ОБЛАСТНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«ЦЕНТР СОЦИАЛЬНОЙ ЗАЩИТЫ НАСЕЛЕНИЯ ПО ДАНКОВСКОМУ РАЙОНУ»

УТВЕРЖДАЮ

Директор ОБУ «ЦСЗН по Данковскому району»

_____ Т.Н. Ражева

«23» мая 2014 г.

ПОЛОЖЕНИЕ
ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2014

СОДЕРЖАНИЕ

1. Термины и определения

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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.

Конфиденциальность персональных данных – обязательное для соблюдения Оператором требование не допускать распространения персональных данных без согласия субъекта персональных данных или наличия иного законного основания.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

Оператор персональных данных (далее Оператор) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

Сотрудник (работник) – физическое лицо, состоящее в трудовых отношениях с Оператором.

Субъект – физическое лицо, обладатель собственных персональных данных.

2. Общие положения

Целью настоящего «Положения по обеспечению безопасности персональных данных» (далее Положение) является регламентация технологического и организационного процесса защиты персональных данных в Областном бюджетном учреждении «Центр социальной защиты населения по Данковскому району» (далее – ЦСЗН).

Положение разработано в соответствии с частью 1 статьи 23, статьи 24 Конституции Российской Федерации, главы 14 Трудового кодекса Российской Федерации «Защита персональных данных работников» от 30.12.2001 № 197-ФЗ, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

Настоящее Положение утверждается и вводится в действие приказом директора ЦСЗН и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

3. Принципы защиты персональных данных субъектов

В целях защиты персональных данных субъектов создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладение персональными данными. Целью и результатом несанкционированного доступа к персональным данным субъектов может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внедрение вредоносных программ, фальсификация содержания реквизитов документа и др.

Основным источником несанкционированного доступа к персональным данным является персонал, работающий с документами и базами данных.

Состав обрабатываемых персональных данных приведён в «Перечне персональных данных, обрабатываемых в Областном бюджетном учреждении «Центр социальной защиты населения по Данковскому району».

Посторонние лица не должны знать информацию о распределении функций, рабочих процессах, технологии составления, оформления, ведения и хранения документов, дел и рабочих материалов в информационных системах персональных данных. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Оператора, например посетители, работники других организационных структур.

Для обеспечения защиты персональных данных сотрудников необходимо соблюдать следующие организационно-технические меры:

– регламентация состава работников, функциональные обязанности которых требуют доступа к персональным данным, и процесса предоставления такого доступа;

– регламентация порядка приёма, учёта и контроля деятельности посетителей;

– поддержания порядка охраны зданий и помещений;

– периодический контроль обеспечения защищённости персональных данных субъектов;

– соблюдение требований к защите персональных данных субъектов при интервьюировании и собеседованиях.

В случаях обнаружения несоблюдения условий хранения носителей персональных данных и/или несоблюдения использования средств защиты информации, а так же в случае обнаружения нарушения порядка предоставления персональных данных, должно производиться разбирательство и составляться заключение по выявленным фактам.

4. Перечень мер по защите персональных данных при их автоматизированной обработке

Для обеспечения защиты персональных данных при их обработке в информационных системах должны приниматься следующие меры:

– определение угроз безопасности персональным данным при их обработке, формирование на их основе модели угроз;

– разработка на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

– проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

– установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

– обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

– учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

– учёт лиц, допущенных к работе с персональными данными в информационной системе;

– контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут

привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению защищённости персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

Требования по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных представлены в Приложении А к настоящему Положению.

Порядок доступа сотрудников ЦСЗН в помещения, в которых ведётся обработка персональных данных, представлен в Приложении Б к настоящему Положению.

5. Перечень мер по защите персональных данных, обрабатываемых без использования средств автоматизации

Для обеспечения защиты материальных носителей, содержащих персональные данные субъектов, Оператор обязан:

– Довести до сотрудников, осуществляющих обработку персональных данных субъектов на материальных носителях, информацию об особенностях и правилах осуществления такой обработки.

– Запретить вынос за пределы ЦСЗН носителей, содержащих персональные данные субъектов, за исключением случаев, установленных законодательством.

– Материальные носители персональных данных субъектов хранить в специально отведенных шкафах, сейфах или выделенных помещениях с ограниченным доступом, обеспечивающих защиту от несанкционированного доступа, а также в стеллажах, с возможностью контроля над каждым материальным носителем. Места хранения носителей определяются приказом директора ЦСЗН.

– Обеспечить учёт материальных носителей, содержащих персональные данные. Система учёта должна предоставлять возможность контроля над местонахождением каждого материального носителя.

– Организационно исключить необоснованное ознакомление с персональными данными лиц, не имеющих соответствующих полномочий.

– Обеспечить защиту от несанкционированного доступа и копирования персональных данных на материальных носителях, согласно организационным и распорядительным документам, принятым в ЦСЗН.

6. Контроль защищённости персональных данных субъектов

Необходимо производить периодический контроль выполнения организационно-технических мер, а также контроль защищённости информационных ресурсов, содержащих персональные данные.

Виды контроля состояния защищённости персональных данных субъектов, обрабатываемых ЦСЗН:

– предварительный контроль (оценочная проверка обоснованности мер защиты персональных данных до начала их обработки). Осуществляется с целью своевременного выявления и предотвращения предпосылок возможных нарушений требований или норм защиты персональных данных;

– текущий контроль (проверка в процессе обработки персональных данных). Осуществляется с целью своевременного выявления возникающих трудностей и недостатков реализации, принятых мер защиты персональных данных и выработки мероприятий по их устранению. Текущий контроль может быть периодическим, повседневным или непрерывным;

– контроль устранения недостатков (проверка, проводимая после устранения ранее допущенных нарушений норм и требований защиты персональных данных, вследствие которых были приостановлены или ограничены работы с защищаемыми персональными данными субъектов). Осуществляется с целью выдачи разрешения на продолжение обработки персональных данных субъектов;

– внутренний контроль. Проводится силами уполномоченных работников ЦСЗН;

– организационный контроль. Подразумевает проверку состояния полноты и обоснованности мероприятий, по защите защищаемых информационных ресурсов требованиям соответствующих руководящих и нормативных документов;

– контроль эффективности. Проводится с целью проверки соответствия количественных или качественных показателей эффективности мероприятий по защите персональных данных установленным требованиям или нормам эффективности защиты;

– технический контроль. Обеспечивает проверку эффективности защиты персональных данных с использованием технических и (или) программных средств контроля и в дальнейшем получение наиболее объективной и достоверной информации о состоянии объектов контроля.

7. Организационная структура и обязанности ответственных лиц

Приказом директора ЦСЗН назначается лицо, ответственное за обработку персональных данных (ответственное лицо), администратор информационной системы персональных данных (ИСПДн) и администратор безопасности ИСПДн, которые проводят мероприятия по защите

персональных данных субъектов. При необходимости дополнительно назначаются лица, ответственные за обработку персональных данных в структурных подразделениях.

Лицо, ответственное за организацию обработки персональных данных:

– осуществляет внутренний контроль над соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

– доводит до сведения работников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

– организует приём и обработку обращений и запросов субъектов персональных данных или их представителей и осуществляет контроль за приёмом и обработкой таких обращений и запросов.

Администратор ИСПДн отвечает за обеспечение работоспособности элементов ИСПДн и средств защиты персональных данных.

Администратор безопасности ИСПДн отвечает за обеспечение необходимого уровня состояния защиты ИСПДн, правильность настройки средств защиты, организацию выдачи, хранения и уничтожения материальных носителей персональных данных.

8. Обязанности Оператора и субъектов персональных данных

Оператор обязан использовать персональные данные только в соответствии с целями обработки, определившими их получение.

Сотрудники ЦСЗН обязаны не отвечать на запросы, связанные с передачей персональных данных, по телефону или факсу.

Для защиты персональных данных субъектов Оператор обязан:

– за свой счёт, в порядке, установленном законодательством РФ, обеспечить защиту персональных данных субъекта от неправомерного их использования или утраты;

– ознакомить сотрудника или его представителей с настоящим Положением под расписку;

– по запросу ознакомить субъекта персональных данных, не являющегося сотрудником, или в случае недееспособности либо несовершеннолетия субъекта, его законного представителя с настоящим Положением под расписку;

– осуществлять передачу персональных данных субъекта только в соответствии с настоящим Положением и законодательством Российской Федерации;

– предоставлять персональные данные субъекта только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей в соответствии с настоящим Положением и законодательством Российской Федерации;

– по требованию субъекта или его законного представителя предоставить ему полную информацию о его персональных данных и порядке обработки этих данных.

При обнаружении нарушений порядка предоставления персональных данных сотрудники ЦСЗН обязаны незамедлительно приостановить предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

Субъект персональных данных или его законный представитель обязуется предоставлять персональные данные, соответствующие действительности.

9. Права субъектов персональных данных

Субъекты персональных данных имеют право:

– На получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных федеральным законом;
- информацию об осуществлённой или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные федеральными законами.

– Получать доступ к своим персональным данным, включая право получать копии любой записи, содержащей собственные персональные данные, за исключением случаев, предусмотренных федеральным законом;

– Требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства;

– При отказе Оператора или уполномоченного им лица исключить или исправить персональные данные субъекта – заявить в письменной форме о своём несогласии, представив соответствующее обоснование;

– Требовать от Оператора уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведённых в них изменениях.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

– обработка персональных данных, включая персональные данные, полученные 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;

– обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма;

– доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

– обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

10.Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных сотрудника:

Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, содержащему персональные данные, несёт персональную ответственность за данное разрешение.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, материальную, административную, уголовную ответственность, предусмотренную действующим законодательством Российской Федерации.

Каждый сотрудник несёт единоличную ответственность за сохранность и конфиденциальность полученных в процессе работы персональных данных субъектов.

За неисполнение или ненадлежащее исполнение сотрудником возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера руководство Оператора вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечёт наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

ПРИЛОЖЕНИЕ А

Требования по обеспечению безопасности персональных данных при обработке в информационных системах персональных данных

Для технического обеспечения безопасности персональных данных при их обработке в ИСПДн в соответствии с установленными классами ИСПДн и актуальными угрозами безопасности, приведёнными в «Модели угроз персональным данным», для информационных систем персональных данных должно быть реализовано:

Класса К3 и К2 при однопользовательском режиме обработки:

В подсистеме управления доступом:

– идентификация и проверка подлинности пользователя при входе в систему информационной системы по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

В подсистеме регистрации и учёта:

– регистрация входа (выхода) пользователя в систему (из системы) либо регистрация 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;

– учёт всех защищаемых носителей информации с помощью их маркировки и занесение учётных данных в журнал учёта;

В подсистеме обеспечения целостности:

– 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 наличию имён (идентификаторов) компонентов системы защиты персональных данных, целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ;

– физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надёжных 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.

Класса К3 и К2 при многопользовательском режиме обработки персональных данных и равных правах доступа к ним пользователей:

В подсистеме управления доступом:

– идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

В подсистеме регистрации и учёта:

– регистрация входа (выхода) пользователя в систему (из системы) либо регистрация 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 неуспешная);

– учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета.

В подсистеме обеспечения целостности:

– 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 наличию имен (идентификаторов) компонентов системы защиты персональных данных, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;

– физическая охрана информационной системы (устройств 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.

Класса К3 и К2 при многопользовательском режиме обработки персональных данных и разных правах доступа к ним пользователей:

В подсистеме управления доступом:

– идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длинной не менее шести буквенно-цифровых символов.

В подсистеме регистрации и учёта:

– регистрация входа (выхода) пользователя в систему (из системы) либо регистрация 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 неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа;

– учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме).

В подсистеме обеспечения целостности:

– 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 информации, 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;

– физическая охрана информационной системы (устройств 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 компонент средств защиты информации, их периодическое обновление и контроль работоспособности.

Класса К1 при однопользовательском режиме обработки персональных данных:

В подсистеме управления доступом:

– идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

В подсистеме регистрации и учёта:

– регистрация входа (выхода) пользователя в систему (из системы) либо регистрация 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 неуспешная);

– регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), краткое содержание документа (наименование, вид, код), спецификация устройства выдачи (логическое имя (номер) внешнего устройства);

– учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета;

– дублирующий учет защищаемых носителей информации;

– очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних носителей информации.

В подсистеме обеспечения целостности:

– 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 наличию имен (идентификаторов) компонентов средств защиты информации, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ;

– физическая охрана технических средств информационных систем (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания;

– 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

Класса К1 при многопользовательском режиме обработки персональных данных и равных правах доступа к ним пользователей:

В подсистеме управления доступом:

– идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

– идентификация технических средств информационных систем и каналов связи, внешних устройств информационных систем по их логическим адресам (номерам);

– идентификация программ, томов, каталогов, файлов, записей, полей записей по именам.

В подсистеме регистрации и учёта:

– регистрация входа (выхода) пользователя в систему (из системы) либо регистрация 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 неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа;

– регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание документа (наименование, вид, шифр, код), идентификатор пользователя, запросившего документ;

– регистрация 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);

– регистрация попыток доступа программных средств (программ, процессов, задач, заданий) 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;

– регистрация 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 к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер));

– учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);

– дублирующий учет защищаемых носителей информации;

– очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационных систем и внешних носителей информации.

В подсистеме обеспечения целостности:

– обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по наличию имен (идентификаторов) ее компонент, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ;

– физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания;

– 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.

Класса К1 при многопользовательском режиме обработки персональных данных и разных правах доступа к ним пользователей:

В подсистеме управления доступом:

– идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

– идентификация терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам;

– идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

– контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа.

В подсистеме регистрации и учёта:

– регистрация входа (выхода) пользователей в систему (из системы), либо регистрация 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 неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке;

– регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание документа (наименование, вид, шифр, код), идентификатор пользователя, запросившего документ;

– регистрация 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);

– регистрация попыток доступа программных средств (программ, процессов, задач, заданий) 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;

– регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, ...шним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В

параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер));

– учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);

– очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних накопителей.

В подсистеме обеспечения целостности:

– обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по контрольным суммам компонентов системы 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 персональных данных;

– физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения 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.

Безопасное межсетевое взаимодействие для информационных систем К3 при их подключении к сетям международного информационного обмена (интернет) обеспечивается путем применения средств межсетевого экранирования (межсетевых экранов), которые обеспечивают:

– 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 кальных 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;

– регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и формационной части, процедуры восстановления.

Безопасное межсетевое взаимодействие для информационных систем К2 при их подключении к сетям международного информационного обмена (интернет) обеспечивается путем применения средств межсетевого экранирования (межсетевых экранов), которые обеспечивают:

– фильтрацию на сетевом уровне независимо для каждого сетевого пакета (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

– фильтрацию пакетов служебных протоколов, служащих для диагностики и управления ботой сетевых устройств;

– 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);

– 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);

– регистрацию запуска программ и процессов (заданий, задач);

– контроль целостности своей программной и информационной части;

– восстановление свойств межсетевого экрана после сбоев и отказов оборудования;

– регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

Безопасное межсетевое взаимодействие для информационных систем К1 при их подключении к сетям международного информационного обмена (интернет) обеспечивается путем применения средств межсетевого экранирования (межсетевых экранов), которые обеспечивают:

– 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);

– фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

– фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;

– фильтрацию с учетом любых значимых полей сетевых пакетов;

– 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 фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);

– регистрацию и учет запросов на установление виртуальных соединений;

– локальную сигнализацию попыток нарушения правил фильтрации;

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

– предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;

– идентификацию и аутентификацию администратора межсетевого экрана при его ленных запросах методами, устойчивыми к пассивному и активному перехвату информации;

– 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);

– регистрацию запуска программ и процессов (заданий, задач);

– регистрацию действия 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 информации;

– контроль целостности своей программной и информационной части;

– контроль целостности программной и информационной части межсетевого экрана по контрольным суммам;

– восстановление свойств межсетевого экрана после сбоев и отказов оборудования;

– регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

Реализованные методы и способы защиты информации должны обеспечивать нейтрализацию всех актуальных угроз безопасности из «Модели угроз персональным данным».

ПРИЛОЖЕНИЕ Б

Порядок доступа в помещения Областного бюджетного учреждения «Центр социальной защиты населения по Данковскому району», в которых ведётся обработка персональных данных

Доступ в помещения, в которых происходит обработка персональных данных, осуществляется в специально отведённые для этого часы. В другое время нахождение в помещении запрещается.

Сотрудникам ЦСЗН не разрешается при любом по продолжительности выходе из помещения оставлять какие-либо документы, содержащие персональные данные на рабочем столе или оставлять шкафы (сейфы), в которых хранятся такие документы, незапертыми.

Сотрудникам запрещено покидать помещения, в которых ведется обработка персональных данных, оставив там посторонних лиц. При отсутствии сотрудников в кабинете, дверь в помещение должна быть заперта.

В конце рабочего дня на рабочем столе не должно оставаться документов с персональными данными.

По завершению работы все материальные носители, содержащие персональные данные, должны быть помещены в специально выделенные места хранения. Места хранения материальных носителей персональных данных определяются приказом директора ЦСЗН.

Уборка помещений допускается только в присутствии ответственных сотрудников.