Приложение 1 к приказу

МБДОУ детского сада № 7 «Белоснежка»

от 25.05.2023г № 51

ПОЛОЖЕНИЕ

об организации и проведении работ по обеспечению безопасности конфиденциальной информации при их автоматизированной обработке в информационных системах

Термины, определения, сокращения

Администратор защиты (безопасности) информации – лицо, ответственное за защиту АС от несанкционированного доступа к информации;

АП – Абонентский пункт - автоматизированная система, подключаемая к Сети с помощью коммуникационного оборудования и предназначенная для работы абонента Сети;

АРМ – Автоматизированное рабочее место - программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида;

ВТСС – Вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях;

Информационные сети общего пользования – вычислительные (информационно-телекоммуникационные) сети, открытые для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано;

ИС – Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

КИ – Конфиденциальная информация - информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну;

ЛВС – Локальная вычислительная сеть - совокупность основных технических средств и систем, осуществляющих обмен информацией между собой и с другими информационными системами, в том числе с ЛВС, через определенные точки входа/выхода информации, которые являются границей ЛВС;

МЭ – Межсетевой экран - это локальное (однокомпонентное) или функционально распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную (информационную) систему и (или) выходящей из неё;

НГМД – портативный сменный носитель информации, используемый для многократной записи и хранения данных. Представляет собой помещённый в защитный пластиковый корпус диск, покрытый ферромагнитным слоем;

НЖМД – запоминающее устройство (устройство хранения информации) произвольного доступа, основанное на принципе магнитной записи;

НСД – Несанкционированный доступ - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых СВТ или автоматизированной (информационной) системы;

Обработка информации - совокупность операций сбора, накопления, ввода-вывода, приема-передачи, записи, хранения, регистрации, уничтожения, преобразования и отображения, осуществляемых над информацией;

Оптический диск – собирательное название для носителей информации, выполненных в виде дисков, чтение с которых ведётся с помощью оптического излучения;

ОТСС – Основные технические средства и системы - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации;

ПО – Программное обеспечение - совокупность программ на носителях данных и программных документов, предназначенных для отладки, функционирования и проверки работоспособности автоматизированной (информационной) системы;

СЗИ от НСД – Система защиты информации от НСД - комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации (несанкционированных действий с ней) в автоматизированной (информационной) системе;

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

Флеш-накопитель – запоминающее устройство, использующее в качестве носителя электрически стираемую перепрограммируемую энергонезависимую память и подключаемое к компьютеру

ФСТЭК России – Федеральная служба по техническому и экспортному контролю Российской Федерации;

ФСБ России – Федеральная служба безопасности Российской Федерации.

1. Общие положения

1.1. Положение «Об организации и проведении работ по обеспечению безопасности конфиденциальной информации при их автоматизированной обработке в информационных системах» МБДОУ детского сада № 7 «Белоснежка» (далее – Положение) разработано в целях обеспечения безопасности конфиденциальной информации при их обработке в информационных системах МБДОУ детского сада № 7 «Белоснежка».

1.2. Положение определяет порядок работы персонала в части обеспечения безопасности КИ при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей с КИ, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления КИ в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в информационных системах, порядок проверки электронного журнала обращений к информационным системам, 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, порядок охраны и допуска посторонних лиц в защищаемые помещения.

1.3. При обеспечении безопасности КИ в информационных системах с использованием криптографических средств защиты информации все сотрудники МБДОУ детского сада № 7 «Белоснежка»обязаны выполнять требования, изложенные в документах «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСБ России, 21.02.2008 № 149/6/6-622) и «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (ФСБ России, 10.07.2014 № 378).

2. Порядок работы персонала в части обеспечения безопасности КИ при их обработке в ИС.

2.1. Настоящий порядок определяет действия персонала в части обеспечения безопасности КИ при их обработке в ИС.

2.2. Допуск пользователей для работы на компьютерах осуществляется на основании приказа, который издается директором МБДОУ детского сада № 7 «Белоснежка» (далее руководитель), и в соответствии со списком лиц, допущенных к работе в ИС. С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в ИС руководителем назначается администратор безопасности; с целью контроля выполнения необходимых мероприятий по обеспечению безопасности ответственный за защиту информации;

2.3. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИС. Полномочия пользователей к информационным ресурсам определяются в матрице доступа, утверждаемой руководителем организации. При этом для хранения информации, содержащей КИ, разрешается использовать только машинные носители информации, учтенные в Журнале учета машинных носителей.

2.4. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники, входа в систему и все действия при работе в ИС.

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

2.6. Запись информации, содержащей КИ, может, осуществляется пользователем на съемные машинные носители информации, соответствующим образом учтенные в Журнале учета машинных носителей.

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

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

– строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС;

– знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИС;

– хранить в тайне свой пароль (пароли). В соответствии с требованиями 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 правила антивирусной защиты в полном объеме;

– немедленно известить ответственного за защиту информации и (или) администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

а) нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках СВТ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к данным защищаемым СВТ;

б) несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИС;

в) отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;

г) некорректного функционирования установленных на компьютеры технических средств защиты;

д) непредусмотренных отводов кабелей и подключенных устройств.

2.9. Пользователю категорически запрещается:

– использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;

– самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИС или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

– осуществлять обработку КИ 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 включенным без присмотра компьютер, 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 ИС так, чтобы с них существовала возможность визуального считывания информации.

2.9. Администратор безопасности (а при его отсутствии – ответственный за защиту информации) обязан:

– знать состав основных и вспомогательных технических систем и средств установленных и смонтированных в ИС, перечень используемого программного обеспечения в ИС;

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

– производить необходимые настройки подсистемы управления доступом установленных в ИС 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 ИС 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 ИС;

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

– контролировать своевременное (не реже чем один раз в течение 360 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИС;

– обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИС;

– 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 в ИС;

– 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 в ИС;

– 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 ИС и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;

– сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок, контролировать соблюдение требований по размещению и использованию технических средств ИС;

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

– обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИС 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 ИС;

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

– поддерживать установленный порядок проведения антивирусного контроля согласно требований настоящего Положений в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

– докладывать ответственному за защиту информации, ответственному за эксплуатацию ИС о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

– вести документацию на ИС в соответствии с требованиями нормативных документов.

2.10. Администратор безопасности и ответственный за защиту информации имеют право:

– требовать от сотрудников - пользователей ИС соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ИС;

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

– 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.

3. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации.

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 ИС, допускаются только зарегистрированные в журнале учета носители.

3.3. Администратор безопасности обязан осуществлять периодическое резервное копирование конфиденциальной информации.

3.4. Еженедельно, по окончанию работы с конфиденциальными документами на компьютере, пользователь, при отсутствии администратора, обязан создавать резервную копию конфиденциальных документов на зарегистрированный носитель (НЖМД, НГМД, оптические диски, флеш-накопитель, другие), создавая тем самым резервный электронный архив конфиденциальных документов.

3.5. Носители информации (НЖМД, НГМД, оптические диски, флеш-накопитель), предназначенные для создания резервной копии и хранения конфиденциальной информации выдаются установленным порядком руководителем, ответственным за защиту информации и (или) администратором. По окончании процедуры резервного копирования электронные носители конфиденциальной информации сдаются на хранение администратору безопасности, или руководителю, или ответственному за защиту информации.

3.6. Перед резервным копированием пользователь или администратор безопасности обязан проверить электронный носитель (НЖМД, НГМД, оптические диски, флеш-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 (НЖМД, НГМД, оптические диски, флеш-накопитель) резервной копии.

3.9. Порядок создания резервной копии:

– вставить в компьютер зарегистрированный электронный носитель (НЖМД, НГМД, оптические диски, флеш-накопитель) для резервного копирования;

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

– при использовании систем управления базами данных необходимо создать файл с резервной копией защищаемой информации с помощью встроенных средств системы;

– выполнить процедуру создания резервной копии;

– произвести копирование на отчуждаемый носитель;

– произвести отключение отчуждаемого носителя и, создав необходимые записи в журналах убрать носитель в хранилище.

3.10. Хранение отчуждаемого носителя с резервной копией защищаемой информации осуществляется в специальном металлическом хранилище совместно с ключевой и аутентифицирующей информацией.

3.11. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

3.12. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором безопасности в специальном хранилище.

3.13. При необходимости ремонта технических средств, с них удаляются опечатывающие пломбы, изымаются носители конфиденциальной информации и по согласованию с администратором безопасности, ответственным за защиту информации и представителем организации, проводившей аттестацию, оборудование передается в сервисный центр производителя. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с порядком уничтожения носителей защищаемой информации. Работа с использованием неисправных технических средств запрещается.

3.14. При работе на компьютерах ИС рекомендуется использовать источники бесперебойного питания, с целью предотвращения повреждения технических средств и (или) защищаемой информации в результате сбоев в сети электропитания.

3.15. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты конфиденциальных данных. Оценку эффективности данных средств защиты должен выполнять сотрудник организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

3.16. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

3.17. Ответственность за проведение резервного копирования в ИС в соответствии с требованиями настоящего Положения возлагается на администратора безопасности.

3.18. Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных возлагается на администратора безопасности.

3.19. Ответственность за проведение мероприятий по восстановлению средств защиты информации возлагается администратора безопасности.

4. Порядок контроля защиты информации в ИС и приостановки предоставления КИ в случае обнаружения нарушений порядка их предоставления. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей конфиденциальных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий.

4.1. Контроль защиты информации в ИС - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами 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 характеристик безопасности информации или работоспособности систем информатизации.

4.2. Основными задачами контроля являются:

– проверка организации выполнения мероприятий по защите информации в подразделениях организации, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

– выявление демаскирующих признаков объектов ИС;

– 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 ИС 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 ИС;

– 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 в ИС организации, осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации. Перечень каналов утечки устанавливается в соответствии с моделью угроз.

4.4. В ходе контроля проверяются:

– соответствие принятых мер по обеспечению безопасности конфиденциальной информации (далее – ОБ КИ);

– своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ КИ;

– 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, могут проводиться необходимые измерения и расчеты, приглашенными для этих целей специалистами организации, имеющей соответствующие лицензии ФСТЭК России.

4.5. Основными видами технического контроля 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 докладывает руководителю для принятия ими решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются актами либо в соответствующих журналах учета результатов контроля.

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

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию руководителя или ответственного за защиту информации проводится расследование.

Для проведения расследования назначается комиссия с привлечением администратора безопасности. 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 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, как правило, силами администратора

безопасности и (или) ответственного за защиту информации, в соответствии с утвержденным планом или по согласованию с руководителем.

4.9. Одной из форм контроля защиты информации является обследование объектов ИС. Оно проводится не реже одного раза в год рабочей группой в составе администратора безопасности, ответственного за защиту информации, ответственного за эксплуатацию объекта. Для обследования ИС может привлекаться организация, имеющая лицензию ФСТЭК России на деятельность по технической защите информации.

4.10. Обследование ИС проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите информации, установленным в «Аттестате соответствия» требованиям по безопасности информации.

4.11. В ходе обследования проверяется:

– соответствие текущих условий функционирования обследуемого объекта условиям, сложившимся на момент проверки;

– соблюдение организационно-технических требований помещений, в которых располагается ИС;

– 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;

– соответствие выполняемых на объекте мероприятий по защите информации данным, изложенным в настоящем положении;

– выполнение требований по защите информационных 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 (особенно иностранного производства), 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 проемов;

– провести аппаратурную проверку помещения на отсутствие возможно внедренных электронных устройств перехвата информации (при наличии соответствующей аппаратуры), при необходимости для проведения данных видов работ могут привлекаться организации, имеющие соответствующие лицензии ФСБ России.

4.13. Государственный контроль состояния защиты информации осуществляется Федеральной службы по техническому и экспортному контролю России и Федеральной службой безопасности России в рамках их полномочий в соответствии с действующим законодательством Российской Федерации. Доступ представителей указанных федеральных органов 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, а также документа установленной формы на право проведения проверки.

5. Порядок обучения персонала практике работы в ИС в части обеспечения безопасности конфиденциальной информации

5.1. Перед началом работы в ИС пользователи должны ознакомиться с инструкциями по использованию программных и технических средств, по использованию средств защиты информации под роспись.

5.2. Пользователи должны продемонстрировать администратору безопасности и(или) ответственному за защиту информации наличие необходимых знаний и умений для выполнения требований настоящего Положения. Администратор безопасности должен вести журнал учета проверок знаний и навыков пользователей.

5.3. Пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности конфиденциальной информации в соответствии с требованиями настоящего положения, к работе в ИС не допускаются.

5.4. Ответственным за организацию обучения и оказание методической помощи в управлении ветеринарии Тамбовской области является администратор безопасности.

Администратор должен организовывать совещательные мероприятия и инструктажи, направленные на:

– разъяснение сотрудникам требований организационно-распорядительной документации и правил работы в ИС;

– повышение уровня их квалификации в области информационной безопасности и применения штатных средств защиты информации;

– разъяснение порядка использования съёмных носителей информации.

Инструктажи должны проводиться периодически (не реже одного раза в три месяца), а так же при возникновении нештатных ситуаций.

5.5. Для проведения занятий, семинаров и совещаний могут привлекаться специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов информатизации, организаций-лицензиатов ФСТЭК России и ФСБ России.

5.6. К работе в ИС допускаются только сотрудники прошедшие первичный инструктаж ОБ в ИС и показавшие твердые теоретические знания и практические навыки, о чём делается соответствующая запись в Журнале учёта допуска к работе в ИС.

5.7. Администратор безопасности должен иметь профильное образование (либо дипломы о повышении квалификации) в области защиты информации. Рекомендуется прохождение администратором специализированных курсов по администрированию средств защиты информации, используемых в ИС.

6. Порядок проверки электронного журнала обращений к ИС.

6.1. Настоящий раздел Положения определяет порядок проверки электронных журналов обращений к ресурсам ИС.

6.2. Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к защищаемой информации в ИС.

6.3. Право проверки электронного журнала обращений имеют:

– администратор безопасности;

– ответственный за защиту информации;

– руководитель.

6.4. На технических средствах ИС, на которых установлены специализированные средства защиты информации типа «Страж», «Secret Net», «Dallas Lock» и другие, проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ Руководством.

6.5. Если в ходе периодических, плановых или внезапных проверок ИС выявлены случаи НСД к информации конфиденциального характера, то вступает в силу п.п. 3.7., 3.8. данного Положения.

6.6. Проверке подлежат все электронные журналы ИС.

6.7. Проверка должна проводиться не реже, чем один раз в неделю с целью своевременного выявления фактов нарушения требований настоящего Положения.

6.8. Факты проверок электронных журналов отражаются в специальном журнале проверок. После каждой проверки Администратор безопасности делает соответствующую отметку в журнале и ставит свою подпись.

7. Правила антивирусной защиты

7.1. Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного программного обеспечения, компьютерных вирусов и устанавливает ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих компьютеры в составе ИС, за их выполнение. Настоящие правила распространяются на все объекты ИС организации.

7.2. К использованию на компьютерах допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

7.3. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором безопасности.

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

7.5. Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы.

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

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

Настройки средств антивирусной защиты должны быть выполнены в соответствии с требованиями безопасности конфиденциальной информации определенной для данного класса. Настройку средств антивирусной защиты выполняет администратор безопасности.

7.7. 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.

7.8. 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 ИС.

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

7.10. 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) должен провести внеочередной антивирусный контроль компьютера.

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

– приостановить обработку данных в ИС;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, а также смежные подразделения, 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 ИС в соответствии с требованиями настоящего Положения возлагается на ответственного за защиту информации.

7.12. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИС и соблюдение требований настоящего Положения возлагается на администратора безопасности и всех пользователей данной ИС.

8. Правила парольной защиты.

8.1. Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИС, 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 ИС 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 предыдущих;

– пользователь не имеет права сообщать личный пароль другим лицам.

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

8.4. 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.

8.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 360 дней.

8.6. Внеплановая смена личного пароля или удаление учетной записи пользователя ИС 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 структурного подразделения.

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

8.8. В случае компрометации личного пароля пользователя ИС должны быть немедленно предприняты меры по восстановлению парольной защиты.

8.9. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора безопасности.

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

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

9.2. Все изменения конфигураций технических и программных средств ИС должны производиться только на основании заявок ответственного за эксплуатацию конкретного ИС.

Перед проведением работ по внесению изменений в состав технических и программных средств ИС необходимо согласовать возможность данных изменений с органом, производившим работы по аттестации. При возможности осуществления подобных изменений представители органа по аттестации осуществляют надзор за всеми проводимыми работами. Проведение работ по изменению состава технических и программных средств ИС без согласования с органом по аттестации автоматически прекращает действие выданного Аттестата.

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

- в отношении системных и прикладных программных средств – администратору безопасности по согласованию с органом по аттестации, проводившим аттестацию данной ИС;

- в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты – администратору безопасности по согласованию с органом по аттестации, проводившим аттестацию данной ИС.

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

9.5. Процедура внесения изменений в конфигурацию системных и прикладных программных средств ИС инициируется заявкой ответственного за эксплуатацию ИС.

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

– установка (развертывание) на компьютер(ы) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИС;

– обновление (замена) на компьютере(ах) программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);

– удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

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

9.8. Заявку ответственного за эксплуатацию ИС, в которой требуется произвести изменения конфигурации, рассматривает руководитель, 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 компьютера указанного в заявке ИС.

9.9. Подготовка обновления, модификации общесистемного и прикладного программного обеспечения ИС 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 компьютерах, (обновление) и удаление системных и прикладных программных средств производится администратором безопасности по согласованию с органом по аттестации, проводившим аттестацию данной ИС. Работы производятся в присутствии ответственного за эксплуатацию данной ИС.

9.10. Установка или обновление подсистем ИС 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 компьютерах 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 компьютера и проверить работоспособность ПО и правильность их настройки и произвести соответствующую запись в Журнале учета нештатных ситуаций в ИС, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИС, делает отметку о выполнении (на обратной стороне заявки) и в Техническом паспорте.

9.14. Формат записей Журнала учета нештатных ситуаций ИС, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИС устанавливается приказом руководителя Организации.

9.15. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за ее эксплуатацию докладывает об этом ответственному за защиту информации, который в свою очередь связывается с сотрудниками органа 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 компьютеров с отметками о внесении изменений в состав программных средств, должны храниться вместе с техническим паспортом на ИС и Журналом учета нештатных ситуаций ИС, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИС у ответственного за защиту информации.

9.16. Копии заявок могут храниться у администратора безопасности:

– для восстановления конфигурации ИС после аварий;

– для контроля правомерности установки на ИС средств для решения соответствующих задач при разборе конфликтных ситуаций;

– для проверки правильности установки и настройки средств защиты ИС.

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

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

9.19. Использование несколькими сотрудниками при работе в ИС 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 ИС инициируется заявкой ответственного за эксплуатацию данной ИС. Форма заявки приведена ниже.

В заявке указывается:

– содержание запрашиваемых изменений (регистрация нового пользователя ИС, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИС ранее зарегистрированного пользователя);

– должность (с полным наименованием структурного подразделения), 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 ИС).

9.21. Заявку рассматривает руководитель, визируя её, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных в заявке задач ресурсам ИС. Затем подписывает задание администратору безопасности на внесение необходимых изменений в списки пользователей соответствующих подсистем ИС.

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), заявленных прав доступа к ресурсам ИС и другие необходимые действия, указанные в задании. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в течение 360 дней.

9.23. После внесения изменений в списки пользователей администратор безопасности должен обеспечить настройки средств защиты соответствующие требованиям безопасности указанной ИС. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписью исполнителя – администратор безопасности.

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

9.25. Исполненные заявка и задание (за подписью администратора безопасности) передаются руководителю на хранение.

Они могут впоследствии использоваться:

– для восстановления полномочий пользователей после аварий ИС;

– для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИС при разборе конфликтных ситуаций;

– для проверки сотрудниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИС.

10. Порядок контроля соблюдения условий использования средств защиты информации, в том числе криптографических

10.1. Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации.

10.2. Технические средства защиты информации являются важным компонентом ОБ КИ.

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

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

– руководитель;

– ответственный за защиту информации;

– администратор безопасности.

10.5. Пользователю ИС категорически запрещается:

– обрабатывать конфиденциальную информацию с отключенными СЗИ;

– менять настройки СЗИ.

10.6. Администратору безопасности запрещается менять настройки программно-аппаратных СЗИ предустановленные специалистом организации, имеющей лицензию на деятельность по технической защите информации, без согласования с этой организацией.

10.7. Если в ходе периодических, плановых или внезапных проверок ИС выявлено нарушение требования п. 10.5. то вступает в силу п.п. 3.7., 3.8. данного Положения.

10.8. Криптографические средства защиты информации должны использоваться в соответствии с технической и эксплуатационной документацией на них, а также в соответствии с правилами пользования ими.

11. Порядок охраны и допуска посторонних лиц в защищаемые помещения

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

11.2. Должна быть организована физическая охрана средств вычислительной техники и носителей информации. Должны быть предусмотрены: контроль доступа в помещения ИС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИС и хранилище носителей информации, особенно в нерабочее время.

Ответственный за обеспечение безопасности информации должен:

– поддерживать в актуальном состоянии списки сотрудников допущенных к вскрытию помещений, списки допущенных в помещения и списки пользователей ИС;

– периодически контролировать, отсутствие в помещениях ИС лиц, не имеющих права находиться в данном помещении;

– периодически контролировать корректность организации доступа в помещения и хранилища носителей информации (надёжность замков, порядок выдачи ключей сотрудникам и т.п.).

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

Список сотрудников, имеющих право вскрывать (сдавать под охрану) утверждается руководителем и передаётся на пост охраны.

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

11.5. 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 убираются для хранения в опечатываемый сейф (металлический шкаф).

11.6. Помещение сдается под охрану следующим образом:

– закрывает помещение;

– факт закрытия помещения подтверждается охранником;

– сдается помещение под подпись с указанием даты и времени сдачи под охрану.

11.7. Сотрудник, имеющий право на вскрытие помещений:

– получает на посту охраны ключи от помещения под подпись в Журнале с указанием даты и времени;

– производит запись в Журнале о вскрытии помещения с указанием фамилии и времени;

– производит проверку исправность запоров;

– вскрывает помещение.

11.8. 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 и (или) ответственному за защиту информации.

Одновременно принимаются меры по охране места происшествия и до прибытия должностных лиц в помещение никто не допускается.

11.9. Руководитель, ответственный за обеспечение безопасности информации и администратор безопасности организуют проверку ИС на предмет несанкционированного доступа к конфиденциальной информации и наличие документов и машинных носителей информации.

11.10. При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за помещение, или ответственному за обеспечение безопасности информации, или руководителю, или администратору безопасности. Помещения вскрывать запрещается.

11.11. Помещения вскрываются ответственным за помещение, или руководителем, или ответственным за обеспечение безопасности информации в присутствии сотрудника охраны с составлением акта.

Если обнаружено вторжение в защищаемое помещение, далее процедура происходит в соответствии с п. 10.8 настоящего Положения.

11.12. При передаче дежурства, если помещение в течение дня не вскрывалось, а также в выходные и праздничные дни принимающая дежурство смена поста охраны проверяет целостность запоров на дверях с отражением в «Журнале приема и сдачи дежурства» и «Журнале приема (сдачи) под охрану режимных помещений и ключей от них».

11.13. В соответствии с требованиями данного Положения при обработке защищаемой информации в ИС исключить не контролируемое пребывание посторонних лиц в пределах границ контролируемой зоны ИС, определенных соответствующим приказом.

12. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним

12.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним, обеспечивают сохранность конфиденциальной информации, криптосредств и ключевых документов к ним.

12.2. Помещения имеют прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, оборудуются охранной сигнализацией.

12.3. Размещение, специальное оборудование, охрана и организация режима в помещениях исключает возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

12.4. Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает ответственный пользователь криптосредств по согласованию, при необходимости, с оператором, в помещениях которого установлены криптосредства или хранятся ключевые документы к ним. Установленный режим охраны

предусматривает периодический контроль за состоянием технических средств охраны, если таковые имеются.

12.5. Двери спецпомещений постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в помещения, под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений должны храниться в сейфе оператора или ответственного пользователя криптосредствами.

12.6. Для предотвращения просмотра извне помещений их окна защищены.

12.7. Помещения, окна которых расположены на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически проверяется ответственным пользователем криптосредств совместно с представителем службы охраны или дежурным по организации с отметкой в соответствующих журналах.

12.8. Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища находится у сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в сейфе ответственного пользователя криптосредств. Дубликат ключа от хранилища ответственного пользователя криптосредств в опечатанной упаковке передается на хранение оператору под расписку в соответствующем журнале.

12.9. По окончании рабочего дня помещение и установленные в нем хранилища закрываются, хранилища опечатываются. Находящиеся в пользовании ключи от хранилищ должны сдаются под расписку в соответствующем журнале ответственному пользователю криптосредств или уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.

Ключи от режимных помещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ режимного помещения, в опечатанном виде сдаются под расписку в соответствующем журнале службы охраны или дежурному по организации одновременно с передачей под охрану самих помещений. Печати, предназначенные для опечатывания хранилищ, находятся у пользователей криптосредств, ответственных за эти хранилища.

12.10. При утрате ключа от хранилища или от входной двери в помещение замок заменяется.

12.11. Помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями криптосредств, ответственным пользователем криптосредств или оператором.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся немедленно сообщается ответственному пользователю криптосредств или оператору. Прибывший ответственный пользователь криптосредств оценивает возможность компрометации хранящихся ключевых и других документов, составляет акт и принимает, при необходимости, меры к локализации последствий компрометации конфиденциальных данных и к замене скомпрометированных криптоключей.

12.12. Техническое обслуживание оборудования, функционирующего с криптосредствами, и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

На время отсутствия пользователей криптосредств указанное оборудование, при наличии технической возможности, выключено, отключено от линии связи и убрано в опечатываемые хранилища.

13. Порядок стирания защищаемой информации и уничтожения носителей защищаемой информации

13.1. В обязательном порядке уничтожению подлежат поврежденные, выводимые из эксплуатации носители, содержащие защищаемую информацию, использование которых не предполагается в дальнейшем. Стиранию подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе ИС. Не допускается стирание неисправных носителей и передача их в сервисный центр для ремонта. Такие носители должны уничтожаться в соответствии с настоящим порядком.

13.2. Стирание должно производиться по технологии, предусмотренной для данного типа носителя, с применением сертифицированных средств гарантированного уничтожения информации (допускается задействовать механизмы затирания встроенные в сертифицированные средства защиты информации).

13.3. Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено гарантирование стирание информации на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны быть достаточны для исключения возможности восстановления информации.

13.4. Бумажные и прочие сгораемые носители (конверты с неиспользуемыми более паролями) уничтожают путем сжигания или с помощью любых бумагорезательных машин.

13.5. По факту уничтожения или стирания носителей составляется акт, в журналах учета делаются соответствующие записи.

13.6. Процедуры стирания и уничтожения осуществляются комиссией, в которую входят: ответственный за эксплуатацию ИС, ответственный за защиту информации, администратор безопасности.

14. Порядок передачи и хранения конфиденциальной информации

14.1. При передаче конфиденциальной информации граждан Оператор должен соблюдать следующие требования:

14.1.1. Не сообщать конфиденциальные данные третьей стороне без письменного согласия гражданина, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом.

14.1.2. Не сообщать конфиденциальные данные гражданина в коммерческих целях без его письменного согласия. Обработка конфиденциальных данных гражданина в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

14.1.3. Предупредить лиц, получивших конфиденциальные данные гражданина, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие конфиденциальные данные, обязаны соблюдать режим конфиденциальности. С данными лицами Оператор подписывает Соглашение о конфиденциальности.

Данное Положение не распространяется на обмен конфиденциальными данными граждан в порядке, установленном федеральными законами.

14.1.4. Осуществлять передачу конфиденциальных данных граждан в пределах Организации в соответствии с настоящим Положением.

14.1.5. Разрешать доступ к конфиденциальным данным граждан только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те конфиденциальные данные, которые необходимы им для выполнения конкретной функции.

14.1.6. Передавать конфиденциальные данные граждан их представителям в порядке, установленном законодательством Российской Федерации, и ограничивать эту информацию только теми конфиденциальные данными, которые необходимы для выполнения указанными представителями их функции.

14.2. Хранение и использование конфиденциальных данных граждан:

14.2.1. Конфиденциальные данные граждан обрабатываются и хранятся в подразделениях управления ветеринарии Тамбовской области.

14.2.2. Конфиденциальные данные граждан могут быть получены, проходить дальнейшую обработку и передаваться на хранение, как на бумажных носителях, так и в электронном виде.

14.3. При получении конфиденциальных данных не от гражданина (за исключением случаев, если конфиденциальные данные были предоставлены на основании федерального закона или если конфиденциальные данные являются общедоступными) Оператор до начала обработки таких конфиденциальных данных обязан предоставить гражданину следующую информацию:

– наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

– цель обработки конфиденциальных данных и ее правовое основание;

– предполагаемые пользователи конфиденциальных данных;

– установленные Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» права субъекта персональных данных.

15. Порядок взаимодействия с информационными сетями общего пользования

15.1. Данный порядок определен, исходя из требований РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», настоящего документа, а также следующих основных угроз безопасности информации, возникающих при взаимодействии с информационными сетями общего пользования:

– несанкционированного доступа к информации, хранящейся и обрабатываемой во внутренних ЛВС (серверах, рабочих станциях) или на автономных ПЭВМ, как из Сетей, так и из внутренних ЛВС;

– несанкционированного доступа к коммуникационному оборудованию (маршрутизатору, концентратору, мосту, мультиплексору, серверу, Web/Proxy серверу), соединяющему внутренние ЛВС организации с Сетями;

– несанкционированного доступа к данным (сообщениям), передаваемым между внутренними ЛВС и Сетями, включая их модификацию, имитацию и уничтожение;

– заражения программного обеспечения компьютерными «вирусами» из Сети, как посредством приема «зараженных» файлов, так и посредством E-mail, апплетов языка JAVA и объектов ActiveX Control;

- внедрения программных закладок с целью получения НСД к информации, а также дезорганизации работы внутренней ЛВС и ее взаимодействия с Сетями;

- несанкционированной передачи защищаемой конфиденциальной информации ЛВС в Сеть;

– возможности перехвата информации внутренней ЛВС за счет побочных электромагнитных излучений и наводок от основных технических средств, обрабатывающих такую информацию.

15.2. Подключение к Сети абонентского пункта осуществляется по решению руководителя организации на основании соответствующего обоснования.

15.3. Обоснование необходимости подключения АП к Сети должно содержать:

– наименование Сети, к которой осуществляется подключение, и реквизиты организации-владельца Сети и провайдера Сети;

– состав технических средств для оборудования АП;

– предполагаемые виды работ и используемые прикладные сервисы Сети (E-Mail, FTP, TelNet, HTTP и т.п.) для АП в целом и для каждого абонента, в частности;

– режим подключения АП и абонентов к Сети (постоянный, в т.ч. круглосуточный, временный);

– состав общего и телекоммуникационного программного обеспечения АП и абонентов (ОС, клиентские прикладные программы для сети - Browsers и т.п.);

– число и перечень предполагаемых абонентов (диапазон используемых IP- адресов);

– меры и средства защиты информации от НСД, которые будут применяться на АП, организация-изготовитель, сведения о сертификации, установщик, конфигурация, правила работы с ними;

– перечень сведений конфиденциального характера, обрабатываемых (хранимых) на АП, подлежащих передаче и получаемых из Сети.

15.4. Подключение к Сети АП, представляющих собой внутренние (локальные) вычислительные сети, на которых обрабатывается информация, не разрешенная к открытому опубликованию, разрешается только после установки на АП средств защиты информации от НСД.

15.5. Подключение ЛВС МБДОУ детского сада № 7 «Белоснежка» к Сети должно осуществляться через средства разграничения доступа в виде МЭ (Firewall, Брандмауэр). Не допускается подключение ЛВС к Сети в обход МЭ. МЭ должны быть сертифицированы по требованиям безопасности информации.

15.6. Доступ к МЭ, к средствам его конфигурирования должен осуществляться только Администратором безопасности. Средства удаленного управления МЭ должны быть исключены из конфигурации.

15.7. На технических средствах АП должно находиться программное обеспечение только в той конфигурации, которая необходима для выполнения работ, заявленных в обосновании необходимости подключения АП к Сети (обоснование может корректироваться в установленном в организации порядке).

15.8. Установку программного обеспечения, обеспечивающего функционирование АП, должен выполнять только Администратор безопасности.

15.9. Устанавливаемые межсетевые экраны должны соответствовать классу защищаемого АП (АС) и отвечать требованиям РД ФСТЭК России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

15.10. СЗИ НСД, устанавливаемая на автономную ПЭВМ, рабочие станции и серверы внутренней ЛВС предприятия при обработке на них конфиденциальной информации, должна осуществлять:

– идентификацию и аутентификацию пользователей при доступе к автономной ПЭВМ, рабочим станциям и серверам внутренней ЛВС по идентификатору и паролю;

– контроль доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС на основе дискреционного принципа;

– регистрацию доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС, включая попытки НСД;

– регистрацию фактов отправки и получения абонентом сообщений (файлов, писем, документов).

При этом СЗИ от НСД должна запрещать запуск абонентом произвольных программ, не включенных в состав программного обеспечения АП.

Модификация конфигурации программного обеспечения АП должна быть доступна только со стороны Администратора безопасности.

Средства регистрации и регистрируемые данные должны быть недоступны для абонента.

СЗИ от НСД должна быть целостной, т.е. защищенной от несанкционированной модификации и не содержащей путей обхода механизмов контроля.

Тестирование всех функций СЗИ от НСД с помощью специальных программных средств должно проводится не реже одного раза в год.

15.11. В целях контроля за правомерностью использования АП и выявления нарушений требований по защите информации:

– осуществлять анализ принимаемой из Сети и передаваемой в Сеть информации, в том числе на наличие «вирусов»;

– проводить постоянный контроль информации, помещаемой на Web-серверы предприятия.

15.12. Абоненты Сети обязаны:

– знать порядок регистрации и взаимодействия в Сети;

– знать инструкцию по обеспечению безопасности информации на АП;

– знать правила работы со средствами защиты информации от НСД, установленными на АП (серверах, рабочих станциях АП);

–уметь пользоваться средствами антивирусной защиты;

– после окончания работы в Сети проверить свое рабочее место на наличие «вирусов».

15.13. Входящие и исходящие сообщения (файлы, документы), а также используемые при работе в Сети носители информации учитываются в журналах делопроизводства.

15.14. При работе в Сети категорически запрещается:

- подключать технические средства (серверы, рабочие станции), имеющие выход в Сеть, к другим техническим средствам (сетям), не определенным в обосновании подключения к Сети;

– изменять состав и конфигурацию программных и технических средств АП без санкции администратора и аттестационной комиссии;

– производить отправку данных без соответствующего разрешения;

– использовать зарегистрированные носители информации на рабочих местах других систем (в том числе и автономных ПЭВМ) без соответствующей санкции.

15.15. Контроль за выполнением мероприятий по обеспечению безопасности информации на АП возлагается на Администратора безопасности, руководителей соответствующих подразделений, определенных приказом по организации.

16. Заключительные положения.

16.1. Требования настоящего Положения обязательны для всех сотрудников обрабатывающих конфиденциальную информацию.

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