АДМИНИСТРАЦИЯ КСТОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА
МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ДЕТСКИЙ САД № 19 «СОЛНЫШКО»
(МАДОУ д/с № 19)
607662, Нижегородская область,
г. Кстово, улица Гражданская, дом № 6, корпус № 1
тел. (83145) 2-78-39, 2-78-11, факс (83145)2-78-39
E-mail: ds19.solnyshko@yandex.ru
https://ds19solnyshko.kinderedu.ru/
ОКПО 71164478, ОГРН 1025201985632
ИНН/КПП 5250024814/525001001

УТВЕРЖДЕНЫ
приказом МАДОУ д/с № 19
от 28.03.2023 года № 93

Положение
об информационной безопасности воспитанников и сотрудников Муниципального автономного дошкольного образовательного учреждения «Детский сад № 19 «Солнышко»

1. Общие положения

1.1. Настоящее Положение об информационной безопасности воспитанников и сотрудников (далее - Положение) муниципальном автономном дошкольном образовательном учреждении «Детский сад № 19 «Солнышко» (далее - Учреждение) Кстовского муниципального округа разработано в соответствии с:
- Федеральным законом от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,
- Федеральным законом от 27.07.2006 года №152-ФЗ «О персональных данных» (в редакции от 28.06.2010 года),
-Указом президента РФ от 17.03.2008 года № 351 (в редакции от 22.05.2015 года) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»,
-Федеральным законом «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 года № 436-ФЗ,
-Концепцией информационной безопасности детей, утвержденной Распоряжением Правительства РФ от 2 декабря 2015 года № 2471-р.

1.2. Настоящее Положение определяет задачи, функции, обязанности, ответственность и права должностных лиц, ответственных за информационную безопасность, имеющих доступ к электронным базам данных, официальному сайту Учреждения, адресам электронной почты Учреждения.

1.3. Должностные лица, ответственные за информационную безопасность, назначаются приказом заведующего Учреждения.

1.4. Должностные лица, ответственные за информационную безопасность, подчиняются заведующему Учреждения.
1.5. Должностные лица, ответственные за информационную безопасность, в своей работе руководствуются настоящим Положением.
1.6. Должностные лица, ответственные за информационную безопасность, в пределах своих функциональных обязанностей обеспечивают безопасность информации, обрабатываемой, передаваемой и хранимой при помощи всех информационных средств в Учреждении.
1.7. К информационным средствам Учреждения относятся электронные базы данных, содержащие информацию административно-хозяйственного содержания, финансовые документы, персональные данные сотрудников и воспитанников Учреждения, организационно-правовую информацию, материалы, регламентирующие организацию образовательного процесса в Учреждении; официальный сайт Учреждения; официальная электронная почта Учреждения.

2. Основные задачи и функции должностных лиц, ответственных за информационную безопасность воспитанников и сотрудников

2.1. Основными задачами должностных лиц, ответственных за информационную безопасность, являются:
2.1.1. Организация эффективной 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.
2.2. Должностные лица, ответственные за информационную безопасность, выполняют следующие основные функции:
2.2.1. Соблюдение инструкций по информационной безопасности: инструкции по организации антивирусной защиты (Приложение 1), инструкции по безопасной работе в системе Интернет (Приложение 2);
2.2.2. При наличии производственной необходимости обучение персонала и пользователей навыкам работы с персональным компьютером (далее - ПК), правилам безопасной обработки информации и правилам работы со средствами защиты информации;
2.2.3. Организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в Учреждение;
2.2.4. Текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации;
2.2.5. Контроль целостности эксплуатируемого ПК программного обеспечения с целью выявления несанкционированных изменений в нём;
2.2.6. Контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК;
2.2.7. Контроль пользования сетью Интернет;
2.2.8. Контроль доступа к официальному сайту Учреждения, к официальной электронной почте Учреждения, к электронным базам данных.

3. Обязанности должностных лиц, ответственных за информационную безопасность воспитанников и сотрудников

3.1. Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах, возложенных на них обязанностей. Немедленно докладывать заведующему Учреждения о выявленных нарушениях и несанкционированных действиях пользователей и сотрудников, а также принимать необходимые меры по устранению нарушений.
3.2. Администрировать работу официального сайта Учреждения (далее - сайт), размещать и классифицировать информацию на сайте.
3.3. Устанавливать по согласованию с заведующим Учреждения критерии доступа пользователей на сайт, к электронным базам официальных документов Учреждения, к официальной электронной почте Учреждения.
3.4. При наличии производственной необходимости формировать и предоставлять пароли для новых пользователей, администрировать права пользователей сайта, электронных баз официальных документов Учреждения, электронной почты Учреждения.
3.5. Отслеживать работу антивирусных программ, проводить один раз в неделю полную проверку ПК на наличие вирусов.
3.6. Регулярно выполнять резервное копирование данных на сайте, в электронных базах официальных документов Учреждения, при необходимости восстанавливать потерянные или поврежденные данные.
3.7. Систематически проверять информацию, поступающую по официальной электронной почте Учреждения, через официальный сайт Учреждения.
3.8. Вести учет пользователей сетью Интернет. В случае необходимости лимитировать время работы пользователей в сети Интернет и объём скачиваемой информации.
3.9. Сообщать незамедлительно заведующему Учреждения о выявлении случаев несанкционированного доступа в сеть Интернет, к электронным базам официальных документов Учреждения, на официальный сайт Учреждения, в официальную электронную почту Учреждения.

4. Права должностных лиц, ответственных за информационную безопасность воспитанников и сотрудников

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, персональные данные сотрудников и воспитанников и т.д.
4.2. Вносить предложения по совершенствованию используемых систем защиты информации и отдельных их компонентов, по организации и контролю доступа в сеть Интернет, к электронным базам официальных документов Учреждения, на официальный сайт Учреждения, в официальную электронную почту Учреждения.

5. Ответственность должностных лиц, ответственных за информационную безопасность воспитанников и сотрудников

5.1. На должностных лиц, ответственных за информационную безопасность воспитанников и сотрудников, возлагается персональная ответственность в соответствии с действующим законодательством РФ:

- за качество проводимых ими работ по обеспечению защиты информации в соответствии с функциональными обязанностями, определёнными настоящим Положением;
- за разглашение информации административно-хозяйственного содержания и финансовых документов без согласования с заведующим Учреждения среди лиц, не имеющих производственной принадлежности к Управлению образования Администрации Кстовского муниципального округа, проверяющих и контролирующих органов;
- за сохранность персональных данных воспитанников и сотрудников Учреждения.

6. Компетенции должностных лиц, ответственных за информационную безопасность воспитанников и сотрудников

№	Должность	Доступ к информационным средствам	Доступ к информации
1	Заведующий Учреждением	- электронные базы официальных документов ДОУ; - официальный сайт ДОУ; - официальная электронная почта ДОУ; - сеть Интернет посредством официального провайдера ДОУ	- информация административно-хозяйственного содержания; - финансовые документы; - персональные данные сотрудников и воспитанников ДОУ; - организационно- правовая информация; - материалы, регламентирующие организацию образовательного процесса в ДОУ
2	Главный бухгалтер	электронные базы официальных документов ДОУ; - официальная электронная почта ДОУ; - сеть Интернет посредством официального провайдера ДОУ; - программное обеспечение персональных данных сотрудников и воспитанников;	информация административно-хозяйственного содержания; - финансовые документы персональные данные сотрудников и воспитанников ДОУ; - организационно- правовая информация
3	Инспектор отдела кадров	- электронные базы официальных документов ДОУ; - официальная электронная почта ДОУ; - сеть Интернет посредством официального провайдера ДОУ; - программное обеспечение	-информация административно-хозяйственного содержания; - финансовые документы персональные данные сотрудников и воспитанников ДОУ; - организационно- правовая информация

		персональных данных сотрудников и воспитанников;	
4	Старший воспитатель	- электронные базы официальных документов ДОУ; - официальный сайт ДОУ; - официальная электронная почта ДОУ; - сеть Интернет посредством официального провайдера ДОУ	- информация административно содержания; - персональные данные воспитанников ДОУ; - организационно- правовая информация; - материалы, регламентирующие организацию образовательного процесса в ДОУ
5	Администратор официального сайта ДОУ и гос паблик. (WKонтакт)	- электронные базы официальных документов ДОУ; - официальный сайт ДОУ; - официальная электронная почта ДОУ; - сеть Интернет посредством официального провайдера ДОУ	- информация административно-хозяйственного содержания; - персональные данные сотрудников и воспитанников ДОУ; - организационно-правовая информация; - материалы, образовательного процесса в ДОУ регламентирующие организацию

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ
в Муниципальном автономном дошкольном образовательном учреждении
«Детский сад № 19 «Солнышко»

1. Настоящая Инструкция определяет требования к организации защиты от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников Муниципального автономного дошкольного учреждения «Детский сад № 19 «Солнышко» Кстовского муниципального округа их выполнение.
2. К использованию в организации допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.
3. Установка средств антивирусного контроля на компьютерах осуществляется уполномоченным сотрудником организации. Настройка параметров средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.
4. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.
5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD-ROM и т.п.).
6. Контроль входящей и исходящей информации на защищаемых серверах и персональных компьютерах (далее ПК) осуществляется непрерывно посредством постоянно работающего компонента антивирусного программного обеспечения («монитора»). Полная проверка информации, хранящейся на серверах и ПК должна осуществляться не реже одного раза в месяц.
7. Обновление баз вирусов антивирусного программного обеспечения, установленного на ПК и серверах, должно осуществляться еженедельно.
8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка:

- на защищаемом автоматизированном рабочем месте (АРМ) - ответственным за обеспечение информационной безопасности.

9. 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.) сотрудник организации самостоятельно или вместе с ответственным за антивирусную защиту организации должен провести внеочередной антивирусный контроль своей рабочей станции.
10. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;

-немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за антивирусную защиту организации, владельца зараженных файлов, а также сотрудников, использующих эти файлы в работе;

- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

-провести лечение или уничтожение зараженных файлов.

11. Ответственность за антивирусный контроль в организации, в соответствии с требованиями настоящей Инструкции возлагается на руководителя организации.

12. Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за антивирусную защиту и всех сотрудников, являющихся пользователями ПК.

13. Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками осуществляется ответственным за антивирусную защиту организации.

Инструкция пользователей по безопасной работе в сети Интернет Муниципального автономного дошкольного образовательного учреждения «Детский сад № 19 «Солнышко»

Персональные компьютера, серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, коммуникационное оборудование являются собственностью Муниципального автономного дошкольного учреждения «Детский сад № 19 «Солнышко» (Далее – Учреждения) Кстовского муниципального округа и предоставляются сотрудникам Учреждения.

1. **Общие положения**

Целью настоящей инструкции является регулирование работы пользователей, распределения сетевых ресурсов коллективного пользованияи поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации.

Работа в системе каждому работнику разрешена только на определенных компьютерах, в определенное время и только с разрешенными программами и сетевыми ресурсами. Если нужно работать вне указанного времени, на других компьютерах и с другими программами, необходимо получить разрешение заведующего Учреждения.

По уровню ответственности и правам доступа к сети пользователи разделяются на следующие категории: системные администраторы и пользователи.

Пользователь подключенного к сети компьютера - лицо, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю за соблюдением прав доступа к ней.

Каждый работник должен пользоваться только своим именем пользователя и паролем для входа в сеть Интернет, передача их кому-либо запрещена.

Для работы на компьютере другому лицу, кроме пользователя, необходимо разрешение заведующего Учреждения или работника, ответственного за Интернет.

В случае нарушения правил пользования сетью, пользователь сообщает работнику, ответственному за Интернет, который проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений. Если виновником нарушения является пользователь данного компьютера, то заведующий Учреждением имеет право отстранить виновника от пользования компьютером или принять иные меры.

Работник, следящий за правильным функционированием сети, выдает IP-адрес компьютеру, создает учетную запись электронной почты для пользователя. Самовольное подключение является серьезнейшим нарушением правил пользования сетью.

Работник, ответственный за Интернет, информирует пользователей обо всех плановых профилактических работах, могущих привести к частичной или полной неработоспособности сети на ограниченное время, а также об изменениях предоставляемых сервисов и ограничениях, накладываемых на доступ к ресурсам сети.

Работник, ответственный за Интернет имеет право отключить компьютер пользователя от сети в случае, если с данного компьютера производились попытки несанкционированного доступа к информации на других компьютерах, и в случаях других серьезных нарушений настоящей инструкции.

Пользователь должен ознакомиться с настоящей инструкцией. Обязанность ознакомления с инструкцией лежит на работнике, ответственном за использование сети Интернет в Учреждении.

2. **Пользователи сети Интернет обязаны:**

Соблюдать правила работы в сети, оговоренные настоящей инструкцией.

При доступе к внешним ресурсам сети, соблюдать правила, установленные системными администраторами для используемых ресурсов.

Немедленно сообщать работнику, ответственному за использование сети Интернет, об обнаруженных проблемах, а также о фактах нарушения настоящей инструкции кем-либо. Администрация Учреждения, при необходимости, с помощью других специалистов, должна провести расследование указанных фактов и принять соответствующие меры.

Не разглашать известную им конфиденциальную информацию (имена пользователей, пароли), необходимую для безопасной работы в сети.

Немедленно отключать от сети компьютер, который подозревается в заражении вирусом.

В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться к работнику, ответственному за функционирование техники или администрации Учреждения.

3. **Пользователи сети Интернет имеют право;**

Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках. Администрация Учреждения вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение графика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов.

Какие-либо действия пользователя, ведущие к изменению объема используемых им ресурсов, или влияющие на загруженность или безопасность системы (например, установка на компьютере коллективного доступа), должны санкционироваться администрацией Учреждения.

Обращаться за помощью к работнику, ответственному за использование сети Интернет.

Вносить предложения по улучшению работы с ресурсом.

4. **Пользователям сети Интернет запрещено:**

Разрешать посторонним лицам пользоваться вверенным им компьютером.

Использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей.

Самостоятельно устанавливать или удалять установленные сетевые программы на компьютерах, подключенных к сети, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов.

Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю.

Вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование, изменять настройки.

Самовольно подключать компьютер к сети, а также изменять IP-адрес компьютера. Передача данных в сеть с использованием других IP-адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах.

Работать с каналоемкими ресурсами,

Получать и передавать в сеть информацию, противоречащую законодательству и нормам морали общества, предоставляющую коммерческую или государственную тайну, распространять через сеть информацию, задевающею честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения,

Обхождение учетной системы безопасности, системы статистики, ее повреждение или дезинформация.

Осуществлять попытки несанкционированного доступа к ресурсам сети, проводить или участвовать в сетевых атаках и сетевом взломе.

Использовать сеть для совершения коммерческих сделок, распространения рекламы, коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз.

Пользователи должны уважать право других пользователей на личную информацию. Это означает, что пользователь не имеет права пользоваться чужими именами и паролями для входа в сеть, читать чужую почту, причинять вред данным, принадлежащим другим пользователям.

Запрещается производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и сервера сети, равно, как и любых других компьютеров.

Закрывать доступ к информации паролями без согласования с администрацией Учреждения.

5. **Работа с электронной почтой:**

Электронная почта предоставляется работникам Учреждения только для выполнения своих служебных обязанностей. Использование ее в личных целях запрещено.

Все электронные письма, создаваемые и хранимые на компьютерах Учреждения, являются ее собственностью и не считаются персональными.

Учреждение оставляет за собой право получить доступ к электронной почте работников, если на то будут веские причины.

Конфигурировать программы электронной почты так, чтобы стандартные действия пользователя, использующие установки по умолчанию, были бы наиболее безопасными.

Входящие письма должны проверяться на наличие вирусов или других вредоносных программ.

Почтовые сервера должны быть сконфигурированы так, чтобы отвергать письма, адресованные не на компьютеры организации.

Администрация Учреждения организует обучение пользователей правильной работе с электронной почтой.

Справочники электронных адресов работников не могут быть доступны всем и являются конфиденциальной информацией.

Никто из посетителей не имеет права использовать электронную почту Учреждения.

Исходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики безопасности.

Пользователи не должны позволять кому-либо посылать письма от чужого имени.

Администрация Учреждения оставляет за собой право осуществлять наблюдение за почтовыми отправлениями работников.

В качестве клиентов электронной почты могут использоваться только утвержденные программы.

Конфиденциальная информация не может быть послана с помощью электронной почты.

Если будет установлено, что работник Учреждения с умыслом неправильно использует электронную почту, он будет наказан.

Открывать или запускать приложения, полученные по электронной почте от неизвестного источника и (или) не затребованные пользователем.

Осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).

Использовать несуществующие обратные адреса при отправке электронных писем.

6. **При работе с веб-ресурсами:**

6.1 Пользователи используют программы для поиска информации в только в случае, если это необходимо для выполнения своих должностных обязанностей.

Использование ресурсов сети Интернет разрешается только в рабочих целях.

Но использованию сети Интернет работником Учреждения, ответственным за Интернет ведется статистика.

Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему санкций.
Работникам Учреждения, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим, фашистским или расистским и не относящимся к деятельности Учреждения.
Все файлы, загружаемые с помощью сети Интернет, должны проверяться на вирусы.
Запрещено размещать в гостевых книгах, форумах, конференциях сообщения, содержащие грубые и оскорбительные выражения.
Запрещено получать и передавать через сеть информацию, противоречащую законодательству и нормам морали общества, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.
Запрещено получать доступ к информационным ресурсам сети Интернет, не являющихся публичными, без разрешения их собственника.

7. **Ответственность:**

Пользователь компьютера отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной ему техники.
Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в сети и за ее пределами.
За нарушение настоящей инструкции пользователь может быть отстранен от работы с сетью.
Нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы компьютеров пользователей, системы или сети компьютеров, может повлечь административную или уголовную ответственность в соответствии с действующим законодательством.