Принят: Педагогическим советом школы
Протокол № 7 от 30.08.2018

Утверждено:
Приказ № 130 от 01.09.2018
Директор МБОУ «Нарымская СШ»
……Гришаева О.А.

Локальный акт

К Уставу МБОУ «Нарымская средняя школа»

ПОЛОЖЕНИЕ
Об использовании сети Интернет и электронной почты

в МБОУ «Нарымская средняя школа»

с. Нарым 2018

Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом № 149-ФЗ от 26.07.2006 «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасности» и другими нормативными правовыми актами и устанавливает порядок использования сети Интернет и электронной почты работниками МБОУ «Нарымская средняя школа» (далее - Учреждение).
1.2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации Учреждения.
1.3. Действие настоящего Положения распространяется на работников Учреждения, внештатных сотрудников и третьих лиц, имеющих доступ к информационным ресурсам Учреждения и подключенных к сети Интернет.

2. Основные термины, сокращения и определения

Адрес IP - уникальный идентификатор АРМ, подключенного к локальной вычислительной сети, а также сети Интернет.
АРМ - автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения определенной производственной задачи.
Интернет - глобальная ИС, обеспечивающая удаленный доступ к ресурсам различного содержания и направленности.
ИС - информационная система - система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.
ИТ - информационные технологии - совокупность методов и процессов, обеспечивающих хранение, обработку, преобразование и передачу информации с использованием средств компьютерной и другой техники.
ПК - персональный компьютер.
ПО - программное обеспечение вычислительной техники, базы данных.
ПО вредоносное - ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.
ПО коммерческое - ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной)основе.
П ользователь - работник, использующий ресурсы Интернет для выполнения своих должностных обязанностей.
Реестр - документ «Реестр разрешенного к использованию ПО». Содержит перечень коммерческого ПО, разрешенного к использованию в Учреждении.
Электронная почта - сервис обмена электронными сообщениями в рамках общедоступных сетей Интернет (внешняя электронная почта).
Электронное почтовое сообщение - сообщение, формируемое отправителем с помощью почтового клиента и предназначенное для передачи получателю посредством электронной почты.
Электронный документ - документ, в котором информация представлена в электронно-цифровой форме.
Электронный почтовый ящик - персональное пространство на почтовом сервере, в котором хранятся электронные сообщения.

3. Порядок использования сети Интернет

3.1. Доступ в сеть Интернет в ИС Учреждения осуществляется централизованно с применением специальных программно-технических средств защиты (межсетевых экранов).
3.2. На рабочих местах, подключенных к сети Internet, в обязательном порядке должно быть установлено антивирусное программное обеспечение с актуальной антивирусной базой.
3.3. Доступ к сети Интернет предоставляется Пользователю в целях выполнения им своих служебных обязанностей.

3.4. Для доступа Пользователя к сети Интернет допускается применение коммерческого или бесплатного ПО, входящего в Реестр разрешенного к использованию в Учреждении ПО.
3.5. При использовании доступа к сети Интернет необходимо:
3.5.1. Соблюдать требования настоящего Положения.
3.5.2. Использовать сеть Интернет исключительно для выполнения своих служебных обязанностей.
3.5.3. Типичные угрозы при работе с Сервисами и рекомендации по их предотвращению приведены в приложении № 1.
3.5.4. Общие меры предосторожности при работе с Сервисами приведены в приложении № 2.
3.6. При использовании доступа к сети Интернет запрещено:
3.6.1. Использовать предоставленный доступ к сети Интернет в личных целях.
3.6.2. Использовать специализированные аппаратные и программные средства, позволяющие Пользователям получить несанкционированный доступ к сети Интернет.
3.6.3. Публиковать, загружать и распространять материалы, содержащие:
конфиденциальную информацию, а также информацию, составляющую коммерческую тайну, персональные данные, за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным;
- информацию, полностью или частично защищенную авторскими или другими правами, без разрешения владельца;
- вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также серийные номера к коммерческому ПО и ПО для их генерации, пароли и прочие средства для получения несанкционированного доступа к платным интернет-ресурсам, а также ссылки на вышеуказанную информацию;
- угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, и т.д.
3.6.4. Фальсифицировать свой IP-адрес, а также прочую служебную информацию.
3.6.5. Распространять и устанавливать на других рабочих местах любое программное обеспечение и данные, полученные с использованием доступа к сети Интернет.
3.6.6. Осуществлять попытки несанкционированного доступа к ресурсам Сети, проведение сетевых атак и сетевого взлома и участие в них.
3.6.7. Публиковать свой электронный адрес либо электронный адрес других работников Учреждения на общедоступных интернет-ресурсах (форумы, конференции и т.п.).
3.6.8. Запрещается использование в качестве паролей для доступа к ресурсам сети Интернет паролей, аналогичных паролям, используемым для доступа к информационным ресурсам Учреждения.
3.6.9. Запрещается отключать установленное на АРМ антивирусное программное обеспечение.
3.7. Содержание интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного
3.8. Информация о посещаемых работниками интернет-ресурсах протоколируется для последующего анализа и при необходимости может
быть предоставлена руководителям структурных подразделений, а также руководителю Учреждения.
3.9. Администрация Учреждения оставляет за собой право блокировать или ограничивать доступ пользователей к интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и российским законодательством.
4.1. Использование личной почты в служебных целях запрещено.
4.2. При пользовании корпоративной электронной почтой необходимо:

4.2.1. соблюдать требования настоящего Положения;
4.2.2. Использовать предоставляемую электронную почту исключительно для выполнения своих служебных обязанностей.
4.3. При пользовании корпоративной электронной почтой запрещено:
4.3.1. по собственной инициативе осуществлять рассылку (в том числе и массовую) электронных сообщений, если рассылка не связана с выполнением служебных обязанностей;
4.3.2. использовать адрес электронной почты для оформления подписки на периодическую рассылку материалов из сети Интернет, не связанных с исполнением служебных обязанностей;
4.3.3. предоставлять другим работникам (за исключением исполняющему функции администратора) и третьим лицам доступ к своему электронному почтовому ящику;
4.3.4. перенаправлять электронные сообщения с личных почтовых ящиков на корпоративный.
4.4. Администрация Учреждения оставляет за собой право доступа к электронным сообщениям работников с целью их архивирования и централизованного хранения, а также мониторинга выполнения требований настоящего Положения.
4.5. В случае нарушения пунктов Положения Администрация Учреждения вправе отключить Пользователя от предоставляемых Сервисов.

5. Ответственность

5.1. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами Учреждения.

6. Заключительные положения

6.1. Контроль над соблюдением требований данного Положения возложен на исполняющего функции технического специалиста.

Приложение 1
к Положению об использовании
сети Интернет и электронной почты

ТИПИЧНЫЕ УГРОЗЫ ПРИ РАБОТЕ С СЕТЬЮ ИНТЕРНЕТ И ЭЛЕКТРОННОЙ ПОЧТОЙ

1.Заражение компьютера вирусом.

Чаще всего заражение вирусами происходит при посещении специально созданных «вредоносных» веб-страниц, «хакерских» сайтов, сайтов «для взрослых»

Рекомендуемые меры предосторожности

- не посещать перечисленные сайты;
- установить, своевременно обновлять и не отключать антивирусное программное обеспечение

2. Заражение компьютера вирусом при просмотре почтовых сообщений

Обычно происходит при открытии прикрепленного к письму файла

Рекомендуемые меры предосторожности

- не открывать письма, если электронный адрес отправителя вам не знаком или выглядит «странно»;
- не открывать прикрепленные файлы, если отправитель письма вам неизвестен;
- установить, своевременно обновлять и не отключать антивирусное программное обеспечение

3.Утечка информации с рабочей станции

Уязвимым может оказаться программное обеспечение (чаще всего таковым является свободно распространяемое ПО, а также ПО от неизвестных или малоизвестных производителей). Также причиной утечки может оказаться заражение компьютера вирусом.

Рекомендуемые меры предосторожности

- использовать только принятое к использованию в Учреждении программное обеспечение;
-установить, своевременно обновлять и не отключать антивирусное программное обеспечение

4. Предоставление возможности удаленного управления компьютером.

Такая возможность может быть получена как с ведома пользователя (при использовании им ПО, выполняющего данную функцию), так и без его ведома (при заражении компьютера вирусом).

Рекомендуемые меры предосторожности

- использовать только принятое к использованию в Учреждении программное обеспечение;
- установить, своевременно обновлять и не отключать антивирусное программное обеспечение

5. Потеря функциональности (полной или частичной) рабочей станцией.

Чаще всего это происходит вследствие использования уязвимостей программного обеспечения лоумышленником или из-за заражения вирусом - использовать только принятое к использованию в Учреждении программное обеспечение;

Рекомендуемые меры предосторожности

- установить, своевременно обновлять и не отключать антивирусное программное обеспечение

6.Кража личной информации

Чаще всего к этому приводит ввод такой информации на вебстраницах, в том числе сайтах-двойниках, которые внешне идентичны настоящим сайтам (например, сайту банка), но на самом деле являются подделкой.

Рекомендуемые меры предосторожности

- не открывать письма (и особенно вложения) от незнакомых адресатов;
- внимательно проверять адрес страницы, на которой вы собираетесь оставить личную информацию;
- не сохранять пароли в формах веб-страниц

7.Захват адресов электронной почты, веб-страниц и т.п.

Чаще всего к этому приводит использование "слабого" пароля для доступа к ресурсу, а также подбор ответа на контрольной вопрос, используемый для восстановления пароля в случае его возможной утери - использовать «стойкие» пароли (от 7 символов с использованием букв различного регистра и цифр);

Рекомендуемые меры предосторожности

- не использовать в качестве ответов на контрольные вопросы (и, конечно, в качестве самих паролей) информацию, которую достаточно легко узнать: дату рождения, имя, фамилию (ваши или близких родственников), кличку собаки, девичью фамилию;
- никогда не раскрывать перечисленную выше информацию (если она используется для описанных целей) незнакомым людям;
- не сохранять пароли в формах веб-страниц

Приложение 2
к Положению об использовании
сети Интернет и электронной почты

ОБЩИЕ МЕРЫ ПРЕДОСТОРОЖНОСТИ ПРИ РАБОТЕ С СЕТЬЮ ИНТЕРНЕТ И ЭЛЕКТРОННОЙ ПОЧТОЙ

1. Использование только разрешенного программного обеспечения

Использование нерегламентированного ПО может привести к утечке информации, заражению компьютера вирусом, выходу компьютера из строя из-за ошибок в написании ПО. Ответственность возлагается на пользователя

2. Отслеживание появления обновлений ПО, используемого на АРМах Учреждения, взаимодействующих с сетью Интернет

ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя. Ответственность возлагается на администраторов соответствующих компонентов В случае обнаружения в используемом ПО критических с точки зрения

безопасности уязвимостей и невозможности их устранения - приостановить эксплуатацию такого ПО Используемое ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя. Ответственность возлагается на пользователей и администраторов соответствующих компонентов АС Учреждения

4. Обязательное использование и своевременное обновление антивирусного ПО на ПК Учреждении, взаимодействующих с сетью Интернет.

Заражение вирусами может произойти и без «интерактивного» участия пользователя - достаточно связи с сетью Интернет. Ответственность возлагается на администраторов соответствующих компонентов

5. При работе с электронной почтой не открывать письма с вложенными файлами от неизвестных авторов, перед запуском/открытием любых файлов производить их антивирусную проверку

В последнее время наиболее распространенный канал распространения вирусов, а также кражи личной информации - электронная почта. В случае возникновения вопросов необходимо обратиться к администратору до принятия решения о дальнейших действиях. Ответственность возлагается на пользователей.

6. Запретить автоматическое сохранение и/или запуск файлов и элементов.

Большинство уязвимостей в программном обеспечении используются через файлы, ActiveX, скриптов из сети Интернет на рабочей станции пользователя загружаемые с веб-страниц, или через сами вебстраницы, которые содержат вредоносный/опасный код. Для опытных пользователей с разрешения Администрации допускается возможность предоставления выбора о необходимости загрузки/запуска таких элементов. Ответственность

возлагается на пользователей

7. Не рекомендуется сохранять пароли в формах при посещении веб-страниц

Это может привести к тому, что кто-то иной воспользуется (в том числе изменит пароль на новый) ресурсом, защищенным паролем. Ответственность возлагается на пользователей.