Муниципальное бюджетное дошкольное образовательное учреждение
«Детский сад №8» города Гусь-Хрустальный Владимирской области

Марфина Мария Александровна

Подписано цифровой подписью: Марфина Мария Александровна
DN: cn=Марфина Мария Александровна, o=Муниципальное бюджетное дошкольное образовательное учреждение "Детский сад №8", ou, email=ya.gusdou8@yandex.ru, c=RU
Дата: 2025.11.20 10:49:53 +03'00'

УТВЕРЖДЕНО:
Заведующий
МБДОУ «Детский сад № 8»
_____М.А. Марфина
Приказ № 01-18/249 от 10.11.2025г

Регламент
обеспечения безопасности персональных данных
при их обработке в информационных системах персональных данных
МБДОУ «Детский сад № 8»

1. Общие положения

Настоящий Регламент обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных МБДОУ «Детский сад № 8» (далее – Регламент) устанавливает и определяет основные организационные и технические меры по защите персональных данных, основные обязанности пользователей и должностных лиц, обрабатывающих персональные данные автоматизированным способом в информационной системе персональных данных МБДОУ «Детский сад № 8» (далее – ИСПДн ДОУ) и телекоммуникационных сетях ДОУ (далее - ДОУ).

Требования Регламента являются обязательными для работников ДОУ и третьих лиц, которые допущены к работе с персональными данными. При приеме на работу работники ДОУ, допущенные к персональным данным, должны быть под расписку ознакомлены с требованиями настоящего Регламента, в части, касающейся их деятельности, информированы об ответственности за их нарушение.

Настоящий Регламент утверждается руководителем ДОУ и носит обязательный характер для всех работников ДОУ.

2 Обеспечение безопасности персональных данных в ИСПДн ДОУ

Обеспечение безопасности персональных данных в ДОУ достигается за счет выполнения требований нормативных актов Российской Федерации в сфере защиты персональных данных и выполнения требований, установленных во внутренних нормативных документах ДОУ, всеми пользователями персональных данных. Персональные данные субъектов персональных данных, обрабатывающиеся в ИСПДн ДОУ подлежат защите от несанкционированного доступа и копирования.

Безопасность персональных данных при их обработке в ИСПДн ДОУ обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации. Технические и программные средства обработки и защиты информации должны удовлетворять устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации, относящейся к персональным данным. Реализация требований по обеспечению безопасности персональных данных в информационных системах возлагается на лицо, ответственное за обеспечение безопасности персональных данных в ИСПДн ДОУ совместно с лицами, обрабатывающими персональные данные согласно Перечню должностей служащих, замещение которых предусматривает осуществление обработки персональных данных.

При обработке персональных данных в информационных системах ответственными лицами должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки ПД, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль обеспечения уровня защищенности персональных данных.

Мероприятия по обеспечению безопасности персональных данных являются неотъемлемой частью работ по созданию ИСПДн ДОУ. Меры по защите персональных данных, обрабатываемых в ДОУ принимаются в соответствии с моделью угроз безопасности персональных данных при их обработке в ИСПДн, для каждой информационной системы персональных данных в частности.

В ДОУ разработан документ «Инструкция пользователя ИСПДн ». Данная инструкция закрепляет должностные обязанности пользователей, устанавливает единый порядок парольной защиты, правила работы в сетях общего доступа и международного информационного обмена на рабочем месте пользователя. Контроль состояния защищенности ИСПДн ДОУ в целях поддержания требуемого уровня безопасности, а так же предотвращения наступления инцидентов информационной безопасности определены регламентом осуществления внутреннего контроля за обеспечением уровня защищенности персональных данных и соблюдением условий использования средств защиты информации, а также соблюдением требований законодательства РФ по обработке персональных данных в ИСПДн ДОУ.

3. Основные направления и методы защиты информации в ИСПДн ДОУ

Назначенное лицо в ДОУ, ответственное за обеспечение безопасности персональных данных в ИСПДн ДОУ обязано организовывать работу по защите персональных данных, осуществлять методическое руководство проведением мероприятий по защите информации, а также контроль за эффективностью предусмотренных мер защиты информации на контролируемой территории.

Руководитель ДОУ обязан контролировать в организации выполнение работниками установленных общих требований по организации работы с персональными данными и предусмотренных организационных и технических мер по защите персональных данных в пределах своих полномочий.

Пользователи ИСПДн обязаны соблюдать правила обработки персональных данных в ИСПДн ДОУ, и отвечают за обеспечение защиты информации согласно трудовому законодательству и нормативным актам ДОУ. В своей работе с персональными данными пользователи руководствуются нормами настоящего положения, Инструкцией пользователя ИСПДн ДОУ.

Лицо, ответственное за обеспечение безопасности персональных данных, контролирует в пределах своей компетенции состояние защиты персональных данных с целью своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию и оценки ее защищенности.

Повседневный и периодический (не реже одного раза в год) контроль за состоянием защиты персональных данных выполняется силами штатных работников, обрабатывающих персональные данные согласно должностным обязанностям, и специалиста ДОУ, ответственного за обеспечение безопасности персональных данных, в соответствии с «Регламентом осуществления внутреннего контроля за обеспечением уровня защищенности персональных данных и соблюдением условий использования средств защиты информации, а также

соблюдением требований законодательства РФ по обработке персональных данных в ИСПДн ДОУ».

Ответственное лицо за обеспечение безопасности персональных данных ежегодно отчитывается о состоянии защиты персональных данных в ДОУ, а также об инцидентах в связи с не выполнением сотрудниками или третьими лицами требований и норм по защите персональных данных, в результате которых имелись или имеются реальные возможности их утечки, руководству ДОУ. В целях предотвращения несанкционированного доступа к техническим средствам обработки, хранения и передачи информации (далее - ТСПИ), их хищения и нарушения работоспособности ИСПДн ДОУ самостоятельно или с привлечением аутсорсинговых организаций обеспечивается охрана и физическая защита помещений объектов информатизации, в которых располагаются технические средства ДОУ.

Защита персональных данных в ИСПДн ДОУ от актуальных угроз безопасности осуществляется по следующим основным направлениям:

- от внедренных специальных электронных устройств;
- от вредоносного кода;
- от несанкционированного доступа;
- от несанкционированного воздействия;
- от непреднамеренного воздействия;
- от разглашения;
- от технических средств разведки (далее - ТСР).

В качестве основных мер защиты персональных данных в ДОУ должностными лицами, обрабатывающими или защищающими персональные данные, а также подразделениями, осуществляющими эксплуатацию технических средства ИСПДн ДОУ, должны выполняться:

а) документальное оформление и обновление «Перечня персональных данных, обрабатываемых в ИСПДн с учетом специфики обработки персональных данных ДОУ;

б) разграничение доступа Пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) персональных данных и защиты информации;

в) ограничение доступа персонала и посторонних лиц в защищаемые помещения и помещения, где размещены средства информатизации и коммуникационное оборудование ИСПДн, а также хранятся носители персональных данных;

г) регистрация действий пользователей, обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

д) учет и надежное хранение машинных носителей персональных данных и их обращение, исключающее хищение, подмену и уничтожение;

е) резервирование технических средств, дублирование массивов и носителей информации ИСПДн;

ж) использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;

з) использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;

и) использование сертифицированных средств защиты информации по требованиям ФСТЭК России и ФСБ России;

к) размещение объекта защиты внутри контролируемой зоны на максимально возможном удалении от ее границ;

н) использование криптографически защищенных каналов связи при передаче конфиденциальной информации по открытым каналам связи;

о) размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр;

п) организация самостоятельно или силами сторонней организации физической защиты помещений и собственно технических средств обработки персональных данных с использованием

технических средств охраны, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и носителей информации, самих средств информатизации ИСПДн;

р) предотвращение внедрения в ИСПДн программ-вирусов, программных закладок.

Объем принимаемых мер защиты информации, в зависимости от возможного ущерба в случае ее утечки, определяют должностные лица, отвечающие за организацию и руководство работами по защите информации в ДОУ.

3.1 Защита информации от вредоносного программного обеспечения

Организация антивирусной защиты информации в ИСПДн ДОУ достигается путем:

- внедрения и применения средств антивирусной защиты информации;
- обновления сигнатурных баз данных средств антивирусной защиты информации;
- спланированных действий должностных лиц при обнаружении заражения информационных ресурсов ИСПДн ДОУ вирусным программным обеспечением.

Система антивирусной защиты ИСПДн включает в себя:

- антивирусную защиту рабочих станций ИСПДн;
- антивирусную защиту серверов и баз персональных данных ИСПДн.

Пользователями ИСПДн «НО» являются лица, использующие при обработке персональных данных средства автоматизированной обработки информации, в том числе средства вычислительной техники, программное обеспечение, электронные носители персональных данных и средства защиты информации:

- возможность автоматического обновления сигнатурных антивирусных баз и версий. Организация работ по антивирусной защите информации возлагается на структурное подразделение или назначенное лицо «НО», ответственное за обеспечение безопасности персональных данных, и должностных лиц, осуществляющих эксплуатацию объектов информатизации ИСПДн ДОУ, а методическое руководство и контроль за эффективностью предусмотренных мер защиты информации - на лицо, ответственное за обеспечение безопасности персональных данных.

Порядок применения средств антивирусной защиты устанавливается с учетом необходимости выполнения следующих требований:

а) пользователями ИСПДн:

- периодическая проверка носителей информации (не реже одного раза в неделю) и обязательная проверка используемых в работе съемных носителей информации перед началом работы с ними на отсутствие программных вирусов;
- внеплановая проверка носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса.

б) работниками подразделения, осуществляющего эксплуатацию ИСПДн:

- обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации съемных и встроенных носителей информации, информационных массивов и баз данных, программных средств общего и специального назначения;
- восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

К использованию в ДОУ допускаются только санкционированные назначенным работником ДОУ, ответственным за обеспечение безопасности персональных данных, антивирусные средства. Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке и руководством по эксплуатации конкретного антивирусного программного продукта. При обнаружении программных вирусов Пользователь ИСПДн обязан прекратить все работы на рабочем месте, поставить в известность руководителя ДОУ, принять меры к локализации и удалению вирусов с помощью имеющихся антивирусных средств защиты.

При функционировании автоматизированного рабочего места в качестве локальной рабочей станции вычислительной сети производится ее отключение от локальной сети, локализация и удаление программных вирусов в вычислительной сети.

3.2 Защита персональных данных от несанкционированного доступа.

Защита ИСПДн ДОУ обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

При обработке или хранении в ИСПДн конфиденциальных персональных данных для защиты проводятся следующие организационные мероприятия:

- документальное оформление персональных данных в виде Перечня;
- определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;
- ознакомление субъекта доступа с «Перечнем персональных данных» и установленным для него уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;
- обеспечение охраны объекта, на котором расположена защищаемая ИСПДн, собственными силами или с привлечением сторонней организации любыми способами, предотвращающими или существенно затрудняющими хищение технических средств ИСПДн ДОУ, съемных, встроенных и резервных носителей, а также предотвращающими несанкционированный доступ к информационным ресурсам ДОУ и каналам связи;
- назначение должностных лиц, осуществляющих учет, хранение и выдачу съемных и резервных носителей информации, паролей, ключей, ведение служебной информации системы защиты информации от несанкционированного доступа, приемку включаемых в ИСПДн программных средств, а также контроль за ходом технологического процесса обработки персональных данных и т. д.;
- разработка системы защиты персональных данных, включая соответствующую организационно-распорядительную документацию. В целях дифференцированного подхода к защите персональных данных комиссией, назначенной заведующим ДОУ, проводится определение уровня защищенности ИСПДн ДОУ с составлением акта.

Основные мероприятия по предотвращению несанкционированного доступа к персональным данным ДОУ:

а) разграничение доступа к персональным данным;

б) управление потоками персональных данных в целях предотвращения несанкционированной записи данных на съемные носители; в) определение единого порядка парольной защиты;

г) идентификация пользователей и подтверждение их права на работу с запрашиваемой информацией;

д) регистрация действий пользователей в ИСПДн;

е) реакция на попытки несанкционированного доступа, например, сигнализация о попытке, блокировка доступа, восстановление после попытки несанкционированного доступа к прежнему безопасному состоянию и т. д.;

ж) тестирование информационных ресурсов ИСПДн с помощью специальных программных средств выявления уязвимостей;

з) очистка оперативной памяти и рабочих областей на съемных носителях персональных данных после прекращения или блокировки работы пользователя с ИСПДн;

и) учет выходных конфиденциальных печатных, графических форм и твердых копий.

3.3. Защита персональных данных от несанкционированного и непреднамеренного воздействия.

Защита персональных данных от несанкционированного и непреднамеренного воздействия осуществляется по следующим направлениям:

а) соблюдение порядка разработки, ввода в действие и эксплуатации объектов информатизации;

б) определение условий размещения информационных ресурсов ИСПДн относительно границ контролируемой зоны;

в) определение технических средств и систем, предполагаемых к использованию в ИСПДн и системах связи, условий их расположения;

г) определение режимов обработки персональных данных в ДОУ в целом и в отдельных компонентах;

д) установление правил разграничения доступа для пользователей с целью минимизации их воздействия на программные и аппаратные средства автоматизации обработки персональных данных;

е) повышение уровня квалификации пользователей и обслуживающего персонала, периодическое и выборочное тестирование знаний и квалификации в области информационной безопасности;

ж) контроль, техническое обслуживание и обеспечение установленных режимов работы ТСПИ в целях предупреждения их сбоев, аварий, неисправностей;

з) применение постоянно обновляемого антивирусного программного обеспечения;

и) защита от природных и техногенных явлений и стихийных бедствий (пожары, наводнения и т.п.);

к) предупреждение передачи конфиденциальных персональных данных по открытым линиям связи и их обработки незащищенными техническими средствами;

л) строгое выполнение работниками установленных в организации требований по защите персональных данных;

м) организация эффективного контроля выполнения предусмотренных мер защиты персональных данных;

н) использование ИСПДн в защищенном исполнении.

3.4 Защита персональных данных от распространения неограниченному кругу лиц.

Правовой основой работы с работниками ДОУ, допущенными к обработке персональных данных, являются:

- наличие в трудовом договоре пункта о правилах работы со сведениями, относящимся к персональным данным;
- наличие в должностном регламенте или должностной инструкции работника пунктов о мерах безопасности при обработке персональных данных и ответственность за ее несанкционированное разглашение;
- наличие «Перечня персональных данных, обрабатываемых в ДОУ, инструкций и регламентов по защите персональных данных, ознакомление с которыми должно проводиться работником в первый день заступления на должность и под обязательную роспись в ознакомлении;
- создание работникам достаточных условий для обеспечения эффективной защиты персональных данных.

В целях предупреждения разглашения персональных данных назначенное лицо ДОУ ответственное за обеспечение безопасности персональных данных, организует мероприятия по аудиту защищенности персональных данных, тестированию уровня осведомленности персонала о мерах защиты, проверки процедур автоматизированной и неавтоматизированной обработки персональных данных на соответствие регламентам информационной безопасности.

4. Порядок резервирования и восстановления работоспособности ИСПДн ДОУ

Ответственным за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, является лицо, ответственное за обеспечение безопасности персональных данных. Ответственным за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, является лицо, ответственное за организацию обработки персональных данных.

4.1 Порядок реагирования на инцидент (происшествие), вызывающее инцидент, может произойти в результате:

- непреднамеренных действий пользователей.
- преднамеренных действий пользователей и третьих лиц.
- нарушения правил эксплуатации технических средств ИСПДн ДОУ;
- возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование работником. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование работники ДОУ предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия согласования может быть нарушена, с целью оперативного получения высококвалифицированной консультации.

4.2 Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов.

4.2.1 Технические меры.

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

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

Системы жизнеобеспечения ИСПДн включают:

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

Все критичные помещения ДОУ (помещения, в которых размещаются элементы ИСПДн МОУ и средства защиты) оборудованы средствами пожарной сигнализации и пожаротушения. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, применяются системы вентиляции и кондиционирования воздуха. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн ДОУ, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции подключаются к сети электропитания через источники бесперебойного питания.

В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров.

Под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн «НО», предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации:

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

Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн ДОУ при сбое в работе оборудования и их автоматической замены без простоев использую методы кластеризации.

Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн ДОУ должны использоваться территориально удаленные системы кластеров.

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

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

4.2.2 Организационные меры.

Резервное копирование и хранение данных должно осуществлять на периодической основе:

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

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования. Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения. Носители должны храниться не менее года, для возможности восстановления данных.

5. Порядок обращения со средствами криптографической защиты информации (СКЗИ).

Использование СКЗИ в ДОУ необходимо для достижения следующих целей:

- обеспечение целостности персональных данных, обрабатываемых в ИСПДн;
- обеспечение конфиденциальности персональных данных, обрабатываемых в ИСПДн;
- обеспечение невозможности отказа от авторства внесенных изменений в обрабатываемые персональные данные.

СКЗИ в ИСПДн ДОУ применяются для решения следующих задач:

- передача персональных данных за пределы контролируемой зоны;
- заверение электронно-цифровой подписью документов.

5.1. Состав СКЗИ.

Для достижения вышеуказанных целей могут использоваться программные и программно-аппаратные СКЗИ, состав которых утверждается Лицом, ответственным за организацию обработки персональных данных.

5.2. Учет используемых СКЗИ СКЗИ, эксплуатационная и техническая документация к ним, используемые в ИСПДн ДОУ, подлежат поэкземплярному учету в Журнале учета СКЗИ.

Поэкземплярный учет осуществляет лицо, ответственное за обеспечение безопасности персональных данных. При ведении учета, программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатная эксплуатация. Единицей поэкземплярного учета СКЗИ является отчуждаемый ключевой носитель многократного использования. При осуществлении перезаписи криптографических ключей на носитель лицо, ответственное за обеспечение безопасности персональных данных, обязано осуществить его повторную регистрацию в Журнале поэкземплярного учета СКЗИ с указанием сведений о вновь записанных криптографических ключах. Нумерация носителей СКЗИ ведется в соответствии с индивидуальными номерами, присваиваемыми изготовителями СКЗИ.

5.3. Допуск работников к СКЗИ.

5.3.1.Порядок оформления допуска к СКЗИ Допуск Пользователей персональных данных к работе с СКЗИ осуществляется на основании заявки, подаваемой ответственному за обеспечение безопасности персональных данных.

В заявке указываются следующие сведения:

- перечень задач, для которых необходимо использование СКЗИ;
- период времени, в течение которого необходимо использование СКЗИ.

Лицо, ответственное за обеспечение безопасности персональных данных, обязано провести под подпись обучение Пользователя персональных данных правилам работы с СКЗИ, к которым он будет допущен. Допуск Пользователей персональных данных к работе со СКЗИ сопровождается занесением информации, указанной в заявке, в Перечень лиц, допущенных к работе с СКЗИ.

5.3.2.Порядок выдачи СКЗИ Экземпляры СКЗИ, эксплуатационной и технической документации к ним выдаются под подпись Пользователю персональных данных, при условии наличия у него допуска к СКЗИ. Пользователи персональных данных несут персональную ответственность за сохранность выданного им экземпляра СКЗИ.

Лицо, ответственное за обеспечение безопасности персональных данных, выдает основной экземпляр СКЗИ лично Пользователю персональных данных, при необходимости, резервный экземпляр того же ключа помещает на хранение в сейф.

5.3.3.Порядок пересмотра прав допуска к СКЗИ Лицо, ответственное за обеспечение безопасности персональных данных, обязано производить ежемесячный пересмотр допуска персональных данных к СКЗИ путем анализа Перечня лиц, допущенных к работе с СКЗИ.

В случае обнаружения Пользователей персональных данных с истекающим сроком использования СКЗИ, лицо, ответственное за обеспечение безопасности ПД, не менее чем за 5 рабочих дней, обязано оповестить пользователя о прекращении использования СКЗИ.

5.3.4.Порядок прекращения прав допуска и изъятия СКЗИ из обращения Прекращение прав доступа Пользователя персональных данных к СКЗИ осуществляется лицом, ответственным за обеспечение безопасности персональных данных, в следующих случаях:

- достигнуты цели использования СКЗИ;
- истек период времени, указанный в заявке;
- увольнение Пользователя персональных данных или его перевод на другую должность, не связанную с необходимостью использования СКЗИ.

При наступлении вышеуказанных случаев, лицо, ответственное за обеспечение безопасности персональных данных, осуществляет исключение Пользователя персональных данных из Перечня лиц, допущенных к работе с СКЗИ и изымает СКЗИ из обращения.

Перед повторным использованием с основного и резервного ключевых носителей СКЗИ при помощи средств гарантированного уничтожения должна быть удалена вся информация.

6. Порядок обращения с материальными носителями персональных данных.

Учету подлежат следующие типы машинных носителей персональных данных:

- отчуждаемые носители информации (внешние жесткие магнитные диски, гибкие магнитные диски, магнитные ленты, USB флеш-накопители, карты флеш-памяти, оптические носители (CD, DVD, Blu-ray и прочее);
- неотчуждаемые носители информации (жесткие магнитные диски).

6.1. Порядок организации учёта машинных носителей, содержащих персональные данные.

Все машинные носители данных, используемые при работе со средствами вычислительной техники (далее СВТ) для обработки и хранения персональных данных, обязательно регистрируются и учитываются в «Журнале учета съемных носителей персональных данных, обрабатываемых в ИСПДн ДОУ с присвоением индивидуального учетного номера.

Ответственность за хранение машинных носителей персональных данных и ведение Журнала учета носителей в ДОУ несёт лицо, ответственное за обеспечение безопасности персональных данных. Учетный номер и гриф «Конфиденциально» наносятся на носитель информации или его корпус. Если невозможно маркировать непосредственно машинный носитель данных, то маркируется упаковка, в которой хранится носитель. Несъемные жесткие магнитные диски закрепляются за работником, ответственным за СВТ, в котором они установлены.

6.1.1. Порядок использования машинных носителей персональных данных.

Машинные носители данных выдаются Пользователям или другим лицам, участвующим в обработке персональных данных, для работы под расписку в Журнале учета носителей. По завершении работы машинные носители данных сдаются лицу, ответственному за обеспечение безопасности персональных данных. Уничтожение персональных данных с материального носителя происходит путем очистки информации с использованием сертифицированных по требованиям безопасности информации систем гарантированного уничтожения информации, а так же с применением прикладного программного обеспечения, позволяющего выполнять многократную перезапись всего электронного носителя псевдослучайной последовательностью.

После уничтожения информации машинные носители продолжают использоваться наравне с другими машинными носителями персональных данных. В последующем эти носители повторно используются для записи информации, содержащей персональных данных. В случае повреждения машинных носителей, содержащих персональные данные, работник, за которым закреплён носитель, сообщает о случившемся своему руководителю. Поврежденные материальные носители уничтожаются электромагнитным или физическим воздействием либо иным способом, предусмотренным эксплуатационной и технической документацией к ним. Передача съёмного носителя, содержащего персональные данные, третьим организациям производится в соответствии с требованиями договора между ДОУ и третьим лицом. Машинные носители данных пересылаются в том же порядке, что и конфиденциальные бумажные документы. При фиксации персональных данных на машинных носителях не допускается фиксация на одном машинном носителе персональные данные, цели обработки которых заведомо не совместимы. Вынос машинных носителей, содержащих персональных данных, за пределы контролируемой зоны «НО» запрещается без соответствующего разрешения лица, ответственного за обеспечение безопасности персональных данных.

6.1.2. Порядок хранения машинных носителей, содержащих персональных данных.

Хранение носителей, содержащих персональные данные, осуществляется в условиях, исключающих возможность хищения, изменения целостности или уничтожения содержащейся на них информации. Отчуждаемые съемные носители после окончания работы с ними должны убираться в сейфы или шкафы, запираемые на ключ. Не допускается оставлять на рабочем столе или в СВТ машинные носители содержащие персональные данные. Персональную ответственность за сохранность полученных машинных носителей и предотвращение несанкционированного доступа к записанным на них персональным данным несет работник, за которым закреплен носитель.

6.1.3. Хранение носителей резервного копирования.

Организация и правила хранения носителей резервного копирования осуществляется в соответствии с правилами, изложенными в разделе 4.2.2 настоящего Регламента.

6.1.4. Порядок уничтожения машинных носителей, содержащих персональные данные Основанием для уничтожения машинных носителей, содержащих персональные данные, является повреждение машинного носителя, исключающее его дальнейшее использование или потеря практической ценности носителя. Решение об уничтожении машинного носителя принимает лицо, ответственное за обеспечение безопасности персональных данных. Списанные машинные носители, подлежащие уничтожению, хранятся у лица, ответственного за обеспечение безопасности персональных данных, в запакованных коробах, короба маркируются пометкой «на уничтожение». Уничтожение производится раз в год путем их физического разрушения с предварительным затиранием (уничтожением) содержащейся на них персональных данных, если это позволяют физические принципы работы носителя. Уничтожение машинных носителей производится Комиссией в составе не менее трех человек, в состав Комиссии должны обязательно входить лицо, ответственное за обеспечение безопасности персональных данных, и лицо, ответственное за организацию обработки персональных данных. После уничтожения всех машинных носителей составляется Акт об уничтожении. При уничтожении машинные носители данных снимаются с учета. Отметка об уничтожении носителей проставляется в Журнале учета носителей.

6.2. Порядок уничтожения (стирания) персональных данных с машинного носителя.

Основанием для уничтожения (стирания) записей или части записей с машинного носителя являются следующие случаи:

- возврат носителя работником;
- передача носителя в ремонт;
- списание носителя.

Хранящиеся на машинных носителях и потерявшие актуальность персональные данные своевременно стираются (уничтожаются). Лицо, ответственное за обеспечение безопасности персональных данных принимает окончательное решение о необходимости их уничтожения.

Ответственный за процесс обработки персональных данных передает машинный носитель лицу, ответственному за обеспечение безопасности персональных данных. Совместно с машинным носителем передается служебная записка, в которой указывается причины возврата и состав персональных данных, которые подлежат уничтожению. Лицо, ответственное за обеспечение безопасности персональных данных, при получении носителя должно обеспечить уничтожение (стирание) записей или части записей с носителя и подготовить Акт об уничтожении (стирании) записей с носителя с внесением данных в Журнал учета носителей. В Акт уничтожения заносится дата, учетный номер носителя и способ уничтожения (стирания) записей персональных данных, также в Акте отображается наименование программного обеспечения, которым производилось стирание.

6.3. Порядок работы комиссии по уничтожению носителей персональных данных определяется «Положением о комиссии по уничтожению носителей персональных данных ДОУ».

7. Порядок обеспечения антивирусной защиты ИСПДн ДОУ

7.1. Порядок использования антивирусных средств, применение средств антивирусного контроля.

Средства антивирусной защиты установлены и настроены на всех допускающих такую установку программно-технических средствах до начала их использования для обработки персональных данных. Модуль средства антивирусной защиты, отвечающий за мониторинг вирусной активности в реальном времени (антивирусный монитор), запускается при загрузке операционной системы в автоматическом режиме вместе с основным модулем средства антивирусной защиты. Антивирусный контроль рабочих станций проводится ежедневно в автоматическом режиме. В тех случаях, когда проверка всех файлов на дисках рабочих станциях занимает неприемлемо большое время, проводится выборочная проверка загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и файлов, загружаемых по сети или с внешних носителей. В этом случае полная проверка осуществляется не реже одного раза в неделю в период неактивности пользователя. Антивирусный контроль серверов проводится ежедневно, а также при перезапуске сервера. Проводится антивирусная проверка на рабочих станциях и серверах, вернувшихся с технического обслуживания или ремонта (в том числе, гарантийного), производимого сторонними организациями. Любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD/DVD – R/RW, USB Flash drive и т.п.) подлежит обязательному антивирусному контролю.

Контроль исходящей информации проводится непосредственно перед архивированием и отправкой (записью на съемный носитель). Файлы, помещаемые в электронный архив, в обязательном порядке проходят антивирусный контроль.

Периодические проверки электронных архивов проводятся не реже одного раза в месяц. Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется на отсутствие вредоносных программ. Непосредственно после установки (изменения) программного обеспечения компьютера системным администратором ИСПДн «НО» выполняется антивирусная проверка.

Обновления антивирусных баз производятся не реже одного раза в сутки в автоматическом режиме, согласно возможностям программного обеспечения. В случае сбоя автоматического обновления обновление баз производится вручную с той же периодичностью. Установка, настройка и использование стандартного антивирусного пакета для серверов и рабочих станций производятся в соответствии инструкциями производителя конкретного антивирусного продукта.

7.2. Действия при обнаружении вредоносных программ.

В случае обращений Пользователей ИСПДн ДОУ, связанных с подозрением на наличие вредоносных программ, проводится внеочередной антивирусный контроль рабочих станций обратившихся Пользователей. В случае подтверждения наличия вредоносных программ в результате проведения контроля делается вывод либо об их уничтожении, либо о необходимости

дальнейшего восстановления работоспособности компьютера. В случае поражения программ вирусом, уничтожение вируса выполняется путем уничтожения программ на диске либо ином носителе. После уничтожения зараженных программ их исходные версии восстанавливаются из резервных копий. Если вирус поразил файлы, его уничтожение производится путем стирания этих файлов, либо путем лечения файлов с использованием возможностей системы антивирусной защиты или специализированных лечащих утилит. Лечение файлов не дает полной гарантии их восстановления. Поэтому после лечения проводится проверка восстановления данных файлов. Лечащие программы используются лишь в тех случаях, когда отсутствует резервная копия зараженных файлов с данными, либо восстановление уничтоженных файлов из резервной копии невозможно выполнить в допустимые сроки. После уничтожения вирусов и восстановления зараженных программ и файлов с данными проводится повторная антивирусная проверка. Перед повторной проверкой компьютер перезагружается через выключение и последующее включение. Если повторная проверка не выявила вирусов, то можно быть уверенным в их отсутствии. При обнаружении вредоносных программ в результате проверки рабочей станции, работающей в локальной сети, проводится проверка всех компьютеров, включенных в эту сеть и работающих с общими данными и программным обеспечением. В зависимости от критичности ситуации антивирусная проверка и выполнение действий по уничтожению вредоносных программ и восстановлению работоспособности системы проводится системным администратором ИСПДн ДОУ самостоятельно, либо инцидент эскалируется на уровень Администратора информационной безопасности ИСПДн ДОУ и лица, ответственного за обеспечение безопасности персональных данных.

7.3. Ответственность.

В рамках организации антивирусной защиты систем обработки персональных данных Администратор информационной безопасности ИСПДн ДОУ несёт ответственность за обеспечение правильного и непрерывного функционирования подсистемы антивирусной защиты. Администратор информационной безопасности производит мониторинг и анализ состояния антивирусной защиты персональных данных. Системный администратор ИСПДн ДОУ несёт ответственность за своевременное обновление антивирусных баз. Администратор информационной безопасности ИСПДн ДОУ несёт ответственность за настройку конфигурации средств антивирусной защиты, используемых для обеспечения безопасности персональных данных. Системный администратор ИСПДн ДОУ производит настройку параметров антивирусной защиты по поручению Администратора информационной безопасности ИСПДн ДОУ. Администратор информационной безопасности ИСПДн ДОУ несёт ответственность за надлежащее хранение эталонных дистрибутивов средств антивирусной защиты. Администратор информационной безопасности ИСПДн ДОУ и системный администратор ИСПДн ДОУ принимают участие в мероприятиях по реагированию на инциденты информационной безопасности, связанные с нарушением антивирусной безопасности.

8. Порядок обеспечения парольной защиты ИСПДн ДОУ.

8.1. Общие требования к использованию паролей.

При создании новой учётной записи для неё устанавливается первичный пароль. При создании первичного пароля используется опция, требующая смены пароля при первом входе в систему, и производится соответствующее уведомление владельца учетной записи о необходимости произвести смену пароля. Пользователи ИСПДн ДОУ всегда положительно идентифицируются до изменения пароля и предоставления нового пароля. Реинициализованные пароли принудительно меняются при первом входе в систему. Система автоматически блокирует учётную запись после 3 неудачных попыток ввода пароля. Блокировка учётной записи автоматически снимается по прошествии одной минуты, после чего пользователь вновь получает возможность авторизоваться в системе. Неудачные попытки авторизации регистрируются в системном журнале. Если система предоставляет автоматизированные инструменты для конфигурирования требуемых опций, то они соответствующим образом настроены. Хранение работником значений своих паролей на материальном носителе допускается только в личном,

опечатанном владельцем пароля сейфе, либо в сейфе у руководителя в опечатанном конверте или пенале.

8.2. Правила формирования пароля.

Персональные пароли генерируются специальными программными средствами Администраторами ИСПДн ДОУ с учетом следующих требований:

- длина пароля составляет не менее 7-ми символов;
- длина пароля для привилегированных пользователей составляет не менее 10-ти символов;
- в составе символов пароля обязательно присутствуют буквы в верхнем и нижнем регистрах, цифры и специальные символы (“ ~ ! @ # $ % ^ & * ( ) - + _ = \ | / ? ,);
- при смене пароля новое значение отличается от предыдущего не менее чем в 4- ех позициях;
- пароль может повторяться не менее чем после использования 5-ти различных паролей;
- личный пароль пользователь не имеет права сообщать никому;
- пароль не включает в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе.

8.3. Срок действия пароля.

Блокирование учетной записи с истекшим паролем автоматизировано. Если это не возможно, пользователь изменяет свои пароли. Учётные записи с некими административными привилегиями или привилегиями внутри приложения, активно используемые, связь компьютер-компьютер, редко используемые людьми msexch, sms, учетные записи владельца приложения, учетные записи для передачи файлов (FTP) Никогда, если не используется персоналом поддержки. В случае обнаружения подозрительной активности пароль должен меняться немедленно.

В случае увольнения работника удаление соответствующей ему учётной записи пользователя ИСПДн ДОУ производится немедленно после окончания последнего сеанса работы данного пользователя. Основанием для прекращения действий прав доступа к ИСПДн ДОУ является заявка в установленной форме. В случае компрометации персонального пароля пользователя системы немедленно выполняется внеплановая смена пароля.

8.4. Ответственность

Администратор информационной безопасности ИСПДн ДОУ несёт ответственность за корректное и непрерывное функционирование подсистемы парольной защиты систем, в которых производится обработка персональных данных. Администратор информационной безопасности ИСПДн ДОУ несёт ответственность за настройку конфигурации подсистемы парольной защиты. Системный администратор ИСПДн ДОУ производит настройку параметров парольной защиты по поручению Администратора информационной безопасности ИСПДн ДОУ.

Администратор информационной безопасности ИСПДн ДОУ и системный администратор ИСПДн ДОУ принимают участие в мероприятиях по реагированию на инциденты информационной безопасности, связанные с нарушением требований к организации парольной защиты ИСПДн ДОУ.