Управление социальной
защиты населения
администрации
города Трехгорного

Приказ № 118
29.12.2015

Об утверждении Положения
по организации работ по обеспечению
безопасности персональных данных
при их обработке в информационных
системах персональных данных УСЗН

Во исполнение «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, а также иных нормативных документов по защите информации

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Положение по организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных УСЗН (Приложение).
2. Делопроизводителю Шаргородской М. М. ознакомить работников УСЗН с настоящим приказом.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник УСЗН Ю. А. Полуконова

Приложение

Утверждено приказом
начальника УСЗН
№_____от _____2015

ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ УСЗН

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение определяет основные мероприятия и порядок проведения работ по обеспечению безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн) УСЗН.

1.2. В Организации обработка ПДн осуществляется в следующих информационных системах (далее - ИС):

- ИСПДн «Сотрудники»,
- ИСПДн «Население»,
- ИСПДн «СМЭВ УСЗН».

1.3. Все работники УСЗН, участвующие в обработке ПДн в ИС УСЗН, должны быть ознакомлены с Положением.

2. ПОРЯДОК ОРГАНИЗАЦИИ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. С целью организации работ по защите ПДн приказом начальника УСЗН назначается должностное лицо, ответственное за обеспечение безопасности ПДн.

2.2. В обязанности ответственного за обеспечение безопасности ПДн входит:

- контроль и организация работ по обеспечению безопасности ПДн;
- согласование организационно-распорядительных документов по вопросам обеспечения безопасности ПДн;
- согласование списка работников, которых необходим доступ к ПДн для выполнения служебных обязанностей;
- согласование базовой конфигурации ИС и СЗПДн УСЗН;
- проведение разбирательств по фактам возникновения событий, которые могут привести к снижению уровня защищенности ПДн.

2.3. Ответственным за выполнение работ по обеспечению безопасности ПДн при их обработке в ИС УСЗН является администратор информационной безопасности (далее – администратор ИБ), назначаемый приказом начальника УСЗН.

2.4. Реализация требований по обеспечению безопасности ПДн осуществляется администраторами, разработчиками и пользователями информационных систем УСЗН.

3. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Требования по обеспечению безопасности ПДн при их обработке в ИС УСЗН формируются на основании установленного уровня защищенности ИСПДн и перечня актуальных угроз безопасности ПДн.

3.2. Требования по обеспечению безопасности ПДн при их обработке в ИСПДн реализуются комплексом организационных и технических мер, средств и механизмов защиты информации, определенных в Техническом задании на создание СЗПДн.

3.3. Применение средства защиты информации разрешается после проверки корректности его функционирования и оформления заключения о готовности средства

защиты информации к эксплуатации (форма заключения приведена в приложении №1). Применяемые средства защиты информации, эксплуатационная и техническая документация к ним подлежат обязательному учету (форма журнала учета средств защиты информации, эксплуатационной и технической документации приведена в приложении №2).

3.4. Требования по обеспечению безопасности ПДн при их обработке в ИСПДн УСЗН реализуются в рамках следующих направлений:

- организация системы допуска и учета лиц, допущенных к работе с ПДн;
- организация системы защиты межсетевого взаимодействия;
- организация режима безопасности помещений ИСПДн;
- организация безопасного хранения и уничтожения носителей ПДн;
- организация защиты от вредоносного кода;
- организация парольной защиты;
- организация управления инцидентами информационной безопасности и реагирования на них;
- организация управления конфигурацией ИСПДн и СЗПДн УСЗН;
- организация системы криптографической защиты информации;
- организация системы резервного копирования и восстановления;
- организация управления СЗПДн УСЗН;
- организация контроля эффективности мер защиты ПДн;
- организация системы обучения по вопросам обеспечения безопасности ПДн.

4. СИСТЕМА ДОПУСКА И УЧЕТА ЛИЦ

4.1. Ответственным за организацию системы допуска к ПДн является ответственный за обеспечение безопасности ПДн.

4.2. Работники УСЗН допускаются к обработке ПДн в ИСПДн, использование которых необходимо для выполнения их функциональных обязанностей.

4.3. Приказом начальника УСЗН утверждается Перечень ПДн, обрабатываемых в УСЗН. Обработка ПДн, не включенных в Перечень, не допускается.

4.4. Перечень определяется и пересматривается в установленном в УСЗН порядке не реже, чем один раз в три года.

4.5. Доступ работников УСЗН к ПДн, обрабатываемым в ИСПДн УСЗН, определяется списком работников, которые имеют доступ к ПДн, утверждаемым приказом по УСЗН.

4.6. Права доступа пользователей ИСПДн УСЗН определяются в соответствии с Матрицами доступа, разрабатываемыми администратором ИБ для каждой ИСПДн УСЗН.

4.7. Управление учетными записями пользователей и распределение прав доступа к информационным ресурсам ИСПДн УСЗН, внешним носителям информации и периферийным устройствам осуществляется администратором ИСПДн УСЗН, назначаемым приказом начальника УСЗН.

4.8. Общий порядок предоставления доступа, изменения и отмены доступа к информационным ресурсам ИСПДн УСЗН устанавливается организационно-распорядительными документами УСЗН.

4.9. Администратор ИБ осуществляет оценку необходимости запрашиваемого уровня доступа к ПДн.

4.10. Администратор ИБ осуществляет учет лиц, допущенных к работе с ПДн в ИСПДн УСЗН.

4.11. Администратор ИБ осуществляет контроль за своевременным блокированием доступа (изменением прав доступа) при увольнении пользователя ИСПДн УСЗН (изменении должностных обязанностей).

4.12. В пределах контролируемой зоны УСЗН запрещено подключение к нформационной сети УСЗН мобильных технических средств, портативных рабочих станций и внешних носителей информации.

4.13. Подключение к информационной сети УСЗН указанных устройств допускается только при наличии согласования с ответственным за обеспечение безопасности персональных данных и защиту информации в УСЗН.

5. СИСТЕМА ЗАЩИТЫ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

5.1. Обеспечение защиты сетевого взаимодействия реализуется по следующим направлениям:

– разграничение доступа пользователей к ресурсам сетей связи общего пользования.

5.2. В информационной сети УСЗН должно быть разделение:

– серверов ИСПДн;
– пользователей ИСПДн;
– элементов СЗПДн.

5.3. Включение новых серверов и рабочих станций в сегменты ИСПДн должно осуществляться только после выполнения требований по защите ПДн.

5.4. Управление сетевым оборудованием УСЗН осуществляется программистом УСЗН.

5.5. Доступ к сетевому оборудованию разрешен только с рабочих станций системных администраторов либо локально.

5.6. В случае производственной необходимости пользователям ИСПДн УСЗН может предоставляться доступ:

– к сети Интернет;
– к сервисам внешней электронной почты.

5.7. Правила работы пользователей ИСПДн с ресурсами сети Интернет и электронной почты устанавливаются организационно-распорядительными документами УСЗН.

6. РЕЖИМ БЕЗОПАСНОСТИ ПОМЕЩЕНИЙ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обеспечение безопасности помещений ИСПДн направлено на исключение возможности несанкционированного доступа к техническим средствам ИСПДн, их хищения и нарушения работоспособности, хищения носителей информации.

6.2. Приказом начальника УСЗН определяются границы контролируемой зоны УСЗН, на территории которой исключено бесконтрольное пребывание посторонних лиц.

6.3. Режим безопасности помещений ИСПДн реализуется в соответствии с Положением об организации режима безопасности помещений ИСПДн.

6.4. Реализация режима безопасности помещений ИСПДн возлагается на лица, работающие в данных помещениях.

7. БЕЗОПАСНОСТЬ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Безопасность информации, хранящейся на бумажных и отчуждаемых электронных носителях ПДн, обеспечивается путем организации системы учета и безопасного хранения носителей ПДн.

7.2. Ответственным за учет и соблюдение условий хранения электронных носителей ПДн является администратор ИБ.

7.3. Порядок учета, хранения и уничтожения носителей ПДн регламентируется Положением об учете, порядке хранения и уничтожения носителей ПДн.

7.4. При уничтожении носителя ПДн должны обеспечиваться и контролироваться гарантированное уничтожение (стирание) ПДн.

8. ЗАЩИТА ОТ ВРЕДОНОСНОГО КОДА

8.1. Средства защиты от вредоносного кода должны быть установлены на всех рабочих станциях и серверах УСЗН.

8.2. Средства защиты от вредоносного кода должны обеспечивать:

– автоматическое блокирование или удаление обнаруженного вредоносного программного обеспечения;
– регулярную проверку программных модулей рабочих станций и серверов ИСПДн УСЗН предмет наличия в них вредоносного программного обеспеченияпо типовым шаблонам и с помощью эвристического анализа;

- возможность отката операций удаления вредоносного программного обеспечения путем помещения файлов, содержащих вредоносное программного обеспечение, в карантин;
- своевременное обновление антивирусных баз (сигнатур угроз) и программных модулей.

8.3. При выявлении фактов заражения вредоносным программным обеспечением ответственным за обеспечение безопасности ПДн проводится разбирательство с целью установления причин возникновения заражения.

8.4. Обязанности по устранению последствий заражения вредоносным программным обеспечением возлагаются на администратора ИБ.

9. ПАРОЛЬНАЯ ЗАЩИТА

9.1. Парольная защита применяется для исключения возможности получения несанкционированного доступа к элементам ИСПДн УСЗН (рабочим станциям, серверам, активному сетевому оборудованию) в целях недопущения утечки, а также несанкционированной модификации или уничтожения ПДн.

9.2. Парольная защита применяется:

- при доступе пользователей к операционным системам рабочих станций и серверов, прикладному программному обеспечению ИСПДн УСЗН, средствам защиты информации;
- при доступе системных администраторов к средствам управления сетевым и серверным оборудованием, операционным системам серверов и рабочих станций, специальному программному обеспечению ИСПДн УСЗН, средствам защиты информации.

9.3. Требования парольной защиты определяются организационно-распорядительными документами УСЗН.

9.4. При выявлении фактов нарушения требований парольной защиты ответственным за обеспечение безопасности ПДн проводится разбирательство.

10. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РЕАГИРОВАНИЕ НА НИХ

10.1. Для регистрации и учета событий, которые могут привести к снижению уровня защищенности ПДн (далее – инцидентов), должны использоваться встроенные механизмы регистраций и учета событий безопасности операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также применяться средства (системы) анализа защищенности.

10.2. Средства (системы) анализа защищенности должны обеспечивать, в том числе:

- выявление и анализ уязвимостей, связанных с ошибками в конфигурации операционных систем и программного обеспечения рабочих станций и серверов ИСПДн УСЗН;
- контроль установки обновлений программного обеспечения рабочих станций и серверов ИСПДн УСЗН.

10.3. В УСЗН должен быть обеспечен контроль заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИСПДн УСЗН.

10.4. Анализ инцидентов осуществляется:

- администратором ИБ при просмотре журналов событий, формируемых средствами защиты информации;
- администратором ИСПДн при просмотре журналов событий, формируемых программным обеспечением ИСПДн и системами управления базами данных; при просмотре журналов событий сетевого и серверного оборудования, операционных систем и системного программного обеспечения.

10.5. Журналы аудита должны просматриваться ответственными работниками регулярно (не реже одного раза в неделю).

10.6. О фактах обнаружения инцидентов ответственные работники должны немедленно сообщать администратору ИБ.

10.7. Права доступа на модификацию и удаление журналов событий безопасности должны быть ограничены для всех пользователей ИСПДн УСЗН.

11. СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

11.1. Система криптографической защиты информации предназначена для криптографической защиты информации, передаваемой по каналам связи, расположенным вне контролируемой зоны УСЗН.

11.2. Криптографическая защита должна реализовываться алгоритмами, определяемыми ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 с применением программно-технических средств шифрования и/или специального прикладного программного обеспечения, сертифицированных в установленном порядке ФСБ России.

11.3. Эксплуатация СКЗИ должна осуществляться в полном соответствии с эксплуатационной и технической документации к ним.

11.4. Допуск работников УСЗН к работе с СКЗИ должен осуществляться в соответствии со списком лиц, допущенных к СКЗИ, утвержденным ответственным за обеспечение безопасности ПДн.

11.5. Допуск работников УСЗН к работе с СКЗИ должен осуществляться после проведения администратором ИБ обучения и ознакомления с требования по работе с СКЗИ.

11.6. Администратор ИБ должен вести учет используемых СКЗИ, технической и эксплуатационной документации к ним в Журнале учета СКЗИ и Журнале учета приема-выдачи СКЗИ.

11.7. Контроль выполнения требований по эксплуатации СКЗИ осуществляет администратор ИБ. При выявлении фактов нарушения требований по эксплуатации СКЗИ ответственным за обеспечение безопасности ПДн проводится разбирательство.

11.8. Порядок использования СКЗИ в УСЗН определяется Положением о контроле использования СКЗИ.

12. ОРГАНИЗАЦИЯ СИСТЕМЫ РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ

12.1. Для обеспечения возможности восстановления функционирования и работоспособности ИСПДн УСЗН и средств защиты информации при возникновении аварийных ситуаций должна быть реализована система резервного копирования и восстановления.

12.2. Резервному копированию подлежит информация следующих основных категорий:

- ПДн, хранящиеся в виде отдельных файлов, каталогов или баз данных ИСПДн;
- системные и конфигурационные файлы операционных систем и специального программного обеспечения серверов;
- конфигурационные файлы сетевого оборудования;
- системные и конфигурационные файлы средств защиты информации.

12.3. Ответственным за осуществление резервного копирования является администратор ИСПДн.

12.4. Требования к периодичности и способам осуществления резервного копирования информационного ресурса определяются особенностями функционирования соответствующего информационного ресурса.

12.5. Администратор ИБ должен осуществлять регулярные проверки выполнения требований резервного копирования информационных ресурсов.

13. УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ И СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

13.1. В УСЗН должно обеспечиваться управление конфигурацией ИСПДн и СЗПДн УСЗН.

13.2. В УСЗН допускается использование ограниченного набора программного обеспечения (ПО), формирующего базовую конфигурацию ИСПДн УСЗН.

13.3. Состав базовой конфигурации ПО на рабочих станциях и серверах ИСПДн УСЗН утверждается приказом начальника УСЗН (форма состава базовой конфигурации ПО приведена в приложении №3). Установка на рабочих станциях и серверах ИСПДн УСЗН ПО, не входящего в состав разрешенного ПО, не допускается.

13.4. Состав базовой конфигурации ПО СЗПДн УСЗН устанавливается эксплуатационной документацией на СЗПДн УСЗН.

13.5. При первоначальной настройке рабочих станций и серверов системными администраторами производится установка ПО на основании перечня разрешенного ПО.

13.6. Пересмотр базовой конфигурации осуществляется администратором ИБ при возникновении необходимости по согласованию с ответственным за обеспечение безопасности ПДн. Пересмотренная базовая конфигурация доводится до сведения всех работников УСЗН путем рассылки по электронной почте с обязательным запросом уведомления о прочтении письма.

13.7. Внесение изменений в конфигурацию ИСПДн УСЗН осуществляется на основании заявки заинтересованного лица, согласованной с руководителем структурного подразделения (форма заявки приведена в приложении №4).

13.8. При согласовании внесения изменений в конфигурацию ИСПДн УСЗН администратору ИБ необходимо учитывать потенциальное воздействие планируемых изменений на возникновение дополнительных угроз безопасности информации и на работоспособность ИСПДн УСЗН.

13.9. ПО, используемое в ИСПДн УСЗН, должно регулярно обновляться. Получение обновлений должно осуществляться из официальных источников производителя ПО. Получение обновлений ПО сертифицированных средств защиты информации должно осуществляться из специализированных источников обновления производителей средств в соответствии с эксплуатационной документацией к ним.

13.10. ПО, используемое на Предприятии, приобретается в соответствии с лицензионной политикой разработчика.

13.11. Установка обновлений ПО не считается внесением изменений в конфигурацию ИСПДн и СЗПДн УСЗН и не требует заполнения заявки на внесение изменений.

14. УПРАВЛЕНИЕ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

14.1. СЗПДн должна обеспечивать управление:

- заведением и удалением учетных записей пользователей, полномочиями пользователей и поддержанием правил разграничения доступа в ИСПДн УСЗН;
- резервным копированием и восстановлением работоспособности ИСПДн и СЗПДн УСЗН;
- обновлением программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации;
- регистрацией и анализом инцидентов ИБ.

14.2. Администрирование СЗПДн осуществляет администратор ИБ.

15. КОНТРОЛЬ ПРИНЯТЫХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

15.1. Ответственным за контроль выполнения принятых мер по обеспечению безопасности ПДн является ответственный за обеспечение безопасности ПДн.

15.2. Администратор ИБ осуществляет постоянный контроль выполнения требований по обеспечению безопасности ПДн в рамках выполнения своих обязанностей.

15.3. Мероприятия по контролю мер выполнения требований по обеспечению безопасности ПДн проводятся в соответствии с Планом внутренних проверок, утвержденным приказом начальника УСЗН.

15.4. Контроль эффективности мер защиты информации должен осуществляться в соответствии с Положением по организации контроля эффективности защиты информации.

16. ОБУЧЕНИЕ ПО ВОПРОСАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

16.1. Администратор ИБ должен регулярно проходить обучение на курсах повышения квалификации по вопросам защиты информации (не реже одного раза в три года).

16.2. Ознакомление работников УСЗН с правилами работы с ПДн осуществляется:

- путем проведения руководителем структурного подразделения УСЗН, в которое принят работник, первичных инструктажей с вновь принятым работником УСЗН по соблюдению установленных правил работы с ПДн;
- путем проведения обучения работников (пользователей средств вычислительной техники) администратором ИБ правилам работы с используемыми средствами защиты информации и СКЗИ;
- путем самостоятельного изучения работником УСЗН организационно-распорядительных документов, регламентирующих вопросы обеспечения безопасности ПДн.

16.3. Допуск работников УСЗН к ресурсам ИСПДн осуществляется только после прохождения первичного инструктажа и ознакомления с организационно-распорядительными документами УСЗН по вопросам обеспечения безопасности ПДн.

16.4. При проведении первичного инструктажа нового пользователя ИСПДн должны быть разъяснены:

- права и обязанности пользователя ИСПДн;
- действия, которые запрещены при обработке ПДн;
- возможные последствия и ответственность в случае нарушения правил работы с ПДн.