ПРАВИТЕЛЬСТВО ЕВРЕЙСКОЙ АВТОНОМНОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

13.04.2018 № 128-пп

г. Биробиджан

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности аппаратом губернатора и правительства Еврейской автономной области, органами исполнительной власти области, формируемыми правительством Еврейской автономной области, и областными государственными учреждениями

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и законом Еврейской автономной области от 27.06.2012 № 79-ОЗ «О правительстве Еврейской автономной области» правительство Еврейской автономной области

ПОСТАНОВЛЯЕТ:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности аппаратом губернатора и правительства Еврейской автономной области, органами исполнительной власти области, формируемыми правительством Еврейской автономной области, и областными государственными учреждениями, согласно приложению к настоящему постановлению.

2. Руководителям органов исполнительной власти области, формируемых правительством Еврейской автономной области, структурных подразделений аппарата губернатора и правительства Еврейской автономной

области, областных государственных учреждений руководствоваться настоящим постановлением при разработке частных моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

3. Контроль за выполнением настоящего постановления возложить на вице-губернатора Еврейской автономной области.

4. Настоящее постановление вступает в силу со дня его подписания.

Губернатор области А.Б. Левинталь

аппарат губернатора и правительства Еврейской автономной области
ОРГАНИЗАЦИОННОЕ УПРАВЛЕНИЕ

Приложение
к постановлению правительства
Еврейской автономной области
от 13.09.2018 № 128-пп

Угрозы
безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности аппаратом губернатора и правительства Еврейской автономной области, органами исполнительной власти области, формируемыми правительством Еврейской автономной области, и областными государственными учреждениями

Учитывая особенности обработки персональных данных в аппарате губернатора и правительства Еврейской автономной области, органах исполнительной власти области, формируемых правительством Еврейской автономной области (далее – органы государственной власти), и областных государственных учреждениях (далее – учреждения), а также категорию и объем обрабатываемых персональных данных в информационных системах персональных данных, основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

Конфиденциальность – обязательное для выполнения лицом, получившим доступ к персональным данным, 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 понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационных системах персональных данных, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Основной целью применения в информационных системах

персональных данных средств криптографической защиты информации является защита персональных данных при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена.

Основными видами угроз безопасности персональных данных в информационных системах персональных данных органов государственной власти и учреждений являются:

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к информационным ресурсам информационных систем персональных данных органов государственной власти и учреждений;

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к информационным системам персональных данных органов государственной власти и учреждений, 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 информационных системах персональных данных органов государственной власти и учреждений;

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

- угрозы, направленные на нарушение нормальной работы технических средств и средств связи, используемых в информационных системах персональных данных органов государственной власти и учреждений;

- угрозы, связанные с недостаточной квалификацией персонала, обслуживающего информационные системы персональных данных органов государственной власти и учреждений.

1.1. Актуальные угрозы безопасности информационных систем персональных данных органов государственной власти и учреждений.

1.1.1. Информационные системы персональных данных органов государственной 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 в информационных системах персональных данных органов государственной власти и учреждений;

- эксплуатацией информационных систем персональных данных органов государственной власти и учреждений сотрудниками органов государственной 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).

1.1.2. Актуальными угрозами безопасности информационных систем персональных данных органов государственной власти и учреждений (включая угрозы, указанные в Банке данных угроз безопасности информации http://bdu.fstec.ru/threat), 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;

- угрозы несанкционированного отключения средств защиты информации;

- 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 ПО;

- угрозы внедрения вредоносного кода;

- угрозы загрузки нештатной операционной системы;

- угрозы реализации целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых средствами криптографической защиты информации персональных данных или создания условий для этого (далее – атака) при нахождении в пределах контролируемой зоны;

- угрозы проведения атаки на этапе эксплуатации средств криптографической защиты информации на следующие объекты:

а) документацию на средства криптографической защиты информации и компоненты среды функционирования средств криптографической защиты информации;

б) помещения, в которых находится совокупность программных и технических элементов информационных систем персональных данных органов государственной власти и учреждений, способных функционировать самостоятельно или в составе других систем, на которых реализованы средства криптографической защиты информации и среда функционирования средств криптографической защиты информации;

- угрозы получения в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

а) сведений о физических мерах защиты объектов, в которых размещены ресурсы информационных систем персональных данных органов государственной власти и учреждений;

б) сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационных систем персональных данных органов государственной власти и учреждений;

в) сведений о мерах по разграничению доступа в помещения, в которых находятся средства вычислительной техники, на которых реализованы средства криптографической защиты информации и среда функционирования средств криптографической защиты информации;

- угрозы использования штатных средств информационных систем персональных данных органов государственной власти и учреждений, ограниченного мерами, реализованными в информационных системах персональных данных органов государственной власти и учреждений, в которых используются средства криптографической защиты информации, и направленными на предотвращение и пресечение несанкционированных действий;

- угрозы физического доступа к средствам вычислительной техники, на которых реализованы средства криптографической защиты информации и среда функционирования средств криптографической защиты информации;

- угрозы возможностей воздействия на аппаратные компоненты средств

криптографической защиты информации и среду функционирования средств криптографической защиты информации, ограниченных мерами, реализованными в информационных системах персональных данных органов государственной власти и учреждений, в которых используются средства криптографической защиты информации, и направленными на предотвращение и пресечение несанкционированных действий;

- угрозы создания способов, подготовки и проведения атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование средств криптографической защиты информации и среду функционирования средств криптографической защиты информации, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО;

- угрозы проведения лабораторных исследований средств криптографической защиты информации, используемых вне контролируемой зоны, ограниченного мерами, реализованными в информационных системах персональных данных органов государственной власти и учреждений, в которых используются средства криптографической защиты информации, и направленными на предотвращение и пресечение несанкционированных действий;

- угрозы проведения работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа средств криптографической защиты информации и среды функционирования средств криптографической защиты информации, в том числе с использованием исходных текстов входящего в среду функционирования средств криптографической защиты информации прикладного ПО, непосредственно использующего вызовы программных функций средств криптографической защиты информации;

- угрозы создания способов, подготовки и проведения атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО;

- угрозы возможностей располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты среды функционирования средств криптографической защиты информации;

- угрозы возможностей воздействия на любые компоненты средств криптографической защиты информации и среды функционирования средств криптографической защиты информации.

1.2. Актуальные угрозы безопасности государственных информационных систем органов государственной власти и учреждений, обрабатывающих персональные данные.

1.2.1. Государственные информационные системы органов государственной власти и учреждений, обрабатывающие персональные данные, отличаются следующими особенностями:

- использованием широкой номенклатуры (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 государственных информационных систем органов государственной власти и учреждений, обрабатывающих персональные данные, на базе распределенной по территории Еврейской автономной 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 средств защиты информации, сертифицированных средств криптографической защиты информации при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена;

- использованием аутсорсинга при создании и эксплуатации государственных информационных систем органов государственной власти и учреждений, обрабатывающих персональные данные;

- сложностью дублирования больших массивов информации, содержащей персональные данные, на бумажных носителях и внешних накопителях информации;

- значительными негативными последствиями при реализации угроз безопасности государственных информационных систем органов государственной власти и учреждений, обрабатывающих персональные данные;

- риском недостаточной квалификации пользователей и персонала, обслуживающего государственные информационные системы органов государственной власти и учреждений, обрабатывающие персональные данные, и средства защиты информации;

- проблемами взаимодействия различных государственных информационных систем органов государственной власти и учреждений, обрабатывающих персональные данные, вызванных несовершенством

действующего законодательства и ведомственных инструкций.

1.2.2. Актуальными угрозами безопасности государственных информационных систем органов государственной власти и учреждений, обрабатывающих персональные данные (включая угрозы, указанные в Банке данных угроз безопасности информации http://bdu.fstec.ru/threat), помимо угроз, указанных в пункте 1.1.2, признаются:

- угрозы использования аппаратно-программных средств виртуализации (при их использовании в государственных информационных системах органов государственной власти и учреждений, обрабатывающих персональные данные);
- 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.