ПРАВИТЕЛЬСТВО КУРГАНСКОЙ ОБЛАСТИ

УПРАВЛЕНИЕ ПО ОБЕСПЕЧЕНИЮ ДЕЯТЕЛЬНОСТИ МИРОВЫХ СУДЕЙ В КУРГАНСКОЙ ОБЛАСТИ

ПРИКАЗ

от 16 мая 2017 года № 64

г. Курган

О внесении изменения в приказ Управления по обеспечению деятельности мировых судей в Курганской области от 16 августа 2016 года № 111 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Управлении по обеспечению деятельности мировых судей в Курганской области при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки»

В целях приведения нормативного правового акта Управления по обеспечению деятельности мировых судей в Курганской области в соответствие с действующим законодательством

ПРИКАЗЫВАЮ:

1. Внести в приказ Управления по обеспечению деятельности мировых судей в Курганской области от 16 августа 2016 года № 111 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Управлении по обеспечению деятельности мировых судей в Курганской области при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки» следующее изменение:

приложение изложить в редакции согласно приложению к настоящему приказу.

2. Опубликовать настоящий приказ в установленном порядке.

3. Контроль за исполнением настоящего приказ оставляю за собой.

Начальник Управления
по обеспечению деятельности
мировых судей в Курганской области А.М. Лаврентьев

Данилов Э.А.
(3522) 41-40-08

Приложение к приказу
Управления по обеспечению деятельности
мировых судей в Курганской области
от 16 августа 2017 года № 64
«О внесении изменения в приказ
Управления по обеспечению
деятельности мировых судей
в Курганской области
от 16 августа 2016 года № 111
«Об определении угроз безопасности
персональных данных, актуальных при
обработке персональных данных в
информационных системах персональных
данных, эксплуатируемых в Управлении
по обеспечению деятельности мировых
судей в Курганской области при
осуществлении соответствующих видов
деятельности, с учетом содержания
персональных данных, характера и
способов их обработки»

«Приложение к приказу
Управления по обеспечению
деятельности мировых судей
в Курганской области
от 16 августа 2016 года № 111
«Об определении угроз безопасности
персональных данных, актуальных при
обработке персональных данных в
информационных системах персональных
данных, эксплуатируемых в Управлении
по обеспечению деятельности мировых
судей в Курганской области 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 Управлении по обеспечению деятельности мировых судей в Курганской области 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 Управлении по обеспечению деятельности мировых судей в Курганской области при осуществлении соответствующих видов деятельности, с

учетом содержания персональных данных, характера и способов их обработки (далее - Актуальные угрозы безопасности ИСПДн Управления, Управление), разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

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

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

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

4. Актуальные угрозы безопасности ПДн, обрабатываемых в ИСПДн, содержащиеся в Актуальных угрозах безопасности ИСПДн Управления, 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 и Федеральной службой безопасности России в установленном порядке.

Раздел II. Особенности обработки ПДн в ИСПДн Управления

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 Управления;

в целях обеспечения кадровой работы, в том числе в целях содействия гражданским служащим, работникам в прохождении государственной гражданской службы в Управлении, выполнении работы, в обучении и должностном росте, обеспечения личной безопасности гражданских служащих, работников и членов их семей, обеспечения сохранности принадлежащего им имущества и имущества Управления, 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 государственной гражданской службе, резерва управленческих кадров Курганской области, противодействия коррупции;

в целях приема, обработки и распределения поступивших в адрес Управления 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 Управления.

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

8. Контролируемой зоной (далее – КЗ) ИСПДн Управления являются ограждающие конструкции первого этажа здания, встроенного помещения. В пределах КЗ находятся рабочие места пользователей, серверы системы, сетевое и телекоммуникационное оборудование ИСПДн, а так же линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

9. В Управлении осуществляется внутриобъектовый режим, неконтролируемое пребывание посторонних лиц и неконтролируемое перемещение (вынос за пределы Управления) компьютеров и оргтехники запрещено.

Помещения оборудованы запирающимися дверями. В коридорах ведется видеонаблюдение.

Раздел III. Угрозы безопасности ПДн в ИСПДн Управления

10. Учитывая особенности обработки ПДн в Управлении, 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.

11. Под угрозами безопасности ПДн понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия при их обработке в ИСПДн.

12. Исходя из состава обрабатываемых ПДн определяется, что для обеспечения безопасности ПДн в ИСПДн Управления необходимо обеспечение четвертого уровня защищенности ПДн (УЗ – 4).

13. Основной целью применения в ИСПДн Управления 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.

14. 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.

15. Основными видами угроз безопасности ПДн в ИСПДн являются:

утечки информации по техническим каналам;

подбор логина/пароля;

несанкционированный доступ к информации;

уничтожение, хищение, вывод из строя узлов и аппаратных средств ИСПДн, персональной электронно-вычислительной машины (далее – ПЭВМ), носителей информации путем физического доступа;

вывод из строя узлов и каналов связи;

кража, несанкционированная модификация или блокирование 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;

преднамеренные, непреднамеренные действия внутренних, внешних нарушителей;

утрата, кража, передача ключей и атрибутов доступа;

кража, умышленная или непреднамеренная модификация (уничтожение) информации;

отключение средств защиты;

выход из строя аппаратно-программных средств вследствии сбоев или стихийных бедствий;

сканирование сети, анализ сетевого трафика с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;

умышленная модификация сети и сетевой инфраструктуры;

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 Управления, 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.

16. Перечень актуальных угроз безопасности ПДн при их обработке в ИСПДн Управления:

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.».