ПРАВИТЕЛЬСТВО САХАЛИНСКОЙ ОБЛАСТИ

П О С Т А Н О В Л Е Н И Е

от 15 июня 2017 г. № 283

г. Южно-Сахалинск

Об утверждении перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Правительстве Сахалинской области, органах исполнительной власти Сахалинской области и подведомственных им учреждениях

С целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Правительстве Сахалинской области, органах исполнительной власти Сахалинской области и подведомственных им учреждениях, в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» Правительство Сахалинской области **п о с т а н о в л я е т**:

1. Утвердить Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Правительстве Сахалинской области, органах исполнительной власти Сахалинской области и подведомственных им учреждениях (прилагается).

2. Рекомендовать администрациям муниципальных образований Сахалинской области и подведомственным им учреждениям, организациям:

- определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в используемых ими информационных

системах персональных данных;

- при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых ими информационных системах персональных данных, руководствоваться настоящим постановлением.

3. Опубликовать настоящее постановление в газете «Губернские ведомости», на официальном сайте Губернатора и Правительства Сахалинской области, на «Официальном интернет-портале правовой информации».

Председатель Правительства
Сахалинской области В.Г.Щербина

УТВЕРЖДЕН

постановлением Правительства
Сахалинской области
от 15 июня 2017 г. № 283

ПЕРЕЧЕНЬ

угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Правительстве Сахалинской области, органах исполнительной власти Сахалинской области и подведомственных им учреждениях

1. Общие положения

Учитывая особенности обработки персональных данных в Правительстве Сахалинской области, органах исполнительной власти Сахалинской области и подведомственных им учреждениях (далее - Органы власти и учреждения), а также категорию и объем обрабатываемых в информационной системе персональных данных (далее – ИСПДн), основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

Конфиденциальность - обязательное для соблюдения Органом власти и учреждением или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Целостность - состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения.

Доступность - состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Под актуальными угрозами безопасности персональных данных пони-

мается 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.

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн, согласно постановлению Правительства Российской Федерации от 01.11.2012 № 1119 подразделяются на угрозы первого, второго, третьего типа. В соответствии с пунктом 7 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором системы, определённым нормативным правовым актом Сахалинской области, с учетом оценки возможного вреда.

Для определения актуальных угроз безопасности из общего перечня угроз безопасности выбираются только те угрозы, которые являются актуальными для ИСПДн в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России от 14.02.2008.

Основной целью применения в ИСПДн Органов власти и учреждений СКЗИ является защита персональных данных при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена.

Основными видами угроз безопасности персональным данным в ИСПДн являются:

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к информационным ресурсам ИСПДн, вклю-

чая пользователей ИСПДн;

- 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;

- угрозы, возникновение которых напрямую зависит от свойств техники и программного обеспечения (далее – ПО), используемого в ИСПДн;

- угрозы, возникающие в результате внедрения аппаратных закладок и вредоносных программ;

- угрозы, направленные на нарушение нормальной работы технических средств и средств связи, используемых в ИСПДн;

- угрозы, связанные с недостаточной квалификацией обслуживающего ИСПДн персонала.

2. Актуальные угрозы безопасности ИСПДн Органов власти и учреждений

2.1. ИСПДн Органов власти и учреждений отличаются следующими особенностями:

- использованием стандартных (унифицированных) технических средств обработки информации;

- использованием типового ПО;

- наличием незначительного количества автоматизированных рабочих мест, участвующих в обработке персональных данных;

- дублированием информации, содержащей персональные данные, на бумажных носителях и внешних накопителях информации;

- незначительными негативными последствиями для субъектов персональных данных при реализации угроз безопасности ИСПДн;

- эксплуатацией ИСПДн (как правило) сотрудниками Органов власти и учреждений без привлечения на постоянной основе сторонних организаций;

- жесткой регламентацией процедуры взаимодействия со сторонними

организациями (банки, пенсионные, страховые и налоговые органы, органы статистики).

2.2. Актуальными угрозами безопасности ИСПДн Органов власти и учреждений (учитывая угрозы, изложенные в Банке данных угроз безопасности информации http://bdu.fstec.ru/threat), учитывая положения, изложенные в настоящем разделе, признаются:

- угрозы внедрения кода или данных;

- угрозы утраты, хищения вычислительных ресурсов и носителей защищаемой информации;

- угрозы несанкционированного воздействия на защищаемую информацию;

- угрозы воздействия на программы с высокими привилегиями;

- угрозы нарушения целостности данных кеша;

- угрозы непреднамеренного или преднамеренного вывода из строя технических средств и средств защиты информации (далее – СЗИ);

- угрозы несанкционированного отключения СЗИ;

- угрозы физического устаревания аппаратных компонентов;

- угрозы форматирования носителей информации;

- угрозы несанкционированного воздействия на идентификационную и аутентификационную информацию;

- угрозы преодоления физической защиты;

- угрозы получения предварительной информации об объекте защиты;

- угрозы подделки записей журнала регистрации событий;

- угрозы несанкционированного воздействия на системный реестр;

- угрозы перехвата привилегированного процесса или потока;

- угрозы некорректного использования функционала программного обеспечения;

- угрозы внедрения вредоносного кода;

- угрозы загрузки нештатной операционной системы.

3. Актуальные угрозы безопасности государственных информационных систем (далее – ГИС) Органов власти и учреждений, обрабатывающих персональные данные

3.1. ГИС Органов власти и учреждений, обрабатывающих персональные данные, отличаются следующими особенностями:

- использованием широкой номенклатуры (зачастую уникальных) технических средств получения, отображения и обработки информации;

- использованием специального (адаптированного под конкретную задачу) ПО;

- наличием значительного количества автоматизированных рабочих мест, участвующих в обработке персональных данных;

- построением ГИС на базе распределенной по территории Сахалинской области 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 СЗИ, сертифицированных СКЗИ 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 СЗИ персонала;

- проблемами взаимодействия различных ГИС, вызванными несовер-

шенством действующего законодательства и ведомственных инструкций.

3.2. Актуальными угрозами безопасности ГИС Органов власти и учреждений, обрабатывающих персональные данные (учитывая угрозы, изложенные в Банке данных угроз безопасности информации http://bdu.fstec.ru/threat), учитывая положения, изложенные в настоящем разделе, помимо угроз, указанных в пункте 2.2 настоящего 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 удаленного внеполосного доступа к аппаратным средствам;

- угрозы неправомерных действий в каналах связи;

- угрозы межсайтового скриптинга;

- угрозы межсайтовой подделки запросов;

- угрозы использования альтернативных путей доступа к ресурсам;

- угрозы «фарминга»;

- угрозы «фишинга»;

- угрозы спама веб-сервера;

- угрозы доступа/перехвата/изменения HTTP cookies;

- угрозы «кражи» учётной 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.
