Муниципальное бюджетное дошкольное образовательное учреждение № 111
«Детский сад комбинированного вида»

Приказ

от 22 октября 2019 г. № 61

«Об ответственном лице за информационную безопасность дошкольного образовательного учреждения»

Руководствуясь требованиями Федерального закона от 29.12.2010 № 436 – ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (с изменениями от 2012г), Федерального закона от 27.07.2006 № 152 «О персональных данных» с целью обеспечения режима конфиденциальности, в целях осуществления ограничения доступа работников детского учреждения к ресурсам и материалам сети Интернет, не имеющих отношения к образовательному процессу, в целях обеспечения информационной безопасности в ДОУ

Приказываю:

1. Назначить ответственного за информационную безопасность в ДОУ заведующего Москвину Ирину Юрьевну.
2. Утвердить и ввести в действие
   - ✓ Положение об ответственном лице за информационную безопасность (Приложение 1)
   - ✓ Положение об информационной безопасности (Приложение 2)
   - ✓ Инструкцию для сотрудников ОУ о порядке действий при осуществлении контроля за использованием работниками учреждения сети Интернет (Приложение 3)
3. Ознакомить с приказом всех работников МБДОУ
4. Разместить настоящий приказ на официальном сайте учреждения в течении 10 рабочих дней со дня его издания
5. Контроль за исполнением оставляю за собой

Заведующий МБДОУ № 111 _____ И.Ю. Москвина

МОСКВИНА ИРИНА ЮРЬЕВНА

Подписано цифровой подписью: МОСКВИНА ИРИНА ЮРЬЕВНА
Дата: 2024.07.29 15:01:05 +07'00'

МОСКВИНА ИРИНА ЮРЬЕВНА

Подписано цифровой подписью: МОСКВИНА ИРИНА ЮРЬЕВНА
Дата: 2024.07.29 15:01:49 +07'00'

Приложение № 1
к приказу №61
от «22» октября 2019 г.

Положение об ответственном лице за информационную безопасность Муниципального бюджетного дошкольного образовательного Учреждения № 111 «Детский сад комбинированного вида»

1. Общие положения

Ответственное лицо за информационную безопасность дошкольного образовательного учреждения (далее Оператор) назначается в целях выполнения требований действующего законодательства Российской Федерации, иных нормативно-правовых актов, регламентирующих обеспечение защиты информации, в том числе обеспечение безопасности при обработке персональных данных, а также обеспечение защиты и безопасности информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных.

2. Структура

Ответственное лицо за информационную безопасность дошкольного образовательного учреждения назначается приказом заведующего ДОУ.

3. Задачи

Основные задачи ответственного лица заключаются в следующем.

1. Разработка и реализация комплекса организационных и технических мер, направленных на выполнение установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.
2. Обеспечение постоянного контроля в подразделениях Оператора за выполнением установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.
3. Разработка и внесение предложений по совершенствованию и развитию корпоративной системы обеспечения безопасности и защиты информации, в том числе персональных данных.

4. Функции

Для выполнения поставленных задач осуществляет следующие функции.

1. Готовит и представляет на рассмотрение руководству проекты локальных нормативных актов по вопросам обеспечения защиты информации, в том числе персональных данных.

2. Организует и проводит во взаимодействии с заинтересованными подразделениями классификацию информационных систем на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных в соответствии с установленными требованиями.

3. Разрабатывает и реализует комплекс организационных и мер по обеспечению защиты информации от:

- неправомерного доступа;
- уничтожения;
- модифицирования;
- блокирования;
- копирования;
- предоставления;
- распространения;
- а также от иных неправомерных действий в отношении такой информации.

4. Для защиты информации, в том числе персональных данных от неправомерного доступа обеспечивает:

- контроль за строгим соблюдением принятого Порядка доступа к конфиденциальной информации, в том числе к персональным данным; - предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации; - своевременное обнаружение фактов несанкционированного доступа к информации;

- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации; - возможность незамедлительного восстановления информации,

модифицированной или уничтоженной вследствие несанкционированного доступа к ней.

5. Ответственное лицо при создании и эксплуатации корпоративных информационных систем:

- самостоятельно разрабатывает и внедряет методы и способы защиты информации, соответствующие установленным требованиям; - согласовывает исполнителю планируемые для использования в целях защиты информации методы и способы при условии их соответствия установленным требованиям.

- разрабатывает и реализует меры организационного и технического по недопущению воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

- организует и(или) проводит экспертизу технических средств, используемых при обработке информации на предмет соответствия

возможностей защиты информации указанных средств установленным требованиям.

6. Разрабатывает и реализует меры по информированию и обучению персонала Оператора, в том числе вновь принимаемых на работу лиц, по вопросам защиты информации и персональных данных.

7. Контролирует выполнение установленных требований по:

- осуществлению обмена персональными данными при их обработке в информационных системах по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств;
- размещению информационных систем, специального оборудования и охране помещений, в которых ведется работа с персональными данными, организации режима обеспечения безопасности в этих помещениях в части обеспечения сохранности носителей персональных данных и средств защиты информации, а также исключения возможности неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;
- соблюдению парольной защиты;
- соблюдению установленного регламента работы с электронной почтой;
- соблюдению требований к программному обеспечению и его использованию.

8. В соответствии с установленными нормативно-правовыми актами требованиями обеспечивает:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к работе с персональными данными в информационной системе;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- разбор и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности

персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

- описание системы защиты информации, в том числе персональных данных;
- ежегодное планирование работы по совершенствованию системы защиты информации, в том числе персональных данных;
- подготовку и предоставление отчетов заведующему, а также по требованию надзорных и иных уполномоченных органов об организационных и технических мероприятиях по защите информации, в том числе персональных данных;
- постоянный контроль за обеспечением уровня защищенности информации.

5. Взаимодействие

Для решения поставленных задач и осуществления предусмотренных настоящим Положением функций Ответственное лицо взаимодействует:

- с руководителем ДОУ и его заместителями;
- с любыми иными подразделениями;
- с государственными, муниципальными органами, учреждениями и организациями, с надзорными органами, а также с иными органами, предприятиями и организациями.

6. Ответственность

Ответственное лицо за информационную безопасность несет ответственность перед руководством ДОУ согласно действующему законодательству, нормативно-правовым и локальным нормативным правовым актам за обеспечение:

- выполнения поставленных перед подразделением задач и функций,
- работы с документами и их сохранности, своевременного и качественного исполнения поручений и обращений,
- выполнения требований правил внутреннего трудового распорядка,
- соблюдения в подразделении правил противопожарной безопасности.
- требований выполнения действующего законодательства Российской Федерации, иных нормативно-правовых документов, регламентирующих обеспечение защиты информации, в том числе обеспечение безопасности при обработке персональных данных;
- обязанностей, предусмотренных Трудовым кодексом РФ, правилами внутреннего трудового распорядка, коллективным договором, настоящим Положением, трудовыми договорами и должностными инструкциями.

Приложение № 2
к приказу № 61
от «22» октября 2019 г.

ПОЛОЖЕНИЕ
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.Общие положения

1.1. Настоящее Положение об информационной безопасности (далее по тексту Положение) Муниципального бюджетного дошкольного образовательного учреждения № 111 «Детский сад комбинированного вида» (далее ДОУ) разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (редакция от 28.06.2010).

1.2. Настоящее Положение определяет задачи, функции, обязанности, ответственность и права ответственных за информационную безопасность.

1.3. Ответственные за информационную безопасность назначаются приказом заведующего ДОУ.

1.4. Ответственные за информационную безопасность подчиняются заведующему ДОУ.

1.5. Ответственные за информационную безопасность в своей работе руководствуются настоящим Положением.

1.6. Ответственные за информационную безопасность в пределах своих функциональных обязанностей обеспечивают безопасность информации, обрабатываемой, передаваемой и хранимой при помощи информационных средств в ДОУ.

2. Основные задачи и функции, ответственных за информационную безопасность

2.1. Основными задачами ответственных за информационную безопасность являются:

2.1.1. Организация эксплуатации технических и программных средств защиты информации.

2.1.2. Текущий контроль работы средств и систем защиты информации.

2.1.3. Организация и контроль резервного копирования информации на сервере ЛВС.

2.1.4. Ответственные за информационную безопасность выполняют следующие основные функции:

2.1.5. Разработка инструкций по информационной безопасности: инструкции по организации антивирусной защиты, инструкции по безопасной работе в Интернете.

2.1.6. Обучение персонала и пользователей ПК правилам безопасной обработки информации и правилам работы со средствами защиты информации.

2.1.7. Организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в ДОУ.

2.1.8. Текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации.

2.1.9. Контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нем.
2.1.10. Контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК.

2.1.11. Контроль пользования Интернетом.

3. Обязанности ответственных за информационную безопасность

3.1. Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных на них обязанностей.

Немедленно докладывать заведующему ДОУ о выявленных нарушениях и несанкционированных действиях пользователей и сотрудников, а также принимать необходимые меры по устранению нарушений.

3.2. Совместно с программистами принимать меры по восстановлению работоспособности средств и систем защиты информации.

3.3. Проводить инструктаж сотрудников и пользователей ПК по правилам работы с используемыми средствами и системами защиты информации.

3.4. Создавать и удалять учетные записи пользователей.

3.5. Администрировать работу сервера ЛВС, размещать и классифицировать информацию на сервере ЛВС.

3.6. Устанавливать по согласованию с заведующим ДОУ критерии доступа пользователей на сервер ЛВС.

3.7. Формировать и представлять пароли для новых пользователей, администрировать права пользователей.

3.8. Отслеживать работу антивирусных программ, проводить один раз в неделю полную проверку компьютеров на наличие вирусов.

3.9. Выполнять регулярно резервное копирование данных на сервере, при необходимости восстанавливать потерянные или поврежденные данные.

3.10. Ежемесячно подавать заведующему ДОУ статистическую информацию по пользованию Интернетом.

3.11. Вести учет пользователей «точки доступа к Интернету». В случае необходимости лимитировать время работы пользователя в Интернете и объем скачиваемой информации.

3.12. Сообщать незамедлительно заведующему ДОУ о выявлении случаев несанкционированного доступа в Интернет.

4. Права ответственных за информационную безопасность

4.1. Требовать от сотрудников и пользователей компьютерной техники безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения и электронных платежей.

4.2. Готовить предложения по совершенствованию используемых систем защиты информации и отдельных их компонентов.

5. Ответственность ответственных лиц за информационную безопасность

5.1. На ответственных за информационную безопасность возлагается персональная ответственность за качество проводимых ими работ по обеспечению защиты информации в соответствии с функциональными обязанностями, определенными настоящим Положением.

Приложение № 3
к приказу № 61
от «22» октября 2019 г.

ИНСТРУКЦИЯ

для сотрудников образовательного учреждения о порядке действий при осуществлении контроля за использованием работниками учреждения сети Интернет

1.Настоящая Инструкция устанавливает порядок действий при обнаружении сотрудниками образовательного учреждения:

- возможности доступа работников учреждения к потенциально опасному контенту;

- вызванного техническими причинами отказа доступа к контенту, не представляющему опасности работников учреждения, доступ к которому не противоречит принятым нормативным актам на федеральном уровне, а также на уровне образовательного учреждения.

2. Контроль за использованием работниками учреждения сети Интернет осуществляют ответственные лица во время использования сети Интернет для свободной работы работников учреждения – администратор точки доступа к сети Интернет в образовательном учреждении.

3. Ответственное лицо, осуществляющее контроль за использованием работниками учреждения сети Интернет:

- определяет время и место работы работников учреждения в сети Интернет с учетом использования соответствующих технических возможностей в образовательном процессе, а также длительность сеанса работы одного работника учреждения;

- способствует осуществлению контроля за объемом трафика образовательного учреждения в сети Интернет;

- наблюдает за использованием компьютеров и сети Интернет работниками учреждения;

- запрещает дальнейшую работу работника учреждения в сети Интернет в случае нарушения работником учреждения порядка использования сети Интернет и предъявляемых работникам учреждения требований при работе в сети Интернет;

- не допускает работника учреждения к работе в сети Интернет в предусмотренных Правилами использования сети Интернет случаях;

- принимает необходимые меры для пресечения дальнейших попыток доступа к ресурсу/группе ресурсов, несовместимых с задачами образования.

4. При обнаружении информации, в отношении которой у лица, осуществляющего контроль за использованием работниками учреждения сети Интернет, возникают основания предполагать, что такая информация относится к числу запрещенной для распространения в соответствии с законодательством Российской Федерации или иному потенциально опасному для работников учреждения контенту, ответственное лицо информирует администратора точки

доступа к сети Интернет или руководителя образовательного учреждения, которые принимают необходимые решения.

5. При обнаружении вызванного техническими причинами отказа доступа к контенту, доступ к которому не противоречит принятым нормативным актам на федеральном уровне, уровне субъекта Российской Федерации, муниципальном уровне, а также на уровне образовательного учреждения, ответственное лицо информирует соответствующие технические службы, осуществляющие контентную фильтрацию.

ПРАВИЛА ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ

1. Общие положения:

1.1. Настоящие Правила регулируют условия и порядок использования сети Интернет через ресурсы образовательного учреждения (далее – Детский сад) педагогическими работниками образовательного учреждения.

1.2. Настоящие Правила имеют статус локального нормативного акта Детского сада. Если нормами действующего законодательства Российской Федерации предусмотрены иные требования, чем настоящими Правилами, применяются нормы действующего законодательства Российской Федерации.

1.3. Использование сети Интернет в Детском саде подчинено следующим принципам:

• соответствия образовательным целям;

• способствования гармоничному формированию и развитию личности;

• уважения закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей Интернета;

• приобретения новых навыков и знаний;

• расширения применяемого спектра учебных и наглядных пособий;

• социализации личности, введения в информационное общество.

2. Организация и политика использования сети Интернет в ДОУ.

2.1. Использование сети Интернет в ДОУ возможно исключительно при условии ознакомления и согласия лица, пользующегося сетью Интернет в ДОУ, с настоящими Правилами. Ознакомление и согласие удостоверяется подписью лица в листе ознакомления и согласия с Правилами.

2.2. Заведующий является ответственным за обеспечение эффективного и безопасного доступа к сети Интернет в ДОУ, а также за внедрение соответствующих технических, правовых и других механизмов в ДОУ.

2.3. Непосредственное определение политики доступа в Интернет осуществляет Совет ДОУ совместно с администрацией.

• принимают решение о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет, содержащим информацию, не совместимую с задачами образовательного процесса;

• определяют характер и объем информации, публикуемой на Интернет-ресурсах ДОУ;

• дает заведующий ДОУ рекомендации о назначении и освобождении от исполнения своих функций лиц, ответственных за непосредственный контроль безопасности работы в сети Интернет и соответствия ее целям и задачам образовательного процесса.

2.4. При использовании сети Интернет в ДОУ осуществляется доступ только на ресурсы, содержание которых не противоречит законодательству Российской

Федерации и не являются несовместимым с целями и задачами образования и воспитания детей.

Проверка такого соответствия осуществляется с помощью специальных технических средств и программного обеспечения контекстного ограничения доступа, установленного в ДОУ или предоставленного оператором услуг связи.

Использование сети Интернет в ДОУ без применения данных технических средств и программного обеспечения (например, в случае технического отказа) допускается только с индивидуального разрешения заведующего ДОУ.

В связи с тем, что технические средства и программное обеспечение не могут осуществлять полную фильтрацию ресурсов сети Интернет связанное с частотой обновления ресурсов сети, возможна опасность столкновения с ресурсом, содержание которого противоречит законодательству Российской Федерации и является несовместимым с целями и задачами образовательного процесса, ДОУ не несет ответственности за случайный доступ к подобной информации, размещенной не на сайте Детского сада.

2.5. Принятие решения о политике доступа к ресурсам/группам ресурсов сети Интернет принимается Советом ДОУ совместно с администрацией самостоятельно либо с привлечением внешних экспертов, в качестве которых могут привлекаться:

• педагоги Детского сада и других образовательных учреждений;

• лица, имеющие специальные знания либо опыт работы в рассматриваемой области;

• представители органов управления образованием. При принятии решения, эксперты руководствуются:

• законодательством Российской Федерации;

• специальными познаниями, в том числе полученными в результате профессиональной деятельности по рассматриваемой тематике;

• интересами воспитанников, целями ДОУ;

• рекомендациями профильных органов и организаций в сфере классификации ресурсов сети Интернет.

2.6. Отнесение определенных категорий и/или ресурсов в соответствующие группы, доступ к которым регулируется техническим средствами и программным обеспечением контекстного технического ограничения доступа к информации, технически осуществляется лицом, уполномоченным заведующим ДОУ.

Категории ресурсов, в соответствии с которыми определяется политика использования сети Интернет в ДОУ и доступ, к которым регулируется техническими средствами и программным обеспечением контекстного технического ограничения доступа к информации, определяются в установленном порядке.

3. Организация использования сайта МБДОУ.

3.1. Принципами размещения информации на сайте ДОУ являются:

- соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;
- защита персональных данных воспитанников и сотрудников;
- достоверность и корректность информации.

3.2. Персональные данные воспитанников (фамилия и имя, класс, возраст, фотография, место жительства, телефоны и иные контакты, иные сведения личного характера) могут размещаться на сайте Детского сада или иных Интернет-ресурсах только с письменного согласия родителей или иных законных представителей детей. Персональные данные сотрудников ДОУ размещаются на сайте образовательного учреждения или иных Интернет-ресурсах только с письменного согласия сотрудника, чьи персональные данные размещаются.

3.3. В информационных сообщениях о мероприятиях на сайте Детского сада или иных Интернет-ресурсах без согласия лица или его законного представителя могут быть упомянуты только фамилия и имя учащегося либо фамилия, имя и отчество сотрудника, родителя.

3.4. При истребовании такого согласия представитель ДОУ должен разъясняет лицу возможные риски и последствия опубликования персональных данных. Детский сад не несет ответственности в случае наступления таких последствий, если имелось письменное согласие лица (его представителя) на опубликование персональных данных.

4. Процедура использования сети Интернет.

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

4.2. Сотрудникам запрещается:

- находиться на ресурсах, содержание и тематика которых является недопустимой для несовершеннолетних и/или нарушающей законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);
- осуществлять любые сделки через Интернет;
- осуществлять загрузки файлов на компьютер Детского сада без разрешения уполномоченного лица;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

4.3. При случайном обнаружении лицом, работающим в сети Интернет, ресурса, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно сообщить о таком ресурсе уполномоченному лицу с указанием его Интернет-адреса (URL) и покинуть данный ресурс.

4.4. Уполномоченное лицо обязано:

- принять сообщение лица, работающего в сети Интернет;
- довести информацию до сведения администрации для оценки ресурса и принятия решения по политике доступа к нему в соответствии с п.2.3 настоящих Правил;
- направить информацию о некатегоризированном ресурсе оператору технических средств и программного обеспечения технического ограничения доступа к информации (в течение суток);
- если обнаруженный ресурс явно нарушает законодательство Российской Федерации – сообщить об обнаруженном ресурсе 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 не совместимости с задачами образовательного процесса;
- Дату и время обнаружения;
- Информацию об установленных в Образовательном учреждении технических средствах технического ограничения доступа к информации.