Приложение № 1

 к приказу №17 от 28.02.2022

Правила использования сети интернет

в МБДОУ д/сад №25

1.ОБЩИЕ ПОЛОЖЕНИЯ

Использование сети Интернет в д/саду №25осуществляется

только в целях организации образовательного процесса в дошкольном учреждении и организации деятельности в целом.

Пользователями являются сотрудники, осуществляющие

бесперебойную деятельность учреждения (далее - пользователи).

К работе допускаются лица, ознакомившиеся с правилами работы в сети Интернет.

2.ПРАВА И ОБЯЗАННОСТИ

За обеспечение эффективного и безопасного доступа к сети Интернет несет

Ответственность администрация Учреждения.

Пользователь имеет право:

- размещать информацию ДОУ в сети согласно законодательству Российской Федерации;

- использовать электронную почту;

- пользоваться электронными государственными услугами;

- осуществлять поиск информации, связанный с воспитательно-образовательным процессом;

- сохранять полученную информацию на съемном диске.

Съемные диски должны предварительно проверяться на наличие вирусов.

При необходимости Пользователь распечатывает информацию на принтере.

Пользователю запрещается:

- обращаться к ресурсам, содержащие сведения о несовершеннолетних или нарушают законодательство Российской Федерации;

- осуществлять любые сделки через Интернет;

- осуществлять загрузки файлов, программ на компьютер без согласования с

администрацией ДОУ.

При случайном обнаружении ресурса, содержащие которого не имеет отношения к образовательному процессу. Пользователь обязан зафиксировать адрес ресурса, заданную формулировку поиска информации, время его обнаружения и сообщить об этом лицу, ответственному за обеспечение безопасного доступа к сети Интернет.

3 ОТВЕТСТВЕННОСТЬ

Пользователь несет ответственность за содержание передаваемой, принимаемой и распечатываемой информации.

Лица, не соблюдающие настоящие правила работы, лишаются права работы в сети Интернет.

При нанесении любого ущерба Пользователь несет материальную.

ответственность.

|  |  |
| --- | --- |
| Согласовано на педагогическом советеПротокол № №5 от 28.02.2022 Секретарь О.И. Ждановская | УтверждаюЗаведующий д/садом №25Н.В. МенжулаПриказ № 17от 28.02.2022  |

ИНСТРУКЦИЯ

по организации антивирусной защиты в МБДОУ д/сад №25

1 Общие положения

* 1. Настоящая инструкция предназначена для организации порядка

проведения антивирусного контроля в МБДОУ д/сад №25 п.Циммермановка (далее - ДОУ) и предотвращения возникновения фактов заражения

Программного обеспечения компьютерными вирусами, а также фильтрации доступа пользователей ДОУ к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

1.2. Заведующим назначается лицо, ответственное за организацию антивирусной защиты в ДОУ.

1.3. В ОУ может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение. Установка, настройка и регулярное обновление антивирусных

Средств осуществляется только ответственным за организацию антивирусной защиты в ДОУ.

1.5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы,

Почтовые сообщения), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация, находящаяся на съемных носителях (магнитных дисках, лентах, CD-ROM, DVD, flash-накопителях и т.п.).

1.6. Контроль информации на съёмных носителях производится непосредственно перед её использованием.

1.7. Файлы, помещаемые в электронный архив или на сервер, должны в обязательном порядке проходить антивирусный контроль.

Устанавливаемое (изменяемое) программное обеспечение должно

Быть предварительно проверено на отсутствие вирусов.

1.9. Факт выполнения антивирусной проверки должен регистрироваться в специальном журнале за подписью лица, ответственного за организацию антивирусной защиты.

2 Мероприятия, направленные на решение задач по антивирусной защите:

2.1. Установка только лицензированного программного обеспечения либо бесплатного антивирусного программного обеспечения.

2.2. Непрерывный контроль над всеми возможными путями проникновения

вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ

на всех объектах информационно-коммуникационной системы (далее ИКС) ДОУ.

2.3. Проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур.

2.4. Внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования.

2.5. Необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения.

2.6. Обеспечение бесперебойной работы ДОУ для случаев вирусного заражения, в том числе резервного копирования всех необходимых данных и программ и их восстановления.

3 Требования к проведению мероприятий по антивирусной защите

3.1. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС – при перезагрузке) в автоматическом режиме должно выполняться

Обновление антивирусных баз и серверов и проводиться антивирусный контроль всех дисков и файлов персонального компьютера и съёмных носителей.

3.2. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю.

3.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

3.3.1, непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети) должна быть выполнена антивирусная проверка на серверах и персональных компьютерах ДОУ;

3.3.2. При возникновении подозрения на наличие компьютерного вируса

(нетипичная работа программ, появление графических и звуковых эффектов,

искажений данных, пропадание файлов, частое появление сообщений о

системных ошибках и т.п.);

3.3.3. При отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

4.1. В случае обнаружения зараженных компьютерными вирусами файлов или электронных писем пользователи обязаны:

4.1.1. Приостановить работу;

4.1.2. Немедленно поставить в известность о факте обнаружения зараженных

вирусом файлов ответственного за обеспечение антивирусной защиты в ДОУ;

4.1.3. Совместно с владельцем зараженных вирусом файлов провести анализ

необходимости дальнейшего их использования;

4.1.4. Провести лечение или уничтожение зараженных файлов.

4.2. При возникновении подозрения на наличие компьютерного вируса ответственный за организацию антивирусной защиты должен провести

Внеочередной антивирусный контроль.

5 Ответственность

5.1. Ответственность за организацию антивирусной защиты и выполнение положений данной инструкции возлагается на лицо, назначенное заведующим ДОУ.

5.2. Ответственность за проведение мероприятий антивирусного контроля в ДОУ возлагается на ответственного за организацию антивирусной защиты.

5.3. Ответственность за соблюдение требований настоящей Инструкции при работе на персональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу компьютеров.

5.4. Периодический контроль за состоянием антивирусной защиты в

ДОУ осуществляется заведующим ДОУ (не реже 1 раза в квартал).

УТВЕРЖДАЮ:

Заведующий МБДОУ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Н.В. Менжула /

Приказ №17 от 28.02.2022 г

Муниципальное бюджетное дошкольное образовательное учреждение

Детский сад №25 п. Циммермановка

РЕГЛАМЕНТ

резервного копирования и восстановления

информации в МБДОУ д/сад №25

1 Общие положения

1.1. Настоящий Регламент резервного копирования и восстановления информации в МБДОУ д/сад №25 (далее – Регламент), хранящихся

на серверах и автоматизированных рабочих местах (далее – АРМ) МБДОУ д/сад №25, разработан в соответствии с требованиями Федерального

закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановления Правительства

Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и методических документов Федеральной службы по техническому и

экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации.

1.2. Настоящий регламент разработан с целью:

- определения порядка резервирования информации;

- определения порядка восстановления информации в случае ее искажения или утраты,

- в связи с попытками несанкционированного доступа, сбоями или отказами

аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

упорядочения работы сотрудников, связанной с резервным копированием и

восстановлением информации;

В настоящем Регламенте определены действия при выполнении следующих

мероприятий:

- резервное копирование;

- контроль резервного копирования;

- хранение резервных копий;

- восстановление информации.

2 Порядок резервного копирования

2.1. Резервному копированию подлежит информация следующих основных категорий:

- информация ограниченного доступа, в том числе персональные данные (далее – ПДн), хранящаяся на серверах МБДОУ д/сад №25(базы

данных, файлы и каталоги);

- информация ограниченного доступа, в том числе ПДн, хранящаяся на АРМ МБДОУ д/сад №25

2.2. Резервное копирование/восстановление информации, хранящейся

На серверах МБДОУ д/сад №25 осуществляется штатными средствами операционных систем с использованием программного обеспечения Windows

и Linux.

2.3. Контроль результата процедур резервного копирования, а также восстановление информации ограниченного доступа, хранящейся на серверах

МБДОУ д/сад №25 осуществляет ответственный за обеспечение

безопасности персональных данных в информационных системах МБДОУ д/сад №25 (далее – Ответственный).

2.4. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) носителей резервных копий без потерь информации, а также обеспечивать восстановление информации в случае отказа любого из устройств резервного копирования.

2.5. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

2.6. Резервное копирование/восстановление информации, хранящейся в д/саду , осуществляется пользователями на учтенные съемные носители.

2.7. Необходимость и периодичность резервного копирования информации, хранящейся на АРМ д/сад №25, а также срок хранения резервных копий такой информации на съемных носителях определяется пользователями

самостоятельно.

11 Резервное копирование информации может осуществляться

Исключительно на съемные машинные носители информации, учтенные в журнале учета съемных носителей информации д/сад №25.

12 Не допускается создание резервных копий на неучтенные и личные носители информации. При использовании съемных машинных носителей как носителей ПДн запись в журнале учета должна содержать отметку «Конфиденциально».

13 Хранение съемных машинных носителей ПДн должно осуществляться в сейфах (металлических шкафах), оборудованных внутренними замками и приспособлениями для опечатывания замочных скважин.

14 В случае отсутствия сейфа (металлического шкафа) у пользователя, осуществляющего хранение, допускается осуществлять хранение в сейфе ответственного.

15 Носители с ПДн, которые перестали использоваться в системе

Резервного копирования, должны стираться (форматироваться) с использованием специального программного обеспечения, реализующим полное физическое уничтожение данных.

16 О выявленных попытках несанкционированного доступа к

Резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, должно быть немедленно сообщено Ответственному.

 3 Восстановление информации из резервной копии

3.1. В случае необходимости, восстановление информации, хранящейся на серверах МБДОУ д/сад №25, может производиться Ответственным на основании заявки пользователя.

3.2. В случае повреждения или утраты информации, хранящейся на АРМ

до начала восстановления их со съемного носителя пользователь должен определить причину утраты или повреждения файлов, содержащих ПДн.

3.3. Если повреждение или удаление информации вызвано действиями

Самого пользователя (непреднамеренное удаление файла), восстановление информации со съёмного носителя может осуществляться пользователем незамедлительно.

3.4. В случае повреждения файловой системы АРМ или работоспособности жесткого диска в результате системного сбоя АРМ пользователь должен

Обратиться к ответственному.

Перенос файлов из резервной копии может выполняться пользователем только после восстановления работоспособности АРМ.

3.5. В случае повреждения или утраты файлов, содержащих конфиденциальную информацию, в том числе ПДн, вследствие несанкционированного доступа (далее – НСД) АРМ пользователь

незамедлительно сообщает о данном факте Ответственному.

Восстановление файлов из резервной копии может осуществляться только после проведения расследования инцидента безопасности НСД с соответствующим устранением угрозы дальнейших инцидентов НСД.

3.6. Если утрата файлов на АРМ МБДОУ д/сада №25произошла в результате вирусного заражения, восстановление файлов возможно только

после выполнения мероприятий в соответствии с инструкцией антивирусной защиты д/сада №25