УТВЕРЖДАЮ
Заведующий МБДОУ д/с № 164
_____Н.Г.Быкова
Приказ № 02/1 - ОД от 09.01.2018г.

Инструкция
об использовании сети Интернет
и электронной почты

1. Общие положения

1.1. Настоящее Инструкция разработана во исполнение Концепции информационной безопасности 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 актами, и устанавливает порядок использования сети Интернет и электронной почты работниками муниципального бюджетного дошкольного образовательного учреждения детский сад комбинированного вида № 164 города Ставрополя (далее Учреждение).

1.2. Действие инструкции распространяется на работников Учреждения, подключенных к сети Интернет, подрядчиков и третью сторону.

2. Основные термины, сокращения и определения

2.1. Адрес IP – уникальный идентификатор АРМ, подключенного к ИС Учреждения, а также сети Интернет.

2.2. АРМ – автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения определенной производственной задачи.

2.3. Интернет- глобальная ИС, обеспечивающая удаленный доступ к ресурсам различного содержания и направленности.

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

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

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

2.7. ПК – персональный компьютер.

1.1. ПК – персональный компьютер.

2.8. ПО – программное обеспечение вычислительной техники, базы данных.

2.9. ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

2.10. ПО коммерческое – ПО сторонних производителей (правообладателей).

2.11. Предоставляется в пользование на возмездной (платной) основе.

2.12. Пользователь – работник Учреждения, использующий ресурсы Интернет для выполнения своих должностных обязанностей.

2.13. Реестр – документ «Реестр разрешенного к использованию ПО». Содержит перечень коммерческого ПО, разрешенного к использованию в Учреждении.

2.14. Электронная почта – сервис обмена электронными сообщениями в рамках АС Учреждения (внутренняя электронная почта) и общедоступных сетей Интернет (внешняя электронная почта).

2.15. Электронное почтовое сообщение – сообщение, формируемое отправителем с помощью почтового клиента и предназначенное для передачи получателю посредством электронной почты.

2.16. Электронный документ – документ, в котором информация представлена в электронно-цифровой форме.

2.17. 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 Учреждения осуществляется централизованно с применением специальных программно-технических средств защиты (межсетевых экранов).

3.2. Доступ к Сервисам с использованием мобильных устройств (мобильного интернета) допускается только в удаленных подразделениях (филиалах) Учреждения. Все мобильные устройства должны быть учтены в журнале учета съемных носителей и устройств передачи данных Учреждения.

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

3.4. 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 Учреждения после ознакомления с настоящим Положением и Приложениями к нему.

3.5. Для доступа работников Учреждения к Сервисам допускается применение коммерческого или бесплатного ПО, входящего в Реестр разрешенного к использованию ПО и указанного в Паспорте ПК.

3.6. Доступ работнику Учреждения 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.

3.7. Операции по предоставлению доступа работников Учреждения к Сервисам и их техническому обеспечению выполняются через заявки на имя руководителя учреждения, подписанные руководителем структурного подразделения и согласованные с начальником отдела по защите информации.

3.8. При использовании Сервисов необходимо:

3.8.1. Соблюдать требования инструкции.

3.8.2. Использовать сеть Интернет исключительно для выполнения своих служебных обязанностей.

3.8.3. Ставить в известность ответственного по защите информации о любых фактах нарушения требований инструкции.

3.8.4. Типичные угрозы при работе с Сервисами и рекомендации по их предотвращению приведены в Приложении №1.

3.8.5. Общие меры предосторожности при работе с Сервисами приведены в Приложении №2.

3.9. При использовании Сервисов запрещено:

3.9.1. Использовать предоставленный Учреждением доступ к Сервисам в личных целях.

3.9.2. Использовать специализированные аппаратные и программные средства, позволяющие работникам Учреждения получить несанкционированный доступ к Сервисам.

3.9.3. 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.

3.9.4. Фальсифицировать свой IP-адрес, а также прочую служебную информацию.

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

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

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

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

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

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

3.9.12. Предоставлять работникам Учреждения (за исключением сотрудников отдела информационных технологий и отдела по защите информации) и третьим лицам доступ к своему электронному почтовому ящику.

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

3.9.14. Запрещается использование в качестве паролей для доступа к ресурсам Сервисов паролей, аналогичных паролям, используемым для доступа к ресурсам Учреждения.

3.9.15. Запрещается отключать установленное на АРМ антивирусное программное обеспечение.

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

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

3.12. Отдел по защите информации 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.

3.13. Учреждение оставляет за собой право доступа к электронным сообщениям работников с целью их архивирования и централизованного хранения, а также мониторинга выполнения требований настоящей инструкции.

3.14. В случае нарушения пунктов инструкции ответственный по защите информации вправе отключить АРМ от Сервисов, уведомив об этом руководителю.

4. Ответственность

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

5. Заключительные положения

5.1. Анализ актуальности инструкции должен проводиться ответственным по защите информации 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 инструкцию.

Приложение № 1

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).	- использовать только принятое к использованию в Организации программное обеспечение; - установить, своевременно обновлять и не отключать
		Также причиной утечки может оказаться заражение компьютера вирусом.	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).	- использовать только принятое к использованию в Организации программное обеспечение; - установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
5.	Потеря или функциональностирабочей (полной частичной) 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 веб-страницах, 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,	- использовать «стойкие» пароли (от 7 символов, с использованием букв различного регистра и цифр);
		используемый для восстановления пароля в случае его возможной утери.	- 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

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 Учреждения, взаимодействующих с сетью Интернет.	ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя. Ответственность возлагается на администратора.
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 администратора.
4.	Обязательное использование и своевременное обновление антивирусного ПО на компонентах АС Учреждения, 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 администратора.

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 ActiveX, скриптов из сети Интернет на рабочей станции пользователя.	Большинство уязвимостей в программном обеспечении используются через файлы, загружаемые с веб-страниц, или 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.