МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ«ДЕТСКИЙ САД «ЛЕСНАЯ СКАЗКА» ПГТ. МОЛОДЕЖНОЕ» СИМФЕРОПОЛЬСКОГО РАЙОНА РЕСПУБЛИКИ КРЫМ
ул.Садовая,2, пгт. Молодежное, Симферопольский район, РК, 297501
тел/факс (3652) 22-97-41, dslesskazka@mail.ru ОГРН 1159102023145, ИНН 9109009689

СОГЛАСОВАНО
На общем собрании трудового коллектива
Протокол от 20.10.17 №3

УТВЕРЖДЕНО
Заведующий МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное»
_____ М.Ф..Жаворонкина
Приказ № 105 от 23.10 2017 г.

Регламент
обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное»

1.Общие положения

Настоящий Регламент обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное» (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 «Лесная сказка» пгт. Молодежное» (далее – ИСПДн ДОУ) и телекоммуникационных сетях МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное» (далее- Учреждение).

Требования Регламента являются обязательными для работников Учреждения и третьих лиц, которые допущены к работе с персональными данными (далее - ПДн).

При приеме на работу работники Учреждения, 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 Учреждения и носит обязательный характер для всех работников Учреждения.

Обеспечение безопасности персональных данных в ИСПДн ДОУ .

Обеспечение безопасности ПДн в МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное» достигается за счет выполнения требований нормативных актов Российской Федерации в сфере защиты персональных данных и выполнения требований, установленных во внутренних нормативных документах МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное», всеми пользователями персональных данных.

Персональные данные субъектов ПДн, 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 Российской Федерации (далее - РФ) требованиям, обеспечивающим защиту информации, относящейся к персональным данным.

Реализация требований по обеспечению безопасности персональных данных в информационных системах возлагается на структурное подразделение или лицо, ответственное за обеспечение безопасности ПДн в ИСПДн ДОУ совместно со структурными подразделениями, обрабатывающими персональные данные согласно Перечню должностей служащих, замещение которых предусматривает осуществление обработки ПД.

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

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

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

В МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное» 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 ПДн и соблюдением условий использования средств защиты информации, а также соблюдением требований законодательства РФ по обработке ПДн в ИСПДн ДОУ.

2. Основные направления и методы защиты информации в ИСПДн

Структурное подразделение или назначенное лицо в МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное» , ответственное за обеспечение безопасности ПДн 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.

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

Лицо, ответственное за обеспечение безопасности ПДн, 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 подразделений (штатных работников), обрабатывающих персональные данные согласно должностным обязанностям, в соответствии с «Регламентом осуществления внутреннего контроля за обеспечением уровня защищенности ПДн и соблюдением условий использования средств защиты информации, а также соблюдением требований законодательства РФ по обработке ПДн в ИСПДн ДОУ .

Ежегодно о состоянии защиты персональных данных , 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, лицо, ответственное за обеспечение безопасности ПДн, лицу, ответственному за организацию обработки ПДн, а тот, соответственно, руководству МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное». В целях предотвращения несанкционированного доступа к техническим средствам обработки, хранения и передачи информации (далее - ТСПИ), их хищения и нарушения работоспособности ИСПДн самостоятельно или с привлечением аутсорсинговых организаций обеспечивается охрана и физическая защита помещений объектов информатизации, в которых располагаются технические средства ИСПДн ДОУ.

Структурное подразделение МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное», ответственного за обеспечение безопасности ПДн, обязано обеспечивать защиту всех компонент информационной структуры ИСПДн ДОУ, поддерживать в актуальном состоянии организационно-распорядительную, проектную и эксплуатационную документацию на систему защиты ПДн ИСПДн ДОУ», телекоммуникационные линии связи, ТСПИ, средства криптографической защиты информации (далее - СКЗИ) и т.д...

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 МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное» 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 ПДн МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное».

б) разграничение доступа Пользователей[1] и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) персональных данных и защиты информации;

---

[1] Пользователями ИСПДн «НО» являются лица, использующий при обработке персональных данных средства автоматизированной обработки информации, в том числе средства вычислительной

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, контролирующих органов Республики Крым;
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 МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное».

2.1. 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;
- 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 ПДн, и должностных лиц, осуществляющих эксплуатацию объектов информатизации

техники, программное обеспечение, электронные носители персональных данных и средства защиты информации

ИСПДн ДОУ; а методическое руководство и контроль за эффективностью предусмотренных мер защиты информации - на лицо, ответственное за обеспечение безопасности ПДн.

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 МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное» допускаются только санкционированные структурным подразделением или назначенным работником ДОУ, ответственным за обеспечение безопасности ПДн, 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 Структурное подразделение ДОУ ответственное за обеспечение безопасности ПДн, и совместно с его специалистами 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.

2.2. 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 ИСПДн 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 руководителем МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное», проводится определение уровня защищенности ИСПДн с составлением акта.

Основные мероприятия по предотвращению несанкционированного доступа к персональным данным МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное»:

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.

2.3. 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 ИСПДн 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.

2.4. Защита ПДн 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 структурное подразделение или назначенное лицо МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное» ответственное за обеспечение безопасности ПДн, 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.

3. Порядок резервирования и восстановления работоспособности ИСПДн

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

3.1. Порядок реагирования на инцидент[2]

Происшествие, вызывающее инцидент, может произойти в результате:

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

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

3.2.1. 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 МБДОУ «Детский сад «Лесная сказка» пгт. Молодежное» (помещения, в которых размещаются элементы ИСПДн и средства защиты) оборудованы средствами пожаротушения.

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

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн , 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:

---

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

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев использую методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн 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.).

3.2.2. 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 – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

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

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

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

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

Пронумеровано, прошито и скреплено
печатью на 9 (девять) листах.
Заведующий Жаворонкина М.О.