УТВЕРЖДЕНО
решением Пелымской
поселковой территориальной
избирательной комиссии
от 27 июня 2025 г. № 4/16

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите персональных данных в Пелымской поселковой территориальной избирательной комиссии

1. Общие положения

1.1. «Положение о порядке организации и проведения работ по защите персональных данных» в Пелымской поселковой территориальной избирательной комиссии (далее – Положение) устанавливает методы и способы защиты информации, применяемые для обеспечения безопасности персональных данных (далее – ПДн) при их обработке в Пелымской поселковой территориальной избирательной комиссии (далее – Комиссия).

1.2. Настоящее Положение разработано в соответствии с действующим законодательством Российской Федерации, в том числе:

- Федеральным законом от 27.07.06 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.3. Действие настоящего документа распространяется на всех членов Комиссии и работников Комиссии, выполняющих обработку персональных данных в ИСПДн, и на администраторов ИСПДн.

1.4. Члены Комиссии и работники Комиссии руководствуются положениями настоящего Положения, руководящими и нормативными документами Избирательной комиссии Свердловского области и регламентирующими документами, разработанными и утвержденными в Комиссии в целях защиты информации и персональных данных.

2. Основные понятия

2.1. Автоматизированная обработка персональных данных – обработка ПДн с помощью средств вычислительной техники (далее – СВТ).

2.2. Аутентификация – процедура проверки принадлежности субъекту доступа предъявленного им идентификатора.

2.3. Блокирование персональных данных – временное прекращение обработки ПДн (за исключением случаев, при которых обработка необходима для уточнения ПДн).

2.4. Вредоносное программное обеспечение – программное обеспечение заведомо созданное для воздействия на информацию или активы информационной системы, и (или) получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети, использования ресурсов ЭВМ; причинения вреда (нанесения ущерба) владельцу информации, и (или) владельцу ЭВМ, и (или) владельцу сети ЭВМ;

2.5. Допуск – это право (возможность) субъекта доступа на получение информации и её использование.

2.6. Доступ к информации – возможность получения информации и ее использования.

2.7. Доступность – состояние информационной системы, при которой существует возможность ознакомления (работы) с информацией, содержащейся внутри информационной системы.

2.8. Идентификация – процедура присвоение субъектам и объектам идентификатора и сравнение идентификатора с перечнем присвоенных идентификаторов.

2.9. Информационная система персональных данных (далее – ИСПДн) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

2.10. Информация – сведения (сообщения, данные) независимо от формы их представления.

2.11. Контролируемая зона – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание работников и посетителей организации, а также транспортных средств.

2.12. Конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

2.13. Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (далее – СКЗИ).

2.14. Ответственный за организацию обработки персональных данных – должностное лицо организации, осуществляемое деятельность по обеспечению информационной безопасности (далее – ИБ).

2.15. Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых ИСПДн.

2.16. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор,

запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

2.17. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту ПДн).

2.18. Правила разграничения доступа – это совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

2.19. Предоставление персональных данных – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

2.20. Распространение персональных данных – действия, направленные на раскрытие ПДн неопределенному кругу лиц.

2.21. Субъект доступа – это лицо или процесс, действия которого регламентируются правилами разграничения доступа.

2.22. Субъект персональных данных (Субъект ПДн) – физическое лицо, к которому относятся ПДн.

2.23. Угроза безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в ИСПДн.

2.24. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

2.25. Управление доступом – механизм безопасности, который управляет процессом взаимодействия пользователей с информационными системами и ресурсами, а также информационными системами между собой.

2.26. Уровень защищенности персональных данных – комплексный показатель, устанавливаемый Правительством Российской Федерации с учетом объема и содержания обрабатываемых ПДн и актуальности угроз безопасности ПДн, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПДн при их обработке в ИСПДн.

2.27. Целостность – состояние информационной системы, при котором информация не может быть случайно или злонамеренно изменена, или уничтожена.

3. Организация обеспечения безопасности персональных данных.

3.1. Безопасность ПДн достигается путем принятия необходимых правовых, организационных и технических мер для защиты данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в их отношении.

3.2. Для обеспечения безопасности ПДн распоряжением председателя Комиссии назначаются ответственный за организацию обработки персональных данных, администратор информационной безопасности ИСПДн и администратор ИСПДн.

3.3. Ответственный за организацию обработки персональных данных обязан:

- осуществлять внутренний контроль за соблюдением работниками организации установленных требований по обеспечению безопасности ПДн;
- организовывать проведение оценки эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- осуществлять контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности ИСПДн;
- организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;
- периодически инициировать процедуры определения угроз безопасности ПДн при их обработке в ИСПДн;
- организовывать и контролировать процедуры обнаружения фактов несанкционированного доступа к ПДн; фактов, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн;
- организовывать и контролировать процедуры принятия мер по предотвращению несанкционированного доступа к ПДн; инцидентов, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн.

3.4. Администратор информационной безопасности ПДн обязан:

- осуществлять установку, настройку и сопровождение технических средств защиты;
- участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн;
- участвовать в приемке новых программных средств;
- обеспечить доступ к защищаемой информации Пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения;
- уточнять в установленном порядке обязанности Пользователей ИСПДн по обработке объектов защиты;
- вести контроль над процессом осуществления резервного копирования объектов защиты;
- анализировать состояние защиты ИСПДн и ее отдельных подсистем;
- контролировать неизменность состояния средств защиты их параметров и режимов защиты;
- контролировать физическую сохранность средств и оборудования ИСПДн;

- контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты;

- контролировать исполнение пользователями парольной политики;

- не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач;

- не допускать к работе на элементах ИСПДн посторонних лиц;

- осуществлять периодические контрольные проверки носителей ПДн, рабочих станций и тестирование правильности функционирования средств защиты ИСПДн;

- оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты;

- периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации;

- в случае отказа работоспособности технических средств и программного обеспечения средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;

- принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3.5. Администратор ИСПДн обязан:

- поддерживать текущий порядок обеспечения безопасности ПДн;

- организовывать доведение до сведения работников организации положений законодательства РФ и локальных нормативных документов по обеспечению безопасности ПДн;

- определять перечень работников организации, которым доступ к ПДн необходим для выполнения служебных обязанностей;

- участвовать в реализации планов и программ поддержки осведомленности (обучения) в области обеспечения ИБ;

- в случае отказа работоспособности технических средств и программного обеспечения ИСПДн принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;

- принимать меры по реагированию, в случае возникновения непредвиденных и аварийных ситуаций, с целью ликвидации их последствий.

3.6. Необходимые технические меры для обеспечения безопасности ПДн реализуются в рамках системы защиты персональных данных (далее – СЗПДн).

3.7. СЗПДн обеспечивает защиту информации, содержащей ПДн, обрабатываемой с применением средств вычислительной техники, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

3.8. Мероприятия по обеспечению безопасности ПДн, реализуемые в рамках СЗПДн, включают:

- определение уровня защищенности ИСПДн;

- создание моделей угроз и нарушителя для каждой ИСПДн;

- применение организационных и технических мер по обеспечению безопасности ПДн для поддержания установленного уровня защищенности ПДн и нейтрализации актуальных угроз безопасности ПДн;

- определение во внутренних нормативных документах порядка применения мер защиты, применяемых для обеспечения безопасности ПДн;

- ознакомление работников организации, непосредственно осуществляющих обработку ПДн, с требованиями законодательных и нормативных актов, локальных нормативных документов, устанавливающих порядок обеспечения безопасности ПДн;

- организацию внутреннего контроля и (или) аудита соответствия порядка обеспечения безопасности ПДн требованиям законодательных и нормативных актов, локальных нормативных документов;

- организацию обучения, инструктажей и повышения осведомленности работников, осуществляющих обработку ПДн, по вопросам обеспечения безопасности ПДн;

- совершенствование СЗПДн в соответствии с изменяемыми внутренними и внешними условиями и факторами, в том числе изменениями требований законодательства РФ.

4. Требования к системе защиты персональных данных

4.1. Требования к СЗПДн устанавливаются исходя из уровня защищенности ПДн и состава актуальных угроз безопасности ПДн.

4.2. Определение уровней защищенности ИСПДн производится в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.3. Определение угроз безопасности ПДн производится в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России от 14.02.2008) на основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России от 15.02.2008).

5. Описание системы защиты персональных данных

5.1. В число мер по обеспечению безопасности ПДн, реализованных в Комиссии, входят:

- определение порядка доступа в помещения, в которых осуществляется обработки ПДн;

- размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;

- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн (в том числе серверное помещение), а также хранятся носители информации;

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным активам, информационной системе и связанным с ее использованием работам, документам только для выполнения функциональных обязанностей;

- установление правил доступа пользователей и обслуживающего персонала к информационным активам, программным средствам обработки (передачи) и защиты информации на основе принципа минимально необходимых полномочий для выполнения своих функциональных обязанностей и поставленными перед ним задачами в объеме, необходимом для их исполнения;

- учет и контроль лиц, допущенных к работе с ПДн;

- регистрация и учет действий пользователей с ПДн, контроль несанкционированного доступа к ПДн;

- размещение технических средства обработки графической, видео и буквенно-цифровой информации, содержащей ПДн, таким образом, чтобы исключить возможность просмотра посторонними лицами текстовой и графической, видовой информации, содержащей ПДн;

- использование СВТ, удовлетворяющих требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видео-дисплейным терминалам средств вычислительной техники;

- учет и хранение съемных носителей, содержащих ПДн, и их обращение, исключающее хищение, подмену и уничтожение;

- предотвращение внедрения в ИСПДн вредоносного программного обеспечения;

- применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

- организация контроля за принимаемыми мерами по обеспечению безопасности ПДн и установленного уровня защищенности ПДн.

5.2. Для реализации указанных мер в составе СЗПДн реализованы следующие функциональные подсистемы:

- идентификация и аутентификация субъектов доступа и объектов доступа;

- управление доступом субъектов доступа к объектам доступа;

- ограничение программной среды;

- обеспечение целостности информационной системы и ПДн;

- обеспечение доступности ПДн;

- регистрация событий безопасности;

- антивирусная защита;

- защита технических средств;

- защита информационной системы, ее средств, систем связи и передачи данных;

5.3. Технические средства защиты информации, используемые для нейтрализации актуальных угроз безопасности ПДн, применяемые Комиссией, проходят в установленном порядке процедуру оценки соответствия.

5.4. Для выбора и реализации мер защиты ПДн Комиссии могут привлекаться на договорной основе сторонние организации, имеющие оформленную в установленном порядке лицензию на соответствующий вид деятельности в области защиты информации.

6. Контроль выполнения требований

6.1. Контроль и надзор за выполнением требований по обработке ПДн осуществляется уполномоченным органом по защите прав субъектов ПДн (Роскомнадзор).

6.2. Федеральные органы исполнительной власти (ФСБ России и ФСТЭК России) могут осуществлять контроль за выполнением организационных и технических мер по обеспечению безопасности ПДн без права ознакомления с ПДн, обрабатываемыми в ИСПДн.

6.3. Для проведения аудита соответствия порядка обеспечения безопасности ПДн требованиям законодательства РФ могут привлекаться внешние организации, имеющие оформленную в установленном порядке лицензию на соответствующий вид деятельности в области защиты информации.

7. Ответственность.

7.1. Обязанности по контролю выполнения положений настоящего Положения возлагаются на лицо, ответственное за организацию обработки персональных данных.

7.2. Ответственность за общий контроль реализации мероприятий по обеспечению безопасности ПДн несет Администратор безопасности ИСПДн.