КОЛЛЕГИЯ
АДМИНИСТРАЦИИ КЕМЕРОВСКОЙ ОБЛАСТИ

П О С Т А Н О В Л Е Н И Е

от « 23 » декабря 2016 г. № 527
г. Кемерово

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в исполнительных органах государственной власти Кемеровской области и в подведомственных им организациях

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», с целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в исполнительных органах государственной власти Кемеровской области и в подведомственных им организациях, Коллегия Администрации Кемеровской области постановляет:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в исполнительных органах государственной власти Кемеровской области и в подведомственных им организациях, согласно приложению к настоящему постановлению.

2. Настоящее постановление подлежит опубликованию на сайте «Электронный бюллетень Коллегии Администрации Кемеровской области».

3. Контроль за исполнением постановления возложить на заместителя Губернатора Кемеровской области (по экономическому развитию) Д.А. Шамгунова.

Губернатор
Кемеровской области А.М. Тулеев

Коллегия Администрации Кемеровской области
Для документов

Приложение
к постановлению Коллегии
Администрации Кемеровской области
от 23 декабря 2016 г. № 527

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в исполнительных органах государственной власти Кемеровской области и в подведомственных им организациях

Общие положения

1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в исполнительных органах государственной власти Кемеровской области и в подведомственных им организациях (далее - актуальные угрозы безопасности персональных данных в ИСПДн), разработаны в соответствии с частью 5 статьи 19 Федерального закона 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», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14.02.2008, 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, утверждёнными

руководством 8-го Центра ФСБ России от 31.03.2015 № 149/7/2/6-432, Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008, и Банком данных угроз безопасности информации, размещенным на официальном сайте ФСТЭК России (http://bdu.fstec.ru).

2. Актуальные угрозы безопасности ИСПДн содержат перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн) в исполнительных органах государственной власти Кемеровской области и в подведомственных им организациях (далее - органы власти).

3. Угрозы безопасности персональных данных, обрабатываемых в ИСПДн, приведенные в актуальных угрозах безопасности ИСПДн, подлежат адаптации в ходе разработки органами власти частных моделей угроз безопасности персональных данных для каждой информационной системы.

4. При разработке частных моделей угроз безопасности персональных данных проводится анализ структурно-функциональных характеристик информационной системы, эксплуатируемой при осуществлении органом власти функций и полномочий, а также применяемых в ней информационных технологий и особенностей ее функционирования.

В частной модели угроз безопасности персональных данных указываются:

описание ИСПДн и ее структурно-функциональных характеристик;

описание угроз безопасности персональных данных с учетом совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;

описание возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Частная модель угроз безопасности персональных данных для государственных органов разрабатывается с учетом требований приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

5. Угрозы безопасности персональных данных, обрабатываемых в ИСПДн, содержащиеся в актуальных угрозах безопасности ИСПДн, уточняются и дополняются по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн. Указанные изменения согласовываются с ФСТЭК России и ФСБ России в установленном порядке.

В органах власти функционируют информационные системы, обрабатывающие специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора, общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора, и персональные данные менее чем 100000 субъектов персональных данных, являющихся сотрудниками оператора.

Информационные системы персональных данных в органах власти имеют сходную структуру, однотипны, характеризуются тем, что в качестве объектов информатизации выступают распределенные информационные системы, имеющие подключение к единому центру обработки данных, а также подключение к сетям общего пользования и (или) сетям международного информационного обмена.

Ввод персональных данных в ИСПДн и вывод данных из ИСПДн осуществляются с использованием бумажных и электронных носителей информации. В качестве электронных носителей информации используются учтенные съемные носители информации и компакт-диски.

Персональные данные субъектов персональных данных обрабатываются с целью получения государственных услуг, а также в целях:

ведения финансово-экономической деятельности в соответствии с требованиями законодательства Российской Федерации;

проведения конкурсного отбора на государственную гражданскую службу Кемеровской области в Администрацию Кемеровской области;

проведения конкурсного отбора на государственную гражданскую службу Кемеровской области в органы государственной власти Кемеровской области;

ведения кадрового резерва Кемеровской области;

ведения кадрового резерва на государственной гражданской службе в Администрации Кемеровской области;

формирования и ведения резерва управленческих кадров Кемеровской области;

формирования и ведения Реестра государственных гражданских служащих Кемеровской области в Администрации Кемеровской области;

ведения Реестра государственных гражданских служащих Кемеровской области;

обеспечения деятельности депутатов Государственной Думы Федерального Собрания Российской Федерации и членов Совета Федерации Федерального Собрания Российской Федерации;

награждения наградами Кемеровской области, Коллегии Администрации Кемеровской области, выплат социального характера в натуральной и денежной форме;

предоставления сведений в Федеральный общественно-государственный фонд по защите прав вкладчиков и акционеров для выплаты компенсаций;

рассмотрения запросов, обращений граждан, объединений граждан, в том числе юридических лиц;

предоставления сведений в комиссию по вопросам помилования на территории Кемеровской области в отношении осужденных, обратившихся с ходатайством о помиловании в управление по взаимодействию с уголовно-исполнительной системой Администрации Кемеровской области, а также в органы местного самоуправления области и территориальные органы внутренних дел о лицах, освободившихся из мест лишения свободы, с целью организации работы по вопросам их социальной реабилитации после отбывания наказания.

Информационный обмен по сетям связи общего пользования и (или) сетям международного информационного обмена осуществляется с использованием сертифицированных средств криптографической защиты информации (далее - СКЗИ).

Контролируемой зоной ИСПДн являются административные здания и отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей, серверы системы, сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

В административных зданиях осуществляется пропускной и внутриобъектовый режим, неконтролируемое пребывание посторонних лиц и неконтролируемое перемещение (вынос за пределы здания) компьютеров и оргтехники запрещено. Помещения оборудованы запирающимися дверями. В коридорах, вестибюлях и холлах ведется видеонаблюдение.

Актуальные угрозы безопасности персональных данных в информационных системах персональных данных

Учитывая особенности обработки персональных данных в органах власти, а также категорию и объем обрабатываемых в ИСПДн персональных данных, основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

Конфиденциальность – 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.

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 информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Основной целью применения в ИСПДн государственных органов Кемеровской области СКЗИ является защита персональных данных, в том числе при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена.

Объектами защиты являются:

персональные данные;

СКЗИ;

среда функционирования СКЗИ (далее-СФ СКЗИ);

информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;

документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к информационным системам персональных данных и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты СФ;

носители защищаемой информации, используемые в информационной системе в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

используемые информационной системой каналы (линии) связи, включая кабельные системы;

помещения, в которых находятся ресурсы информационной системы, имеющие отношение к криптографической защите персональных данных.

Основными актуальными угрозами безопасности персональных

данных в ИСПДн органов власти Кемеровской области согласно требованиям ФСТЭК России являются:

угрозы несанкционированного доступа (далее-НСД) на рабочих местах, связанные с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн;

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

угрозы, реализуемые после загрузки операционной системы и направленные на выполнение НСД 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.);

угрозы локального внедрения вредоносных программ;

угрозы выявления паролей;

угрозы типа «Отказ в обслуживании»;

угрозы удаленного запуска приложений;

угрозы внедрения по сети вредоносных программ;

угрозы «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой в ИСПДн из внешних сетей информации;

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

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

угрозы подмены доверенного объекта сети;

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

угрозы непреднамеренного или преднамеренного вывода из строя технических средств и средств защиты информации;

угрозы несанкционированного отключения средств защиты информации;

угрозы непреднамеренной модификации (уничтожения) информации пользователями;

угрозы недостаточности надежности технических средств и коммуникационного оборудования;

угрозы снижения достаточности и качества применяемых средств защиты информации;

угрозы самостоятельного создания способов атак, подготовки и проведения атак за пределами контролируемой зоны;

угрозы проведения атак при нахождении в пределах контролируемой зоны;

угрозы утечки видовой информации;

угрозы нарушения изоляции пользовательских данных внутри виртуальной машины;

угрозы нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия;

угрозы нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин;

угрозы несанкционированного доступа к виртуальным каналам передачи;

угрозы несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети;

угрозы несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин;

угрозы несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети;

угрозы перехвата управления средой виртуализации.

Основными актуальными угрозами безопасности персональных данных в ИСПДн органов власти Кемеровской области согласно требованиям ФСБ России являются:

угрозы непредумышленного искажения или удаления программных компонентов ИСПДн;

угрозы внедрения и использования неучтенных программ;

угрозы игнорирования организационных ограничений (установленных правил) при работе с ресурсами ИСПДн, включая средства защиты информации;

угрозы нарушения правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности: ключевой, парольной и аутентифицирующей информации);

угрозы предоставления посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требованиям;

угрозы несообщения о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа;

угрозы внесения негативных функциональных возможностей в технические и программные компоненты СКЗИ и СФ СКЗИ, в том числе с использованием вредоносных программ (компьютерные вирусы и т.д.);

угрозы реализации целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения

безопасности защищаемых СКЗИ персональных данных или создания условий для этого (далее - атака) при нахождении в пределах контролируемой зоны;

угрозы проведения атак на этапе эксплуатации СКЗИ на следующие объекты:

1) документацию на СКЗИ и компоненты СФ СКЗИ;

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

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

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

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

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

угрозы использования штатных средств ИСПДн, не ограниченного мерами, реализованными в информационной системе, в которой используются СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

угрозы физического доступа к СВТ, на которых реализованы СКЗИ и СФ СКЗИ;

угрозы возможностей воздействия на аппаратные компоненты СКЗИ и СФ СКЗИ, не ограниченных мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

угрозы создания способов, подготовки и проведения атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ СКЗИ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного программного обеспечения;

угрозы проведения лабораторных исследований СКЗИ, используемых вне контролируемой зоны, не ограниченного мерами, реализованными в информационной системе, в которой используется СКЗИ, 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 СКЗИ и СФ СКЗИ, в том числе с использованием исходных текстов входящего в СФ СКЗИ прикладного программного

обеспечения, непосредственно использующего вызовы программных функций СКЗИ;

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

угрозы возможностей располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ СКЗИ;

угрозы возможностей воздействовать на любые компоненты СКЗИ и СФ СКЗИ.