государственное казенное учреждение Владимирской области
«Отдел социальной защиты населения по Камешковскому району»

П Р И К А З

от 17.05.2011 № 27

О проведении работ по защите персональных данных

В целях исполнения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» п р и к а з ы в а ю:

1. Утвердить следующие документы по защите информации:

- политику информационной безопасности (приложение № 1);
- положение о разграничении прав доступа к персональным данным (приложение № 2);
- перечень персональных данных (приложение № 3);
- акт классификации информационных систем персональных данных (приложение № 4);
- порядок резервирования и восстановления работоспособности (приложение № 5);
- инструкцию администратора безопасности информационной системы персональных данных (приложение № 6);
- инструкцию пользователя информационной системы персональных данных (приложение № 7);
- инструкцию по обеспечению безопасности рабочих мест обработки персональных данных (приложение № 8);
- инструкцию по работе с обращениями субъектов персональных данных (приложение № 9);
- инструкцию по работе со съемными носителями, содержащими персональные данные (приложение № 10);
- инструкцию по обработке персональных данных без использования средств автоматизации (приложение № 11);
- описание технологического процесса обработки персональных данных (приложение № 12);
- план мероприятий по внутреннему контролю за соблюдением безопасности персональных данных (приложение № 13);
- положение о комиссии по классификации информационных систем персональных данных (приложение № 14);
- список лиц, допущенных к обработке персональных данных работников отдела (приложение № 15);

- список работников, допущенных к обработке персональных данных получателей мер социальной поддержки (приложение № 16).

2. Ввести вышеуказанные документы в действие с момента подписания настоящего приказа.

3. Контроль за исполнением настоящего приказа возложить на заместителя директора Ширканову Л.И.

Директор учреждения О.В. Егорова

Приложение № 1
к приказу директора
ГКУ ОСЗН
по Камешковскому району
от 17.05.2011 № 27

ПОЛИТИКА
информационной безопасности государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району»

СОДЕРЖАНИЕ

Термины и определения

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление,

изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

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

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов,

религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность 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 при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Перечень сокращений

АВПО – антивирусной программное обеспечение
АРМ – автоматизированное рабочее место
ИСПДн – информационная система персональных данных
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПО – программное обеспечение
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
ТКУ И – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных

Введение

Настоящая Политика информационной безопасности (далее политика) государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району» (далее оператор) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных.

Политика разработана в соответствии с требованиями нормативных документов:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 11.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Положения о методах и способах защиты информации в информационных системах персональных данных», утвержденных Приказом ФСТЭК России от 05.02.2010 № 58;
- «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае из использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-662.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району».

Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты Оператора от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации УБПДн.

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 УБПДн.

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

Область действия

Требования настоящей Политики распространяются на всех сотрудников Оператора (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

Система защиты персональных данных

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

- перечня персональных данных;
- акта классификации информационных систем персональных данных;
- частной модели актуальных угроз и вероятного нарушителя;
- положения о разграничении прав доступа к персональным данным;
- нормативных документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Оператора. На основании анализа актуальных угроз безопасности ПДн описанного в Частной модели актуальных угроз и вероятного нарушителя, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по внутреннему контролю за соблюдением безопасности персональных данных.

Организационные мероприятия должны включать:

- правовое основание для сбора персональных данных;
- определение ответственных лиц за соблюдением мер безопасности;
- защиту персональных данных, обрабатываемых без средств автоматизации;
- защиту персональных данных, обрабатываемых с применением средств автоматизации;
- защиту объектов от хищения;
- защиту съемных накопителей, содержащих персональные данные;
- вопросы уничтожения персональных данных.

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

- защиты от несанкционированного доступа к персональным данным;
- антивирусной защиты для рабочих станций пользователей и серверов;
- межсетевого экранирования;
- криптографической защиты информации, при передаче защищаемой информации по каналам связи;
- средства защиты от утечки по ТКУИ.

Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- контроля отсутствия недекларированных возможностей;
- криптографической защиты;
- защиты от утечки по ТКУИ.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн.

Подсистема управления доступом должна осуществлять:

- идентификацию и проверку подлинности субъектов доступа при входе в операционную систему ИСПДн по идентификатору и паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;
- идентификацию терминалов, технических средств информационной системы, каналов связи и внешних устройств ИСПДн по их логическим адресам (номерам);
- идентификацию программ, томов, каталогов, файлов, записей, полей записей по именам;
- контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа.

Подсистема регистрации и учета должна осуществлять:

- регистрацию входа (выхода) пользователя в систему (из системы) либо регистрацию загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или не успешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке.
- учет всех защищаемых носителей информации с помощью их маркировки и занесение данных в журнал учета с отметкой об их выдаче (приеме);
- регистрацию выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращений к подсистеме вывода), краткое содержание документа (наименование, вид, код), спецификация устройства выдачи (логическое имя (номер) внешнего устройства);
- очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних носителей информации;
- регистрацию запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных. В параметрах регистрации

указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный);

- регистрацию попыток доступа программных средств (программ, процессов, задач) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла;

- регистрацию попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются дата и время попытки доступа у защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер)).

Подсистема обеспечения целостности должна осуществлять:

- обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

- физическую охрану информационной системы(технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;

- периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;

- наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

Межсетевое экранирование 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);

- идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;

- 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 аппаратурного отключения межсетевого экрана);

- контроль целостности своей программной и информационной части;
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
- регламентированное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления;
- фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
- фильтрацию с учетом любых значимых полей сетевых пакетов;
- регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
- регистрация запуска программ и процессов (заданий, задач);
- фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя;
- фильтрацию на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя;
- фильтрацию с учетом даты и времени;
- аутентификацию входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети;
- регистрацию и учет запросов на установление виртуальных соединений;
- локальную сигнализацию попыток нарушения правил фильтрации;
- предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;
- идентификацию и аутентификацию администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;
- регистрацию действий администратора межсетевого экрана по изменению правил фильтрации;
- возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной формы;
- контроль целостности программной и информационной части межсетевого экрана по контрольным суммам.

Защита от ПЭМИН:

- использование технических средств в защищенной исполнении;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

- размещение объектов защиты в соответствии с предписанием на эксплуатацию;

- размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории;

- обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;

- обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.

Защита от утечки по акустическому каналу:

- реализация организационных и технических мер для обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположена информационная система, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при голосовом вводе персональных данных в информационной системе или воспроизведении информации акустическими средствами;

- величина звукоизоляции определяется оператором исходя из характеристик помещения, его расположения и особенностей обработки персональных данных в информационной системе.

Защита от утечки видовой информации:

- размещение устройств вывода информации средств вычислительной техники информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

В информационных системах, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования), или при функционировании которых предусмотрено использование съемных носителей информации, используются средства антивирусной защиты.

Обнаружение вторжений должно обеспечиваться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений (СОВ).

Для информационных систем 1 класса применяется программное обеспечение средств защиты информации, соответствующее 4 уровню контроля отсутствия недекларированных возможностей.

Пользователи ИСПДн

В ИСПДн Оператора можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администраторы безопасности ИСПДн;
- пользователи ИСПДн;
- системные администраторы.

Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в Положении о разграничении прав доступа к персональным данным.

Администраторы безопасности ИСПДн:

Администратором безопасности является штатный сотрудник Оператора, ответственный за функционирование СЗПДн, назначается приказом директора учреждения.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других учреждений.

Пользователь ИСПДн

Пользователем ИСПДн является штатный сотрудник Оператора, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователь ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

Системные администраторы:

Системным администратором может быть штатный сотрудник Оператора или лица сторонних организаций, осуществляющих свои функции на основании двухстороннего договора. Системный администратор не имеет полномочий для управления подсистемами обработки данных и безопасности.

Системный администратор обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

- обладает частью информации о технических средствах и конфигурации ИСПДн;

- имеет физический доступ к техническим средствам обработки информации и средствам защиты;

- знает, по меньшей мере, одно легальное имя доступа.

Требования к персоналу по обеспечению защиты ПДн

Все сотрудники Оператора, 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 сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

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

Сотрудники Оператора, 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.

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

Сотрудники Оператора 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.

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

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

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

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

Сотрудники Оператора 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 сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники 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.

Ответственность сотрудников

В соответствии со ст. 24 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

Администраторы безопасности ИСПДн несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками Оператора – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приложение №2
к приказу директора
ГКУ ОСЗН
по Камешковскому району
от 17.05.2011 № 27

ПОЛОЖЕНИЕ
о разграничении прав доступа к персональным данным государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району»

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

В данном документе представлен список лиц ответственных за обработку персональных данных в информационных системах персональных данных, а так же их уровень прав доступа к обрабатываемым персональным данным.

Обслуживание технических и программных средств осуществляется штатным сотрудником.

ИСПДн «Сотрудники»

Перечень групп, участвующих в обработке персональных данных в ИСПДн

Группа	Уровень доступа к ПДн	Разрешенные действия
1	2	3
Системные администраторы	-	-
Администраторы безопасности ИСПДн	-	-
Пользователи ИСПДн	Пользователь	Чтение, запись, копирование, сортировка, удаление

Перечень лиц, получивших доступ к персональным данным

№	Роль	ФИО сотрудника	Должность
1	2	3	4
1.	Пользователи ИСПДн	Егорова О.В.	Директор учреждения
2.	Пользователи ИСПДн	Ширканова Л.И.	Заместитель директора учреждения
3.	Пользователи ИСПДн	Шаленная Т.Н.	Заведующая сектором бухгалтерского учета и отчетности
4.	Пользователи ИСПДн	Ландышева З.И.	Бухгалтер 1 категории
5.	Пользователи ИСПДн	Жунина И.В	Бухгалтер 2 категории
6.	Администратор безопасности ИСПДн	Писковой В.Н.	Администратор баз данных получателей мер социальной поддержки 1 категории
7.	Системные администраторы	Писковой В.Н.	Администратор баз данных получателей мер социальной поддержки 1 категории

2. ИСПДн «Социальная защита населения»

Перечень групп, участвующих в обработке персональных данных в ИСПДн

Группа	Уровень доступа к ПДн	Разрешенные действия
1	2	3
Системные администраторы	-	-
Администраторы безопасности ИСПДн	-	-
Пользователи ИСПДн	Пользователь	Чтение, запись, копирование, сортировка, удаление

Перечень лиц, получивших доступ к персональным данным

№	Роль	ФИО сотрудника	Должность
1	2	3	4
1.	Пользователи ИСПДн	Егорова О.В.	Директор учреждения
2.	Пользователи ИСПДн	Ширканова Л.И.	Заместитель директора учреждения
3.	Пользователи ИСПДн; Системные администраторы	Писковой В.Н.	Администратор баз данных получателей мер социальной поддержки 1 категории
4.	Пользователи ИСПДн	Рахова Е.В.	Заведующая сектором по назначению и выплате пособий и компенсаций семьям с детьми
5.	Пользователи ИСПДн	Рокашевская Н.М.	Инспектор по предоставлению мер социальной поддержки 1 категории
6.	Пользователи ИСПДн	Козлова Н.А.	Инспектор по предоставлению мер социальной поддержки 1 категории
7.	Пользователи ИСПДн	Агеева Л.А.	Инспектор по предоставлению мер социальной поддержки 2 категории
8.	Пользователи ИСПДн	Андреева Т.Е.	Инспектор по предоставлению мер социальной поддержки 1 категории
9.	Пользователи ИСПДн	Панова Е.В.	Заведующая сектором по предоставлению мер социальной поддержки отдельным категориям граждан
10.	Пользователи ИСПДн	Павлова Е.Е.	Старший инспектор по предоставлению мер социальной поддержки
11.	Пользователи ИСПДн	Кротова О.Е.	Инспектор по предоставлению мер социальной поддержки 1 категории

1	2	3	4
12.	Пользователи ИСПДн	Булырева Г.Л.	Инспектор по предоставлению мер социальной поддержки 2 категории
13.	Пользователи ИСПДн	Смирнова М.В.	Инспектор по предоставлению мер социальной поддержки 1 категории
14.	Пользователи ИСПДн; Администраторы безопасности ИСПДн	Писковой В.Н.	Администратор баз данных получателей мер социальной поддержки 1 категории

Приложение № 3
к приказу директора
ГКУ ОСЗН
по Камешковскому району
от 17.05.2011 № 27

ПЕРЕЧЕНЬ
персональных данных
государственного казенного учреждения Владимирской области
«Отдел социальной защиты населения по Камешковскому району»

1. ПЕРСОНАЛЬНЫЕ ДАННЫЕ ИСПДн «СОТРУДНИКИ»

1.1. Перечень персональных данных (ПДн) сотрудников государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району» (далее Оператор):

- ФИО;
- Паспортные данные;
- Адрес места регистрации;
- Дата рождения;
- Образование;
- Профессия;
- Семейное положение;
- Сведения о доходах;
- Сведения о стаже работы;
- ИНН;
- СНИЛС.

ПДн сотрудников обрабатываются Оператором на основании Трудового Кодекса Российской Федерации.

Согласие субъекта на обработку его ПДн не требуется.

Средствами обработки ПДн являются: ОС Windows XP Pro; MS Office 2003; 1С Предприятие; ПФР

ПДн сотрудников обрабатываются в отделе: сектор бухгалтерского учёта и отчетности.

Срок хранения ПДн сотрудников составляет 75 лет.

ПДн сотрудников представлены в электронном и бумажном виде.

Места хранения ПДн: локально на АРМ.

2. ПЕРСОНАЛЬНЫЕ ДАННЫЕ ИСПДн «СОЦИАЛЬНАЯ ЗАЩИТА НАСЕЛЕНИЯ»

Перечень персональных данных (ПДн) граждан, которым предоставляются меры социальной поддержки (далее Граждан):

- Фамилия, имя, отчество;
- Дата рождения;
- Пол;
- Данные документа, удостоверяющего личность;
- Данные документа, удостоверяющее право на льготы;
- Страховой номер индивидуального лицевого счета;
- Индивидуальный налоговый номер;
- Сведения о семейном положении;
- Сведения о рождение детей;
- Образование;
- Сведения о воинском учете;
- Сведения о доходах;
- Сведения об имуществе на праве собственности;
- Адрес места жительства, (места пребывания);
- Дата назначения пенсии, ЕДВ и иных социальных выплат;
- Срок, на который установлена пенсия, ЕДВ и иные социальные выплаты;
- Группа инвалидности, степень ограничения способности к трудовой деятельности;
- Иные данные, необходимые для оказания мер социальной поддержки.

ПДн граждан обрабатываются Оператором в соответствии с нормативными документами:

- Федеральный закон от 12.01.1995 № 5-ФЗ «О ветеранах»;
- Закон Российской Федерации от 18.10.1991 № 1761-1 «О реабилитации жертв политических репрессий»;
- Закон Владимирской области от 02.10.2007 № 120-ОЗ «О социальной поддержке и социальном обслуживании отдельных категорий граждан во Владимирской области»;
- постановление Губернатора области от 24.01.2005 № 30 «О порядке предоставления мер социальной поддержки отдельным категориям граждан в соответствии с областным законодательством»;
- постановление Губернатора области от 25.12.2006 № 917 «О порядке предоставления мер социальной поддержки по оплате проезда на железнодорожном транспорте пригородного сообщения отдельных категорий граждан»;
- постановление Губернатора области от 01.02.2006 № 64 «О порядке постановки на учет и обеспечения жилыми помещениями реабилитированных лиц и членов их семей в случае возвращения на прежнее место жительства»;
- постановление Губернатора Владимирской обл. от 24.10.2007 № 791 «Об утверждении административного регламента исполнения департаментом социальной защиты населения администрации области государственной функции по

предоставлению мер социальной поддержки ветеранам труда и гражданам, проработавшим в тылу в период с 22 июня 1941 года по 9 мая 1945 года не менее шести месяцев, исключая период работы на временно оккупированных территориях СССР, либо награжденным орденами или медалями СССР за самоотверженный труд в период Великой Отечественной войны, гражданам, подвергшимся политическим репрессиям и впоследствии реабилитированным, а также признанным пострадавшими от политических репрессий»;

- Федеральный закон от 19.05.1995 № 81-ФЗ «О государственных пособиях гражданам, имеющим детей»;

- Основами законодательства Российской Федерации об охране здоровья граждан от 22.07.1993 № 5487-1;

- Закон Владимирской области от 02.10.2007 № 120-ОЗ «О социальной поддержке и социальном обслуживании отдельных категорий граждан во Владимирской области»;

- постановление Губернатора области от 14.12.2004 № 683 «Об утверждении Положения о порядке назначения и выплаты ежемесячного пособия гражданам, имеющим детей»;

- постановление Губернатора области от 14.12.2004 № 684 «О порядке предоставления льгот на проезд на междугородном транспорте для детей, не являющихся инвалидами, нуждающихся в санаторно-курортном лечении»;

- постановление Губернатора области от 17.12.2004 № 700 «О порядке учета и исчисления величины среднедушевого дохода семьи, дающего права на получение ежемесячного пособия на ребенка»;

- постановление Губернатора области от 17.10.2005 № 580 «О порядке назначения и выплате денежных компенсаций беременным женщинам, кормящим матерям, а также на детей в возрасте до трех лет в семьях, со среднедушевым доходом, не превышающим величину прожиточного минимума, установленную на территории Владимирской области, для обеспечения их полноценным питанием по заключению врачей»;

- постановление Губернатора области от 19.12.2007 № 940 «О порядке предоставления мер социальной поддержки многодетным семьям во Владимирской области»;

- постановление Губернатора области от 17.01.2008 № 16 «Об утверждении Порядка осуществления единовременной денежной выплаты при рождении ребенка»;

- постановление Губернатора области от 15.10.2007 № 756 (ред. от 10.06.2008) «Об утверждении Административного регламента исполнения департаментом социальной защиты населения администрации области государственной функции по предоставлению мер социальной поддержки семьям с детьми»;

- Федеральным законом от 12.01.1996 № 8-ФЗ «О погребении и похоронном деле» («Российская газета», 20.01.1996 № 12);

- постановлением Губернатора области от 25.10.2004 № 562 «О порядке возмещения стоимости гарантированного перечня услуг по погребению и выплаты

социального пособия на погребение за счет средств областного бюджета» («Владимирские ведомости», 10.11.2004 № 307);

- постановлением Губернатора области от 15.10.2007 № 757 (ред. от 30.06.2009) «Об утверждении административного регламента исполнения департаментом социальной защиты населения администрации области государственной функции по предоставлению материальной и иной помощи для погребения»;

- Постановление Губернатора области от 31.12.2004 № 742 «О ведении регистра лиц, проживающих на территории Владимирской области и имеющих право на получение мер социальной поддержки» (в редакции от 05.12.2007 №894).

Согласие субъекта на обработку его ПДн требуется, форма согласия приведена в Приложении.

Средствами обработки ПДн являются: ОС Windows XP Pro; MS Office 2003; Open Office; 1С Предприятие; НВПО «Регистр» (Регистр лиц, имеющих право на получение мер социальной поддержки по областным и федеральным законам); ПО «Назначение и выплата пособий и компенсаций»; ПО «Назначение и выплата пенсий и ЕДВ»; ПО «Общегосударственная база данных «Ветераны»; ПО «Студенты»; ПО «Обманутые вкладчики); Программа "Формирование ЗАЯВКИ по спискам получателей компенсаций (пособий) – граждан, подвергшихся воздействию радиации вследствие радиационных аварий и ядерных испытаний; Программа для подготовки в электронном виде реестров лиц, фактически осуществляющих уход за ребенком, не подлежащих обязательному социальному страхованию и получающих ежемесячное пособие по уходу за ребенком; Программа для формирования списков получателей выплат на проведение ремонта индивидуальных жилых домов, принадлежащих членам семей военнослужащих, потерявших кормильца (Постановление Правительства Российской Федерации от 27.05.2006 № 313); Программа для формирования Реестра получателей компенсационных выплат (Постановление Правительства Российской Федерации от 02.08.2005 № 475).

ПДн Граждан обрабатываются в отделах: сектор по предоставлению мер социальной поддержки отдельным категориям граждан; сектор по назначению и выплате пособий и компенсаций семьям с детьми.

Срок хранения ПДн Граждан составляет ____ лет.

ПДн Граждан представлены в электронном и бумажном виде.

Места хранения ПДн: локально на АРМ.

Приложение
к перечню
персональных данных

Согласие субъекта персональных данных

1. ФИО субъекта:_____
2. Персональные данные субъекта:

Фамилия, имя, отчество
Дата рождения
Пол
Данные документа, удостоверяющего личность
Данные документа, удостоверяющее право на льготы
Страховой номер индивидуального лицевого счета
Индивидуальный налоговый номер
Сведения о семейном положении
Сведения о рождение детей
Образование
Сведения о воинском учете
Сведения о доходах
Сведения об имуществе на праве собственности
Адрес места жительства, (места пребывания)
Дата назначения пенсии, ЕДВ и иных социальных выплат
Срок, на который установлена пенсия, ЕДВ и иные социальные выплаты
Группа инвалидности, степень ограничения способности к трудовой деятельности
Иные данные, необходимые для оказания мер социальной поддержки

3. Субъект дает согласие на обработку Оператором своих персональных данных, то есть совершение, в том числе, следующих действий: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, при этом общее описание вышеуказанных способов обработки данных приведено в ФЗ №152 от 27.07.2006 г., а также право на передачу такой информации в медицинский информационно-аналитический центр.

4. Оператор обязуется использовать данные Субъекта исключительно для оказания мер социальной поддержки. Оператор может раскрыть правоохранительным органам любую информацию по официальному запросу в случаях, установленных законодательством в стране проживания Субъекта.

5. Субъект персональных данных по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных (в соответствии с п.4 ст. 14 ФЗ №152 от 27.06.2006 г.).

6. Обработка персональных данных, не включенных в общедоступные источники, прекращается по истечении ___ лет с даты прекращения оказания социальной поддержки Субъекту.

7. При поступлении Оператору письменного заявления Субъекта о прекращении действия Согласия, персональные данные деперсонализируются в 15-дневый срок.

8. Настоящее согласие действует в течение срока хранения персональных данных Субъекта.

_____ _____

ФИО подпись

«___»_____2011

Приложение № 4
к приказу директора
ГКУ ОСЗН
по Камешковскому району
от 17.05.2011 № 27

АКТ
классификации информационных систем персональных данных государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району»

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Классификация ИСПДн была проведена в соответствии с совместным Приказом ФСТЭК/ФБС/Минсвязи «Об утверждении порядка проведения классификации информационных систем персональных данных» от 13.02.2008г. № 55/86/20.

Классификацию ИСПДн проводила комиссия, назначенная приказом директора учреждения от 17.05.2011 № 26, в составе:

Председатель комиссии	- Ширканова Людмила Ивановна, заместитель директора учреждения
Члены комиссии	- Панова Елена Владимировна, заведующая сектором предоставления мер социальной поддержки отдельным категориям граждан; - Писковой Валерий Николаевич, администратор баз данных; - Рахова Екатерина Владимировна, заведующая сектором по назначению и выплате пособий и компенсаций семьям с детьми; - Шаленнная Татьяна Николаевна, заведующая сектором бухгалтерского учета и отчетности.

2. АКТ КЛАССИФИКАЦИИ ИСПДн «СОТРУДНИКИ»

Категория персональных данных (Хпд):

категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.

Объем обрабатываемых персональных данных (Хнпд):

3 - в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

Заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе:

Специальные информационные системы - информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

К специальным информационным системам должны быть отнесены:

информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;

информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

Структура ИСПДн:

локальные информационные системы - комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа.

Наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена:

Есть одноточечное подключение к сети Интернет.

Режим обработки персональных данных:

многопользовательский

Режим разграничения прав доступа пользователей информационной системы:

системы с разграничением прав доступа

Местонахождение технических средств информационной системы:

находится в пределах Российской Федерации

По результатам анализа исходных данных ИСПДн присваивается класс К3.

класс 3 (К3) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может

привести к незначительным негативным последствиям для субъектов персональных данных.

Председатель:

_____ Ширканова Л.И.

подпись

Члены комиссии:

_____ Писковой В.Н.

подпись

_____ Рахова Е.В.

подпись

_____ Панова Е.В.

подпись

_____ Шалённая Т.Н.

подпись

3. АКТ КЛАССИФИКАЦИИ ИСПДн «СОЦИАЛЬНАЯ ЗАЩИТА НАСЕЛЕНИЯ»

Категория персональных данных (Хпд):

категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.

Объем обрабатываемых персональных данных (Хнпд):

2 - в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования.

Заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе:

Специальные информационные системы - информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

К специальным информационным системам должны быть отнесены:

информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;

информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

Структура ИСПДн:

локальные информационные системы - комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа.

Наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена:

Есть одноточечное подключение к сети Интернет.

Режим обработки персональных данных:

многопользовательский

Режим разграничения прав доступа пользователей информационной системы:

системы с разграничением прав доступа

Местонахождение технических средств информационной системы:

находится в пределах Российской Федерации

По результатам аынализа исходных данных ИСПДн присваивается класс К2.

класс 2 (К2) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных.

Председатель:

_____ Ширканова Л.И.

подпись

Члены комиссии:

_____ Писковой В.Н.

подпись

_____ Рахова Е.В.

подпись

_____ Панова Е.В.

подпись

_____ Шалённая Т.Н.

подпись

Приложение № 5
к приказу директора
ГКУ ОСЗН
по Камешковскому району
от 17.05.2011 № 27

ПОРЯДОК
резервирования и восстановления работоспособности

СОДЕРЖАНИЕ

1. Назначение и область действия

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации (далее – Инструкция) определяет действия, связанные с функционированием ИСПДн государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району» (далее Оператор), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Задачей данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех пользователей Оператора, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящих к потере защищаемой информации и контроль обеспечения мероприятий по предотвращению инцидентов безопасности, назначается Администратор безопасности ИСПДн.

2. Порядок реагирования на инцидент

В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей.
- в результате преднамеренных действий пользователей и третьих лиц.
- в результате нарушения правил эксплуатации технических средств ИСПДн.

В результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Оператора предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. Меры обеспечения непрерывной работы и восстановления ресурсов при возникновении инцидентов

3.1. Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все критичные помещения Оператора (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

3.2. Организационные меры

Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

Носители должны храниться не менее года, для возможности восстановления данных.

Приложение № 6
к приказу директора
ГКУ ОСЗН
по Камешковскому району
от 17.05.2011 № 27

ИНСТРУКЦИЯ
администратора безопасности информационной системы персональных данных государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району»

СОДЕРЖАНИЕ

1. Общие положения

1.1. Администратором безопасности (АБ) ИСПДн является штатный сотрудник государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району», назначенный приказом директора учреждения.

1.2. АБ ИСПДн в своей работе руководствуется:

- положением по защите персональных данных;
- политикой информационной безопасности;
- инструкциями по обеспечению безопасности персональных данных;
- настоящей инструкцией;
- нормативными документами ФСТЭК России.

1.3. АБ ИСПДн осуществляет проведение и контроль мероприятий по обеспечению безопасности персональных данных.

1.4. АБ ИСПДн осуществляет методическое руководство работой пользователей ИСПДн.

1.5. АБ ИСПДн отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.

1.6. АБ ИСПДн несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

2. Должностные обязанности

АБ ИСПДн обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);
- аппаратных средств;
- аппаратных и программных средств защиты.

2.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.7. Проводить периодический контроль принятых мер по защиты, в пределах возложенных на него функций.

2.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля Оператором ИСПДн.

2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.11. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.12. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.

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

Приложение № 7
к приказу директора
ГКУ ОСЗН
по Камешковскому району
от 17.05.2011 № 27

ИНСТРУКЦИЯ
пользователя информационной системы персональных данных государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району»

СОДЕРЖАНИЕ

1. Общие положения

1.1. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является каждый сотрудник государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется:

- положением по защите персональных данных;
- политикой информационной безопасности;
- инструкциями по обеспечению безопасности персональных данных;
- настоящей инструкцией;
- нормативными документами ФСТЭК России.

1.5. Методическое руководство работой пользователя осуществляется администратором безопасности (АБ) ИСПДн.

2. Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к персональным данным .

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики.

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к АБ ИСПДн.

2.8. Пользователям запрещается:

- разглашать защищаемую информацию третьим лицам;
- копировать защищаемую информацию на внешние носители без разрешения своего руководителя;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к папкам на своей рабочей станции;
- запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.9. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>

2.10. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий в пределах возложенных на него функций.

Приложение № 8
к приказу директора
ГКУ ОСЗН
по Камешковскому району
от 17.05.2011 № 27

ИНСТРУКЦИЯ
по обеспечению безопасности рабочих мест обработки персональных данных государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району»

СОДЕРЖАНИЕ

1. Общие положения

1.1. Настоящая инструкция определяет требования по защите рабочих мест ИСПДн, на которых ведется обработка и хранение персональных данных.

1.2. Настоящая инструкция составлена на основании требований нормативных документов ФСТЭК России.

1.3. В понятие защиты рабочих мест ИСПДн входит:

- физическая защита технических средств от несанкционированного доступа;
- парольная защита рабочих мест от несанкционированного доступа к персональных данным;
- антивирусная защита рабочих мест от несанкционированного доступа к персональным данным из сети Интернет.

2. Требования по защите от несанкционированного доступа

В соответствии с требованиями нормативных документов ФСТЭК России методами и способами защиты информации от несанкционированного доступа являются:

2.1. реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

2.2. ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;

2.3. разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

2.4. регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

2.5. учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

2.6. резервирование технических средств, дублирование массивов и носителей информации;

2.7. использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

2.8. использование защищенных каналов связи;

2.9. размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

2.10. организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

2.11. предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

3. Требования по парольной защите

3.1. С целью контроля учетных записей для доступа к информационным ресурсам персональных данных, все легализованные учетные записи ведутся в Журнале учета Логинов (приложение 1).

3.2. Личные пароли доступа к элементам ИСПДн создаются пользователям самостоятельно.

3.3. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.4. Правила формирования пароля:

Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

Пароль должен состоять не менее чем из 8 символов.

В пароле должны присутствовать символы трех категорий из числа следующих четырех:

- прописные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- десятичные цифры (от 0 до 9);
- символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #,%).

Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

Запрещается выбирать пароли, которые уже использовались ранее.

3.5. Правила ввода пароля:

Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.6. Правила хранение пароля:

Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.7. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.

- своевременно сообщать администратору безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Требования по антивирусной защите

4.1. На каждом рабочем месте и серверах ИСПДн должно быть установлено антивирусное программное обеспечение (АВПО).

4.2. Антивирусные базы всегда должны быть в актуальном состоянии.

4.3. Запрещается работа на элементах ИСПДн с выключенным или неработоспособным АВПО.

4.4. Определение параметров и режимов работы средств антивирусного контроля осуществляется администратором безопасности (АБ) ИСПДн в соответствии с руководствами по применению конкретных антивирусных средств.

4.5. Проверка на наличие вирусов должна проводиться регулярно. Проверке подлежат:

- все файлы на НЖМД сервером и рабочих мест;
- съемные носители, содержащие персональные данные;
- получаемые из сторонних организации файлы;
- передаваемые в сторонние организации файлы.

4.6. Результаты проверок должны фиксироваться в Журнале антивирусных проверок (приложение 2).

4.7. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь обязан немедленно сообщить о своих подозрениях АБ. АБ совместно с пользователем должен выполнить внеочередной антивирусный контроль.

5. Требования по работе в сети интернет

5.1. Работа в сети Интернет на элементах ИСПДн, должна проводиться при служебной необходимости.

5.2. При работе в сети Интернет запрещается:

Осуществлять работу при отключенных средствах защиты (антивирус и других).

Передавать по сети защищаемую информацию без использования средств шифрования.

Запрещается скачивать из сети программное обеспечение и другие файлы.

Запрещается посещение сайтов сомнительной репутации (сайты содержащие нелегально распространяемое ПО и другие).

Запрещается нецелевое использование сети Интернет.

6. Требования по работе со средствами защиты

6.1. На рабочих местах и серверах ИСПДн, исходя из Частной модели актуальных угроз, должны быть установлены специальные средства защиты. К ним могут относится:

средства защиты от несанкционированного доступа;

межсетевые экраны;

антивирусные средства защиты;

криптографические средства защиты;

средства защиты от утечки информации по техническим каналам.

6.2. Все средства защиты могут быть установлены только организацией, имеющей лицензию на техническую защиту конфиденциальной информации.

6.3. Все средства защиты, установленные в ИСПДн, а также эксплуатационная документация на них, подлежат учету в Журнале учета средств защиты (приложение 3).

6.4. Настройка средств защиты проводиться в соответствии с эксплуатационной документацией и требованиями нормативных документов ФСТЭК России.

Приложение № 1
к инструкции
по обеспечению безопасности рабочих
мест обработки персональных данных

Форма Журнала учета Логинов

№	ФИО	Должность	Подразделение	Логин	Дата заведения	Дата удаления	Причина удаления	Подпись системного администратора

Приложение № 2
к инструкции
по обеспечению безопасности рабочих
мест обработки персональных данных

Форма Журнала учета антивирусных проверок

№	Дата проверки	Форма проверки (регулярная/внепланова)	Проверенные АРМ	Результат проверки	Подпись АБ

Приложение № 3
к инструкции
по обеспечению безопасности рабочих
мест обработки персональных данных

Форма Журнала учета СЗИ

№	Уч.№ СЗИ	Наименование СЗИ	Место установки	Дата установки	Подпись установившего	Дата изъятия	Подпись изъявшего

Приложение № 9
к приказу директора
ГКУ ОСЗН
по Камешковскому району
от 17.05.2011 № 27

ИНСТРУКЦИЯ
по работе с обращениями субъектов персональных данных государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району»

СОДЕРЖАНИЕ

1. Общие положения

В соответствии с требованиями Федерального Закона «О персональных данных» от 27.07.2006 № 152-ФЗ, каждый субъект имеет право знать, как проходит обработка его персональных данных.

2. Права субъектов персональных данных

Право субъекта персональных данных на доступ к своим персональным данным:

2.1. Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2.2. Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

2.3. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации. Форма запроса субъекта приведена в Приложении 1.

2.4. Субъект персональных данных имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором, а также цель такой обработки;
- способы обработки персональных данных, применяемые оператором;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

2.5. Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:

- обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и

разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

- обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

- предоставление персональных данных нарушает конституционные права и свободы других лиц.

2.6. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

2.7. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

3. Обязанности оператора персональных данных

Обязанности оператора при сборе персональных данных:

3.1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию.

3.2. Если обязанность предоставления персональных данных установлена федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

3.3. Если персональные данные были получены не от субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены оператору на основании федерального закона или если персональные данные являются общедоступными, оператор до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

- наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные настоящим Федеральным законом права субъекта персональных данных.

3.4. Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

3.5. Оператор обязан сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

3.6. В случае отказа в предоставлении субъекту персональных данных или его законному представителю при обращении либо при получении запроса субъекта персональных данных или его законного представителя информации о наличии персональных данных о соответствующем субъекте персональных данных, а также таких персональных данных оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на законодательную базу, являющееся основанием для такого отказа, в срок, не превышающий семи рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо с даты получения запроса субъекта персональных данных или его законного представителя.

3.7. Оператор обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с

персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы. Форма заявки приведена в Приложении 2.

3.8. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение семи рабочих дней с даты получения такого запроса. Форма уведомления приведена в Приложении 3.

3.9. В случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

3.10. В случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование.

3.11. В случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган. Форма уведомления приведена в приложении 4.

3.12. В случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных или его законного представителя, а в случае, если обращение

или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган.

3.13. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

3.14. Оператор обязан вести учет обращений субъектов. Форма Журнала приведена в приложении 5.

Приложение 1
к инструкции
по работе с обращениями субъектов
персональных данных

Форма запроса субъекта на доступ к его персональным данным

Директору государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району» Егоровой О.В.

От _____
ФИО субъекта

_____
вид документа

_____
номер документа

_____
дата выдачи и кем выдан документ

Запрос

Прошу предоставить информацию об обработке моих персональных данных. Прошу указать состав персональных данных, цель, способы и срок обработки, какие юридические последствия могут возникнуть в следствии обработки.

_____/ _____ /

«___»_____20_

Приложение 2
к инструкции
по работе с обращениями субъектов
персональных данных

Форма заявки субъекта на действия с его персональными данными

Директору государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району» Егоровой О.В.

От _____
ФИО субъекта

_____
вид документа

_____
номер документа

_____
дата выдачи и кем выдан документ

Заявка

Прошу предоставить информацию об обработке моих персональных данных. Прошу указать состав персональных данных, цель, способы и срок обработки, какие юридические последствия могут возникнуть вследствие обработки.

_____/_____/
подпись/расшифровка

«___»_____20_

Приложение 3
к инструкции
по работе с обращениями субъектов
персональных данных

Форма уведомления органа по защите прав субъектов

Руководителю органа_____
_____

От государственного казенного
учреждения Владимирской области
«Отдел социальной защиты населения по
Камешковскому району»

Уведомление

Сообщаю Вам о том, что персональные данные субъекта_____(ФИО) обрабатываются в _____(название организации) с целью_____, на основании_____, и составляют:_____(перечень ПДн).

_____/ О.В.Егорова/

«___»_____20_

Приложение 4
к инструкции
по работе с обращениями субъектов
персональных данных

Форма уведомления субъекта об устранении неправомерных действий с его персональными данными

Субъекту персональных данных
_____
ФИО

От государственного казенного
учреждения Владимирской области
«Отдел социальной защиты населения по
Камешковскому району»

Уведомление

Сообщаю Вам, что допущенные нарушения при обработке персональных данных, а именно_____устранены.
(указать допущенные нарушения)

_____/ О.В.Егорова/

«___»_____20_

Приложение 5
к инструкции
по работе с обращениями субъектов
персональных данных

Форма Журнала учета обращений субъектов ПДн

№	ФИО субъекта	Дата обращения	Цель обращения	Результат	Дата ответа	Исх. № ответа
1.						
2.						
3.						
4.						
5.						

Приложение № 10
к приказу директора
ГКУ ОСЗН
по Камешковскому району
от 17.05.2011 № 27

ИНСТРУКЦИЯ
по работе со съемными носителями, содержащими персональные данные

СОДЕРЖАНИЕ

1. Инструкция по работе со съемными носителями

1.1. Съемными накопителями являются:
- USB-накопители (флеш-диски);
- съемные накопители на жестких магнитных дисках (НЖМД);
- дискеты;
- диски;
- и т.д.

1.2. Съемные накопители применяются для хранения электронных баз данных персональных данных в сейфах или других местах хранения, передачи персональных данных в вышестоящие организации, в филиалы оператора или в сторонние организации. Так же съемные накопители могут служить ля переноса персональных данных на автономное рабочее место ИСПДн.

1.3. Перед использованием съемный носитель должен быть проверен антивирусными средствами на наличие вирусов.

1.4. Хранение съемных накопителей должно осуществляться в местах не доступных для посторонних лиц, также для должностных лиц оператора, не имеющих полномочий на обработку персональных данных для выполнения должностных обязанностей.

1.5. Учет съемных накопителей должен вестись в Журнале учета (приложение № 1).

1.6. Уничтожение съемных носителей персональных данных должно проводиться комиссионно с оформлением акта уничтожения (приложение № 2).

Приложение 1
к инструкции по работе
со съемными носителями

Форма Журнала учета съемных носителей

№	Уч.№ носителя	Назначение носителя	Дата начала использования носителя	Дата уничтожения носителя	№ и дата Акта уничтожения носителя	Подпись АБ

Приложение 2
к инструкции по работе
со съемными носителями

Форма Акта уничтожения съемного носителя

АКТ № ___
уничтожения съемных носителей персональных данных

_____ «___»_____20_
населенный пункт

Настоящий акт составлен в том, что комиссией в составе:
Члены комиссии: _____ _____
ФИО должность
_____ _____
ФИО должность
_____ _____
ФИО должность
проведено уничтожение съемных носителей:

№	Уч. № носителя	Форма носителя	Способ уничтожения
1.			
2.			
3.			
4.			

Члены комиссии: _____ _____
ФИО должность
_____ _____
ФИО должность
_____ _____
ФИО должность

Приложение № 11
к приказу директора
ГКУ ОСЗН
по Камешковскому району
от 17.05.2011 № 27

ИНСТРУКЦИЯ
по обработке персональных данных без использования средств автоматизации государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району»

СОДЕРЖАНИЕ

1. Общие положения

Настоящая инструкция разработана в соответствии с Постановлением Правительства «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008г. № 687.

1.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

1.2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

1.3. В государственном казенном учреждении Владимирской области «Отдел социальной защиты населения по Камешковскому району» персональные данные, обрабатываемые без использования средств автоматизации, представлены:

- трудовыми договорами и личными делами сотрудников Оператора;
- документами, содержащими персональные данные граждан, которым предоставляются меры социальной поддержки.

2. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

2.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

2.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

2.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

2.4. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

- необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных

данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

2.5. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

2.5. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

2.6. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

3.1. У Оператора выделяются две категории персональных данных, обрабатываемых без использования средств автоматизации, в различных целях: сотрудники и граждане, которым предоставляются меры социальной поддержки (далее граждане).

3.2. Персональные данные сотрудников и граждан должны храниться на разных носителях (съемные носители и бумажные носители).

3.3. При хранении материальных носителей у Оператора соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

Приложение № 12
к приказу директора
ГКУ ОСЗН
по Камешковскому району
от 17.05.2011 № 27

ОПИСАНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА
обработки персональных данных
государственного казенного учреждения Владимирской области
«Отдел социальной защиты населения по Камешковскому району»

Описание технологического процесса обработки персональных данных

1. Ввод ПДн осуществляется с АРМ ИСПДн Оператора, удаленных мест доступа нет.

2. Использование ПДн (просмотр, сортировка, составление отчетных файлов) производиться только штатными сотрудниками Оператора, выполняющими должностные обязанности, только с АРМ ИСПДн.

3. Хранение ПДн осуществляется локально на АРМ, в каталогах, размещенных на НЖМД АРМ.

4. Передача ПДн осуществляется по каналу Интернет в: УФНС и ПФР по Владимирской области; Департамент социальной защиты населения; Сбербанк.

5. Средствами обработки являются: ОС Windows 7; ОС Windows XP Pro; MS Office 2003; MS Office 2007; Open Office; 1С Предприятие; 1С Зарплата;ПФР; НВПО «Регистр» (Регистр лиц, имеющих право на получение мер социальной поддержки по областным и федеральным законам); ПО «Назначение и выплата пособий и компенсаций»; ПО «Назначение и выплата пенсий и ЕДВ»; ПО «Общегосударственная база данных «Ветераны»; ПО «Студенты»; ПО «Обманутые вкладчики); Программа "Формирование ЗАЯВКИ по спискам получателей компенсаций (пособий) – граждан, подвергшихся воздействию радиации вследствие радиационных аварий и ядерных испытаний; Программа для подготовки в электронном виде реестров лиц, фактически осуществляющих уход за ребенком, не подлежащих обязательному социальному страхованию и получающих ежемесячное пособие по уходу за ребенком; Программа для формирования списков получателей выплат на проведение ремонта индивидуальных жилых домов, принадлежащих членам семей военнослужащих, потерявших кормильца (Постановление Правительства Российской Федерации от 27.05.2006 № 313); Программа для формирования Реестра получателей компенсационных выплат (Постановление Правительства Российской Федерации от 02.08.2005 № 475).

6. Объектами доступа являются АРМ ИСПДн, БД ПДн и сами ПДн.

7. Субъекты доступа приведены в Положении о разграничении прав доступа к ПДн.

Технологический процесс обработки персональных данных в каждой подсистеме информационных систем персональных данных приведен в таблице ниже

№	Подсистемы информационных систем персональных данных	Технологический процесс
1	2	3
1.	Регистр лиц, имеющих право на получение мер социальной поддержки	Ввод данных, обработка, просмотр, выборки по различным параметрам, статистика, передача по модему («Клиент-Банк») в Сбербанк, передача по VipNet в департамент социальной защиты населения
2.	База данных детей военнослужащих по призыву	Ввод данных, обработка, просмотр, выборки по различным параметрам, статистика, передача по модему («Клиент-Банк») в Сбербанк, передача по VipNet в департамент социальной защиты населения
3.	База данных получателей детских пособий и компенсаций	Ввод данных, обработка, просмотр, выборки по различным параметрам, статистика, передача по модему («Клиент-Банк») в Сбербанк, передача по VipNet в департамент социальной защиты населения
4.	Реестр получателей пособия по уходу за ребенком (ФСС)	Ввод данных, обработка, просмотр, выборки по различным параметрам, статистика, передача по VipNet в департамент социальной защиты населения
5.	База данных по зарплате	Ввод данных, обработка, передача по модему («Клиент-Банк») в Сбербанк
6.	База данных по доходам физических лиц	Ввод данных, обработка, передача по модему (СбиС++) в налоговый орган
7.	База данных по персонифицированному учету ПФР	Ввод данных, обработка, передача по VipNet в ОПФР по Владимирской области
8.	Общегосударственная база данных «Ветераны»	ПД передаются и получаются по VipNet в (из) Департамента социальной защиты населения области. Ввод данных, обработка
9.	База данных получателей денежной компенсации	Ввод данных, обработка, просмотр, выборки по различным параметрам,

1	2	3
	взамен молочных продуктов на детей первого-второго года жизни	статистика, передача по модему («Клиент-Банк») в Сбербанк, передача по VipNet в департамент социальной защиты населения
10.	База данных получателей компенсацион-ных выплат по постановлению Правительства Российской Федерации от 04.08.2006 № 472	Ввод данных, обработка, просмотр, выборки по различным параметрам, статистика, передача по по VipNet в департамент социальной защиты населения
11.	База данных получателей компенсацион-ных выплат по постановлению Правительства Российской Федерации от 02.08.2005 № 475	Ввод данных, обработка, просмотр, выборки по различным параметрам, статистика, передача по по VipNet в департамент социальной защиты населения
12.	База данных получателей компенсацион-ных выплат по постановлению Правительства Российской Федерации от 15.10.2005 № 614	Ввод данных, обработка, просмотр, выборки по различным параметрам, статистика, передача по по VipNet в департамент социальной защиты населения
13.	База данных получателей компенсаций в возмещение вреда, причиненного здоровью граждан в связи с радиацион-ным воздействием вследствие чернобыльской катастрофы по постановлению Правительства Российской Федерации от 30.12.2006 № 872	Ввод данных, обработка, просмотр, выборки по различным параметрам, статистика, передача по по VipNet в департамент социальной защиты населения
14.	Реестр «Обманутые вкладчики»	Ввод данных, обработка, просмотр, выборки по различным параметрам, статистика, передача по по VipNet в департамент социальной защиты населения
15.	База данных ежемесячных денежных выплат по областным и федеральным полномочиям и база данных пенсионных дел	Ввод данных, обработка, просмотр, выборки по различным параметрам, статистика, передача по модему («Клиент-Банк») в Сбербанк, передача по VipNet в департамент социальной защиты населения

1	2	3
16.	База данных студентов, получающих социальные стипендии	Ввод данных, обработка, просмотр, выборки по различным параметрам, статистика, передача по VipNet в департамент социальной защиты населения
17.	База данных получателей компенсаций, подвергшихся воздействию радиацион-ных аварий и ядерных испытаний.	Ввод данных, обработка, просмотр, статистика, передача по СЭД в ОФК

Приложение № 13
к приказу директора
ГКУ ОСЗН
по Камешковскому району
от 17.05.2011 № 27

ПЛАН МЕРОПРИЯТИЙ
по внутреннему контролю за соблюдением безопасности персональных данных государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району»

СОДЕРЖАНИЕ

1. Общие положения

План мероприятий по обеспечению защиты персональных данных (далее – План), содержит необходимый перечень мероприятий для обеспечения защиты персональных данных.

План составлен на основании списка мер, методов и средств защиты, определенных в политике информационной безопасности.

Выбор конкретных мероприятий осуществляется на основании анализа частной модели актуальных угроз и частной модели вероятного нарушителя.

В План включены следующие категории мероприятий:

- организационные (административные);
- технические (аппаратные и программные);
- физические;
- контролирующие.

В План включена следующая информация:

- название мероприятия;
- периодичность мероприятия (разовое/периодическое);
- исполнитель мероприятия/ответственный за исполнение.

2. План мероприятий по обеспечению безопасности ПДН

Мероприятие	Периодичность	Исполнитель/ Ответственный
1	2	3
Организационные мероприятия		
Определение обрабатываемых ПДн и объектов защиты	Разовое срок до	
Определение перечня ИСПДн	Разовое срок до	
Определение круга лиц участвующих в обработке ПДн	Разовое срок до	
Определение ответственности лиц участвующих в обработке	Разовое срок до	
Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей	Разовое срок до	
Назначение ответственного за безопасность ПДн	Разовое срок до	
Введение режима защиты ПДн	Разовое срок до	
Собрание коллегиального органа по классификации ИСПДн	Разовое срок до	
Классификация всех выявленных ИСПДн	Разовое срок до	
Выбор помещений для установки аппаратных средств ИСПДн в помещениях, с целью исключения НСД лиц не допущенных к обработке ПДн	Разовое срок до	
Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИСПДн.	Разовое срок до	
Организация порядка восстановления работоспособности технических средств, ПО, баз данных с подсистем СЗПДн	Разовое срок до	
Введение в действие инструкции по порядку формирования, распределения и применения паролей	Разовое срок до	
Организация информирования и обучения сотрудников о порядке обработки ПДн	Разовое срок до	

1	2	3
Организация информирования и обучения сотрудников о введенном режиме защиты ПДн	Разовое срок до	
Разработка должностных инструкций о порядке обработки ПДн и обеспечении введенного режима защиты	Разовое срок до	
Разработка инструкций о порядке работы при подключении к сетям общего пользования и (или) международного обмена	Разовое срок до	
Организация журнала учета обращений субъектов ПДн	Разовое срок до	
Организация перечня по учету технических средств и средств защиты, а так же документации к ним	Разовое срок до	
Физические мероприятия		
Организация постов охраны для пропуска в контролируемую зону	Разовое срок до	
Внедрение технической системы контроля доступа в контролируемую зону и помещения (по электронным пропускам, токену, биометрическим данным и т.п.)	Разовое срок до	
Внедрение технической системы контроля доступа к элементам ИСПДн (по электронным пропускам, токену, биометрическим данным и т.п.)	Разовое срок до	
Внедрение видеонаблюдения	Разовое срок до	
Установка дверей на входе в помещения с аппаратными средствами ИСПДн	Разовое срок до	
Установка замков на дверях в помещениях с аппаратными средствами ИСПДн	Разовое срок до	
Установка жалюзи на окнах	Разовое срок до	
Установка решеток на окнах здания	Разовое срок до	
Установка системы пожаротушения в помещениях, где расположены элементы ИСПДн	Разовое срок до	

1	2	3
Установка систем кондиционирования в помещениях, где расположены аппаратные средства ИСПДн	Разовое срок до	
Установка систем бесперебойного питания на ключевые элементы ИСПДн	Разовое срок до	
Внедрение резервных (дублирующих) технических средств ключевых элементов ИСПДн	Разовое срок до	
Технические (аппаратные и программные) мероприятия		
Внедрение специальной подсистемы управления доступом, регистрации и учета	Разовое срок до	
Внедрение антивирусной защиты	Разовое срок до	
Внедрение межсетевого экранирования	Разовое срок до	
Внедрение подсистемы анализа защищенности	Разовое срок до	
Внедрение подсистемы обнаружения вторжений	Разовое срок до	
Внедрение криптографической защиты	Разовое срок до	
Контролирующие мероприятия		
Создание журнала внутренних проверок и поддержание его в актуальном состоянии	Ежемесячно	
Контроль над соблюдением режима обработки ПДн	Еженедельно	
Контроль над соблюдением режима защиты	Ежедневно	
Контроль над выполнением антивирусной защиты	Еженедельно	
Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно	

1	2	3
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно	
Контроль за обеспечением резервного копирования	Ежемесячно	
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно	
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	
Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО, специально дорабатываемое собственными разработчиками или сторонними организациями.	Ежемесячно	

Приложение № 14
к приказу директора
ГКУ ОСЗН
по Камешковскому району
от 17.05.2011 № 27

ПОЛОЖЕНИЕ
о комиссии по классификации информационных систем персональных данных государственного казенного учреждения Владимирской области «Отдел социальной защиты населения по Камешковскому району»

СОДЕРЖАНИЕ

1. Общие положения

В государственном казенном учреждении Владимирской области «Отдел социальной защиты населения по Камешковскому району» (далее Оператор) для проведения классификации информационных систем персональных данных создается Комиссия.

Члены и председатель комиссии назначаются приказом директора учреждения.

Комиссия в своей работе руководствуется Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, Приказом ФСТЭК/ФСБ/МИТС от 13.02.2008 № 55/86/20.

2. Функции комиссии

Комиссия проводит анализ информационных систем персональных данных Оператора. На основании анализа Комиссия производит классификацию информационных систем персональных данных Оператора в соответствии с характеристиками, заданными нормативными документами. По результатам Комиссия оформляет акт классификации информационных систем.

3. Права и обязанности комиссии

3.1. Комиссия имеет право:

- получать необходимые для своей работы сведения;
- присваивать класс информационным системам персональных данных на основании полученных сведений и нормативных документов.

3.2. Комиссия обязана:

- собрать необходимый объем информации;
- проанализировать полученные данные;
- сделать заключение о классе информационной системы персональных данных;
- подготовить акт классификации информационных систем персональных данных.

4. Порядок работы комиссии

4.1. Комиссия назначается приказом директора учреждения.

4.2. Состав комиссии может быть изменен приказом директора учреждения.

4.3. Комиссия прекращает свою работу после проведения всех мероприятий по классификации информационных систем персональных данных.

Приложение № 15
к приказу директора
ГКУ ОСЗН
по Камешковскому району
от 17.05.2011 № 27

Список лиц, допущенных к обработке персональных данных работников

№ п/п	ФИО	Должность
1	2	3
1.	Авдеева Ирина Валерьевна	Специалист по кадрам
2.	Жунина Ирина Викторовна	Бухгалтер 2 категории сектора бухгалтерского учета и отчетности
3.	Ландышева Зоя Ивановна	Бухгалтер 1 категории сектора бухгалтерского учета и отчетности
4.	Писковой Валерий Николаевич	Администратор баз данных получателей мер социальной поддержки 1 категории
5.	Шаленная Татьяна Николаевна	Заведующая сектором бухгалтерского учета и отчетности
6.	Ширканова Людмила Ивановна	Заместитель директора учреждения

Приложение № 16
к приказу директора
ГКУ ОСЗН
по Камешковскому району
от 17.05.2011 № 27

Список работников, допущенных к обработке персональных данных получателей мер социальной поддержки

№ п/п	ФИО	Должность
1	2	3
1.	Агеева Людмила Алексеевна	Инспектор 2 категории по предоставлению мер социальной поддержки сектора по назначению и выплате пособий и компенсаций семьям с детьми
2.	Андреева Татьяна Евгеньевна	Инспектор 1 категории по предоставлению мер социальной поддержки сектора по назначению и выплате пособий и компенсаций семьям с детьми
3.	Булырева Галина Леонидовна	Инспектор 2 категории по предоставлению мер социальной поддержки сектора по предоставлению мер социальной поддержки отдельным категориям граждан
4.	Козлова Наталья Александровна	Инспектор 1 категории по предоставлению мер социальной поддержки сектора по назначению и выплате пособий и компенсаций семьям с детьми
5.	Кротова Ольга Вячеславовна	Инспектор 1 категории по предоставлению мер социальной поддержки сектора по предоставлению мер социальной поддержки отдельным категориям граждан
6.	Павлова Елена Евгеньевна	Старший инспектор по предоставлению мер социальной поддержки сектора по предоставлению мер социальной поддержки отдельным категориям граждан

1	2	3
7.	Панова Елена Владимировна	Заведующая сектором по предоставлению мер социальной поддержки отдельным категориям граждан
8.	Писковой Валерий Николаевич	Администратор баз данных получателей мер социальной поддержки 1 категории
9.	Рахова Екатерина Владимировна	Заведующая сектором по назначению и выплате пособий и компенсаций семьям с детьми
10.	Рокашевская Наталья Михайловна	Инспектор 1 категории по предоставлению мер социальной поддержки сектора по назначению и выплате пособий и компенсаций семьям с детьми
11.	Смирнова Марина Вячеславовна	Инспектор 1 категории по предоставлению мер социальной поддержки сектора по предоставлению мер социальной поддержки отдельным категориям граждан
12.	Ширканова Людмила Ивановна	Заместитель директора учреждения