ПРАВИТЕЛЬСТВО ЛЕНИНГРАДСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 26 декабря 2017 года № 615

Об определении угроз безопасности персональных данных, актуальных при их обработке в государственных информационных системах персональных данных Ленинградской области

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" Правительство Ленинградской области п о с т а н о в л я е т:

Определить угрозы безопасности персональных данных, актуальные при их обработке в государственных информационных системах персональных данных Ленинградской области, согласно приложению.

Губернатор
Ленинградской области А.Дрозденко

ОПРЕДЕЛЕНЫ
постановлением Правительства
Ленинградской области
от 26 декабря 2017 года № 615
(приложение)

УГРОЗЫ
безопасности персональных данных, актуальные при их обработке в государственных информационных системах персональных данных Ленинградской области

Настоящий документ определяет перечень угроз безопасности персональных данных, актуальных при их обработке в государственных информационных системах персональных данных Ленинградской области.

В настоящем документе используются термины и понятия, установленные Федеральным законом от 27 июля 2006 года № 152-ФЗ "О персональных данных", 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" (далее – Требования к защите персональных данных), Методикой определения актуальных угроз безопасности персональных данных, утвержденной заместителем директора Федеральной службы по техническому и экспортному контролю от 14 февраля 2008 года, Методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденными ФСБ России 31 марта 2015 года № 149/7/2/6-432.

Под актуальными угрозами безопасности персональных данных при их обработке в информационных системах персональных данных Ленинградской области понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия (далее – угрозы безопасности).

1. Информационные системы

Органами исполнительной власти Ленинградской области с целью исполнения государственных функций создаются

и эксплуатируются информационные системы персональных данных (далее – ИСПДн).

Учет и регистрация ИСПДн Ленинградской области осуществляется в соответствии с постановлением Правительства Ленинградской области от 23 мая 2006 года № 156 "Об утверждении Положения о порядке учета и регистрации государственных информационных ресурсов и информационных систем Ленинградской области" в Едином реестре государственных информационных ресурсов и информационных систем Ленинградской области.

В ИСПДн Ленинградской области обрабатываются специальные, биометрические, общедоступные и иные категории персональных данных работников органов государственной власти Ленинградской области и иных субъектов персональных данных.

В соответствии с Требованиями к защите персональных данных для ИСПДн Ленинградской области рассматриваются:

угрозы второго типа, актуальные для информационных систем, если для них в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей (далее – НДВ) в прикладном программном обеспечении, используемом в информационной системе;

угрозы третьего типа, актуальные для информационных систем, если для них актуальны угрозы, не связанные с наличием НДВ в системном и прикладном программном обеспечении, используемом в информационной системе.

Необходимость обеспечения защиты персональных данных в ИСПДн Ленинградской области рассматривается до второго уровня защищенности включительно.

2. Структура

ИСПДн Ленинградской области являются региональными, территориально-распределенными системами, по характеру содержания и технологии обработки данных относятся к однотипным и разноплановым системам.

Хранилища (носители) баз данных ИСПДн размещаются в зданиях органов государственной власти и органов местного самоуправления Ленинградской области, подведомственных им организациях, расположенных на территории Санкт-Петербурга и Ленинградской области, а также, при условии заключения государственных контрактов (соглашений, договоров), в иных организациях на территории Российской Федерации.

Взаимодействие территориальных распределенных сегментов ИСПДн осуществляется посредством проводных каналов связи и каналов подвижной сотовой связи.

Пользователями ИСПДн являются государственные и муниципальные органы Ленинградской области.

3. Угрозы безопасности персональных данных, актуальные при их обработке в информационных системах персональных данных

3.1. Факторы, воздействующие на безопасность информации

Факторы, воздействующие на безопасность информации в информационных системах (факторы угроз), по характеру возникновения подразделяются на объективные и субъективные, по отношению к объектам информатизации – на внешние и внутренние.

Объективные (естественные) факторы угроз – физические процессы или стихийные природные явления, не зависящие от человека (пожары, наводнения, ураганы, землетрясения и т.п.), приводящие к угрозе безопасности информации.

Субъективные (искусственные) факторы угроз – преднамеренно или непреднамеренно совершаемые действия, приводящие к нарушениям безопасности информации.

К внешним факторам угроз относятся стихийные бедствия, техногенные катастрофы, возникающие за пределами контролируемой территории, на которой размещены объекты информатизации, и (или) субъекты, которые не связаны с защищаемой информацией, но могут нарушить или нарушают состояние ее безопасности.

К внутренним факторам угроз относятся техногенные аварии, которые возникают на территории объекта защиты (отказы и сбои технических средств жизнеобеспечения (электропитание, водоснабжение, климатическое обеспечение и т.п.), лица, которые своими действиями (бездействием) могут нарушить или нарушают состояние информационной безопасности на территории объекта защиты.

К факторам угроз безопасности информации (персональных данных) в ИСПДн относятся объективные внутренние факторы – дефекты, сбои и отказы, аварии технических средств и систем объектов информатизации, субъективные внешние и внутренние факторы угроз безопасности информации – неправомерные действия нарушителей, ошибки пользователей и обслуживающего персонала.

3.2. Актуальные угрозы безопасности

К угрозам безопасности персональных данных при их обработке в информационных системах персональных данных Ленинградской области относятся:

выход из строя аппаратно-программных средств;

а) угрозы, связанные с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн:

угроза преднамеренного физического вывода из строя средств вычислительной техники, каналов связи,

угроза несанкционированного доступа к машинным носителям и хранящейся на них конфиденциальной информации,

угроза перехвата паролей или идентификаторов,

угроза модификации базовой системы ввода/вывода (BIOS),

угроза перехвата управления загрузкой,

угрозы выполнения несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы, прикладного программного обеспечения (далее – ПО), специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.),

угрозы внедрения вредоносных программ с отчуждаемых носителей,

несанкционированное подключение модемов;

б) угрозы, реализуемые с использованием протоколов межсетевого взаимодействия из внешних сетей (в том числе по каналам подвижной сотовой связи):

угрозы анализа сетевого трафика с перехватом передаваемой из ИСПДн и принимаемой в ИСПДн из внешних сетей информации,

угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.,

угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях,

угрозы подмены доверенного объекта,

угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях,

несанкционированное подключение средств удаленного администрирования,

угрозы выявления паролей,

угрозы типа "Отказ в обслуживании",

угрозы удаленного запуска приложений,

угрозы внедрения вредоносных программ по сети;

в) угрозы, связанные с использованием технологии виртуализации:

угроза атаки на активное и/или пассивное виртуальное и/или физическое сетевое оборудование из физической и/или виртуальной сети,

угроза атаки на виртуальные каналы передачи,

угроза атаки на гипервизор из виртуальной машины и/или физической сети,

угроза атаки на защищаемые виртуальные устройства из виртуальной и/или физической сети,

угроза атаки на защищаемые виртуальные машины из виртуальной и/или физической сети,

угроза атаки на систему хранения данных из виртуальной и/или физической сети,

угроза выхода процесса за пределы виртуальной машины,

угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение,

угроза нарушения изоляции пользовательских данных внутри виртуальной машины,

угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия,

угроза перехвата управления гипервизором,

угроза перехвата управления средой виртуализации,

угроза неконтролируемого роста числа виртуальных машин,

угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов,

угроза нарушения технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин,

угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации,

угроза ошибок обновления гипервизора;

г) угрозы, связанные с использованием средств защиты информации:

угроза нарушения технологического/производственного процесса из-за задержек, вносимых средством защиты,

угроза несанкционированного изменения параметров настройки средств защиты информации,

угроза несанкционированного воздействия на средство защиты информации.

3.3. Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых средствами криптографической защиты информации (далее – СКЗИ) персональных данных или создания условий для этого

Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, содержит систему взглядов на потенциальных нарушителей безопасности информации, обрабатываемой в информационных системах, причины и мотивацию их действий, преследуемые ими цели и общий характер действий в процессе подготовки и совершения воздействия на информацию.

В качестве обобщенных возможностей источников атак на информационные системы рассматриваются:

возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны;

возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования;

возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования;

возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения).

При выборе СКЗИ для информационных систем рассматриваются следующие возможности создания способов подготовки и проведения атак:

а) создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;

б) создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ;

в) проведение атаки, находясь вне контролируемой зоны;

г) проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и на этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:

внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ, и в совокупности представляющие среду функционирования СКЗИ (далее – компоненты СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ,

внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ;

д) проведение атак на этапе эксплуатации СКЗИ на:

персональные данные,

ключевую, аутентифицирующую и парольную информацию СКЗИ,

программные компоненты СКЗИ,

аппаратные компоненты СКЗИ,

программные компоненты СФ, включая программное обеспечение BIOS,

аппаратные компоненты СФ,

данные, передаваемые по каналам связи,

иные объекты, которые установлены при формировании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учетом применяемых в информационной системе информационных технологий, аппаратных средств и программного обеспечения;

е) получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть "Интернет") информации об информационной системе, в которой используется СКЗИ. При этом может быть получена следующая информация:

общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы),

сведения об информационных технологиях, базах данных, аппаратных средствах, ПО, используемых в ИСПДн совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, аппаратные средства, ПО, используемые в информационной системе совместно с СКЗИ,

содержание конструкторской документации на СКЗИ,

содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ,

общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ,

сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее – канал связи),

все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами,

сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ,

сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ,

сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ;

ж) применение:

находящихся в свободном доступе или используемых за пределами контролируемой зоны аппаратных средств и ПО, включая аппаратные и программные компоненты СКЗИ и СФ,

специально разработанных аппаратных средств и ПО;

з) использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки:

каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами,

каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;

и) проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;

к) использование на этапе эксплуатации находящихся за пределами контролируемой зоны аппаратных средств и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее – штатные средства);

л) проведение атаки при нахождении в пределах контролируемой зоны;

м) проведение атак на этапе эксплуатации СКЗИ на следующие объекты:

документацию на СКЗИ и компоненты СФ,

служебные помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и компоненты СФ (далее – СВТ);

н) получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы,

сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы,

сведений о мерах по разграничению доступа в служебные помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;

о) использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

п) физический доступ к СВТ, на которых реализованы СКЗИ и СФ;

р) возможность располагать аппаратными компонентами СКЗИ;

с) создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак НДВ прикладного ПО;

т) проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

у) проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ.

3.4. Иные угрозы безопасности информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи, не рассматривается в связи с отсутствием необходимости голосового ввода персональных данных в информационные системы и функций воспроизведения персональных данных акустическими средствами.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации информационных систем.

Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок в технических средствах, проводах, кабелях и иных токопроводящих коммуникациях и конструкциях информационных систем, вызванные побочными и/или паразитными электромагнитными излучениями, несущими информацию, не рассматриваются в связи с необоснованными затратами применения таких способов по отношению к их эффективности.

Угрозы персональных данных, связанные с наличием НДВ в системном программном обеспечении, также не рассматриваются в силу следующих причин:

информация, обрабатываемая в информационных системах Ленинградской области, не представляет ценности для разработчиков программного обеспечения (стоимость информации не сопоставима с потерями разработчиков программного обеспечения, в случае реализации такой угрозы);

закупка программного обеспечения осуществляется для информационных систем Ленинградской области таким образом, что разработчикам программного обеспечения невозможно определить, в каких именно информационных системах будет использоваться закупаемое программное обеспечение, а следовательно, и внедрить в программное обеспечение соответствующие НДВ;

для защиты информации в информационных системах используются средства защиты, прошедшие в установленном порядке, в соответствии с законодательством Российской Федерации, процедуру оценки соответствия требованиям безопасности информации.

4. Моделирование угроз безопасности информации

Для информационных систем Ленинградской области разрабатываются частные модели угроз безопасности информации с учетом обязательных требований законодательства Российской Федерации, руководящих документов и рекомендаций уполномоченных в данной сфере органов исполнительной власти.

В зависимости от характера и условий обработки персональных данных в информационных системах перечисленные угрозы могут быть дополнены или урезаны, при условии наличия факторов, обеспечивающих их нейтрализацию.

5. Меры по защите информации

Организационные меры по обеспечению безопасности информации направлены на исключение или существенное затруднение физического доступа посторонних лиц к носителям информации и техническим средствам ее обработки с целью предотвращения их хищения, нарушения функционирования или разрушения, а также предусматривают мероприятия по предупреждению и ликвидации последствий объективных внутренних угроз, связанных с пожарами, затоплениями, иными авариями на территории размещения объекта защиты.

Для защиты от объективных внутренних угроз применяются противопожарные системы, системы бесперебойной подачи электроэнергии, иные аналогичные системы, а также предусматривается резервирование технических средств, выход из строя которых будет являться критичным для выполняемых информационных процессов.

Предотвращение физического доступа посторонних лиц к объектам информатизации обеспечивается установкой прочных дверей, надежных замков, при необходимости – решеток на окнах, устройством пропускных пунктов, применением систем охранной сигнализации, систем видеонаблюдения, автоматизированных систем контроля управлением доступа в здание, в помещения.

Организационно-технические меры по обеспечению безопасности информации направлены на предотвращение доступа к ней посторонних лиц и предупреждение преднамеренных программных и технических воздействий с целью неправомерного искажения, блокирования или уничтожения в процессе ее производства, сбора, хранения, обработки, передачи с использованием средств вычислительной техники, а также предотвращение нарушения функционирования технических средств.

Выполнение организационно-технических мер по безопасности информации реализуется с помощью применения технических средств ее защиты.

К техническим средствам защиты информации относятся средства и системы антивирусной защиты информации, разграничения доступа, обнаружения вторжений, анализа защищенности, анализа уязвимостей, резервного копирования, межсетевые экраны, виртуальные вычислительные сети, иные.

Для нейтрализации возможных угроз безопасности информации с помощью технических средств выполняются следующие мероприятия:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации;

регистрация событий безопасности;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности информации;

обеспечение целостности информационной системы и информации;

обеспечение доступности информации;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

проведение работ по подбору персонала;

доступ в контролируемую зону, где располагаются СВТ, документация на СКЗИ и компоненты СФ, обеспечивается в соответствии с контрольно-пропускным режимом;

представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СВТ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации;

сотрудники, являющиеся пользователями информационных систем, но не являющиеся пользователями СКЗИ, информированы о правилах работы в информационных системах и ответственности за несоблюдение правил обеспечения безопасности информации;

пользователи СКЗИ информированы о правилах работы в информационных системах, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации;

утверждены правила доступа в помещения, где располагаются СВТ, документация на СКЗИ и компоненты СФ, в рабочее и нерабочее время, а также в нештатных ситуациях;

осуществляется регистрация и учет действий пользователей с персональными данными;

осуществляется контроль целостности средств защиты; на автоматизированных рабочих местах и серверах, на которых установлены СКЗИ:

используются сертифицированные средства антивирусной защиты информации;

документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе;

служебные помещения, в которых располагаются СВТ, документация на СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода;

утвержден перечень лиц, имеющих право доступа в служебные помещения, в которых располагаются СВТ, документация на СКЗИ и компоненты СФ;

осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;

расположение средств визуализации информационных систем существенно затрудняющее или исключающее просмотр информации не допущенным к ней лицам.

Уточненные меры по обеспечению безопасности информации формируются в зависимости от угроз, рассматриваемых для конкретных информационных систем, и отражаются во внутренних организационно-распорядительных документах операторов персональных данных.