Приложение 2

к приказу Департамента
социальной защиты населения
Ивановской области

от 10.07.2014 № 263-о.д.

1

Политика информационной безопасности информационных систем персональных данных Департамента социальной защиты населения Ивановской области

СОДЕРЖАНИЕ

Введение 4

1 Общие положения 5

2 Область действия 6

3 Система защиты персональных данных 7

4 Требования к персоналу по обеспечению защиты ПДн 10

5 Должностные обязанности пользователей ИСПДн 12

6 Заключительные положения 13

Обозначения и сокращения

АВС – антивирусные средства

АРМ – автоматизированное рабочее место

ВТСС – вспомогательные технические средства и системы

ИСПДн – информационная система персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

САЗ – система анализа защищенности

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

СОВ – система обнаружения вторжений

СУБД – система управления базами данных

ТКУ И – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

Введение

Настоящая Политика информационной безопасности Департамента социальной защиты населения Ивановской области (далее – Политика и Департамент) является официальным, основополагающим внутренним документом, регулирующим вопросы обработки персональных данных в Департаменте.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенных в Концепции информационной безопасности ИСПДн Департамента социальной защиты населения Ивановской области.

Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», на основании:

- рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных Заместителем директора ФСТЭК России от 15.02.2008 г.;

- типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.

1. Общие положения

Безопасность персональных данных достигается путем исключения 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.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности ПДн (УБПДн).

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

2. Область действия

Требования настоящей Политики распространяются на всех государственных гражданских служащих Департамента (далее - служащих), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3. Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:

- отчета о результатах проведения внутренней проверки;
- перечня персональных данных, подлежащих защите;
- модели угроз безопасности персональных данных;
- положения о разграничении прав доступа к обрабатываемым персональным данным;
- руководящих документов ФСТЭК и ФСБ России.

На основании вышеперечисленных документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Департамента. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз и Отчета о результатах проведения внутренней проверки, делается заключение о необходимости использования технических средств и проведения организационных мероприятий для обеспечения безопасности ПДн. Необходимые мероприятия, выбранные из указанных в приказе ФСТЭК № 17 от 11.02.2013, отражаются в Плане мероприятий по обеспечению защиты ПДн в ИСПДн Департамента.

Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- сервера приложений;
- СУБД;
- граница ЛВС;
- каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;

- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты.

Список функций защиты может включать:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечение целостности данных;
- обнаружение вторжений.

Список используемых технических средств отражается в Плане мероприятий по обеспечению защиты ПДн в ИСПДн Департамента. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн соответствующие изменения должны быть внесены в Список и утверждены начальником Департамента или лицом, ответственным за обеспечение защиты ПДн.

Во исполнение настоящей Политики в Департаменте утверждаются следующие локальные нормативные правовые акты:

- Положение о порядке обработки персональных данных в Департаменте;
- Инструкция администратора ИСПДн Департамента;
- Инструкция администратора безопасности ИСПДн Департамента;
- Инструкция пользователя ИСПДн Департамента;
- Инструкция пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций;
- Перечень по учету применяемых СЗИ, эксплуатационной и технической документации к ним;
- Приказ о введении режимов обработки и защиты персональных данных в Департаменте;

- Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в ИСПДн Департамента;

- План внутренних проверок режима защиты персональных данных в ИСПДн Департамента;

- иные локальные документы Департамента, принимаемые во исполнение требований действующих федеральных нормативных правовых актов в области обработки ПДн.

4. Требования к персоналу по обеспечению защиты ПДн

Все служащие Департамента, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового служащего руководитель структурного подразделения, в которое он поступает, обязан организовать его ознакомление с должностным регламентом и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Служащий должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Служащие Департамента, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Служащие Департамента должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Служащие Департамента должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Служащим запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Служащим запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Департамента, третьим лицам.

При работе с ПДн в ИСПДн служащие Департамента обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн служащие обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Служащие Департамента должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на служащих, которые нарушили принятые политику и процедуры безопасности ПДн.

Служащие обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

5. Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора ИСПДн;
- Инструкция администратора безопасности ИСПДн;
- Инструкция пользователя ИСПДн;
- Инструкция пользователя при возникновении внештатных ситуаций.

6. Заключительные положения

Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

Контроль исполнения требований настоящей Политики осуществляется ответственным за обеспечение безопасности персональных данных Департамента.

При нарушениях служащими Департамента – пользователями ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.