ПРИЛОЖЕНИЕ 1

УТВЕРЖДЕНО
приказом от «10» 11 2022 № 128

Положение
по организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

I. Общие положения

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) в муниципальном казенном учреждении «Управление социальной защиты населения города Снежинска» (далее УСЗН г. Снежинска).

2. Обработка ПДн в УСЗН г. Снежинска осуществляется в следующих информационных системах (далее - ИС):

- ИС «Граждане»;
- ИС «Сотрудники»
- ИС «АИСТ».

3. Все работники УСЗН г. Снежинска, участвующие в обработке ПДн в ИС, должны быть ознакомлены с Положением.

II. Организация работ по обеспечению безопасности персональных данных

1.С целью организации работ по защите ПДн назначаются должностные лица, ответственные за обеспечение безопасности ПДн в ИСПДн, а также администратор безопасности ИСПДн.

2. Обязанности ответственного за обеспечение безопасности ПДн, администратора безопасности ИСПДн отражены в инструкциях ответственных лиц за обеспечение безопасности ПДн в ИСПДн, утвержденных приказами начальника УСЗН г. Снежинска.

3. Назначенные должностные лица несут ответственность за выполнение работ по обеспечению безопасности ПДн при их обработке в ИС.

III. Требования по обеспечению безопасности персональных данных

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

2. Требования по обеспечению безопасности ПДн при их обработке в ИСПДн реализуются комплексом организационных и технических мер, средств и механизмов защиты информации.

3. Применение средства защиты информации разрешается после проверки корректности его функционирования и оформления заключения о готовности средства защиты информации к эксплуатации. Применяемые средства защиты информации, эксплуатационная и техническая документация к ним подлежат обязательному учету.

4. Требования по обеспечению безопасности ПДн при их обработке в ИСПДн 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;
– организация системы криптографической защиты информации;
– организация системы резервного копирования и восстановления;
– организация управления СЗПДн;
– организация контроля эффективности мер защиты ПДн;
– организация системы обучения по вопросам обеспечения безопасности ПДн.

IV. Система допуска и учета лиц

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

2. Сотрудники УСЗН г. Снежинска допускаются к обработке ПДн в ИСПДн, использование которых необходимо для выполнения их функциональных обязанностей.

3. Приказом начальника УСЗН г. Снежинска утверждается Перечень ПДн, обрабатываемых в УСЗН. Обработка избыточных ПДн не допускается.

4. Доступ сотрудников к ПДн, обрабатываемым в ИСПДн, определяется приказом начальника УСЗН г. Снежинска.

5. Права доступа пользователей ИСПДн определяются в соответствии с Матрицами доступа (Прилагается).

6. Управление учетными записями пользователей и распределение прав доступа к информационным ресурсам ИСПДн, внешним носителям информации и периферийным устройствам осуществляется администратором ИСПДн.

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

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

V. Система защиты межсетевого взаимодействия

1. Обеспечение защиты межсетевого взаимодействия реализуется по следующим направлениям:
– выделение сетевых сегментов обработки ПДн в информационной сети;
– межсетевое экранирование выделенных сегментов обработки ПДн;
– разграничение доступа пользователей к ресурсам сетей связи общего пользования.

2. В информационной сети должны быть выделены:

– сегменты серверов ИСПДн;
– сегменты пользователей ИСПДн;
– сегмент локальной вычислительной сети (далее – ЛВС);
– сегмент СЗПДн.

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

4. Доступ к сегментам ИСПДн из других сегментов информационной должен ограничиваться межсетевыми экранами.

5. Межсетевое экранирование сегментов ИСПДн должно обеспечивать:
– фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
– регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы), либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратного отключения межсетевого экрана);
– восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
– защиту беспроводных соединений, применяемых в ИСПДн.

6. Межсетевое экранирование должно обеспечивать отделение ЛВС и сети среды виртуализации от сетей связи общего пользования.

7. Серверы, доступные из сетей связи общего пользования, должны быть размещены в выделенном сегменте демилитаризованной зоны. Доступ к таким серверам из сетей связи общего пользования разрешается только по необходимым сетевым портам.

8. Используемые межсетевые экраны должны быть сертифицированы в соответствии с требованиями к средствам межсетевого экранирования.

9. Доступ к сетевому оборудованию разрешен только с рабочих станций администратора безопасности либо локально.

10. В случае производственной необходимости пользователям ИСПДн может предоставляться доступ:
– к сети Интернет;
– к сервисам внешней электронной почты.

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

VI. Режим безопасности помещений информационных систем персональных данных

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

2. Приказом определяются границы контролируемой зоны, на территории которой исключено бесконтрольное пребывание посторонних лиц.

3. Режим безопасности помещений ИСПДн реализуется в соответствии организационно-распорядительными документами УСЗН г. Снежинска об организации режима безопасности.

4. Реализация режима безопасности помещений ИСПДн возлагается на сотрудников, работающих в данных помещениях.

VII. Безопасность носителей персональных данных

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

2. Ответственным за учет и соблюдение условий хранения электронных носителей ПДн является ответственный за организацию обеспечения безопасности ПДн в ИСПДн..

3. Порядок учета, хранения и уничтожения носителей ПДн регламентируется организационно-распорядительными документами УСЗН г. Снежинска об учете, порядке хранения и уничтожения носителей ПДн.

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

VIII. Защита от вредоносного кода

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

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 на предмет наличия в них вредоносного программного обеспечения по 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.

3. При выявлении фактов заражения вредоносным программным обеспечением ответственными лицами проводится разбирательство с целью установления причин возникновения заражения.

IX. Парольная защита

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

2. Парольная защита применяется:

– при доступе пользователей к операционным системам рабочих станций и серверов, прикладному программному обеспечению ИСПДн, средствам защиты информации;

– при доступе администраторов к средствам управления сетевым и серверным оборудованием, операционным системам серверов и рабочих станций, специальному программному обеспечению ИСПДн, средствам защиты информации.

3. Требования парольной защиты определяются организационно-распорядительными документами УСЗН г. Снежинска.

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

X. Управление инцидентами информационной безопасности и реагирование на них

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

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;

– контроль установки обновлений программного обеспечения рабочих станций и серверов ИСПДн.

3. Должен быть обеспечен контроль заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИСПДн.

4. О фактах обнаружения инцидентов ответственные работники должны немедленно сообщать ответственным лицам за обеспечение безопасности ПДн. Все инциденты фиксируются в журнале.

5. УСЗН г. Снежинска обязано в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

XI. Система криптографической защиты информации

1. Система криптографической защиты информации (далее по тексту СКЗИ) предназначена для криптографической защиты информации, передаваемой по каналам связи, расположенным вне контролируемой зоны Организации.

2. Криптографическая защита должна реализовываться алгоритмами, определяемыми ГОСТ с применением программно-технических средств шифрования и/или специального прикладного программного обеспечения, сертифицированных в установленном порядке ФСБ России.

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

4. Допуск сотрудников к работе с СКЗИ осуществляется в соответствии организационно-распорядительными документами УСЗН г. Снежинска.

5. Должно быть обеспечено ведение журнала учета используемых СКЗИ, технической и эксплуатационной документации к ним в Журнале учета СКЗИ.

6. Должен быть обеспечен контроль выполнения требований по эксплуатации СКЗИ.

XII. Организация системы резервного копирования и восстановления

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

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.

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

XIII. Управление конфигурацией информационных систем персональных данных и системы защиты персональных данных

1. Должно обеспечиваться управление конфигурацией ИСПДн и СЗПДн.

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

3. Установка на рабочих станциях и серверах ИСПДн ПО, не входящего в состав разрешенного ПО, не допускается.

4. Состав базовой конфигурации ПО СЗПДн устанавливается эксплуатационной документацией на СЗПДн.

5. Пересмотр базовой конфигурации осуществляется при возникновении необходимости.

6. Внесение изменений в конфигурацию ИСПДн осуществляется на основании разрещения начальника УСЗН г. Снежинска при согласовании с ответственными за безопасность ПДн лицами.

7. ПО, используемое в ИСПДн, 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.

8. Используемое ПО приобретается в соответствии с лицензионной политикой разработчика.

XIV. Контроль принятых мер по обеспечению безопасности персональных данных

1. Ответственными за контроль выполнения принятых мер по обеспечению безопасности ПДн являются ответственные за обеспечение безопасности ПДн в УСЗН г. Снежинска.

2. Ответственными за обеспечение безопасности ПДН осуществляется постоянный контроль выполнения требований по обеспечению безопасности ПДн в рамках выполнения своих обязанностей.

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

Приложение
к Положению по организации работ по обеспечению безопасности
персональных данных при их обработке в информационных
системах персональных данных

Матрица доступа к ресурсам информационных систем персональных данных в УСЗН г. Снежинска

Субъект доступа	Объект доступа							
	Основные конфигурационные файлы операционной системы	Средства настройки и управления операционной системой	Основные конфигурационные файлы средств защиты информации	Средства настройки и управления средств защиты информации	Прикладное программное обеспечение	Периферийные устройства	Съемные машинные носители информации	Обрабатываемые, хранимые данные
Администратор информационной системы	F	F	F	F	F	F	F	-
Ответственный за обеспечение безопасности персональных данных в информационных системах	F	F	F	F	F	P/S	F	F
Пользователь	R-E	-	-	-	R-E	P	F	F

Типы доступа:
- чтение (R) – субъекту доступа разрешено просматривать содержимое объекта доступа;
- запись (W) – субъекту доступа разрешено просматривать, записывать и создавать новый объект доступа;
- выполнение (E) - субъекту доступа разрешено запускать/выполнять объект доступа;
- печать (P) – субъекту доступа разрешена печать;
- сканирование (S) - субъекту доступа разрешено сканирование;
- полный (F) - субъект доступа имеет полный доступ к объектам доступа.