Муниципальное бюджетное дошкольное образовательное учреждение
«Детский сад № 28 «Теремок»

Приложение № 41 к приказу
№ 80 от 11.08.2026г

ПРИНЯТО:
на Педагогическом совете
«Детский сад № 28 «Теремок»
Протокол № 6 от 10.08.2026 г.

Согласовано с Профсоюзным комитетом

Протокол от 11.08.2026 г. № 1

УТВЕРЖДЕНО:
Заведующий МБДОУ «Детский сад № 28 «Теремок»
_____ /Г.В.Карташева/
подпись расшифровка подписи
Приказ № 80 от 11.08.2026 г.

ПОЛОЖЕНИЕ
об обеспечении информационной безопасности в
МБДОУ «Детский сад № 28 «Теремок»

х. Большая Кирсановка
2026г

1. Общие положения

1.1. Настоящее **Положение об обеспечении информационной безопасности в ДОУ** разработано в соответствии с Федеральным законом от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации» с изменениями **от 25 апреля 2026 года [1]**, Трудовым кодексом Российской Федерации **[2]**, Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» с изменениями от 29 декабря 2025 года **[3]**, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» с изменениями от 24 июня 2025 года **[4]**, Постановлением Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» **[5]**, Приказом ФСТЭК РФ от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» с изменениями от 14 мая 2020 года **[6]**, а также Уставом дошкольного образовательного учреждения и другими нормативными правовыми актами Российской Федерации, регламентирующими деятельность организаций, осуществляющих образовательную деятельность.
1.2. Положение об обеспечении информационной безопасности в детском саду определяет систему правовых, организационных и технических мероприятий, направленных на обеспечение информационной безопасности воспитанников и работников в дошкольном образовательном учреждении.
1.3. Под информационной безопасностью дошкольного образовательного учреждения следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности. Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

1.4. Использование сети Интернет в ДОУ подчинено следующим принципам:

- соответствие образовательным целям;
- способствование гармоничному формированию и развитию личности;
- уважение закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей сети Интернет;
- приобретение новых навыков и знаний;
- расширение применяемого спектра учебных и наглядных пособий;
- социализация личности, введение в информационное общество.

1.5. К объектам информационной безопасности в ДОУ относятся:

- информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;
- информацию, защита которой предусмотрена законодательными актами Российской Федерации, в т. ч. персональные данные;
- средства и системы информатизации – средства вычислительной и организационной техники, локальной сети, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации.

1.6. Система информационной безопасности (далее СИБ) должна обязательно обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);
- целостность (точность и полноту информации и компьютерных программ);
- доступность (возможность получения пользователями информации в пределах их компетенции).

1.7. Обеспечение информационной безопасности осуществляется по следующим направлениям:

- *правовая защита* – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- *организационная защита* – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;
- *инженерно-техническая защита* – это использование различных технических средств, препятствующих нанесению ущерба.

2. Основные термины и их определения

2.1. ***Аутентификация*** – действия по проверке подлинности субъекта доступа в информационной системе [ГОСТ р 58833-2020, пункт 3.4].
2.2. ***Безопасность информации*** – состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность [ГОСТ р 50922-2006, пункт 2.4.5].
2.3. ***Государственная информационная система*** – информационная система, создаваемая в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях [3, часть 1 статьи 14].
2.4. ***Доступ к информации*** – возможность получения информации и ее использования [3, пункт 6 статьи 2].
2.5. ***Доступность*** – состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.
2.6. ***Защита информации от несанкционированного доступа*** – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации [ГОСТ р 50922-2006, пункт 2.3.6].
2.7. ***Защищаемая информация*** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации [ГОСТ р 50922-2006, пункт 2.5.2].
2.8. ***Идентификация*** – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов [ГОСТ р 58833-2020, пункт 3.24].
2.9. ***Информационная система*** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [3, пункт 3 статьи 2].
2.10. ***Информационные ресурсы*** – отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах

других видов) [ГОСТ р 58833-2020, пункт 3.25].
2.11. ***Информационные технологии*** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов [3, пункт 2 статьи 2].
2.12. ***Информация*** – сведения (сообщения, данные) независимо от формы их представления [3, пункт 1 статьи 2].
2.13. ***Контролируемая зона*** – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.
2.14. ***Конфиденциальность*** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [3, пункт 7 статьи 2].
2.15. ***Обработка персональных данных*** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных [4, пункт 3 статьи 3].
2.16. ***Оператор*** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными [4, пункт 2 статьи 3].
2.17. ***Персональные данные*** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу [4, пункт 1 статьи 3].
2.18. ***Угроза безопасности информации*** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации, и/или несанкционированными и/или непреднамеренными воздействиями на нее [ГОСТ р 51624-2000, пункт 3.1.17].
2.19. ***Уязвимость*** – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации [ГОСТ р 58142-2018/ISO/IEC TR 20004:2015, пункт 3.8].
2.20. ***Целостность*** – устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

3. Цели и задачи обеспечения безопасности информации

3.1. Главной целью обеспечения безопасности информации, циркулирующей в дошкольном образовательном учреждении, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа (далее по тексту – конфиденциальной или защищаемой информации) и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационной среды ДОУ.

3.2. Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в дошкольном образовательном учреждении;
- предотвращение нарушений прав личности воспитанников, работников ДОУ на сохранение конфиденциальности информации;
- предотвращение несанкционированных действий по блокированию информации.

3.3. Основными задачами обеспечения безопасности информации являются:

- соответствие положениям законодательных актов и нормативным требованиям по защите информации;
- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам дошкольного образовательного учреждения, нарушению нормального функционирования и развития ДОУ;
- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;
- эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;
- развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;
- развитие и совершенствование защищенного юридически значимого электронного документооборота;
- создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности;
- создание механизмов управления системой информационной безопасности.

4. Основные принципы построения системы обеспечения информационной безопасности

Построение системы обеспечения информационной безопасности ДОУ и его функционирование должны осуществляться в соответствии со следующими основными принципами:

4.1. *Законность.* Предполагает осуществление защитных мероприятий и разработку системы защиты информации дошкольного образовательного учреждения 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.

4.2. *Системность.* Системный подход к построению системы обеспечения информационной безопасности в дошкольном образовательном учреждении 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 дошкольного образовательного учреждения, 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.

4.3. *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.
4.4. *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 локальными нормативными актами и организационно-распорядительными документами дошкольного образовательного учреждения.
4.5. *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.
4.6. *Преемственность и совершенствование.* Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем дошкольного образовательного учреждения 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.
4.7. *Персональная ответственность.* Предполагает возложение ответственности за обеспечение информационной безопасности на каждого работника дошкольного образовательного учреждения 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.
4.8. *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.
4.9. *Гибкость системы информационной безопасности.* Предполагает способность системы информационной безопасности реагировать на изменения внешней среды и условий осуществления дошкольным образовательным учреждением 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.

4.10. ***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.
4.11. ***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.
4.12. ***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 необходимые лицензии в случаях, когда наличие таких лицензий предусмотрено законодательством Российской Федерации. Реализация административных мер и эксплуатация средств защиты осуществляется профессионально подготовленными специалистами защиты информации дошкольного образовательного учреждения.
4.13. ***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 дошкольного образовательного учреждения недостатки системы защиты информации доводятся до сведения непосредственного руководителя. О существенных недостатках сообщается заведующему ДОУ.

5. Меры, методы и средства обеспечения информационной безопасности

Меры обеспечения информационной безопасности:

5.1. К *законодательным (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 дошкольного образовательного учреждения.
5.2. К *технологическим* мерам обеспечения информационной безопасности относятся технологические решения и приемы, направленные на уменьшение возможности совершения работниками дошкольного образовательного учреждения ошибок и нарушений в рамках предоставленных им прав и полномочий.
5.3. *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:

- регламентация доступа в здание дошкольного образовательного учреждения;
- регламентация допуска работников к использованию информационных ресурсов;
- 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.

5.4. *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.
5.5. *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).

6. Правовые нормы обеспечения информационной безопасности

6.1. Дошкольное образовательное учреждение имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных воспитанников, работников ДОУ, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.
6.2. Детский сад обязан обеспечить сохранность конфиденциальной информации.

6.3. Администрация дошкольного образовательного учреждения:

- назначает ответственного за обеспечение информационной безопасности;
- назначает ответственного за организацию обработки персональных данных либо возлагает данные обязанности на ответственного за обеспечение информационной безопасности с закреплением соответствующих полномочий и обязанностей в приказе и должностной инструкции;
- издает локальные нормативные и распорядительные документы, определяющие порядок обработки и защиты информации и персональных данных, цели обработки персональных данных, категории субъектов и перечни обрабатываемых персональных данных, способы и сроки их обработки и хранения, порядок уничтожения персональных данных;
- определяет перечень сведений конфиденциального характера в соответствии с законодательством Российской Федерации;
- включает требования по защите информации и персональных данных в договоры и локальные нормативные акты в случаях, когда это необходимо и предусмотрено законодательством Российской Федерации;
- принимает меры по защите прав и законных интересов ДОУ в государственных органах и судах.

6.4. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ заведующего дошкольным образовательным учреждением о назначении ответственного за обеспечение информационной безопасности;
- должностные обязанности ответственного за обеспечение информационной безопасности;
- перечень защищаемых информационных ресурсов и баз данных;
- инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников ДОУ и др.

6.5. Порядок допуска сотрудников ДОУ к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
- ознакомление работника с нормами законодательства Российской Федерации и ДОУ об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
- инструктаж работника специалистом по информационной безопасности;
- контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

7. Использование сети Интернет

7.1. Использование сети Интернет в дошкольном образовательном учреждении осуществляется исключительно в целях реализации образовательной деятельности, воспитания, развития воспитанников, методического обеспечения образовательной деятельности и выполнения работниками своих должностных обязанностей.

7.2. Работники дошкольного образовательного учреждения вправе:

- размещать информацию в сети Интернет на интернет-ресурсах ДОУ;
- иметь учетную запись электронной почты на интернет-ресурсах ДОУ.

7.3. Работникам ДОУ запрещено размещать в сети Интернет и на образовательных ресурсах информацию:

- противоречащую требованиям законодательства Российской Федерации и локальным нормативным актам детского сада;
- не относящуюся к образовательной деятельности и не связанную с деятельностью ДОУ;
- нарушающую нравственные и этические нормы, требования профессиональной этики.

7.4. Запрет и снятие такого запрета на допуск пользователей к работе в сети Интернет устанавливает уполномоченное лицо, назначенное приказом заведующего детским садом.
7.5. Если в процессе работы пользователем будет обнаружен ресурс, содержимое которого не совместимо с целями образовательной деятельности, он обязан незамедлительно сообщить об этом уполномоченному лицу с указанием интернет-адреса (URL) и покинуть данный ресурс.

7.6. Уполномоченное лицо обязано:

- принять сообщение пользователя;

- принять меры по отключению выхода на данный ресурс с интернет-ресурсов дошкольного образовательного учреждения;
- если обнаруженный ресурс явно нарушает законодательство Российской Федерации – сообщить о нем по специальной «горячей линии» для принятия мер в соответствии с законодательством Российской Федерации (в течение суток).

Передаваемая информация должна содержать:

- интернет-адрес (URL) ресурса;
- тематику ресурса, предположения о нарушении ресурсом законодательства Российской Федерации либо несовместимости с задачами образовательной деятельности;
- дату и время обнаружения;
- информацию об установленных в ДОУ технических средствах ограничения доступа к информации.

8. Мероприятия по обеспечению информационной безопасности

8.1. Для обеспечения информационной безопасности в ДОУ требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности ДОУ;
- защита компьютеров, локальных сетей и сети подключения к системе Интернета;
- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и воспитанников детского сада;
- учет всех носителей конфиденциальной информации.

9. Организация работы с информационными ресурсами и технологиями

9.1. Система организации делопроизводства:

- учет всей документации дошкольного образовательного учреждения, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
- регистрация и учет всех входящих (исходящих) документов ДОУ в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, – классификация (письмо, приказ, распоряжение и т. д.);
- регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);
- особый режим уничтожения документов.

9.2. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:

9.2.1. Все документы, независимо от грифа, передаются исполнителю под подпись в журнале учета документов.
9.2.2. Документы, дела и издания с грифом «Для служебного пользования» должны храниться в служебных помещениях в надежно запираемых шкафах (сейфах), обеспечивающих их сохранность и исключающих доступ посторонних лиц.
9.2.3. Выданные для работы дела и документы с грифом «Для служебного пользования» («Ограниченного пользования») подлежат возврату в канцелярию в тот же день.
9.2.4. Передача документов исполнителю производится только через ответственного за организацию делопроизводства.

9.2.5. Запрещается выносить документы с грифом «Для служебного пользования» («Ограниченного пользования») за пределы ДОУ.
9.2.6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется акт приема-передачи документов в произвольной форме.
9.3. Для организации делопроизводства приказом заведующего дошкольным образовательным учреждением назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной заведующим ДОУ. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

10. О системном администрировании и обязанностях ответственного за информационную безопасность

10.1. Задачи, связанные с мерами системного администрирования, обеспечивающего информационную безопасность, являются частью работы системного администратора в дошкольном образовательном учреждении.
10.2. Для решения задач информационной безопасности системный администратор обязан:

- следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава и пр.);
- обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи;
- обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей;
- обеспечивать нормальное функционирование системы резервного копирования.

11. Антивирусная защита

Правила пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.).
11.1. Основным способом проникновения компьютерных вирусов на компьютер пользователя в настоящее время является Интернет и электронная почта. В связи с этим не допускается работа без организации антивирусной защиты. Антивирусная защита организуется посредством лицензионного антивирусного программного обеспечения или стандартного ПО в ОС.
11.2. Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически по мере выпуска обновлений производителем, а при невозможности – не реже одного раза в сутки.
11.3. За своевременное обновление антивирусного программного обеспечения отвечает системный администратор.

12. Обязанности и права должностных лиц дошкольного образовательного учреждения по обеспечению информационной безопасности

12.1. Заведующий дошкольным образовательным учреждением организует работу по построению системы обеспечения информационной безопасности и защиты персональных данных в ДОУ. В частности:

- назначает ответственного за организацию информационной безопасности;

- назначает ответственного за организацию обработки персональных данных либо возлагает обе функции на одного работника с разграничением его обязанностей и полномочий;
- утверждает перечень лиц, имеющих доступ к защищаемой информации и персональным данным, а также порядок такого доступа;
- утверждает локальные нормативные акты, определяющие политику в отношении обработки персональных данных, меры по обеспечению информационной безопасности, процедуры предотвращения и выявления нарушений законодательства Российской Федерации и порядок устранения последствий таких нарушений;
- организует контроль за соблюдением требований законодательства Российской Федерации в области информационной безопасности и персональных данных.

12.2. Ответственный за организацию информационной безопасности:

- разрабатывает организационно-распорядительные документы по вопросам информационной безопасности и 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;
- по поручению заведующего дошкольным образовательным учреждением запрашивает у работников письменные объяснения по фактам нарушения требований информационной безопасности и режима конфиденциальности в порядке, предусмотренном трудовым законодательством Российской Федерации;
- в случае выявления попыток несанкционированного доступа к информации или попыток хищения, копирования, изменения, незамедлительно принимает меры пресечения и докладывает заведующему дошкольным образовательным учреждением;
- 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.

12.3. Лица, виновные в нарушении требований законодательства и локальных нормативных актов дошкольного образовательного учреждения в области информационной безопасности и защиты персональных данных, несут ответственность в случаях и порядке, предусмотренных законодательством Российской Федерации.
12.4. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, ответственное лицо обязано незамедлительно принять меры по прекращению нарушения, сохранению сведений об инциденте и уведомить заведующего дошкольным образовательным учреждением.
Дошкольное образовательное учреждение проводит внутреннее расследование инцидента и направляет в уполномоченный орган по защите прав субъектов персональных данных:

- в течение двадцати четырех часов с момента выявления инцидента — сведения о произошедшем инциденте, его предполагаемых причинах и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий инцидента, а также сведения о лице, уполномоченном взаимодействовать с уполномоченным органом;
- в течение семидесяти двух часов с момента выявления инцидента — сведения о результатах внутреннего расследования и лицах, действия которых стали причиной выявленного инцидента, при наличии таких сведений.

13 Заключительные положения

13.1. Настоящее Положение об обеспечении информационной безопасности является локальным нормативным актом ДОУ, принимается на Педагогическом совете и утверждается (либо вводится в действие) приказом заведующего дошкольным образовательным учреждением.
13.2. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии действующим законодательством Российской Федерации.
13.3. Данное Положение об обеспечении информационной безопасности в ДОУ принимается на неопределенный срок. Изменения и дополнения к Положению принимаются в порядке, предусмотренном п. 13.1 настоящего Положения.
13.4. После принятия Положения (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически утрачивает силу.