Аппарат Администрации Ненецкого автономного округа

ПРИКАЗ

от 28 июня 2017 г. № 53
г. Нарьян-Мар

Об утверждении Модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных Аппарата Администрации Ненецкого автономного округа

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» ПРИКАЗЫВАЮ:

1. Утвердить Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных Аппарата Администрации Ненецкого автономного округа согласно Приложению.

2. Настоящий приказ вступает в силу со дня его официального опубликования.

Первый заместитель губернатора
Ненецкого автономного округа –
руководитель Аппарата Администрации
Ненецкого автономного округа М.В. Васильев

Приложение
к приказу Аппарата Администрации
Ненецкого автономного округа
от 28.06.2017 № 53
«Об утверждении Модели угроз
безопасности персональных данных
при их обработке в информационных
системах персональных данных
Аппарата Администрации Ненецкого
автономного округа»

Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных Аппарата Администрации Ненецкого автономного округа

Раздел I
Общие положения

1. Настоящая Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных Аппарата Администрации Ненецкого автономного округа (далее – Модель угроз) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Угрозы безопасности персональных данных 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 персональных данных, которое ведет к ущербу жизненно важных интересов личности, общества и государства.

Модель угроз содержит исходные данные по угрозам безопасности персональных данных, обрабатываемых в информационных системах персональных данных Аппарата Администрации Ненецкого автономного округа (далее – ИСПДн), связанным:

с перехватом (съемом) персональных данных 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 персональных данных или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них персональных данных с использованием

программных и программно-аппаратных средств с целью уничтожения или блокирования персональных данных.

2. Настоящая Модель угроз разработана в соответствии с:

Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённой Федеральной службой по техническому и экспортному контролю 15.02.2008;

Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённой Федеральной службой по техническому и экспортному контролю 15.02.2008.

3. С применением Модели угроз решаются следующие задачи:

1) разработка частных моделей угроз безопасности персональных данных в конкретных ИСПДн с учетом их назначения, условий и особенностей функционирования;

2) анализ защищенности ИСПДн от угроз безопасности персональных данных в ходе организации и выполнения работ по обеспечению безопасности персональных данных;

3) разработка системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса ИСПДн;

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

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

6) контроль обеспечения уровня защищенности персональных данных.

4. В настоящей Модели угроз используются следующие понятия:

1) 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 персональных данных;

2) блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

3) вредоносная программа — программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на

персональные данные или ресурсы информационной системы персональных данных;

4) 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 персональных данных;

5) доступ в операционную среду компьютера (информационной системы персональных данных) — получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ;

6) доступ к информации — возможность получения информации и ее использования;

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

8) информативный сигнал — электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных;

9) информационная система персональных данных — это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

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

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

12) контролируемая зона — это пространство, в котором исключено неконтролируемое пребывание сотрудников оператора, иных лиц и посторонних транспортных, технических и иных материальных средств.

13) конфиденциальность персональных данных — обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

14) нарушитель безопасности персональных данных — физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их

обработке техническими средствами в информационных системах персональных данных;

15) 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;

16) 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;

17) перехват информации — неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов;

18) 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;

19) пользователь информационной системы персональных данных — лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования;

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

21) средства вычислительной техники — совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

22) технические средства информационной системы 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), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации;

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

24) 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 персональных данных;

25) уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

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

27) уязвимость информационной системы персональных данных — недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных данным;

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

Раздел II
Классификация и исходный уровень защищённости информационных систем персональных данных Аппарата Администрации Ненецкого автономного округа

5. Состав и содержание угроз 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 ИСПДн, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы.

6. В зависимости от целей и содержания обработки персональных данных осуществляется их обработка в ИСПДн различных типов.

7. ИСПДн объединяют обобщённые характеристики:

по структуре ИСПДн: локальные информационные системы 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 персональных данных в информационной системе информационные системы: многопользовательские;

по разграничению прав доступа пользователей: системы с разграничением прав доступа.

Все технические средства ИСПДн находятся в пределах Российской Федерации.

8. В зависимости от технологий, состава и характеристик технических средств ИСПДн, а также опасности реализации угроз безопасности персональных данных и наступления последствий в результате несанкционированного или случайного доступа все ИСПДн можно классифицировать как следующие типы ИСПДн:

локальные ИСПДн, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

распределенные ИСПДн, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

9. Исходный уровень защищённости ИСПДн определен как средний, так как не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний».

Показатели исходной защищенности ИСПДн определены в Приложении 1 к настоящей Модели угроз.

Раздел III
Классификация актуальных угроз безопасности персональных данных

10. 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.

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

11. При обработке персональных данных в локальных ИСПДн, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих угроз безопасности персональных данных:

1) угрозы утечки информации по техническим каналам;

2) угрозы несанкционированного доступа к персональным данным, обрабатываемым на автоматизированном рабочем месте.

12. Угрозы утечки информации по техническим каналам включают в себя:

1) угрозы утечки акустической (речевой) информации;

2) угрозы утечки видовой информации;

3) угрозы утечки информации по каналу побочных электромагнитных излучений и наводок.

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

14. Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средства обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

15. Угрозы утечки информации по каналу побочных электромагнитных излучений и наводок возможны из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из-за наличия электромагнитных излучений монитора.

16. Угрозы несанкционированного доступа в локальных ИСПДн связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

17. Угрозы несанкционированного доступа в ИСПДн, связанные с действиями нарушителей, имеющих доступ к ИСПДн, включают в себя:

1) угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;

2) угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.);

3) угрозы внедрения вредоносных программ.

18. Угрозы несанкционированного доступа в локальных ИСПДн включают в себя:

1) угрозы «Анализа сетевого трафика» с перехватом передаваемой по локальной сети информации;

2) угрозы выявления паролей;

3) угрозы удаленного запуска приложений;

4) угрозы внедрения по сети вредоносных программ.

Раздел IV
Угрозы утечки информации по техническим каналам

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

20. 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.

21. При обработке персональных данных в ИСПДн за счет реализации технических каналов утечки информации возможно возникновение следующих угроз безопасности персональных данных:

1) угрозы утечки акустической (речевой) информации;

2) угрозы утечки видовой информации;

3) угроз утечки информации по каналам побочных электромагнитных излучений и наводок.

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

23. Перехват акустической (речевой) информации 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.

Перехват акустической (речевой) информации также возможен с использованием специальных электронных устройств съема речевой информации, внедренных в технические средства обработки персональных данных, вспомогательные технические средства и системы и помещения или подключенных к каналам связи.

24. В ИСПДн функции голосового ввода персональных данных или функции воспроизведения персональных данных акустическими средствами отсутствуют.

Вероятность реализации угрозы утечки акустической (речевой) информации определена как маловероятная, возможность реализации угрозы является низкой, показатель опасности угрозы — неактуальная.

25. Угрозы утечки видовой информации реализуются за счет просмотра персональных данных 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) персональных данных также возможен с использованием специальных электронных устройств съема, внедренных в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений.

В Аппарате Администрации Ненецкого автономного округа доступ посторонних лиц ограничен в соответствии с Положением о пропускном и внутриобъектовом режимах в административном здании органов государственной власти Ненецкого автономного округа, утвержденным приказом Аппарата Администрации Ненецкого автономного округа от 17.01.2017 № 1.

Рабочие места пользователей ИСПДн организованы таким образом, чтобы был исключён случайный просмотр информации с экранов автоматизированных рабочих мест. На окнах установлены жалюзи.

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

27. 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 персональных данных техническими средствами ИСПДн.

Все элементы ИСПДн находятся внутри контролируемой зоны на достаточном расстоянии от её 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.

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

29. Обобщённая информация по угрозам утечки информации по техническим каналам представлена в Приложении 2 к настоящей Модели угроз.

Раздел V
Угрозы несанкционированного доступа к информации в информационных системах персональных данных Аппарата Администрации Ненецкого автономного округа

30. Угрозы несанкционированного доступа 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) персональных данных, и включают в себя:

1) угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);

2) 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.;

3) угрозы внедрения вредоносных программ (программно-математического воздействия);

4) комбинированные угрозы, представляющие собой сочетание угроз, указанных в подпунктах 1 – 3 настоящего пункта.

31. Источниками угроз несанкционированного доступа в ИСПДн могут быть:

1) нарушитель;

2) носитель вредоносной программы;

3) аппаратная закладка.

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

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

2) нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, — внутренние нарушители.

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

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

2) встроенные носители информации (жёсткие 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);

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

34. 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:

1) пакеты передаваемых по компьютерной сети сообщений;

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

35. Причинами возникновения уязвимостей ИСПДн являются:

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

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

3) неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;

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

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

6) несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;

7) 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.).

36. Угрозы доступа (проникновения) в операционную среду компьютера и несанкционированного доступа к персональным данным связаны с доступом:

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

2) в операционную среду, то есть в среду функционирования локальной операционной системы отдельного технического средства ИСПДн

с возможностью выполнения несанкционированного доступа путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия;

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

4) 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.

37. 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 несанкционированный доступ к персональным данным 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.

38. 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.

39. Обобщённая информация по угрозам несанкционированного доступа к информации в информационной системе персональных данных представлена в Приложении 3 к настоящей Модели угроз.

Приложение 1
к Модели угроз безопасности
персональных данных при их
обработке в информационных
системах персональных данных
Аппарата Администрации Ненецкого
автономного округа, утвержденной
приказом Аппарата Администрации
Ненецкого автономного округа
от 28.06.2017.2017 № 53

Показатели исходной защищенности информационных систем персональных данных Аппарата Администрации Ненецкого автономного округа

Технические и эксплуатационные характеристики	Уровень защищенности
1. По территориальному размещению	Средний
2. По наличию соединения с сетями общего пользования	Средний
3. По встроенным (легальным) операциям с записями баз персональных данных	Средний
4. По разграничению доступа к персональным данным	Средний
5. По наличию соединений с другими базами персональных данных иных информационных систем персональных данных	Высокий
6. По уровню обобщения (обезличивания) персональных данных	Средний
7. По объему персональных данных, которые предоставляются сторонним пользователям информационных систем персональных данных без предварительной обработки	Высокий

Приложение 2
к Модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных Аппарата Администрации Ненецкого автономного округа, утвержденной приказом Аппарата Администрации Ненецкого автономного округа
от 28.06.2017 № 53

Обобщённая информация
по угрозам утечки информации по техническим каналам

Наименование угрозы	Вероятность реализации угрозы	Возможность реализации угрозы	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе
Угрозы утечки информации по техническим каналам					
Угрозы утечки акустической информации	Маловероятная	Низкая	Средняя	Неактуальная	Не требуются
Угрозы утечки видовой информации	Низкая	Средняя	Средняя	Актуальная	Порядок обращения со служебной информацией ограниченного доступа
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок	Маловероятная	Низкая	Средняя	Неактуальная	Не требуются

Приложение 3
к Модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных Аппарата Администрации Ненецкого автономного округа, утвержденной приказом Аппарата Администрации Ненецкого автономного округа
от 28.06.2017 № 53

Обобщенная информация по угрозам несанкционированного доступа к информации в информационной системе персональных данных

Наименование угрозы	Вероятность реализации угрозы	Возможность реализации угрозы	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе
Угрозы несанкционированного доступа к информации в информационной системе персональных данных					
Угрозы, реализуемые в ходе загрузки операционной системы	Низкая	Средняя	Средняя	Актуальная	Применение сертифицированных средств защиты информации от несанкционированного доступа
Угрозы, реализуемые после загрузки операционной системы	Низкая	Средняя	Средняя	Актуальная	Применение сертифицированных средств защиты информации от несанкционированного доступа, инструкция пользователя информационной системы персональных данных

Наименование угрозы	Вероятность реализации угрозы	Возможность реализации угрозы	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе
Угрозы несанкционированного доступа к информации в информационной системе персональных данных					
Угрозы внедрения вредоносных программ	Низкая	Средняя	Средняя	Актуальная	Применение сертифицированных средств защиты информации от несанкционированного доступа, антивирусного программного обеспечения
Угрозы «Анализа сетевого трафика»	Маловероятная	Средняя	Средняя	Неактуальная	Не требуется
Угрозы выявления паролей	Низкая	Средняя	Средняя	Актуальная	Применение сертифицированных средств защиты информации от несанкционированного доступа, инструкция пользователя информационной системы персональных данных
Угрозы удаленного запуска приложений	Низкая	Средняя	Средняя	Актуальная	Применение сертифицированных средств защиты информации от несанкционированного доступа, инструкция пользователя информационной системы персональных данных, инструкция администратора информационной системы персональных данных

Наименование угрозы	Вероятность реализации угрозы	Возможность реализации угрозы	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе
Угрозы несанкционированного доступа к информации в информационной системе персональных данных					
Угрозы внедрения по сети вредоносных программ	Низкая	Средняя	Средняя	Актуальная	Применение сертифицированных средств защиты информации от несанкционированного доступа, инструкция пользователя информационной системы персональных данных