Муниципальное бюджетное дошкольное образовательное учреждение Детский сад «Радость» с. Сергиевка Оренбургского района Оренбургской области.

Утверждаю:
Заведующий МБДОУ «Радость» с. Сергиевка
Татаренко Т.П._____
Приказом от 20.06.2024 № 1- ОД

ПОЛОЖЕНИЕ

об информационной безопасности Муниципальное бюджетное дошкольное образовательное учреждение Детский сад «Радость» с. Сергиевка Оренбургского района Оренбургской области.

с. Сергиевка,
МО Оренбургский район
2024г.

1. Общие положения

1.1. Информационная безопасность является одним из составных элементов комплексной безопасности в Муниципальном бюджетном дошкольном образовательном учреждении Детский сад «Радость» с. Сергиевка Оренбургского района Оренбургской области (далее — МБДОУ), порядок организации работ по ее созданию и функционированию.

1.2. Данное положение разработано в соответствии с Федеральным законом Российской Федерации от 29 декабря 2012 г. № 273-ФЗ "Об образовании в Российской Федерации", Трудовым кодексом РФ от 30.12.2001 № 197-ФЗ (с изм. и доп.), Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" от 29.12.2010 N 436-ФЗ (последняя редакция), Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция), Федеральный закон от 25 июля 2002 г. N 114-ФЗ "О противодействии экстремистской деятельности", Федеральный закон от 2 июля 2013 г. N 187-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях" и имеет статус локального нормативного акта образовательной организации. Если нормами действующего законодательства РФ предусмотрены иные требования, чем настоящим Положением, применяются нормы законодательства РФ.

1.3. Под информационной безопасностью МБДОУ 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 образовательной организации 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 МБДОУ относятся:

- информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;
- информацию, защита которой предусмотрена законодательными актами РФ, 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 зашита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная зашита – 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;

1.8. Информационная безопасность включает:

- защиту интеллектуальной собственности образовательной организации;
- защиту компьютеров, локальных сетей и сети подключения к системе Интернета;
- организацию защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся;
- учет всех носителей конфиденциальной информации.

2. Цели и задачи обеспечения безопасности информации

2.1. Главной целью обеспечения безопасности информации, циркулирующей в МБДОУ, 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 МБДОУ.

2.2. Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в МБДОУ;
- предотвращение нарушений прав личности обучающихся, работников МБДОУ на сохранение конфиденциальности информации;
- предотвращение несанкционированных действий по блокированию информации.

2.3. 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 МБДОУ, нарушению нормального функционирования и развития МБДОУ;

- 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.

2.4. В целях реализации стоящих перед системой обеспечения информационной безопасности задач в МБДОУ устанавливаются:

- защита персональных данных персонала и обучающихся;

- контроль за использованием электронных средств информационного обеспечения деятельности МБДОУ по прямому назначению;

- противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности МБДОУ нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами;

- внутрисетевой контроль за перемещением информации;

- принятие мер к воспрещению доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими;

- проверка целесообразности использования персоналом и обучающимися МБДОУ интернет - ресурса, предоставляемого им администрацией, анализ допускаемых нарушений и принятие мер к недопущению его нецелевого использования средствами технического противодействия;

- обучение персонала МБДОУ по вопросам обеспечения информационной безопасности;

- контроль за правильностью использования имеющихся в МБДОУ средств телефонной и радиосвязи;

- защита персональных данных персонала и обучающихся - мероприятия по недопущению несанкционированного доступа к персональным данным персонала и обучающихся МБДОУ при их обработке с использованием средств автоматизации или без использования таких средств;

- контроль за использованием электронных средств информационного обеспечения деятельности МБДОУ по прямому назначению - плановые и внеплановые проверки. Содержание проверок - сложившаяся практика использования персональных компьютеров, мультимедийных систем, интерактивных средств обучения, телевизионных приемников, копировально-множительной аппаратуры и сканирующих устройств, электронных средств проектирования и инженерной

графики, телефонных аппаратов и радиостанций, а также программного обеспечения к указанным средствам и устранение выявленных в ходе проверок недостатков;

- противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности МБДОУ нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами - контроль за используемым программным обеспечением и проверка его подлинности, ограничение в использовании съемных и компакт-дисков сотрудниками и обучающимися МБДОУ;

- принятие мер к воспрещению доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими, постоянное ознакомление со сведениями об информационных материалах признанных в соответствии с действующим законодательством экстремистскими, доведение этих сведений до администрации и персонала МБДОУ и принятие мер к воспрещению доступа к этим материалам (мерами технического противодействия - в отношении материалов находящихся в сети Интернет, и путем изъятия – в отношении печатных изданий, хранящихся в методическом кабинете МБДОУ);

- проверка целесообразности использования персоналом и обучающимися МБДОУ интернет - ресурса, предоставляемого им администрацией, анализ допускаемых нарушений и принятие мер к недопущению его нецелевого использования средствами технического противодействия - установление и доведение в форме инструкций до персонала и обучающихся МБДОУ общедоступных требований об ограничениях при использовании ресурса, предоставляемого им администрацией МБДОУ, постоянный контроль за выполнением указанных ограничений, разработка, внедрение, и применение технических (программных) средств противодействия возникающим нарушениям, либо злоупотреблениям;

- обучение персонала МБДОУ по вопросам обеспечения информационной безопасности - проведение занятий с персоналом в целях формирования у них соответствующих знаний, умений и навыков позволяющих соблюдать требования по обеспечению информационной безопасности МБДОУ;

- контроль за правильностью использования имеющихся в МБДОУ средств телефонной и радиосвязи - выявление фактов нецелевого использования средств телефонной и радиосвязи и принятие мер технического и организационного характера по их недопущению.

3. Правовые нормы обеспечения информационной безопасности

3.1. МБДОУ имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников МБДОУ, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

3.2. МБДОУ обязана обеспечить сохранность конфиденциальной информации.

3.3. Администрация МБДОУ:

- назначает ответственного за обеспечение информационной безопасности;

- издает нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;

- имеет право включать требования по обеспечению информационной безопасности в коллективный договор;

- имеет право включать требования по защите информации в договоры по всем видам деятельности;

- разрабатывает перечень сведений конфиденциального характера;

- имеет право требовать защиты интересов школы со стороны государственных и судебных инстанций.

3.4. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ заведующий МБДОУ 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 МБДОУ и др.

3.5. Порядок допуска сотрудников МБДОУ к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;

- ознакомление работника с нормами законодательства РФ и МБДОУ 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.

4. Использование сети Интернет

4.1. Использование сети Интернет в МБДОУ осуществляется в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области компьютерной грамотности лицо может осуществлять доступ к ресурсам не образовательной направленности.

4.2. Работники МБДОУ вправе:

- размещать информацию в сети Интернет на Интернет-ресурсах МБДОУ;

- иметь учетную запись электронной почты на Интернет-ресурсах МБДОУ.

4.3. Работникам МБДОУ запрещено размещать в сети Интернет и на образовательных ресурсах информацию:

- противоречащую требованиям законодательства РФ и локальным нормативным актам МБДОУ;

- не относящуюся к образовательному процессу и не связанную с деятельностью МБДОУ;

- нарушающую нравственные и этические нормы, требования профессиональной этики.

4.4. Обучающиеся МБДОУ вправе:

- использовать ресурсы, размещенные в сети Интернет, в том числе Интернет-ресурсы МБДОУ, в порядке и на условиях, которые предусмотрены настоящим Положением;

- размещать информацию и сведения на Интернет-ресурсах МБДОУ.

4.5. Обучающемуся запрещено:

- находиться на ресурсах, содержание и тематика которых недопустима для несовершеннолетних и/или нарушает законодательство РФ;

- осуществлять любые сделки через интернет;

- загружать файлы на компьютер МБДОУ без разрешения уполномоченного лица;

- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

4.6. Запрет и снятие такого запрета на допуск пользователей к работе в сети Интернет устанавливает уполномоченное лицо, назначенное приказом заведующего МБДОУ.

4.7. Если в процессе работы пользователем будет обнаружен ресурс, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно сообщить об этом уполномоченному лицу с указанием интернет-адреса (URL) и покинуть данный ресурс.

4.8. Уполномоченное лицо обязано:

- принять сообщение пользователя;

- принять меры по отключению выхода на данный ресурс с Интернет-ресурсов МБДОУ;

- если обнаруженный ресурс явно нарушает законодательство РФ - сообщить о нем по специальной «горячей линии» для принятия мер в соответствии с законодательством РФ (в течение суток).

Передаваемая информация должна содержать:

- интернет-адрес (URL) ресурса;

- тематику ресурса, предположения о нарушении ресурсом законодательства РФ либо несовместимости с задачами образовательного процесса;

- дату и время обнаружения;

- информацию об установленных в образовательной организации технических средствах ограничения доступа к информации.

5. Мероприятия по обеспечению информационной безопасности

5.1. Для обеспечения информационной безопасности в МБДОУ требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности МБДОУ;

- защита компьютеров, локальных сетей и сети подключения к системе Интернета;

- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся МБДОУ;

- учет всех носителей конфиденциальной информации.

6. Организация работы с информационными ресурсами и технологиями

6.1. Система организации делопроизводства:

- учет всей документации МБДОУ, в т.ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;

- регистрация и учет всех входящих (исходящих) документов МБДОУ 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.

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

6.2.1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.

6.2.2. Документы, дела и издания с грифом «Для служебного пользования» («Ограниченного пользования») должны храниться в служебных помещениях в надежно запираемых и опечатываемых МБДОУ. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.

6.2.3. Выданные для работы дела и документы с грифом «Для служебного пользования» («Ограниченного пользования») подлежат возврату в канцелярию в тот же день.

6.2.4. Передача документов исполнителю производится только через ответственного за организацию делопроизводства.

6.2.5. Запрещается выносить документы с грифом «Для служебного пользования» за пределы МБДОУ.

6.2.6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.

6.3. Для организации делопроизводства приказом заведующего МБДОУ назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной заведующего МБДОУ. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

7. О системном администрировании и обязанностях ответственного за информационную безопасность

7.1. Задачи, связанные с мерами системного администрирования, обеспечивающего информационную безопасность, являются частью работы системного администратора в МБДОУ Д/с «Радость» с. Сергиевка

7.2. 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.

8. Антивирусная защита

8.1. Правила пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.). 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.

8.2. Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в день.

8.3. За своевременное обновление антивирусного программного обеспечения отвечает системный администратор.