Муниципальное бюджетное дошкольное образовательное учреждение детский сад № 31 города Пензы «Волшебная страна»

ПРИНЯТО	**УТВЕРЖДАЮ**
на заседании Педагогического совета МБДОУ детского сада № 31 г. Пензы Протокол № 1 от 31.08.2026 г.	Заведующий МБДОУ детского сада № 31 г. Пензы Н. В. Егер Приказ № 183 от 31.08.2026 г.

ПОЛОЖЕНИЕ

о защите информации в Муниципальном бюджетном дошкольном образовательном учреждении детский сад № 31 города Пензы «Волшебная страна»

1. Общие положения

1.1. Настоящее Положение о защите информации в Муниципальном бюджетном дошкольном образовательном учреждении детском саду № 31 города Пензы «Волшебная страна» (далее – ДОУ) разработано в соответствии Федеральным законом № 273-ФЗ от 29.12.2012г. «Об образовании в Российской Федерации» (с изменениями и дополнениями), Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями), Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (с изменениями и дополнениями), Постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 18.02.2013 №21 (с изменениями и дополнениями) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями и дополнениями), а также Уставом ДОУ и другими нормативными правовыми актами Российской Федерации, регламентирующими деятельность учреждения.

1.2. Положение регулирует политику ДОУ по безопасности информационных и коммуникационных ресурсов и технологий и общий порядок обращения с документами, содержащими служебную информацию ограниченного распространения и устанавливает:

- объекты защиты информации и субъекты доступа к информации информационных систем и ресурсов;
- основные угрозы информационной безопасности (далее – информационная безопасность) ДОУ;
- основные принципы построения системы защиты информации ДОУ;
- меры, методы и средства обеспечения информационной безопасности ДОУ.

1.3. Настоящее Положение разработано с целью установления надлежащего порядка работы и создание безопасных условий для обучающихся и сотрудников ДОУ, а также исключения возможности проникновения посторонних лиц, выноса материальных ценностей, иных нарушений общественного порядка.

1.4. Данное Положение размещается на официальном сайте ДОУ в информационно-телекоммуникационной сети «Интернет».

2. Объекты, подлежащие защите

2.1. В ДОУ обрабатывается информация, содержащая сведения ограниченного распространения (служебная информация, персональные данные), и открытые сведения. Защите подлежат все информационные системы ДОУ независимо от их местонахождения, числящиеся на бухгалтерском учете ДОУ.

2.2. Основные объекты, подлежащие защите:

- информационные системы персональных данных (далее – ИСПДн), а также открытая (общедоступная) информация, необходимая для работы ДОУ независимо от формы и вида ее представления;
- процессы обработки информации в информационных системах ДОУ, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации.

2.3. Особенности объектов, подлежащих защите:

- объединение в единую систему большого количества технических средств обработки и передачи информации;
- необходимость обеспечения непрерывности функционирования ДОУ;
- высокая интенсивность информационных потоков;
- разнообразие категорий пользователей.

3. Цель и задачи системы обеспечения информационной безопасности

3.1. Субъекты доступа к информации при обеспечении информационной безопасности ДОУ являются:

- работники ДОУ, участвующие в информационном обмене в соответствии с возложенными на них должностными обязанностями;
- физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах ДОУ (в соответствии со ст.14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»);
- сотрудники внешних организаций, занимающихся разработкой, поставкой, ремонтом и обслуживанием оборудования или информационных систем.

3.2. Перечисленным субъектам доступа к информации необходимо обеспечить:

- своевременность доступа к необходимой им информации (ее доступность);
- достоверность (полноту, точность, актуальность, целостность) информации;
- конфиденциальность (сохранение в тайне) определенной части информации, защиту от навязывания ложной (недостоверной, искаженной) информации;
- возможность осуществления контроля и управления процессами обработки и передачи информации;
- защиту информации от незаконного распространения.

3.3. Целью защиты информации, на достижение которой направлено настоящее Положение, является защита от возможного нанесения субъектом доступа к информации материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи. Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

- доступности информации для авторизованных субъектов доступа (устойчивого функционирования системы, при котором авторизованные субъекты доступа имеют возможность получения необходимой информации);
- целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой в системах Учреждения и передаваемой по каналам связи;
- конфиденциальности – сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи. Необходимый уровень доступности, целостности и конфиденциальности информации обеспечивается методами и средствами, соответствующими множеству значимых угроз.

3.4. Основные задачи системы обеспечения информационной безопасности. Для достижения основной цели защиты и обеспечения указанных свойств информации система информационная безопасность должна обеспечивать решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, нарушению нормального функционирования систем;
- создание механизма оперативного реагирования на угрозы безопасности информации;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования систем Учреждения посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам - обеспечение доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей;
- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- защиту от несанкционированной модификации используемых в системах программных средств, а также защиту систем от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

3.5. Основные пути решения задач системы информационной безопасности ДОУ. Основные цели обеспечения информационной безопасности и решение перечисленных выше задач достигаются:

- учётом всех подлежащих защите информационных систем ДОУ;
- учётом действий персонала, осуществляющего обслуживание и модификацию программных и технических средств корпоративной информационной системы;
- полнотой, реальной выполнимостью и непротиворечивостью требований локальных нормативных актов ДОУ по вопросам обеспечения информационной безопасности;
- подготовкой должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению информационной безопасности;
- наделением каждого работника (пользователя) ДОУ минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам ДОУ;
- четким знанием и строгим соблюдением всеми пользователями информационных систем ДОУ требований локальных нормативных актов ДОУ по вопросам обеспечения информационной безопасности;
- персональной ответственностью за свои действия каждого работника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам ДОУ;
- непрерывным поддержанием необходимого уровня защищенности элементов информационных систем ДОУ;
- применением программно-аппаратных средств защиты информации и непрерывной административной поддержкой их использования;
- эффективным контролем над соблюдением пользователями информационных ресурсов Учреждения требований по обеспечению информационной безопасности.

4. Основные угрозы информационной безопасности

4.1. Существует два вида угроз информационной безопасности:

- искусственные – угрозы, вызванные деятельностью человека;
- естественные – угрозы, вызванные воздействиями на информационную систему и ее элементы объективных физических процессов техногенного характера или стихийных природных явлений, не зависящих от человека.

4.2. Наиболее значимыми угрозами информационной безопасности ДОУ (способами нанесения ущерба субъектам информационных отношений) являются:

- нарушение функциональности компонентов информационных систем ДОУ, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;
- нарушение целостности (искажение, подмена, уничтожение) информационных ресурсов ДОУ, а также фальсификация (подделка) документов;
- нарушение конфиденциальности (разглашение, утечка) персональных данных.

4.3. Основные источники угроз информационной безопасности ДОУ:

- непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей информационных систем ДОУ (в том числе работников, отвечающих за обслуживание и администрирование элементов информационных систем), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности элементов информационных систем;
- преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия легально допущенных к информационным ресурсам ДОУ пользователей (в том числе работников, отвечающих за обслуживание и администрирование элементов информационных систем), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности элементов информационных систем ДОУ;
- удаленное несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения (прежде всего через сеть Интернет), через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к информационным ресурсам;

- ошибки, допущенные при разработке элементов информационных систем ДОУ и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации);

- технические сбои элементов информационных систем.

4.4. Пути реализации угроз информационной безопасности ДОУ.

4.4.1. Пути реализации непреднамеренных искусственных угроз информационной безопасности ДОУ.

Работники ДОУ, являющиеся авторизованными субъектами доступа информационных систем, а также работники, обслуживающие отдельные элементы информационных систем, являются внутренними источниками случайных воздействий. Основные пути реализации непреднамеренных искусственных (субъективных) угроз информационной безопасности ДОУ (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

- неосторожные действия, приводящие к частичному или полному нарушению функциональности элементов информационных систем ДОУ;

- неосторожные действия, приводящие к разглашению информации ограниченного распространения или делающие ее общедоступной;

- разглашение, передача или утрата атрибутов разграничения доступа (ключей (логинов), паролей, ключевых носителей и т. п.);

- игнорирование установленных правил при работе с информационными ресурсами;

- проектирование алгоритмов обработки данных, разработка программного обеспечения с возможностями, представляющими опасность для функционирования информационных систем и информационной безопасности ДОУ;

- пересылка информации по ошибочному электронному адресу (устройства); ввод ошибочных данных;

- неосторожная порча носителей информации;

- неосторожное повреждение каналов связи;

- неправомерное отключение оборудования или изменение режимов работы элементов информационных систем;

- заражение компьютеров вирусами;

- несанкционированный запуск технологических программ, способных вызвать потерю работоспособности элементов информационных систем или осуществляющих необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных);

- некомпетентное использование, настройка или неправомерное отключение средств защиты.

4.4.2. Пути реализации преднамеренных искусственных (субъективных) угроз информационной безопасности.

Основные возможные пути умышленной дезорганизации работы, вывода элементов информационных систем из строя, несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить):

- умышленные действия, приводящие к частичному или полному нарушению функциональности элементов информационных систем ДОУ;

- действия по дезорганизации функционирования информационных систем ДОУ, хищение электронных документов и носителей информации; несанкционированное копирование электронных документов и носителей информации;

- умышленное искажение информации, ввод неверных данных;

- отключение или вывод из строя подсистем обеспечения функционирования элементов информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи);

- перехват данных, передаваемых по каналам связи и их анализ;

- незаконное получение атрибутов разграничения доступа (используя халатность пользователей, путем подделки, подбора пароля);

- несанкционированный доступ к ресурсам информационных систем с рабочих станций авторизованных субъектов доступа;

- хищение или вскрытие шифров криптозащиты информации;

- внедрение аппаратных и программных закладок с целью скрытно осуществлять доступ к

информационным ресурсам или дезорганизации функционирования элементов информационных систем ДОУ;

- незаконное использование элементов информационных систем, нарушающее права третьих лиц;

- применение подслушивающих устройств, фото и видео съемка для несанкционированного съема информации.

4.5. Пути реализации основных естественных угроз информационной безопасности:

- выход из строя оборудования информационных систем и оборудования обеспечения его функционирования;

- выход из строя или невозможность использования линий связи;

- пожары и стихийные бедствия.

4.6. Модель возможных нарушителей.

4.6.1. Типы нарушителей:

С учетом категории лиц, мотивации, квалификации, наличия специальных средств:

- Некомпетентный (невнимательный) пользователь – работник ДОУ (или подразделения внешней организации, занимающейся обслуживанием информационных систем ДОУ), предпринимающий попытки выполнения запрещенных действий, доступа к защищаемым ресурсам информационных систем с превышением своих полномочий, ввода некорректных данных, нарушения правил и регламентов работы с информацией, действуя по ошибке, некомпетентности или халатности без умысла и использующий при этом только штатные средства.

- Любитель – работник ДОУ (или подразделения внешней организации, занимающейся обслуживанием информационных систем Учреждения), пытающийся нарушить систему защиты без корыстных целей, умысла или для самоутверждения. При этом используются различные методы получения дополнительных полномочий доступа к ресурсам, недостатки в построении системы защиты и доступные ему штатные средства (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств), нештатные инструментальные и технологические программные средства, самостоятельно разработанные программы или стандартные дополнительные технические средства.

- Внутренний (внешний) злоумышленник - авторизованный субъект доступа (постороннее лицо) действующий целенаправленно (в том числе в сговоре с лицами, не являющимися работниками ДОУ). При этом используются методы и средства взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне ДОУ.

4.6.2. Внутренние нарушители:

Внутренним нарушителем может быть лицо из следующих категорий работников ДОУ:

- зарегистрированные пользователи и персонал, обслуживающий технические средства информационных систем ДОУ;

- работники, в том числе руководители, не являющиеся зарегистрированными пользователями и не допущенные к информационным ресурсам ДОУ, но имеющие доступ в здания и помещения;

- работники, в том числе руководители, задействованные в разработке и сопровождении программного обеспечения.

4.6.3. Внешние нарушители:

Внешним нарушителем может быть лицо из следующих категорий:

- работники ДОУ, с которыми прекращен (расторгнут) трудовой договор;

- представители внешних организаций, занимающихся разработкой, поставкой, ремонтом и обслуживанием элементов информационных систем;

- члены преступных организаций или лица, действующие по их заданию;

- лица, случайно или умышленно проникшие в локальную вычислительную сеть ДОУ из внешних телекоммуникационных сетей (хакеры);

- администраторы автоматизированных систем ДОУ, имеющие неограниченный доступ к информационным ресурсам компонентов корпоративной информационной системы. Администраторы автоматизированных систем могут относиться как к внешним, так и к внутренним нарушителям.

4.7. Утечка информации по техническим каналам. При проведении мероприятий и эксплуатации

технических средств устанавливаются следующие каналы утечки или нарушения целостности информации, нарушения работоспособности технических средств:

- побочные электромагнитные излучения информативного сигнала от технических средств ДОУ и линий передачи информации;

- наводки информативного сигнала, обрабатываемого техническими средствами локальной вычислительной сети ДОУ, на провода и линии, выходящие за пределы контролируемой зоны ДОУ, в т.ч. на цепи заземления и электропитания;

- электрические сигналы или радиоизлучения, обусловленные воздействием на средства передачи информации высокочастотных сигналов, создаваемых с помощью разведывательной аппаратуры, по эфиру и проводам, либо сигналов промышленных радиотехнических устройств (радиовещательные, радиолокационные станции, средства радиосвязи и т.п.), и модуляцией их

информативным сигналом;

- акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации;

- электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации;

- вибрационные сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации выделенных помещений;

- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности информационного обмена, в том числе электромагнитное, через специально внедренные электронные и программные средства («закладки»);

- перехват информации или воздействие на нее с использованием технических средств может вестись непосредственно из зданий, расположенных в непосредственной близости от объекта, мест временного пребывания, заинтересованных в перехвате информации или воздействии на нее лиц при посещении ими ДОУ, а также с помощью скрытно устанавливаемой автономной автоматической аппаратуры.

5. Основные принципы построения системы защиты информации

Построение системы защиты информации ДОУ и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

5.1. Законность.

Предполагает осуществление защитных мероприятий и разработку системы защиты информации ДОУ в соответствии с действующим законодательством в области информации, информатизации и защиты информации, а также других нормативных актов по информационной безопасности, утвержденных органами государственной власти.

Принятые меры информационной безопасности не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях к ресурсам конкретных информационных систем. Все пользователи информационных систем ДОУ должны иметь представление об ответственности за правонарушения в области информации.

5.2. Системность.

Системный подход к построению системы защиты информации в ДОУ предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности ДОУ. При создании системы защиты учитываются все слабые и наиболее уязвимые места информационных систем ДОУ, а также характер, возможные объекты и направления атак на неё со стороны нарушителей, пути несанкционированного доступа к информации. Система защиты должна строиться с учетом возможности появления принципиально новых путей реализации угроз безопасности.

5.3. Комплексность.

Комплексное использование методов и средств защиты информационных систем предполагает согласованное применение программных и технических средств при построении целостной системы защиты, перекрывающей все значимые каналы реализации угроз. Защита должна строиться

эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

5.4. Непрерывность защиты.

Для обеспечения этого принципа необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, перераспределение полномочий). Порядок получения доступа к информационным ресурсам регламентируется в Инструкции пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники.

5.5. Своевременность.

Предполагается упреждающий характер мер обеспечения информационной безопасности, то есть постановка задач по комплексной защите информации и реализация мер обеспечения безопасности информации на ранних стадиях разработки информационных систем. Разработка системы защиты ведется параллельно с разработкой и развитием самой подлежащей защите информационной системы.

5.6. Преемственность и совершенствование.

Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем ДОУ и систем информационной защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

5.7. Персональная ответственность.

Предполагает возложение ответственности за обеспечение информационной безопасности на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

5.8. Минимизация полномочий.

Предполагает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том случае и объёме, если это необходимо работнику для выполнения его должностных обязанностей.

5.9. Гибкость системы информационной безопасности.

Предполагает способность системы информационной безопасности реагировать на изменения внешней среды и условий осуществления ДОУ своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры ДОУ;
- изменение существующих или внедрение принципиально новых информационных систем;
- ввод в эксплуатацию новых технических средств.

5.10. Простота применения средств защиты.

Механизмы и методы системы защиты информации должны быть понятны и просты в использовании. Применение средств и методов защиты не связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не требует от пользователя выполнения малопонятных ему операций.

5.11. Обоснованность и техническая реализуемость.

Предполагает, что информационные технологии, технические и программные средства, средства и меры защиты информации реализуются на современном техническом уровне и обоснованы для достижения заданного уровня безопасности информации и экономической целесообразности, а также соответствуют установленным нормам и требованиям по безопасности информации.

5.12. Специализация и профессионализм.

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты осуществляется профессионально подготовленными специалистами защиты информации ДОУ.

5.13. Обязательность контроля.

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения

установленных правил обеспечения безопасности информации.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты осуществляется на основе применения средств оперативного контроля и регистрации и охватывает санкционированные и несанкционированные действия пользователей. Выявленные работниками ДОУ недостатки системы защиты информации доводятся до сведения непосредственного руководителя. О существенных недостатках сообщается руководителю ДОУ.

6. Меры, методы и средства обеспечения информационной безопасности

6.1. Меры обеспечения информационной безопасности.

6.1.1. Законодательные (правовые) меры обеспечения информационной безопасности к правовым мерам обеспечения информационной безопасности относятся действующие в Российской Федерации законодательные и иные нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры обеспечения информационной безопасности носят упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационных систем ДОУ.

6.1.2. Технологические меры обеспечения информационной безопасности к данному виду мер обеспечения информационной безопасности относятся технологические решения и приемы, направленные на уменьшение возможности совершения работниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

6.1.3. Организационные (административные) меры обеспечения информационной безопасности.

Организационные (административные) меры обеспечения информационной безопасности – это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации. Организационными (административными) мерами обеспечения информационной безопасности являются:

-Приказ заведующего ДОУ «Об организации пропускного режима в здании МБДОУ детского сада № 31 г. Пензы и его филиалов №№ 1,2,3»;

- анализ требований к элементам системы на основе заявок пользователей на обслуживание и модификацию аппаратных и программных ресурсов;

- обеспечение и контроль физической целостности (неизменности конфигурации) средств вычислительной техники;

- обучение пользователей;

- деятельность по обеспечению информационной безопасности;

- условия обработки информационных ресурсов конфиденциального характера, ответственность за нарушения установленного порядка пользования информационными ресурсами ДОУ.

6.1.4. Физические меры обеспечения информационной безопасности.

Физические меры обеспечения информационной безопасности основаны на применении механических, электронных или электронно-механических устройств, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к элементам информационных систем и защищаемой информации.

6.1.5. Технические меры обеспечения информационной безопасности.

Технические (аппаратно-программные) меры обеспечения информационной безопасности основаны на использовании электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации).

7. Особенности обработки информации, содержащей персональные данные

7.1. Все персональные данные субъекта ДОУ следует получать у него самого (для обучающихся ДОУ от родителей, законных представителей). Если персональные данные возможно получить только у

третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

Должностное лицо ДОУ должно сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению ПД и последствиях отказа дать письменное согласие на их получение.

7.2. ДОУ не имеет права получать и обрабатывать данные субъекта персональных данных о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

7.3. Субъект персональных данных самостоятельно принимает решение о предоставлении своих персональных данных и даёт согласие на их обработку.

7.4. Обработка указанных данных возможна без его согласия в соответствии со ст.6 Федеральным законом от 27.07.2006 №152 «О персональных данных».

7.5. Согласие на обработку персональных данных оформляется в письменном виде.

7.6. Письменное согласие на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе; наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных; цель обработки персональных данных; перечень персональных данных, на обработку которых дается согласие субъекта персональных данных; перечень действий с персональных данных на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных; срок, в течение которого действует согласие, а также порядок его отзыва.

7.7. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных по письменному запросу на имя заведующего ДОУ.

7.8. Субъект персональных данных имеет право на получение следующей информации:

- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ; перечень обрабатываемых персональных данных и источник их получения; сроки обработки персональных данных, в том числе сроки их хранения;

- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

7.9. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональных данных являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

7.10. Сведения о персональных данных должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться в персональных данных, относящиеся к другим субъектам персональных данных.

7.11. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при получении письменного запроса субъекта персональных данных или его законного представителя. Письменный запрос должен быть адресован на имя заведующего ДОУ или уполномоченного руководителем лицо.

7.12. Субъект в праве обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия персональных данных должностных лиц ДОУ при обработке и защите его персональных данных.

8. Обязанности и права должностных лиц

8.1. Руководитель ДОУ организует работу по построению системы защиты информационной системы. В частности:

- назначает ответственного за организацию защиты информации из числа сотрудников ДОУ;

- утверждает круг лиц, имеющих доступ к защищаемой информации и порядок их работы;

- утверждает комплект документов, определяющих политику в отношении защиты информации в ДОУ, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и

выявление нарушений законодательства РФ.

8.2. Ответственный за защиту информации:

- разрабатывает организационно-распорядительные документы по вопросам защиты информации при её обработке с помощью информационной системы;
- контролирует исполнение приказов и распоряжений вышестоящих организаций по вопросам обеспечения безопасности информации;
- обеспечивает защиту информации, циркулирующей на объектах информатизации;
- проводит систематический контроль работы систем защиты информации, применяемых в информационной системе, а также за выполнением комплекса организационных мероприятий по обеспечению безопасности информации;
- проводит инструктаж пользователей информационной системы;
- контролирует выполнение администратором информационной системы обязанностей по обеспечению функционирования систем защиты информации (настройка и сопровождение подсистемы управления доступом пользователя к защищаемым информационным ресурсам информационной системы, антивирусная защита, резервное копирование данных и т.д.);
- контролирует порядок учёта и хранения машинных носителей конфиденциальной информации;
- участвует в работах по внесению изменений в аппаратно-программную конфигурацию информационной системы;
- определяет порядок и осуществляет контроль ремонта средств вычислительной техники, входящих в состав информационной системы;
- принимает меры по оперативному изменению паролей при увольнении или перемещении сотрудников, имевших допуск к информационной системе;
- требует устранения выявленных нарушений и недостатков, дает обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации;
- требует от работников представления письменных объяснений по фактам нарушения режима конфиденциальности;
- в случае выявления попыток несанкционированного доступа к информации или попыток хищения, копирования, изменения, незамедлительно принимает меры пресечения и докладывает руководителю Учреждения;
- об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите информации.

8.3. Несоответствие мер установленным требованиям или нормам по защите информации, является нарушением и влечёт административное наказание ответственных лиц в соответствии с законодательством РФ.

9. Заключительные положения.

9.1. Настоящее Положение является локальным нормативным актом ДОУ, принимается на Педагогическом совете и утверждается (либо вводится в действие) приказом заведующего ДОУ.

9.2. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии действующим законодательством Российской Федерации.

9.3. Настоящее Положение принимается на неопределенный срок. Изменения и дополнения к Положению принимаются в порядке, предусмотренном п.9.1 настоящего Положения.

9.4. После принятия Положения (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически утрачивает силу.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДЕТСКИЙ САД № 31 ГОРОДА ПЕНЗЫ "ВОЛШЕБНАЯ СТРАНА", Егер Наталия Викторовна, Заведующая

16.11.26 12:18 (MSK) Сертификат F127617C06A5FDD2A0E7F7139436ACC4