

2.3. Для работы в сети «Интернет» используются автоматизированные рабочие места, удовлетворяющие техническим требованиям, необходимым для выполнения этих задач. В качестве программного обеспечения для в сети «Интернет», рекомендуются к использованию браузеры семейства Microsoft Internet Explorer. Возможно использование других браузеров либо лицензионных, либо свободно распространяемых, при согласовании специалистом по защите информации.

2.4. В целях контроля использования ресурсов сети «Интернет», разграничения прав доступа в «Интернет», снижения нагрузки на каналы передачи данных, обеспечения безопасности доступа в Учреждении используется прокси-сервер. Любое программное обеспечение авторизованное для применения в Учреждении и имеющее функционал доступа к информационным системам с использованием сети «Интернет» должно функционировать только через прокси-сервер.

2.5. Используемое в учреждении программное обеспечение, в том числе для доступа к ресурсам «Интернет», не должно предоставлять возможности создания несанкционированных, неконтролируемых подключений из сети «Интернет» к локальной сети Учреждения.

2.6. При работе в сети Интернет пользователями запрещается:

- загружать, самостоятельно устанавливать прикладное, операционное, сетевое и другие виды программного обеспечения, а также осуществлять обновления, если эта работа не входит в его должностные обязанности;
- подтверждать любые запросы ресурсов в сети «Интернет» на установку любого программного обеспечения, а так же переход на другие ресурсы «Интернет», если они не известны пользователю.
- использование рабочего времени и ресурсов сети Интернет в личных целях;
- подключаться к ресурсам «Интернет», используя персональный компьютер Учреждения через не служебный канал доступа (сотовый телефон, модем, и другие устройства);
- посещение ресурсов, создание, распространение информационных материалов и сообщений, содержащих оскорбительную или провокационную информацию (к примеру, материалы, касающиеся сексуальных домогательств, расовых унижений, дискриминации по половому признаку, затрагивающие в оскорбительной форме вопросы возраста или сексуальной ориентации, религиозные или политические пристрастия, национальность или состояние здоровья, нарушающие законодательство РФ);
- несанкционированное распространение информации рекламного характера;
- осуществлять доступ в социальные сети в «Интернет», если соответствующие функциональные обязанности не указаны в должностной инструкции;
- применять программные средства удаленного управления автоматизированным рабочим местом и использовать таковые в любом виде;
- использовать личный адрес электронной почты Учреждения для регистрации в публичных сервисах, если персонализированный доступ к публичному сервису (или получение информации от публичных сервисов) не требуется для выполнения функциональных обязанностей;
- подключать к автоматизированному рабочему месту любое неавторизованное телекоммуникационное оборудование, осуществлять с помощью него доступ в «Интернет» на территории Учреждения без согласования с руководителем Учреждения;
- использовать специальные программные средства обеспечения анонимности доступа в «Интернет».

2.7. Работники Учреждения при работе в «Интернет» должны самостоятельно обеспечивать конфиденциальность информации Учреждения, доступ к которой они получили в рамках функциональной деятельности.

2.8. Любые сообщения, кроме официальных публикаций Учреждения, размещаемые пользователем в публичный доступ сети «Интернет», должны включать ссылку о том, что выраженная точка зрения является личной, и не может быть расценена как официальная позиция Учреждения.

2.9. Запрещенные в п. 2.6 для использования ресурсы «Интернет» должны блокироваться на прокси-сервере. Пользователи обязаны незамедлительно сообщать руководителю об обнаруженных и доступных из локальной сети незаблокированных ресурсах «Интернет». Прокси-сервер протоколирует и хранит действия пользователей в сети «Интернет» на срок не менее чем один год. Протоколы прокси-сервера защищаются от несанкционированного доступа.

III. Основные правила работы.

3.1. За одним рабочим местом должно находиться не более одного работника. Запрещается

работать под чужим регистрационным именем, сообщать кому-либо свой пароль, одновременно входить в систему более чем с одного персонального компьютера.

3.2. Каждому работнику, при наличии технической возможности, предоставляется персональный каталог, предназначенный для хранения личных файлов общим объемом не более 100 Мб, а также возможность работы с почтовым ящиком для отправки и получения электронной почты.

3.3. Работнику разрешается записывать полученную информацию на личные носители информации, предварительно проверенные на наличие вирусов.

3.4. Работнику запрещено вносить какие-либо изменения в программное обеспечение, установленное на персональном компьютере.

3.5. Разрешается использовать оборудование только для работы с информационными ресурсами и электронной почтой и только в образовательных целях или для осуществления научных изысканий, выполнения гуманитарных и культурных проектов. Любое использование оборудования в коммерческих целях запрещено.

3.6. Работник обязан сохранять оборудование в целостности и сохранности.

3.7. Работник обязан помнить свой пароль.

3.8. При нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния) работник несет материальную ответственность.

3.9. Доступ к информационным системам сети «Интернет» для обучающихся Учреждения отсутствует.

IV. Заключительные положения.

4.1. Положение вступает в силу с момента его утверждения.

4.2. Положение является локальным актом образовательного Учреждения. Внесение изменений и дополнений в Положение осуществляется в порядке его принятия.

4.3. Настоящее Положение может быть изменено (дополнено) локальным актом образовательного Учреждения.