РЕСПУБЛИКА ТАТАРСТАН

Исполнительный комитет
Аксубаевского
муниципального района

ТАТАРСТАН РЕСПУБЛИКАСЫ

Аксубай муниципаль
районы башкарма
комитеты

ПОСТАНОВЛЕНИЕ **КАРАР**

28.06.2011 № 271

пгт.Аксубаево

Об утверждении Положения по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Исполнительного комитета Аксубаевского муниципального района

В соответствии с Законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России, ФСБ России, Мининформсвязи России № 55/86/20 от 13 февраля 2008 года и методическими рекомендациями ФСТЭК России в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн), Исполнительный комитет Аксубаевского муниципального района Республики Татарстан

ПОСТАНОВЛЯЕТ:

1. Утвердить Положение по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Исполнительного комитета Аксубаевского муниципального района Республики Татарстан.
2. Постановление Исполнительного комитета Аксубаевского муниципального района от 28.08.2009 № 198 «Об утверждении Положения о защите персональных данных работников Исполнительного комитета Аксубаевского муниципального района Республики Татарстан» считать утратившим силу.
3. Контроль за исполнением настоящего постановления оставляю за собой.

Руководитель
Исполнительного комитета Н.Н.Становов

Утверждено

постановлением Исполнительного
комитета Аксубаевского
муниципального района
Республики Татарстан

от 22.06.2011 № 271

ПОЛОЖЕНИЕ

по обеспечению безопасности ПДн при их обработке в ИСПДн

в Исполнительном комитете Аксубаевского муниципального района Республики Татарстан

1. Общие положения.

1.1. Данное «Положение по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Положение) разработано в соответствии с Законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России, ФСБ России, Мининформсвязи России № 55/86/20 от 13 февраля 2008 года и методическими рекомендациями ФСТЭК России в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.2. Положение определяет порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок проверки электронного журнала обращений к ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в защищаемые помещения.

2. Порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.1. Настоящий порядок определяет действия персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.2. Допуск пользователей для работы на персональной электронной вычислительной машине (далее – ПЭВМ) осуществляется на основании приказа,

руководителя учреждения/организации в соответствии со списком лиц допущенных к работе в ИСПДн.

2.3. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для записи и хранения информации, содержащей ПДн, разрешается использовать только учтенные носители информации.

2.4. Пользователь несет ответственность за правильность включения и выключения ПЭВМ, входа в систему и все действия при работе в ИСПДн.

2.5. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.

2.6. При работе со съемными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на ПЭВМ. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

2.7. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на ПЭВМ;
- хранить в тайне свой пароль (пароли). В соответствии с п.п. 8.5., 8.6. данного Положения и с установленной периодичностью менять свой пароль (пароли);
- хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);
- выполнять требования организации антивирусной защиты в полном объеме.

Немедленно известить администратора безопасности ИСПДн в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при их обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках ПЭВМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к данной защищенной ПЭВМ;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ПЭВМ, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на ПЭВМ технических средств защиты;
- непредусмотренных отводов кабелей и подключенных устройств.

Пользователю ПЭВМ категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения ПЭВМ;

- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);

- оставлять включенной без присмотра ПЭВМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

- размещать средства ИСПДн так, чтобы исключить возможность визуального считывания информации.

3. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации. Распределение ответственности субъектов обработки ПДн при работе в ИСПДн, их права и обязанности.

3.1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации.

3.2. К использованию, для создания резервной копии в ИСПДн, допускаются только зарегистрированные носители конфиденциальной информации.

3.3. Постоянный пользователь обязан осуществлять периодическое резервное копирование конфиденциальной информации.

3.4. Ежедневно, по окончанию работы с конфиденциальными документами (ПДн) на ПЭВМ, пользователь самостоятельно, при отсутствии администратора безопасности, обязан создавать резервную копию конфиденциальных документов на зарегистрированный носитель (ЖМД, ГМД, CD, DVD – диски, USB накопитель, другие), создавая тем самым резервный электронный архив конфиденциальных документов.

3.5. Носители информации (ЖМД, ГМД, CD-ROM, USB совместимое устройство, FLASH накопитель и другие), предназначенные для создания резервной копии и хранения конфиденциальной информации хранятся, учитываются и выдаются администратором безопасности ИСПДн. По окончании процедуры резервного копирования электронные носители конфиденциальной информации сдаются на хранение администратору безопасности ИСПДн.

3.6. Перед резервным копированием пользователь обязан проверить электронный носитель (ЖМД, ГМД, CD-ROM, USB совместимое устройство, FLASH накопитель) на отсутствие вирусов.

3.7. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль в соответствии с п. 7 настоящего Положения.

3.8. Запрещается запись посторонней информации на электронные носители (ЖМД, ГМД, CD-ROM, USB совместимое устройство, FLASH накопитель и другие) полученные у администратора безопасности ИСПДн исключительно для создания резервной копии.

3.9. Порядок создания резервной копии:

- вставить в ПЭВМ зарегистрированный электронный носитель (ЖМД, ГМД, CD-ROM, USB совместимое устройство, FLASH накопитель, другие) предназначенный для резервного копирования;

- выбрать необходимый каталог (файл) для создания резервного архива;

- нажать по выбранному каталогу (файлу) правой кнопкой манипулятора и в появившемся меню выбрать пункт «Добавить в архив…»;

- на вкладке «Общие» нажать на кнопку «Обзор» и в появившемся окне перейти на электронный носитель (ЖМД, ГМД, CD-ROM, USB совместимое устройство, FLASH накопитель, другие), после чего нажать кнопку «Открыть»;

- на вкладке «Общие» в поле «Имя архива» ввести имя архива следующего вида: «Имя каталога (файла) резервного копирования (Персонал). Дата архивирования в формате (ДДММГГ). Имя пользователя - к примеру (Петрова).
Пример – «Персонал 110509 Петрова. rar»;

- нажать кнопку «ОК».

3.10. Ответственность за проведение резервного копирования ПДн в ИСПДн в соответствии с требованиями настоящего Положения возлагается на пользователя.

3.11. Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных возлагается на штатного специалиста обслуживающего указанные выше средства в ИСПДн. Работы по обслуживанию выполняются только в присутствии администратора безопасности ИСПДн.

3.12. Ответственность за проведение мероприятий по восстановлению средств защиты информации (далее – СЗИ) возлагается на администратора безопасности ИСПДн.

3.13. Администратор безопасности ИСПДн обязан:

- знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;

- контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных ПЭВМ и других устройствах;

- производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом:

- реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

- вводить описания пользователей ИСПДн в информационную базу СЗИ от НСД;

- своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;

- контролировать доступ лиц в помещение в соответствии со списком сотрудников, допущенных к работе в ИСПДн;

- проводить инструктаж сотрудников - пользователей ПЭВМ по правилам работы с используемыми техническими средствами и системами защиты информации;

- контролировать своевременное (не реже чем один раз в течение 180 дней) проведение смены паролей для доступа пользователей к ПЭВМ;

- обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;

- осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;

- настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе на ПЭВМ;

- вводить в базу данных СЗИ от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале;

- проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам не реже одного раза в 10 дней;

- организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных

носителей информации. Сопровождать подсистемы обеспечения целостности информации на ПЭВМ в ИСПДн;

- периодически тестировать функции СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;

- восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;

- вести две копии программных средств СЗИ от НСД и контролировать их работоспособность;

- контролировать отсутствие на магнитных носителях остаточной информации по окончании работы пользователей;

- периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования:

- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;

- сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок (далее – ПЭМИН), контролировать соблюдение требований по размещению и использованию ПЭВМ;

- контролировать соответствие документально утвержденного состава аппаратной и программной части ИСПДн реальным конфигурациям ИСПДн, вести учет изменений аппаратно-программной конфигурации;

- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях с составлением соответствующего акта);

- присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;

- вести «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств ПЭВМ»;

- поддерживать установленный порядок проведения антивирусного контроля согласно требованиям настоящего Положения в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

- докладывать руководителю учреждения/организации о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

- вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

3.14. Администратор безопасности ИСПДн имеет право:

- требовать от сотрудников - пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения организационно распорядительных документов по обеспечению безопасности и защите информации в ИСПДн;

- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ОВТ;

- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

4. Порядок контроля ИСПДн, приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления. Порядок разбирательства и составления

заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий.

4.1. Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения техническими средствами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

4.2. Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в подразделениях учреждения/организации, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;
- выявление демаскирующих признаков объектов ИСПДн;
- уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;
- проверка выполнения требований по защите ИСПДн от несанкционированного доступа;
- проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;
- проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;
- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн учреждения/организации;
- разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

4.3. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей на объектах учреждения/организации и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации.

4.4. В ходе контроля проверяются:

- соответствие принятых мер по обеспечению безопасности персональных данных (далее – ОБ ПДн);
- своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ ПДн;
- полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- эффективность применения организационных и технических мероприятий по защите информации;
- устранение ранее выявленных недостатков.

Кроме того, проводятся необходимые измерения и расчеты, приглашенными для этих целей специалистами организации, выполняющей работы по аттестации ИСПДн в учреждении/организации.

4.5. Основными видами технического контроля на объектах, являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

4.6. Полученные в ходе ведения контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации администратор безопасности ИСПДн докладывает руководителю учреждения/организации, для принятия решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются в виде записей в соответствующих журналах.

4.7. Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее - предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию руководителя учреждения/организации/проводится расследование.

Для проведения расследования назначается комиссия с привлечением штатных сотрудников осуществляющих обслуживание баз данных, технических и программных средств, с обязательным участием администратора безопасности ИСПДн. Комиссия обязана установить, имела ли место утечка сведений и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования руководитель учреждения/организации принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

4.8. Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и внезапные проверки объектов организации проводятся, силами штатных сотрудников осуществляющих обслуживание баз данных, технических и программных средств с участием администратора безопасности ИСПДн в соответствии с утвержденным руководителем учреждения/организации планом или по предварительному с ним согласованию.

4.9. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год.

4.10. Обследование объектов информатизации и связи проводится с целью определения соответствия защищаемых помещений, основных и вспомогательных технических средств и систем требованиям по защите информации, установленным в техническом паспорте объекта или "Аттестате соответствия".

4.11. В ходе обследования проверяется:

- соответствие категории обследуемого объекта ИСПДн условиям, сложившимся на момент проверки;
- соблюдение организационно-режимных требований защищаемых помещений;
- сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;
- наличие электробытовой, радио и телевизионной аппаратуры и устройств непромышленного изготовления (пультов связи, устройств вызова и оповещения, усилителей, генераторов и других вспомогательных технических средств и систем), которые могут способствовать возникновению каналов утечки информации;

- выполнение требований предписаний на эксплуатацию на основные технические средства и системы по их размещению относительно вспомогательных технических средств и систем, организации электропитания и заземления;

- соответствие выполняемых на объекте ИСПДн мероприятий по защите информации данным, изложенным в техническом паспорте;

- выполнение требований по защите автоматизированных систем от несанкционированного доступа;

- выполнение требований по антивирусной защите.

4.12. Для выявления радиоэлектронных устройств и проводов неизвестного назначения, преднамеренного нарушения защитных свойств оборудования, а также не предусмотренных правилами эксплуатации отводов от оборудования и соединительных линий, проложенных в выделенных и защищаемых помещениях, а также других нарушений и способов возникновения каналов утечки информации необходимо:

- тщательно осмотреть мебель, сувениры, оборудование, установленное в этом помещении, осветительную аппаратуру, ниши отопительных батарей, шторы, оконные проемы и т.д.;

- вскрыть и осмотреть розетки, выключатели осветительной сети, люки вентиляции и каналы скрытой проводки;

- проверить качество установки стеклопакетов оконных приемов;

- провести аппаратурную проверку помещения на отсутствие возможно внедренных электронных устройств перехвата информации (при наличии соответствующей аппаратуры).

4.13. Периодический контроль состояния защиты информации осуществляется Федеральной службы по техническому и экспортному контролю России в соответствии с действующим законодательством Российской Федерации. Доступ представителя указанного федерального органа исполнительной власти на объекты для проведения проверки, а также к работам и документам в объеме, необходимом для осуществления контроля, обеспечивается в установленном порядке по предъявлении служебного удостоверения сотрудника, справки о допуске, а также предписания установленной формы на право проведения проверки.

5. Порядок обучения персонала практике работы в ИСПДн.

5.1. Обучение практике и методике в ИСПДн должно быть непрерывным, систематическим, разделенным по категориям, при этом наибольшее внимание следует уделять практике работы пользователя с ИСПДн.

5.2. Обучение по методике делятся на:

- совещания;
- обучающие занятия, семинары;
- инструктажи;
- методическая помощь и практические занятия на месте.

5.3. Совещания, обучающие занятия и семинары проводятся согласно плана учреждения/организации по организации защиты информации на год.

5.4. Инструктажи, методическая помощь и практические занятия по вопросам обеспечения безопасности ИСПДн должны проводиться в ходе плановых, периодических и внезапных проверок состояния обеспечения безопасности ИСПДн на местах.

5.6. Первичные инструктажи проводятся администратором безопасности ИСПДн с пользователями ИСПДн при поступлении сотрудника на работу в учреждение/организацию, где происходит обработка конфиденциальной информации в ИСПДн. Дополнительные инструктажи проводятся после проведения аттестационных испытаний ИСПДн, при получении Аттестата соответствия по требованиям безопасности ИСПДн.

5.7. Ответственным за организацию обучения и оказание методической помощи учреждении/организации является администратор безопасности ИСПДн.

5.8. Для проведения занятий, семинаров и совещаний могут привлекаться специалисты организаций лицензиатов, а также органов по аттестации объектов ИСПДн.

5.9. К работе в ИСПДн допускаются только сотрудники прошедшие первичный инструктаж обеспечения безопасности в ИСПДн и показавшие твердые теоретические знания и практические навыки, о чём делается соответствующая запись в матрице доступа к ИСПДн.[1].

6. Порядок проверки электронного журнала обращений к ИСПДн.

6.1. Настоящий раздел Положения определяет порядок проверки электронного журнала обращений к ИСПДн.

6.2. Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к конфиденциальной информации в ИСПДн.

6.3. Право проверки электронного журнала обращений имеют:

- руководитель учреждения/организации;
- администратор безопасности ИСПДн.

6.4. В ИСПДн, где установлены средства защиты информации (далее – СЗИ), проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ Руководством.

6.5. В ИСПДн, где защита от несанкционированного доступа (далее - НСД) реализована организационно-распорядительными мероприятиями, проверка электронного журнала обращений проводится внутренними средствами операционной системы по следующему пути C:\Documents and Settings\ UserAccount \Recent, при этом рекомендуется в настройках данного каталога изменить настройки «Доступ» и «Безопасность» только в пользу Администратора ПЭВМ для разграничения прав доступа.

6.6. Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлены случай НСД к информации конфиденциального характера то вступает в силу п.п. 4.7., 4.8. данного Положения.

7. Правила антивирусной защиты.

7.1. Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного ПО, вирусов и устанавливает ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих ПЭВМ ОВТ, за их выполнение. Настоящие правила распространяются на все объекты ИСПДн учреждений/организаций.

7.2. К использованию на ПЭВМ ОВТ допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств, сертифицированные ФСТЭК России.

7.3. Установка и начальная настройка средств антивирусного контроля на ПЭВМ ОВТ осуществляется представителем разработчика (поставщика) в присутствии администратора безопасности ИСПДн.

7.4. Администратор безопасности осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

7.5. Ярлык для запуска антивирусной программы должен быть вынесен в окно «Рабочий стол» операционной системы.

7.6. Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов ПЭВМ.

7.7. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

7.8. Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

7.9. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором безопасности должна быть выполнена антивирусная проверка ИСПДн.

7.10. На ПЭВМ запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

7.11. 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 самостоятельно (или вместе с администратором безопасности ИСПДн) должен провести внеочередной антивирусный контроль своей ПЭВМ.

7.12. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить обработку данных в ИСПДн;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, владельца зараженных файлов, а также смежные подразделения/организации, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

7.11. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на руководителя учреждения/организации.

7.12. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн возлагается на администратора безопасности и всех пользователей данной ИСПДн.

8. Правила парольной защиты.

8.1. Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями.

8.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на администратора безопасности.

8.3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ОВТ самостоятельно с учетом следующих требований:

- пароль должен быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);

- символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

- при смене пароля новое значение должно отличаться от предыдущего;

- пользователь не имеет права сообщать личный пароль другим лицам.

8.4. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

8.5. В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей сотрудников (исполнителей) в их отсутствие, сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение руководителю структурного подразделения. Запечатанные конверты (пеналы) с паролями исполнителей должны храниться в недоступном месте у руководителя структурного подразделения.

8.6. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 180 дней.

8.7. Внеплановая смена личного пароля или удаление учетной записи пользователя ОВТ в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться администратором безопасности (либо новым постоянным пользователем) немедленно после окончания последнего сеанса работы данного пользователя с системой на основании указания руководителя подразделения.

8.8. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора безопасности.

8.9. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты соответствующие меры по восстановлению парольной защиты.

8.10. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на руководителя структурного подразделения и администратора безопасности ИСПДн.

9. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн.

9.1. Настоящие правила регламентируют обеспечению безопасности информации при проведении обновлении, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

9.2. Все изменения конфигураций технических и программных средств ПЭВМ должны производиться только на основании заявок согласованных с администратором безопасности ИСПДн.

9.3. Право внесения изменений в конфигурацию аппаратно-программных средств защищенных ПЭВМ предоставляется:

- в отношении системных и прикладных программных средств – администратору безопасности по согласованию с организацией выполняющей работы по аттестации;

- в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты – уполномоченными сотрудниками организации выполняющей работы по аттестации ИСПДн.

9.4. Изменение конфигурации аппаратно-программных средств ПЭВМ кем-либо, кроме вышеперечисленных уполномоченных сотрудников и подразделений, запрещено.

9.5. Процедура внесения изменений в конфигурацию системных и прикладных программных средств ПЭВМ инициируется заявкой ответственного за эксплуатацию ИСПДн. Форма заявки приведена ниже.

9.6. В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ПЭВМ подразделения:

- установка (развертывание) на ПЭВМ программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн;
- обновление (замена) на ПЭВМ программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);
- удаление с ПЭВМ программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данной ПЭВМ).

9.7. Также в заявке указывается условное наименование ИСПДн. Наименования задач указываются в соответствии с перечнем задач архива дистрибутивов установленного программного обеспечения, которые можно решать с использованием указанной ПЭВМ.

9.8. Заявку ответственного за эксплуатацию ИСПДн, в которой требуется произвести изменения конфигурации, рассматривает руководитель учреждения/организации, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений. После чего заявка передается администратору безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию ПЭВМ указанного в заявке ИСПДн.

9.9. Подготовка обновления, модификации общесистемного и прикладного программного обеспечения ИСПДн тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на ПЭВМ, (обновление) и удаление системных и прикладных программных средств производится уполномоченными специалистами организации выполняющей работы по аттестации. Работы производятся в присутствии администратора безопасности данной ИСПДн.

9.10. Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

9.11. Установка и обновление ПО (системного, тестового и т.п.) на ПЭВМ производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком, прикладного ПО – с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

9.12. Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

9.13. После установки (обновления) ПО, администратор безопасности должен произвести требуемые настройки средств управления доступом к компонентам ПЭВМ и проверить работоспособность ПО и правильность их настройки и произвести соответствующую запись в Приложении 1 к данному Положению «Журнале учета нештатных ситуаций ПЭВМ, выполнения профилактических работ, установки и модификации программных средств ПЭВМ», делает отметку о выполнении (на обратной стороне заявки) и в «Техническом паспорте » (Приложение 3).

9.14. Формат записей «Журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств ПЭВМ»:

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО исполнителей и их подписи	ФИО ответственного за эксплуатацию ПЭВМ, подпись	Подпись администатора безопасности ИСПДн	Примечание (ссылка на заявку)
1	2	3	4	5	6	7

9.15. При возникновении ситуаций, требующих передачи ПЭВМ в ремонт, ответственный за ее эксплуатацию докладывает об этом администратору безопасности ИСПДн, который в свою очередь связывается с сотрудниками организации выполняющей работы по аттестации и в дальнейшем действует согласно их инструкций. В данном случае администратор безопасности обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств ПЭВМ с отметками о внесении изменений в состав программных средств, должны храниться вместе с техническим паспортом на ИСПДн и «Журналом учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств ПЭВМ» у руководителя подразделения в котором эксплуатируется данная ИСПДн.

9.16. Копии заявок должны храниться у администратора безопасности ИСПДн и впоследствии используются:

- для восстановления конфигурации ИСПДн после аварий;
- для контроля правомерности установки на ИСПДн средств для решения соответствующих задач при разборе конфликтных ситуаций;
- для проверки правильности установки и настройки средств защиты ПЭВМ

9.17. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора безопасности и сотрудника ответственного за эксплуатацию данной ИСПДн.

9.18. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на ПЭВМ конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать на данной ПЭВМ.

9.19. Использование несколькими сотрудниками при работе на ПЭВМ одного и того же имени пользователя («группового имени») запрещено.

9.20. Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой ответственного за эксплуатацию данной ИСПДн (Приложение 2).

В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя ПЭВМ, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ПЭВМ ранее зарегистрированного пользователя);
- должность (с полным наименованием отдела), фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

9.21. Заявку рассматривают руководитель учреждения/организации и руководитель структурного подразделения визируя её, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника

к необходимым для решения им указанных в заявке задач ресурсам ИСПДн. Затем руководитель учреждения/организации подписывает задание администратору безопасности на внесение необходимых изменений в списки пользователей соответствующих подсистем ИСПДн.

9.22. На основании задания, в соответствии с документацией на средства защиты от несанкционированного доступа, администратор безопасности производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля (возможно также регистрацию персонального идентификатора __identificator), заявленных прав доступа к ресурсам ИСПДн и другие необходимые действия, указанные в задании. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в течение 180 дней.

9.23. После внесения изменений в списки пользователей администратор безопасности должен обеспечить настройки средств защиты соответствующие категории защиты указанной ИСПДн. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания (оборотная сторона Приложения 2) за подписью исполнителя – администратор безопасности.

9.24. Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор __identificator (для работы в режиме усиленной аутентификации) и начальное (-ые) значение (-ия) пароля (-ей), которое (-ые) он обязан сменить при первом же входе в систему ПЭВМ.

9.25. Исполненные заявка и задание (за подписью администратора безопасности) передаются на хранение руководителю подразделения, в котором производится эксплуатация подсистем ИСПДн.

Они могут впоследствии использоваться:

- для восстановления полномочий пользователей после аварий ПЭВМ;
- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;
- для проверки сотрудниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.

10. Порядок контроля соблюдения условий использования средств защиты информации.

10.1. Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации (далее - СЗИ).

10.2. Технические средства защиты информации являются важным компонентом обеспечения безопасности ПДн.

10.3. Порядок работы с техническими СЗИ определен в соответствующих Инструкциях к СЗИ, в Руководстве по настройке и использованию СЗИ, обязательных для исполнения, как сотрудниками обрабатывающими конфиденциальную информацию, так и администратором безопасности ИСПДн.

10.4. Право проверки соблюдения условий использования средств защиты информации имеют:

- руководитель учреждения/организации;
- администратор безопасности ИСПДн.

10.5. Пользователю ИСПДн категорически запрещается:

- обработка конфиденциальной информации с отключенными СЗИ;
- менять настройки СЗИ, местоположение – для генератора шума.

10.6. Администратору безопасности запрещается менять настройки программно-аппаратных СЗИ предустановленные сотрудником организации выполняющей работы по

аттестации в ходе настройки системы обеспечения безопасности ПДн при аттестации ИСПДн.

10.7. Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлено нарушение требования п. 10.5. то вступает в силу п.п. 4.7., 4.8. данного Положения.

11. Порядок охраны и допуска посторонних лиц в защищаемые помещения.

11.1. Настоящее Положение устанавливает порядок охраны (сдачи под охрану) защищаемых помещений ИСПДн.

11.2. Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях.

Список сотрудников, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения утверждается руководителем учреждения/организации и передаётся на пост охраны.

11.3. При отсутствии сотрудников, ответственных за вскрытие (сдачу под охрану) помещений, данные помещения могут быть вскрыты комиссией, созданной на основании приказа, о чем составляется акт.

11.4. При закрытии помещений и сдачей их под охрану сотрудники, ответственные за помещения проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации на которых содержится конфиденциальная информация сдаются руководителю структурного подразделения (управления) для хранения в опечатываемом сейфе (металлическом шкафу).

11.5. Помещение сдается под охрану следующим образом:

- опечатывается помещение и пенал с ключами;
- получается подтверждение от охранника о включение сигнализации и постановке помещения под охранную сигнализацию;
- факт опечатывания помещения подтверждается охранником;
- сдается помещение и опечатанный пенал с ключами, под роспись с указанием даты и времени сдачи под охрану.

11.6. Сотрудник, имеющий право на вскрытие помещений:

- получает на посту охраны пенал с ключами от помещения под роспись в Журнале с указанием даты и времени;
- проверяет целостность оттиска печати на пенале;
- производит запись о вскрытии помещения с указанием фамилии и времени;
- производит проверку оттиска печати на двери помещения и исправность запоров;
- вскрывает помещение.

11.7. При обнаружении нарушений целостности оттисков печатей, повреждения запоров или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается руководителю учреждения/организации и администратору безопасности ИСПДн.

Одновременно принимаются меры по охране места происшествия и до прибытия руководителя структурного подразделения и администратора безопасности ИСПДн в помещение никто не допускается.

11.8. Руководитель структурного подразделения и администратор безопасности ИСПДн организуют проверку АРМ, ИСПДн на предмет несанкционированного доступа к конфиденциальной информации и наличие документов и машинных носителей информации о чём докладывается непосредственно руководителю учреждения/организации.

11.9. В соответствии с требованиями данного Положения при обработке конфиденциальной информации в ИСПДн необходимо исключить возможность неконтролируемого пребывания посторонних лиц в пределах границ контролируемой зоны ИСПДн определенные Техническим паспортом ограждающими конструкциями и межэтажными перекрытиями.

12. Заключительные положения.

12.1. Требования настоящего Положения обязательны для всех сотрудников обрабатывающих конфиденциальную информацию в ИСПДн.

12.2. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Управляющий делами
Исполнительного комитета И.И.Ислямов

ОБЩИЙ ОТДЕЛ