УТВЕРЖДАЮ
Директор ГПОАУ АТК
_____Кривцов О.А.
_____12.02_____2018

ПОЛОЖЕНИЕ
об использовании сети Интернет и электронной почты

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее положение устанавливает порядок использования сети Интернет и электронной почты сотрудниками Государственного профессионального образовательного автономного учреждения Амурской области «Амурский технический колледж» (далее по тексту – ГПОАУ АТК).
1.2. Настоящее положение имеет статус локального нормативного акта ГПОАУ АТК, регламентирующего использование сети Интернет. Если нормами действующего законодательства Российской Федерации предусмотрены иные требования, чем настоящим Положением, применяются нормы действующего законодательства.

2. ОСНОВНЫЕ ТЕРМИНЫ, СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

Адрес IP – уникальный идентификатор АРМ, подключенного к информационной системы ГПОАУ АТК, а также сети Интернет.
АРМ – автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения служебных обязанностей.
Интернет – глобальная информационная система, обеспечивающая удаленный доступ к ресурсам различного содержания и направленности.
АС – автоматизированная система ГПОАУ АТК – система, обеспечивающая хранение, обработку, преобразование и передачу информации ГПОАУ АТК с использованием компьютерной и другой техники.
ИТ – информационные технологии – совокупность методов и процессов, обеспечивающих хранение, обработку, преобразование и передачу информации ГПОАУ АТК с использованием средств компьютерной и другой техники.
Паспорт АРМ – 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 ГПОАУ АТК, использующий ресурсы Интернет для выполнения своих должностных обязанностей.
Реестр – документ «Реестр разрешенного к использованию ПО». Содержит перечень ПО, разрешенного к использованию в ГПОАУ АТК.
Электронная почта – сервис обмена электронными сообщениями в рамках АС ГПОАУ АТК (внутренняя электронная почта) и 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 ГПОАУ АТК осуществляется централизованно с применением специальных программно-технических средств защиты (Интернет Контроль Сервер).

3.2. На АРМ, подключенное к сети Интернет, 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 ГПОАУ АТК после ознакомления с настоящим Положением и Приложениями к нему.

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

3.5. При использовании Сервисов необходимо:

- соблюдать требования настоящего Положения;

- использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;
- ставить в известность системного администратора ГПОАУ АТК 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.

3.6. При использовании Сервисов запрещено:

3.6.1. Использовать предоставленный ГПОАУ АТК доступ к Сервисам в личных целях.

3.6.2. Использовать специализированные аппаратные и программные средства, позволяющие работникам ГПОАУ АТК получить несанкционированный доступ к Сервисам.

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, согласованным с системным администратором 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.

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

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

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

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

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

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

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

3.6.11. Предоставлять работникам ГПОАУ АТК (за исключением системного администратора ГПОАУ АТК) и третьим лицам доступ к своему электронному почтовому ящику.

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

3.6.13. Запрещается использование в качестве паролей для доступа к ресурсам Сервисов паролей, аналогичных паролям, используемым для доступа к ресурсам ГПОАУ АТК.

3.6.14. Запрещается отключать установленное на АРМ антивирусное программное обеспечение.

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

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

3.11. Системный администратор ГПОАУ АТК 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.

3.12. ГПОАУ АТК 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 системный администратор ГПОАУ АТК вправе отключить АРМ от Сервисов, уведомив об этом руководство структурного подразделения.

4. ОТВЕТСТВЕННОСТЬ

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

5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

5.1. Анализ актуальности данного Положения должен проводиться системным администратором ГПОАУ АТК 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 ГПОАУ АТК.

5.2. Контроль над соблюдением требований данного Положения проводится системным администратором ГПОАУ АТК.

Приложение №1

к Положению об использовании сети Интернет и электронной почты в ГПОАУ АТК

Типичные угрозы при работе с сетью Интернет и электронной почтой

№	Угроза	Примечание	Рекомендуемые меры предосторожности
1	Заражение компьютера вирусом	Чаще всего заражение происходит при посещении специально созданных «вредоносных» веб-страниц, сайтов «для взрослых»	➢ Посещать только надежные Интернет-ресурсы ➢ Использовать антивирус и регулярно обновлять антивирусные базы ➢ Не отключать антивирус
2	Заражение компьютера вирусом при просмотре электронной почты	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 вам неизвестен
3	Утечка информации	Уязвимым может оказаться неизвестное, бесплатное и малораспространенное программное обеспечение. Также причиной утечки информации может оказаться заражение компьютера вирусом.	➢ Использовать только принятое к использованию в ГПОАУ АТК программное обеспечение ➢ Использовать антивирус и регулярно обновлять антивирусные базы ➢ Не отключать антивирус
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 ГПОАУ АТК программное обеспечение ➢ Использовать антивирус и регулярно обновлять антивирусные базы ➢ Не отключать антивирус
5	Потеря функциональнос	Происходит чаще всего вследствие использования	➢ Использовать только принятое к использованию в ГПОАУ

	ти (полной или частичной) ПК	уязвимостей ПО злоумышленником или из-за заражения вирусом	АТК программное обеспечение ➢ Использовать антивирус и регулярно обновлять антивирусные базы ➢ Не отключать антивирус
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 собираетесь оставить личную информацию ➢ Не сохранять пароли в формах веб-страниц
7	Захват адресов электронной почты, личных кабинетов и т.п.	Чаще всего к этому приводит использование «слабого» пароля для доступа к ресурсу	➢ Использовать «стойкие» пароли (от 7 символов, с использованием букв различного регистра, цифр и других символов) ➢ Не сохранять пароли в формах веб-страниц

Приложение №2

Общие меры предосторожности при работе с сетью Интернет и электронной почтой

№	Мера предосторожности	Примечание
1	Использование только разрешенного системным администратором программного обеспечения	Использование нерегламентированного ПО может привести к утечке информации, заражению компьютера вирусом, выходу компьютера из строя. Ответственность возлагается на пользователей.
2	Отслеживание появления обновлений ПО, используемого на компьютерах, взаимодействующих с сетью Интернет.	ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компьютера из строя. Ответственность возлагается на системного администратора.
3	В случае обнаружения в используемом ПО критических с точки зрения безопасности уязвимостей и невозможности их устранения – приостановить эксплуатацию такого ПО.	ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компьютера из строя. Ответственность возлагается на системного администратора.
4	Обязательное использование и своевременное обновление антивирусного ПО на компьютерах, взаимодействующих с сетью Интернет	Заражение вирусами может произойти и без «интерактивного» участия пользователя – достаточно связи с сетью Интернет. Ответственность возлагается на системного 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 к системному администратору 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	Большинство уязвимостей в программном обеспечении используются через файлы, загружаемые с веб-страниц, или через сами веб-страницы, которые содержат

	пользователя.	вредоносный/опасный код. Для опытных пользователей с разрешения системного администратора 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 то числе – изменит пароль на новый) ресурсом, защищенным паролем. Ответственность возлагается на пользователей.