КУРГАНСКАЯ ОБЛАСТЬ

ШАДРИНСКИЙ РАЙОН

АДМИНИСТРАЦИЯ ШАДРИНСКОГО РАЙОНА

ПОСТАНОВЛЕНИЕ

от 13.10.2017 № 775

г. Шадринск

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации Шадринского района при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и 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» Администрация Шадринского района

ПОСТАНОВЛЯЕТ:

1.Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации Шадринского района при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки согласно приложению к настоящему постановлению.

2. Обнародовать настоящее постановление на стенде информации в здании Администрации Шадринского района и разместить на официальном сайте муниципального образования Шадринского района в сети «Интернет».

3. Контроль за исполнением настоящего постановления возложить на управляющего делами Администрации Шадринского района Верхотурцеву В.С.

Глава Шадринского района В.В. Осокин

Приложение к постановлению
Администрации Шадринского района
от « 13 » 10 2017 года
№ 475 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации Шадринского района при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки»

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации Шадринского района при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки

Раздел I. Общие положения

1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации Шадринского района при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки (далее - Актуальные угрозы безопасности ИСПДн), разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Актуальные угрозы безопасности ИСПДн содержат перечень актуальных угроз безопасности персональных данных (далее - ПДн) при их обработке в информационных системах персональных данных (далее - ИСПДн).

2.Основные понятия и термины, используемые в Актуальных угрозах безопасности ИСПДн, применяются в значениях, определенных действующим законодательством.

3.При определении угроз безопасности ПДн проводится анализ структурно — функциональных характеристик ИСПДн, применяемых в ней информационных технологий и особенностей её функционирования.

4.Актуальные угрозы безопасности ПДн, 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 ПДн в ИСПДн, а так же в связи с изменениями требований законодательства Российской Федерации о защите информации, нормативных, правовых актов и методических документов, регламентирующих защиту информации.

Указанные изменения согласовываются с Федеральной службой по техническому и экспортному контролю России по Уральскому федеральному округу и Федеральной службой безопасности России по Курганской области в установленном порядке.

Раздел II. Особенности обработки ПДн в ИСПДн

5.Ввод ПДн в ИСПДн и их вывод из ИСПДн осуществляется с использованием бумажных и электронных носителей информации.

В качестве электронных носителей информации используются учтенные отчуждаемые и неотчуждаемые носители информации.

6.ПДн субъектов ПДн обрабатываются:

с целью обеспечения деятельности Администрации Шадринского района;

в целях обеспечения кадровой работы, в том числе в целях содействия муниципальным служащим, работникам в прохождении муниципальной службы в Администрации Шадринского района, выполнении работы, в обучении и должностном росте, обеспечения личной безопасности муниципальных служащих, работников и членов их семей, обеспечения сохранности принадлежащего им имущества и имущества Администрации Шадринского района, учета результатов исполнения ими должностных обязанностей, обеспечения установленных законодательством Российской Федерации условий осуществления служебной деятельности и труда, гарантий и компенсаций;

в целях формирования кадрового резерва на муниципальной службе, резерва управленческих кадров Курганской области, противодействия коррупции;

в целях приема, обработки и распределения поступивших в адрес Администрации Шадринского района документов, обращений граждан и организаций, а также регистрации и отправки исходящей корреспонденции;

в целях ведения внутренней служебной переписки;

в целях формирования внутренних документов, регламентирующих деятельность Администрации Шадринского района.

7.Информационный обмен по сетям связи общего пользования и (или) сетям международного информационного обмена осуществляется с использованием межсетевых экранов.

8.В Администрации Шадринского района осуществляется внутриобъектовый режим, неконтролируемое пребывание посторонних лиц и неконтролируемое перемещение. Вынос за пределы здания Администрации Шадринского района компьютеров и оргтехники запрещено. Помещения оборудованы запирающимися дверями.

Раздел III. Угрозы безопасности ПДн в ИСПДн

9.Учитывая особенности обработки ПДн в Администрации Шадринского района, а также категорию и объем обрабатываемых в ИСПДн ПДн, основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

Конфиденциальность - обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространение без согласия субъекта ПДн 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.

10.Под угрозами безопасности ПДн при их обработке в ИСПДн понимается 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.

11.Исходя из состава обрабатываемых ПДн определяется, что для обеспечения безопасности ПДн в ИСПДн Администрации Шадринского района необходимо обеспечение четвертого уровня защищенности ПДн (УЗ - 4).

12.Основной целью применения в ИСПДн Администрации Шадринского района средств криптографической защиты информации (далее - СКЗИ) является защита ПДн при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена с государственными информационными системами.

13.Объектами защиты являются:

ПДн;

СКЗИ;

среда функционирования (далее - СФ) СКЗИ;

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

документы, дела, журналы, картотеки, издания, технические документы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к ИСПДн 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 ПДн, 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 ПДн.

14.Основными видами угроз безопасности ПДн в ИСПДн являются:

угрозы утечки информации по техническим каналам;

угрозы утечки акустической информации;

угрозы утечки видовой информации;

угрозы утечки информации по каналам побочных электромагнитных излучений и наводок;

подбор логина/пароля;

угрозы несанкционированного доступа к информации;

угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн;

кража персональной электронно-вычислительной машины (далее - ПЭВМ);

кража носителей информации;

кража ключей и атрибутов доступа;

кража, модификация, уничтожение информации;

вывод из строя узлов ПЭВМ, каналов связи;

несанкционированное отключение средств защиты;

угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (далее - НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);

внедрение вирусов или иного вредоносного программного кода;

использование не декларированных возможностей системного программного обеспечения (далее - ПО) и ПО для обработки ПДн;

угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и системы защиты ПДн (далее - СЗПДн) в ее составе из-за сбоев в ПО, а также от угроз не антропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного характера (ударов молний, пожаров, наводнений и т.п.);

утрата, кража, передача ключей и атрибутов доступа;

непреднамеренная модификация (уничтожение) информации сотрудниками;

непреднамеренное отключение средств защиты;

выход из строя аппаратно-программных средств;

сбой системы электроснабжения;

стихийное бедствие;

угрозы преднамеренных действий внутренних нарушителей;

доступ к информации, модификация, уничтожение информации лицами, не допущенными к ее обработке;

разглашение информации, её модификация или уничтожение сотрудниками, допущенными к ее обработке;

угрозы несанкционированного доступа по сети и каналам связи;

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

перехват за переделами КЗ;

перехват в пределах КЗ внешними нарушителями;

перехват в пределах КЗ внутренними нарушителями;

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 навязывания ложного маршрута сети;

угрозы подмены доверенного объекта в сети;

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

угрозы типа «Отказ в обслуживании»;

угрозы удаленного запуска приложений;

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

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

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

При определении актуальных угроз безопасности ПДн используются следующие положения:

единый подход к созданию, развитию (модернизации) и эксплуатации информационных систем Администрации Шадринского района, основанный на согласовании технологий обработки информации;

реализация единого порядка согласования технических заданий и технических проектов на создание информационных систем и входящих в их состав систем защиты информации с использованием не криптографических средств защиты информации (далее - СЗИ) и (или) с использованием СКЗИ.

15.Актуальные угрозы безопасности ПДн в ИСПДн Администрации Шадринского района:

подбор логина/пароля;

внедрение вирусов или иного вредоносного программного кода;

вынос ПДн за пределы КЗ на съемном носителе информации;

передача ПДн по открытым каналам связи за пределы КЗ;

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

угрозы, реализуемые после загрузки операционной системы и направленные на выполнение НСД с применением стандартных функций операционной системы или какой-либо прикладной программы с применением специально созданных для выполнения НСД;

умышленное неправомерное внесение изменений в ПДн;

кража/утеря съемных носителей информации, содержащих ПДн;

утрата, кража, передача ключей и атрибутов доступа;

искажение или удаление ПДн;

просмотр или копирование в ходе ремонта, модификации и утилизации программно-аппаратных средств;

блокирование доступа к информации (отказ в обслуживании ИСПДн);

проведение атаки при нахождении в пределах КЗ;

проведение атак на этапе эксплуатации СКЗИ в отношении документации на СКЗИ и компонентов СФ, помещений, 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;

получение в рамках предоставленных полномочий, а также в результате наблюдений сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы, сведений о мерах по обеспечению КЗ объектов, в которых размещены ресурсы информационной системы, сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;

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

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

возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.

Управляющий делами
Администрации Шадринского района В.С. Верхотурцева