых систем. Безопасность телекоммуникаций. Технологии, применяемые для противодействия спаму, рассылаемому по электронной почте»).
- ITU-T X.1241. Series X: Data Networks, Open System Communications and Security, Telecommunication Security – Technical framework for countering email spam. (Рекомендации МСЭ-Т. X.1241. Серия X: «Сети передачи данных. Взаимодействие и безопасность открытых систем. Безопасность телекоммуникаций. Технический фреймворк противодействия спаму, рассылаемому по электронной почте»).
- ITU-T X.1244. Series X: Data Networks, Open System Communications and Security, Telecommunication Security – Overall aspects of countering spam in IP-based multimedia applications. (Рекомендации МСЭ-Т. X.1244. Серия X: «Сети передачи данных. Взаимодействие и безопасность открытых систем. Безопасность телекоммуникаций. Общие аспекты противодействия спаму в мультимедийных приложениях, использующих IP-технологии»).

Обмен информацией, имеющей отношение к кибербезопасности

- ITU-TX.1500-X.1598 Серия (CYBEX). Series X: Data networks, Open System Communications and Security – Cybersecurity Information Exchange. (Рекомендации МСЭ-Т. X.1500- X.1598 (CYBEX). Серия X: «Сети передачи данных. Взаимодействие и безопасность открытых систем. Безопасность телекоммуникаций. Обмен информацией по вопросам кибербезопасности»).ПРИМЕЧАНИЕ. Поскольку в МСЭ-Т работа над рекомендациями серии CYBEX по состоянию на сентябрь 2011 года еще не была завершена, в качестве готовых рекомендаций или драфт-версий были доступны только X.1500, X.1520, X.1521, иX.1570. Для получения новейшей доступной информации пользователям следует регулярно обращаться к веб-сайту МСЭ-Т (ITU-T).