

РЕГЛАМЕНТ использования информационных ресурсов сети Интернет

1. Общие положения

- 1.1. Настоящий регламент устанавливает единые требования по обеспечению информационной безопасности МАОДО «Детская школа искусств им.А.В.Ливна» (далее - учреждение) при использовании ресурсов и каналов передачи данных сети Интернет.
- 1.2. Служебный сервис доступа к сети Интернет предназначен для обслуживания сотрудников учреждения с целью предоставления возможности оперативного получения, обработки информации, обмена информацией и повышения эффективности выполнения функциональных задач.
- 1.3. В настоящем Регламенте используются следующие основные термины и понятия:
браузер - специализированное ПО, являющееся средством обработки и отображения на автоматизированных рабочих местах (далее - АРМ) разных составляющих информационных систем (далее - ИС), а так же для предоставления интерфейса между ИС и её пользователем;
прокси-сервер - программный комплекс, используемый в качестве промежуточного звена между браузером и конечной ИС;
публичный сервис - ИС в сети Интернет, использование которой осуществляется на бесплатной основе или использование которой не регулируется договорными отношениями между учреждением и владельцем сервиса (его полномочным представителем).

2. Основные требования

- 2.1. В связи с тем, что с помощью локальной сети пользователи получают доступ к ИС учреждения, содержащим служебную информацию различной степени конфиденциальности, локальная сеть изолирована от сети Интернет. Деятельность пользователей в Интернет может контролироваться, протоколироваться и периодически проверяться ответственным за информационную безопасность работником.
- 2.2. Доступ в сеть Интернет предоставляется работникам учреждения исключительно для выполнения ими своих функциональных обязанностей. При осуществлении доступа в Интернет, в отношении информации учреждения ограниченного использования должен соблюдаться режим конфиденциальности.
- 2.3. Для работы в сети Интернет используются АРМ, удовлетворяющие техническим требованиям, необходимым для выполнения этих задач. В качестве программного обеспечения (далее - ПО) 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 ПО авторизованное для применения в учреждении и имеющее функционал доступа к ИС с использованием сети Интернет должно функционировать только через прокси-сервер.
- 2.5. Используемое в учреждении ПО, 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 пользователям запрещается:

- использование рабочего времени и ресурсов сети Интернет в личных целях; посещение ресурсов, создание, распространение информационных материалов и сообщений, содержащих оскорбительную или провокационную информацию предусмотренную действующим законодательством Российской Федерации (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 АРМ 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 АРМ любое неавторизованное телекоммуникационное оборудование, осуществлять с помощью него доступ в Интернет на территории учреждения;
- самостоятельно изменять конфигурацию ПО используемого для доступа в Интернет;
- использовать специальные программные средства обеспечения анонимности доступа в Интернет;
- подтверждать любые запросы ресурсов в сети Интернет на установку любого ПО, а так же переход на другие ресурсы Интернет, если они не известны пользователю.

2.7. Пользователи 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 для использования ресурсы Интернет должны блокироваться на прокси-сервере. Пользователи обязаны незамедлительно сообщать лицу, ответственному за защиту информации либо директору учреждения 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.

2.10. Контроль выполнения требований настоящего Регламента, возлагается на ответственное в учреждении лицо.

3. Основные правила работы

3.1. Пользователь обязан выполнять все требования лица, ответственного за защиту информации. В начале работы пользователь обязан зарегистрироваться в системе, т.е. ввести свое имя регистрации (логин) и пароль. За одним рабочим местом должно находиться не более одного пользователя. Запрещается работать под чужим регистрационным именем, сообщать кому-либо свой пароль, одновременно входить в систему более чем с одной рабочей станции.

3.2. Пользователю разрешается записывать полученную информацию на личные носители информации, предварительно проверенные на наличие вирусов.

3.3. Пользователю запрещено вносить какие-либо изменения в ПО, установленное как на рабочей

станции, так и на серверах, а также производить без согласования со специалистом по защите информации установку ПО на жесткий диск рабочей станции.

- 3.4. 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.
- 3.5. Пользователь обязан сохранять оборудование в целостности и сохранности.
- 3.6. Пользователь обязан помнить свой пароль.
- 3.7. При нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность.
- 3.8. Пользователь обязан руководствоваться действующим законодательством РФ, включая, но не ограничиваясь:
 - Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
 - Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"
 - иные законы и нормативные акты Российской Федерации
- 3.9. При возникновении технических проблем пользователь обязан поставить в известность администрацию учреждения.