УТВЕРЖДЕНА

постановлением Администрации города Вологды

от 24.06.2024 № 820

**Базовая модель угроз безопасности персональных данных**

**при их обработке в информационных системах персональных данных Администрации города Вологды**

1. **Общие положения**
   1. Настоящая базовая модель угроз безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн) Администрации города Вологды (далее – Модель угроз) содержит систематизированный перечень угроз безопасности ПДн при их обработке в ИСПДн Администрации города Вологды.

Угрозы безопасности ПДн могут быть обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности ПДн, которое ведет к ущербу жизненно важных интересов личности, общества   
и государства.

Модель угроз содержит исходные данные по угрозам безопасности ПДн, обрабатываемых в ИСПДн Администрации города Вологды, связанным:

с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;

с несанкционированным, в том числе случайным, доступом в ИСПДн   
с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн   
с использованием программных и программно-аппаратных средств, с целью уничтожения или блокирования ПДн.

* 1. Настоящая Модель угроз разработана в соответствии с:

пунктом 1 части 2 статьи 19 [Федерального закона от 27 июля 2006 года   
№ 152-ФЗ «О персональных данных»](http://docs.cntd.ru/document/901990046) (с последующими изменениями);

[постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»](http://docs.cntd.ru/document/902377706);

базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной Федеральной службой по техническому и экспортному контролю 15 февраля 2008 года.

* 1. С применением Модели угроз решаются следующие задачи:

разработка частных моделей угроз безопасности ПДн в конкретных ИСПДн   
с учетом их назначения, условий и особенностей функционирования;

анализ защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;

разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;

проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;

контроль обеспечения уровня защищенности ПДн.

* 1. В настоящей Модели угроз используются следующие понятия:

безопасность ПДн – состояние защищенности ПДн, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность ПДн при их обработке в ИСПДн;

вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на ПДн или ресурсы ИСПДн;

вспомогательные технические средства и системы – технические средства   
и системы, не предназначенные для передачи, обработки и хранения ПДн, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки ПДн, или в помещениях, в которых установлены ИСПДн;

доступ в операционную среду компьютера ИСПДн – 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 и использования информации;

защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых актов или требованиями, устанавливаемыми собственником информации;

информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в ИСПДн;

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

источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации;

контролируемая зона – пространство, в котором исключено неконтролируемое пребывание сотрудников оператора, иных лиц и посторонних транспортных, технических и иных материальных средств;

нарушитель безопасности ПДн – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПДн при их обработке техническими средствами в ИСПДн;

несанкционированный доступ (далее – НСД) – 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;

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 электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания;

пользователь ИСПДн – лицо, участвующее в функционировании ИСПДн   
или использующее результаты ее функционирования;

программное (программно-математическое) воздействие – это несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ;

средства вычислительной техники (далее – СВТ) – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

технические средства ИСПДн – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (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;

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

угрозы безопасности ПДн (далее - УБПДн) – совокупность условий   
и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий при их обработке в ИСПДн;

уничтожение ПДн – действия, в результате которых невозможно восстановить содержание ПДн в ИСПДн или в результате которых уничтожаются материальные носители ПДн;

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

уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности ПДн;

целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

1. **Классификация угроз безопасности ПДн**
   1. Состав и содержание УБПДн определяется совокупностью условий   
      и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды, путей распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы.

К характеристикам ИСПДн, обусловливающим возникновение УБПДн, относятся категория и объем обрабатываемых в ИСПДн ПДн, структура ИСПДн, наличие подключения ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, характеристики подсистемы безопасности ПДн, обрабатываемых в ИСПДн, режимы обработки ПДн, режимы разграничения прав доступа пользователей ИСПДн, местонахождение и условия размещения технических средств ИСПДн.

ИСПДн представляют собой совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых   
при обработке ПДн.

Основными элементами ИСПДн являются:

ПДн, содержащиеся в базах данных, как совокупность информации и ее носителей, используемых в ИСПДн;

информационные технологии, применяемые при обработке ПДн;

технические средства, осуществляющие обработку ПДн (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн, 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) (далее – технические средства ИСПДн);

программные средства (операционные системы, системы управления базами данных и т.п.);

средства защиты информации;

вспомогательные технические средства и системы (далее - ВТСС) – технические средства и системы, их коммуникации, не предназначенные   
для обработки ПДн, но размещенные в помещениях (далее – служебные помещения), в которых расположены ИСПДн, 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).

Свойства среды, пути распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической среды, в которой распространяются ПДн, и определяются при оценке возможности реализации УБПДн.

Возможности источников УБПДн обусловлены совокупностью способов несанкционированного и (или) случайного доступа к ПДн, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

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

Основными элементами канала реализации УБПДн (рисунок 1) являются:

источник УБПДн – субъект, материальный объект или физическое явление, создающие УБПДн;

среда, путь распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать   
на защищаемые свойства (конфиденциальность, целостность, доступность) ПДн;

носитель ПДн – физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Среда, путь распространения ПДн или воздействий на защищаемые свойства ПДн

Носитель ПДн

Источник угроз безопасности ПДн

Рисунок 1. Обобщенная схема канала реализации угроз безопасности ПДн.

Носители ПДн могут содержать информацию, представленную в следующих видах:

акустическая (речевая) информация, содержащаяся непосредственно   
в произносимой речи пользователя ИСПДн при осуществлении им функции голосового ввода ПДн в ИСПДн, либо воспроизводимая акустическими средствами ИСПДн (если такие функции предусмотрены технологией обработки ПДн),   
а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;

видовая информация, представленная в виде текста и изображений различных устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн;

информация, обрабатываемая (циркулирующая) в ИСПДн, в виде электрических, электромагнитных, оптических сигналов;

информация, обрабатываемая в ИСПДн, представленная в виде бит, байт, файлов и других логических структур.

* 1. В целях формирования систематизированного перечня УБПДн при их обработке в ИСПДн и разработке на их основе частных моделей применительно   
     к конкретному виду ИСПДн угрозы классифицируются в соответствии   
     со следующими признаками:

по виду защищаемой от УБПДн информации, содержащей ПДн;

по видам возможных источников УБПДн;

по типу ИСПДн, на которые направлена реализация УБПДн;

по способу реализации УБПДн;

по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);

по используемой уязвимости;

по объекту воздействия.

* + 1. По виду информации, содержащей ПДн, в процессе установления уровня защищенности и организации мероприятий, направленных на нейтрализацию угроз безопасности, ИСПДн разделяются на:

общедоступные – ПДн, которые опубликованы в открытых источниках с согласия субъекта ПДн;

специальные – ПДн, которые касаются сексуальной жизни субъекта, его политических, философских и религиозных воззрений, а также расовой и половой принадлежности;

биометрические – любые биологические либо физиологические особенности, которые дают возможность определить личность субъекта, к примеру, ДНК, фотографии, группа крови, рисунок сетчатки глаза, отпечатки пальцев и т.д.;

иные – ПДн, которые нельзя определить ни в одну из других групп.

* + 1. По видам возможных источников УБПДн выделяются следующие классы угроз:

угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн (внутренний нарушитель);

угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель).

* + 1. В зависимости от целей и содержания обработки ПДн осуществляется их обработка в ИСПДн различных типов:

по структуре ИСПДн разделяются на локальные и распределенные информационные системы;

по наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена: системы, имеющие подключения,   
и системы, не имеющие подключений;

по режиму обработки ПДн в ИСПДн: информационные системы однопользовательские и многопользовательские;

по разграничению прав доступа пользователей: системы с разграничением   
и без разграничения прав доступа.

* + 1. По способам реализации УБПДн выделяются следующие классы угроз:

угрозы, связанные с несанкционированными действиями к ПДн (в том числе угрозы внедрения вредоносных программ);

угрозы утечки ПДн по техническим каналам утечки информации;

угрозы специальных воздействий на ИСПДн.

* + 1. По виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн) выделяются следующие классы угроз:

угрозы, приводящие к нарушению конфиденциальности ПДн (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 ПДн или их уничтожение;

угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы ИСПДн,   
в результате которого осуществляется блокирование ПДн.

* + 1. По используемой уязвимости выделяются следующие классы угроз:

угрозы, реализуемые с использованием уязвимости системного программного обеспечения (далее – ПО);

угрозы, реализуемые с использованием уязвимости прикладного ПО;

угрозы, возникающие в результате использования уязвимости, вызванной наличием в автоматизированных средствах аппаратной 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 НСД;

угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;

угрозы, реализуемые с использованием уязвимостей средств защиты информации.

* + 1. По объекту воздействия выделяются следующие классы угроз:

УБПДн, обрабатываемых на автоматизированных рабочих местах;

УБПДн, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.);

УБПДн, передаваемых по сетям связи;

угрозы прикладным программам, с помощью которых обрабатываются ПДн;

угрозы системному ПО, обеспечивающему функционирование ИСПДн.

1. **Угрозы утечки информации по техническим каналам**

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

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

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).

Носителем ПДн является пользователь ИСПДн, осуществляющий голосовой ввод ПДн в ИСПДн, акустическая система ИСПДн, воспроизводящая ПДн,   
а также технические средства ИСПДн и вспомогательные технические средства   
и системы (ВТСС), создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений   
и процессов, количественных характеристик физических величин.

При обработке ПДн в ИСПДн за счет реализации технических каналов утечки информации возможно возникновение следующих УБПДн:

угрозы утечки акустической (речевой) информации;

угрозы утечки видовой информации;

угрозы утечки информации по каналам побочных электромагнитных излучений и наводок.

* 1. Угрозы утечки акустической (речевой) информации.

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

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 ПДн, ВТСС и строительных конструкциях   
и инженерно-технических коммуникациях под воздействием акустических волн.

Кроме этого, перехват акустической (речевой) информации возможен   
с использованием специальных электронных устройств съема речевой информации, внедренных в технические средства обработки ПДн, ВТСС и помещения   
или подключенных к каналам связи.

Угрозы безопасности ПДн, связанные с перехватом акустической информации с использованием специальных электронных устройств съема речевой информации (закладочных устройств), определяются в соответствии с нормативными документами Федеральной службы безопасности Российской Федерации в установленном ею порядке.

Перехват акустической (речевой) информации может вестись:

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

портативной возимой 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.

В ИСПДн Администрации города Вологды функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют. Вероятность реализации угрозы утечки акустической (речевой) информации определена как маловероятная, возможность реализации угрозы является низкой, показатель опасности угрозы – неактуальная.

* 1. Угрозы утечки видовой информации.

Угрозы утечки видовой информации реализуются за счет просмотра ПДн   
с помощью оптических (оптикоэлектронных) 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 ИСПДн.

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

Рабочие места пользователей ИСПДн должны быть организованы таким образом, чтобы был исключен случайный просмотр информации с экранов автоматизированных рабочих мест.

Вероятность реализации угрозы утечки видовой информации определена   
как низкая, возможность реализации угрозы является средней, показатель опасности угрозы – актуальная.

3.4. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок.

Возникновение угрозы утечки информации по каналам побочных электромагнитных излучений и наводок возможно за счет перехвата техническими средствами побочных (не связанных с прямым функциональным значением элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническими средствами ИСПДн.

Все элементы ИСПДн находятся внутри контролируемой зоны   
на достаточном расстоянии от ее границ. Информативный сигнал в каналах побочных электромагнитных излучений и наводок современных средств вычислительной техники очень низок и он маскируется множеством других излучений от автоматизированных рабочих мест, не состоящих в ИСПДн,   
а также от прочих элементов современной информационной инфраструктуры.

Вероятность реализации угрозы утечки информации по каналам побочных электромагнитных излучений и наводок определена как маловероятная, возможность реализации угрозы является низкой, показатель опасности угрозы – неактуальная.

1. **Угрозы несанкционированного доступа к информации в ИСПДн Администрации города Вологды**

4.1. Угрозы НСД в ИСПДн 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) ПДн,   
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);

комбинированные угрозы – представляют собой сочетание угроз, перечисленных выше.

* 1. Источниками угроз НСД в ИСПДн могут быть:

нарушитель;

носитель вредоносной программы;

аппаратная закладка.

* 1. По наличию права постоянного или разового доступа   
     в контролируемую зону ИСПДн нарушители подразделяются на два типа:

нарушители, не имеющие доступа к ИСПДн, реализующие угрозы   
из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, – внешние нарушители;

нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, – внутренние нарушители.

* 1. Носителем вредоносной программы является аппаратный элемент компьютера или программный контейнер. Если вредоносная программа   
     не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

отчуждаемый носитель, то есть дискета, оптический диск (CD-R, CD-RW), флэш–память, отчуждаемый жесткий диск и т.п.;

встроенные носители информации (жесткие диски, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок: видеоадаптера, сетевой платы, звуковой платы, модема, устройств ввода/вывода магнитных жестких и оптических дисков, блока питания и т.п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода/вывода);

микросхемы внешних устройств (монитора, клавиатуры, принтера, модема, сканера и т.п.).

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

пакеты передаваемых по компьютерной сети сообщений;

файлы (текстовые, графические, исполняемые и т.д.).

* 1. Причинами возникновения уязвимостей ИСПДн являются:

ошибки при проектировании и разработке программного (программно–аппаратного) обеспечения;

преднамеренные действия по внесению уязвимостей в ходе проектирования   
и разработки программного (программно-аппаратного) обеспечения;

неправильные настройки ПО, неправомерное изменение режимов работы устройств и программ;

несанкционированное внедрение и использование неучтенных программ   
с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

внедрение вредоносных программ, создающих уязвимости в программном   
и программно-аппаратном обеспечении;

несанкционированные неумышленные действия пользователей, приводящие   
к возникновению уязвимостей;

сбои в работе аппаратного и программного обеспечения (вызванные сбоями   
в электропитании, выходом из строя аппаратных элементов в результате старения   
и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

* 1. Угрозы доступа (проникновения) в операционную среду компьютера   
     и несанкционированного доступа к ПДн связаны с доступом:

к информации и командам, хранящимся в базовой системе ввода/вывода (BIOS) ИСПДн, с возможностью перехвата управления загрузкой операционной системы и получением прав доверенного пользователя;

в операционную среду, то есть в среду функционирования локальной операционной системы отдельного технического средства ИСПДн   
с возможностью выполнения НСД путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия;

в среду функционирования прикладных программ (например, к локальной системе управления базами данных);

непосредственно к информации пользователя (к файлам, текстовой, аудио   
и графической информации, полям и записям в электронных базах данных)   
и обусловлены возможностью нарушения ее конфиденциальности, целостности   
и доступности.

* 1. В случае если ИСПДн реализована на базе локальной   
     или распределенной информационной системы, то в ней могут быть реализованы угрозы безопасности информации путем использования протоколов межсетевого взаимодействия. При этом может обеспечиваться НСД к ПДн или реализовываться угроза отказа в обслуживании. Особенно опасны угрозы, когда ИСПДн представляет собой распределенную информационную систему, подключенную   
     к сетям общего пользования и (или) сетям международного информационного обмена.
  2. Программно-математическое воздействие – это воздействие с помощью вредоносных программ.

Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

скрывать признаки своего присутствия в программной среде компьютера;

обладать способностью к самодублированию, ассоциированию себя   
с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

разрушать (искажать произвольным образом) код программ в оперативной памяти;

выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирование, уничтожение, блокирование и т.п.);

сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся   
в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.