ПРИНЯТО
педагогическим советом
30 августа 2016 года
протокол №1

УТВЕРЖДАЮ
_____ и. о. директора Трегубов О. В.
Приказ № 61-А от 31 августа 2016 года

ПОЛОЖЕНИЕ
об использовании сети Интернет и электронной почты в МБОУСОШ №5

1. Общие положения

1.1. Настоящее Положение разработано во исполнение Концепции информационной безопасности МБОУСОШ №5 в соответствии с Федеральным законом № 149-ФЗ от 26.07.2006 г. «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами, и устанавливает порядок использования сети Интернет и электронной почты работниками МБОУСОШ №5 (далее Организация).

1.2. Действие настоящего Положения распространяется на работников Организации, подключенных к сети Интернет и учащихся.

2. Основные термины, сокращения и определения

Адрес IP - уникальный идентификатор АРМ, подключенного к ИС Организации, 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.

АС - автоматизированная система Организации - система, обеспечивающая хранение, обработку, преобразование и передачу информации Организации с использованием компьютерной и другой техники.

ИТ - информационные технологии - совокупность методов и процессов, обеспечивающих хранение, обработку, преобразование и передачу информации Организации с использованием средств компьютерной и другой техники.

Паспорт ПК - документ, содержащий полный перечень оборудования и программного обеспечения АРМ.

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.

Пользователь - работник Организации, использующий ресурсы Интернет для выполнения своих должностных обязанностей.

Реестр - документ «Реестр разрешенного к использованию ПО». Содержит перечень коммерческого ПО, разрешенного к использованию в Организации.

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 и электронной почты

3.1. Доступ в сеть Интернет и к электронной почте (далее - к Сервисам) в Организации осуществляется централизованно с применением специальных программно-технических средств защиты (межсетевых экранов).

3.2. На АРМ, подключенное к сети 1п1егпе1, в обязательном порядке должно быть установлено антивирусное программное обеспечение с актуальной антивирусной базой.

3.3. Доступ к Сервисам предоставляется ограниченному кругу Пользователей в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам, для обмена служебной информацией в виде электронных сообщений и документов в электронном виде в интересах Организации после ознакомления с настоящим Положением и Приложениями к нему.

3.4 Для доступа работников Организации к Сервисам допускается применение коммерческого или бесплатного ПО, входящего в Реестр разрешенного к использованию ПО.

3.5. Доступ работнику Организации к Сервисам может быть инициирован Руководителем структурного подразделения в случаях:

- необходимости организации АРМ для нового работника;
- необходимости выполнения работника новых (дополнительных) обязанностей, для которых требуется доступ к внешним ресурсам.

3.6. Операции по предоставлению доступа работников Организации к Сервисам и их техническому обеспечению выполняются в соответствии с Порядком доступа к информационным, программным и аппаратным ресурсам МБОУСОШ №5 директором МБОУСОШ №5 Организации через заявки на имя руководителя Организации, подписанные руководителем структурного подразделения и согласованные с заместителем директора по ИТ.

При использовании Сервисов необходимо:

- соблюдать требования настоящего Положения;
- использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;
- ставить в известность отдел по защите информации о любых фактах нарушения требований настоящего Положения;

- типичные угрозы при работе с Сервисами и рекомендации по их предотвращению приведены в Приложении №1;
- общие меры предосторожности при работе с Сервисами приведены в Приложении №2.

3.7. При использовании Сервисов запрещено:

3.7.1. Использовать предоставленный Организацией доступ к Сервисам в личных целях.

3.7.2. Использовать специализированные аппаратные и программные средства, позволяющие работникам Организации получить несанкционированный доступ к Сервисам.

3.7.3. 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, согласованным с отделом по защите информации заранее;
- информацию, полностью или частично, защищенную авторскими или другим 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.

3.7.4. Фальсифицировать свой 1Р-адрес, а также прочую служебную информацию.

3.7.5. Распространять и устанавливать на других ПЭВМ любое программное обеспечение и данные, полученные с использованием Сервисов.

3.7.6. Осуществлять попытки несанкционированного доступа к ресурсам Сети, проведение сетевых атак и сетевого взлома и участие в них.

3.7.7. Переходить по ссылкам и открывать вложенные файлы входящих электронных сообщений, полученных от неизвестных отправителей.

3.7.7. По собственной инициативе осуществлять рассылку (в том числе и массовую) электронных сообщений, если рассылка не связана с выполнением служебных обязанностей.

3.7.10. Использовать адрес электронной почты для оформления подписки на периодическую рассылку материалов из сети Интернет, не связанных с исполнением служебных обязанностей.

3.7.11. Публиковать свой электронный адрес, либо электронный адрес других работников Организации на общедоступных Интернет-ресурсах (форумы, конференции и т.п.).

3.7.12. Предоставлять работникам Организации и третьим

лицам доступ к своему электронному почтовому ящику.

3.7.13. Перенаправлять электронные сообщения с личных почтовых ящиков на корпоративный.

3.7.14. Запрещается использование в качестве паролей для доступа к ресурсам Сервисов паролей, аналогичных паролям, используемым для доступа к ресурсам Организации.

3.7.15. Запрещается отключать установленное на АРМ антивирусное программное обеспечение.

3.8. Содержание Интернет-ресурсов, а также файлы, загружаемые из Сервисов, подлежат обязательной проверке на отсутствие вредоносного ПО.

3.9. Информация о посещаемых работниками Организации Интернетресурсах протоколируется для последующего анализа и, при необходимости, может быть предоставлена Руководителям структурных подразделений, а также Руководству Организации для контроля.

3.11. Директор МБОУСОШ №5оставляет 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.

3.12. Организация оставляет за собой право доступа к электронным сообщениям работников с целью их архивирования и централизованного хранения, а также мониторинга выполнения требований настоящего Положения.

3.13. В случае нарушения пунктов Положения директор МБОУСОШ №5вправе отключить АРМ от Сервисов, уведомив об этом руководство структурного подразделения.

3.14. Расследование допущенных нарушений Положения производится на основании Регламента реагирования на инциденты информационной безопасности, утвержденного в Организации.

4. Ответственность

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

5. Заключительные положения

5.1. Анализ актуальности данного Положения должен проводиться директором МБОУСОШ №5 не реже одного раза в год, а также в каждом случае внедрения новых сервисов в дополнение к имеющимся. В случае если в ходе такого анализа была установлена необходимость внесения изменений в Положение, новая редакция Положения должна быть утверждена приказом по Организации.

5.2. Контроль над соблюдением требований данного Положения проводится директором МБОУСОШ №5.

Приложение №1 к Положению об использования сети Интернет и электронной почты в МБОУСОШ №5

Типичные угрозы
при работе с сетью Интернет и электронной почтой

№ п/п	Угроза	Примечание	Рекомендуемые меры предосторожности
1.	Заражение компьютера вирусом.	Чаще всего заражение вирусами происходит при посещении специально созданных «вредоносных» вебстраниц, «хакерских» сайтов, сайтов «для взрослых».	- не посещать перечисленные сайты; - установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
2.	Заражения компьютера вирусом при просмотре почтовых сообщений.	Обычно происходит при открытии прикрепленного к письму файла.	- 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.	- использовать только принятое к использованию в Организации программное обеспечение; - установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
4.	Предоставление возможности	Такая возможность может быть получена как	- использовать только принятое к

	удаленного управления компьютером.	с ведома пользователя (при использовании им ПО, выполняющего данную функцию), так и без его ведома (при заражении компьютера вирусом).	использованию в Организации 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 злоумышленником или из-за заражения вирусом.	- использовать только принятое к использованию в Организации программное обеспечение; - 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.	- 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); - 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 использования сети Интернет и электронной почты в МБОУСОШ №5

Общие меры предосторожности при работе с сетью Интернет и электронной почтой

№ п/п	Мера предосторожности	Примечание
1.	Использование только разрешенного отделом информационных технологий и отделом по защите информации 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 компонентах АС Организации, 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.
3.	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 Организации.
4.	Обязательное использование и своевременное обновление антивирусного ПО на компонентах АС Организации, взаимодействующих с сетью Интернет, в режиме мониторинга событий.	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 в отдел по защите информации до принятия решения о дальнейших действиях. Ответственность возлагается на пользователей.
6.	Запретить автоматическое сохранение и/или запуск файлов и элементов Ac1^eX, скриптов из сети Интернет на рабочей станции	Большинство уязвимостей в программном обеспечении используются через файлы, загружаемые с веб-страниц, или

	пользователя.	через сами веб-страницы, которые содержат вредоносный/опасный код. Для опытных пользователей с разрешения отдела по защите информации допускается возможность предоставления выбора о необходимости загрузки/запуска таких элементов. Ответственность возлагается на пользователей.
7.	Не рекомендуется сохранять пароли в формах при посещении вебстраниц.	Это может привести к тому, что кто-то иной воспользуется (в то числе - изменит пароль на новый) ресурсом, защищенным паролем. Ответственность возлагается на пользователей.