

**МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ  
ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ДЕТСКИЙ САД №8 «БЕЛОСНЕЖКА»**

620681 Российская Федерация, Ханты-Мансийский автономный округ- Югра, г. Мегион, ул. Новая, д. 4/1,  
тел. 8(34643) 2-16-12, 8(34643) 2-14-23

---

СОГЛАСОВАНО


общим собранием (конференцией) работников муниципального автономного дошкольного образовательного учреждения «Детский сад №8 «Белоснежка»

Протокол №7 от 02.07.2020

УТВЕРЖДЕНО

приказом муниципального автономного дошкольного образовательного учреждения «Детский сад №8 «Белоснежка» приказ от 14 июля 2020 года №167-О

Заведующий \_\_\_\_\_ В.А.Павленко

  
(личная подпись)

СОГЛАСОВАНО

педагогическим советом муниципального автономного дошкольного образовательного учреждения «Детский сад №8 «Белоснежка»

Протокол № 6 от 03.07.2020

**ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ  
ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СЕТИ ИНТЕРНЕТ  
МУНИЦИПАЛЬНОГО АВТОНОМНОГО ДОШКОЛЬНОГО  
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ «ДЕТСКИЙ САД №8 «БЕЛОСНЕЖКА»**

**1. Общие положения**

1.1. Инструкция пользователя по компьютерной безопасности при работе в сети Интернет муниципального автономного дошкольного образовательного учреждения «Детский сад №8 «Белоснежка» (далее по тексту – Инструкция) разработана для муниципального автономного дошкольного образовательного учреждения «Детский сад №8 «Белоснежка» с целью регулирования работы пользователей, распределения сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации, более эффективного использования сетевых ресурсов и уменьшения риска умышленного или неумышленного неправильного их использования.

1.2. Персональные компьютеры, серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование локальной вычислительной сети, коммуникационное оборудование являются собственностью муниципального автономного дошкольного образовательного учреждения «Детский сад №8 «Белоснежка» (далее по тексту – Учреждение) и предоставляются работникам Учреждения для осуществления ими их должностных обязанностей.

1.3. Персональные компьютеры, серверы, программное обеспечение, оборудование ЛВС и коммуникационное, пользователи образуют систему корпоративной сети (далее по тексту – СЕТЬ).

1.4. Работа в системе каждому работнику Учреждения 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 руководителя Учреждения.

1.5. 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.

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

1.7. К работе в системе допускаются лица, прошедшие инструктаж.

1.8. Для работы на компьютере кроме пользователя необходимо разрешение системного администратора (инженера-программиста). Никто не может давать разрешение даже на временную работу на компьютере без разрешения системного администратора.

1.9. В случае нарушения правил пользования СЕТЬЮ, связанных с администрируемым им компьютером, пользователь сообщает системному администратору, который проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений. Если виновником нарушения является пользователь данного компьютера, администратор имеет право отстранить виновника от пользования компьютером или принять иные меры.

1.10. В случае появления у пользователя компьютера сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах несанкционированного удаленного доступа к информации, размещенной на контролируемом им компьютере или каком-либо другом, пользователь должен немедленно сообщить об этом системному администратору СЕТИ.

1.11. Системный администратор и лицо, обслуживающее сервер и следящее за правильным функционированием СЕТИ. Системный администратор дает разрешение на подключение компьютера к СЕТИ. Самовольное подключение является серьезнейшим нарушением правил пользования СЕТЬЮ.

1.12. Системный администратор 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.

1.13. Системный администратор 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.

1.14. Пользователь должен ознакомиться с настоящей инструкцией.

## **2. Обязанности пользователей СЕТИ**

Пользователи СЕТИ обязаны:

2.1. Соблюдать правила работы в СЕТИ, оговоренные настоящей инструкцией.

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

2.3. Немедленно сообщать системному администратору, руководителю об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящей инструкции кем-либо.

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

2.5. Немедленно отключать от СЕТИ компьютер, который подозревается в заражении вирусом. Компьютер не должен подключаться к СЕТИ до тех пор, пока системный администратор не удостоверится в удалении вируса.

2.6. Обеспечивать беспрепятственный доступ системному администратору к сетевому оборудованию и компьютерам пользователей.

2.7. Выполнять предписания системного администратора, направленные на обеспечение безопасности СЕТИ.

2.8. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться к системному администратору.

2.9. Не допускать посещения «хакерских», порно и других сайтов с потенциально вредоносным содержанием.

2.10. Быть крайне осторожным при работе с электронной почтой. Категорически запрещается открывать присоединенные к письмам, полученным от незнакомых лиц, файлы.

2.11. В обязательном порядке проверять антивирусным программным обеспечением любые внешние носители информации перед началом работы с ними.

2.12. При появлении признаков нестандартной работы компьютера («тормозит», на экране появляются и исчезают окна, сообщения, изображения, самостоятельно запускаются программы и т.п.) немедленно отключить компьютер от Ethernet сети, загрузить компьютер с внешнего загрузочного диска (CD, DVD) и произвести полную антивирусную проверку всех дисков компьютера. При появлении аналогичных признаков после проделанной процедуры переустановить операционную систему с форматированием системного раздела диска.

### **3. Права пользователей СЕТИ**

3.1. Пользователи СЕТИ имеют право:

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

3.1.2. Обращаться к системному администратору по вопросам, связанным с распределением ресурсов компьютера. 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 системным администратором СЕТИ.

3.1.3. Обращаться за помощью к системному администратору при решении задач использования ресурсов СЕТИ.

3.1.4. Вносить предложения по улучшению работы с ресурсом.

3.2. Пользователям сети Интернет запрещено:

3.2.1. Разрешать посторонним лицам пользоваться вверенным им компьютером (кроме случаев подключения/отключения ресурсов, выполняемого системным администратором).

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

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

3.2.4. Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю.

3.2.5. Вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без ведома системного администратора, изменять настройки BIOS, а также производить загрузку рабочих станций с дискет.

3.2.6. Самовольно подключать компьютер к СЕТИ, а также изменять IP-адрес компьютера, выданный системным администратором. 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.

3.2.7. Обходжение учетной системы безопасности, системы статистики, ее повреждение или дезинформация.

3.2.8. Использовать иные формы доступа к сети Интернет, за исключением разрешенных системным администратором: пытаться обходить установленный системным администратором межсетевой экран при соединении с сетью Интернет.

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

3.2.10. Использовать СЕТЬ для совершения коммерческих сделок, распространения рекламы, коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.

3.2.11. Пользователи должны уважать право других пользователей на личную информацию. Это означает, что пользователь (системный администратор) не имеет права пользоваться чужими именами и паролями для входа в сеть, читать чужую почту, причинять вред данным (кроме случаев, указанных выше), принадлежащих другим пользователям.

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

3.2.13. Закрывать доступ к информации паролями без согласования с системным администратором.

#### **4. Работа с электронной почтой**

4.1. Электронная почта предоставляется сотрудникам Учреждения только для выполнения своих служебных обязанностей. Использование ее в личных целях запрещено. Никто из посетителей или временных служащих не имеет права использовать электронную почту Учреждения.

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

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

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

4.5. Руководитель Учреждения оставляет за собой право осуществлять наблюдение за почтовыми отправлениями сотрудников.

4.6. Если будет установлено, что сотрудник неправильно использует электронную почту с умыслом, ему будет вынесено дисциплинарное взыскание.

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

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

4.9. Запрещается использовать несуществующие обратные адреса при отправке электронных писем.

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

4.11. В качестве клиентов электронной почты могут использоваться только утвержденные почтовые программы.

4.12. Конфиденциальная информация не может быть послана с помощью электронной почты.

4.13. Запрещено использовать несуществующие обратные адреса при отправке электронных писем.

## **5. Работа с веб-ресурсами**

При работе с веб-ресурсами:

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

5.2. Использование ресурсов сети Интернет разрешается только в рабочих целях, использование её ресурсов не должно потенциально угрожать информационной системе Учреждения.

5.3. Сотрудникам Учреждения, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим, фашистским или расистским и не относящимся к деятельности Учреждения.

5.4. Запрещено размещать в гостевых книгах, форумах, конференциях сообщения, содержащие грубые и оскорбительные выражения.

5.5. Запрещено получать и передавать через СЕТЬ информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую тайну, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.

5.6. Запрещено получать доступ к информационным ресурсам СЕТИ или сети Интернет, не являющихся публичными, без разрешения их собственника.

5.7. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему в санкций.

5.8. Все программы, используемые для доступа к сети Интернет, должны быть утверждены сетевым администратором и на них должны быть настроены необходимые уровни безопасности.

5.9. Все файлы, загружаемые с помощью сети Интернет, должны проверяться на вирусы с помощью утвержденных руководством антивирусных программ.

5.10. В школе должна быть организована фильтрация запрещенных ресурсов Интернет. Программы для работы с Интернет должны быть сконфигурированы так, чтобы к этим сайтам нельзя было получить доступ.

## **6. Ответственность**

6.1. Пользователь компьютера отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники.

6.2. Системный администратор отвечает за бесперебойное функционирование вверенной ему СЕТИ, качество предоставляемых пользователям сервисов.

6.3. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в СЕТИ и за ее пределами.

6.4. За нарушение настоящей инструкции пользователь может быть отстранен от работы с СЕТЬЮ.

6.5. 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.

*Разработчик: инженер-программист Кожеватов А.В.*