ПРИНЯТ
на заседании Ученого совета
Самарской государственной
академии культуры и искусств
22 октября 2013 г.,
протокол №2

ПОРЯДОК

доступа работников к информационно-телекоммуникационным сетям, базам данных, учебным и методическим материалам, музейным фондам, материально-техническим средствам обеспечения образовательной деятельности, необходимым для качественного осуществления педагогической, научной или исследовательской деятельности академии

I. Общие положения

1. Настоящим Порядком определяются организационные условия доступа работников академии к информационно-телекоммуникационным сетям, базам данных, учебным и методическим материалам, музейным фондам, материально-техническим средствам обеспечения образовательной деятельности, необходимым для качественного осуществления педагогической, научной или исследовательской деятельности федеральной государственной образовательной организации высшего образования «Самарская государственная академия культуры и искусств» (далее – академия, СГАКИ).

2. Настоящий Порядок разработан на основании:

Федерального закона от 29.12.2012 г. №273-ФЗ «Об образовании в Российской Федерации»;

Устава СГАКИ;

Положения о корпоративной компьютерной сети СГАКИ;

Положения о веб-сайте СГАКИ;

других локальных актов академии.

3. Доступ педагогических работников к вышеперечисленным услугам осуществляется в целях качественного осуществления ими педагогической, методи-

ческой, научно-исследовательской и иной профессионально значимой деятельности.

4. В соответствии с подпунктом 7 пункта 3 ст. 47 Федерального закона Российской Федерации от 29 декабря 2012 г. №273-ФЗ «Об Образовании в Российской Федерации» педагогические работники имеют право на бесплатное пользование библиотеками и информационными ресурсами, а также доступ к информационно-телекоммуникационным сетям и базам данных, учебным и методическим материалам, музейным фондам, материально-техническим средствам обеспечения образовательной деятельности, необходимым для качественного осуществления педагогической, научной или исследовательской деятельности.

5. Действие настоящего Порядка распространяется на пользователей любого компьютерного оборудования (компьютеры, компьютерная периферия, мультимедийное оборудование, коммуникационное оборудование и другие компьютерные материально-технические средства обеспечения образовательной деятельности), локальной сети академии, информационных ресурсов и баз данных, включая информационные библиотечные и музейные фонды (далее – ресурсы), а также на пользователей, осуществляющих удаленный доступ к оборудованию локальной сети, информационным ресурсам и базам данных, из других локальных сетей и Интернет.

6. В Порядке определены права и обязанности пользователей информационно-вычислительной техники, информационных ресурсов и баз данных вне зависимости от прав доступа, а также ответственность за несоблюдение данного Порядка.

7. Настоящий Порядок доводится в установленном порядке руководителями структурных подразделений академии до сведения работников при приеме их на работу.

II. Основные термины и определения

1. В настоящем Порядке используются следующие понятия и определения:

а) аппаратные средства, оборудование – материальные объекты, используемые в технике;

б) защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями законодательных и иных нормативных документов или в соответствии с требованиями, устанавливаемыми собственником информации;

в) несанкционированный доступ – доступ к информации, нарушающий установленные правила разграничения доступа, с использованием технических средств;

г) пользователь – обучающиеся и работники академии, получающие доступ к информационным и вычислительным ресурсам сети, оборудованию и другому материально-техническому обеспечению образовательной деятельности;

д) ответственный пользователь информационных ресурсов - это сотрудник СГАКИ, который в силу своих полномочий, должностных обязанностей или на основании указаний руководства академии, несет ответственность за содержание информационного ресурса или базы данных;

е) программные средства (программное обеспечение) – программы, а также средства экранного и печатного представления – пользовательский интерфейс;

ж) автоматизированное рабочее место (АРМ) – аппаратно-программный комплекс, зарегистрированный и подключенный к сети, и имеющий возможность использовать сетевые ресурсы и услуги, программное обеспечение и периферийное оборудование в производственных целях;

з) сервер – компьютер, подключенный к сети и предоставляющий сетевые ресурсы и услуги;

и) сетевые ресурсы – логические устройства или другие структуры представления данных для пользователей, доступные через сеть;

к) технические средства обучения – системы, комплексы, устройства и аппаратура, применяемые для предъявления и обработки информации в образовательном процессе с целью повышения его эффективности.

III. Режим доступа к сетевым ресурсам академии

1. Серверное и сетевое оборудование локальной вычислительной сети академии (далее – сети) работает круглосуточно.

2. Гарантированный доступ пользователей к информационным и вычислительным ресурсам - с 8.15 до 17.00 в рабочие дни.

3. В нерабочие дни и с 17.00 до 8.15 в рабочие дни, ресурсы доступны без гарантии их непрерывной работы, то есть Центр информационных технологий (далее ЦИТ) оставляет за собой право отключать пользователей от ресурсов без предупреждения и не несет ответственность за возможную потерю несохраненных данных.

4. При необходимости обеспечения гарантированной работы с сетевыми ресурсами вне рамок установленного выше регламента пользователь должен заранее (не менее чем за 3 часа до окончания рабочего дня) подать на имя начальника ЦИТ письменную заявку, утвержденную руководителем подразделения.

5. При профилактиках сетевого оборудования, обновлении программного обеспечения, переходе на новую системную платформу, версию СУБД или сайта и т.п. режим доступа регламентируется распоряжением по академии.

IV. Порядок получения доступа к информационным ресурсам академии

1. На новые подключения к ресурсам оформляется заявка, в которой указывается фамилия, имя, отчество, должность, номер аудитории, телефон пользователя, ресурс, к которому требуется подключиться, обоснование такого подключения, за счет каких средств осуществляется оплата за пользование ресурсом и подписывается руководителем подразделения и (или) ответственным пользователем информационных ресурсов.

2. Пользователь допускается к работе на персональном компьютере (далее – ПК), подключенном к сети, после прохождения инструктажа в ЦИТ. При изменении прав доступа пользователя или изменении подразделения (смена места работы) или увольнение руководитель подразделения обязан известить в течение суток ЦИТ для блокирования учетных записей данного пользователя.

3. При необходимости пользователю выдается уникальный идентификатор (логин) и пароль, обеспечивающие авторизованный доступ к ресурсам.

4. Работники академии осуществляют доступ к полнотекстовым электронным базам данных (например, электронные библиотечные системы, базы данных, электронные каталоги, репозитарии и т.п.) на условиях, указанных в договорах, лицензионных соглашениях заключенных СГАКИ с правообладателем электронных ресурсов.

5. В зависимости от условий, определенных в договорах и лицензионных соглашениях с правообладателями информационных ресурсов, работа с электронными документами и изданиями возможна:

в залах научной библиотеки;

с ПК подключенных к локальной сети академии;

с любого ПК, подключенного к сети Интернет.

6. Сотрудники научной библиотеки предоставляют заинтересованным работникам академии информацию об образовательных, научных, нормативно-технических и других электронных ресурсах доступных к пользованию, условиях и порядке доступа к каждому отдельному электронному ресурсу.

7. Доступ педагогических работников, а также обучающихся и организованных групп обучающихся под руководством работника (работников) к библиотечным и музейным фондам академии, а также структурных подразделений осуществляется на основании соответствующих локальных актов, регламентирующих деятельность этих подразделений.

V. Порядок получения материально-технического обеспечения учебного процесса и программно-технических средств обучения во временное пользование

1. Доступ работников академии к материально-техническим средствам обеспечения образовательной деятельности осуществляется:

без ограничения к учебным аудиториям и иным местам проведения занятий во время, определенное в расписании занятий;

к учебным аудиториям и местам проведения занятий во время вне определенного расписанием занятий по письменному согласованию с должностным лицом, ответственным за данное помещение с уведомлением учебно-методического управления о параметрах его использования.

2. Движимые (переносные) материально-технические средства обеспечения образовательной деятельности (видеопроекторы, звуковое и световое оборудование и др. имущество) предоставляется преподавателю по письменной заявке (с указанием, целей, места и сроков использования оборудования) по предварительному согласованию с руководителем структурного подразделения, на балансе которого числится данное имущество.

3. Руководитель структурного подразделения, на балансе которого числятся материально-технические средства обеспечения образовательной деятельности, вправе отказать работнику в предоставлении требуемого оборудования в случае его недоступности (занятости) или неисправности.

4. Работник, получивший во временное пользование движимые (переносные) материально-технические средства обеспечения образовательной деятельности, принимает на себя обязанности по обеспечению сохранности, технической исправности и правильной эксплуатации названного оборудования.

5. По истечении времени, указанного в заявке, работник обязан вернуть все предоставленное оборудование в распоряжение структурного подразделения, на балансе которого числится данное имущество.

VI. Обязанности и права пользователей при использовании оборудования и сетевых ресурсов

1. Пользователи обязаны:

а) ознакомиться с настоящим Порядком до начала работы с оборудованием;

б) пройти регистрацию, инструктаж и получить личные атрибуты доступа (логин, пароль) для работы с информационными системами и оборудованием с установленными полномочиями;

в) устанавливать личный пароль доступа в соответствии с требованиями к

паролям пользователей и порядком работы с ними;

г) использовать компьютерное оборудование исключительно для деятельности, предусмотренной производственной необходимостью и должностными инструкциями;

д) обеспечить установку компьютерного оборудования в удобном для работы месте, на прочной (устойчивой) поверхности, вдали от потенциальных источников загрязнения (открытые форточки, цветочные горшки, аквариумы, чайники, вазы с цветами и прочее), так, чтобы вентиляционные отверстия средств вычислительной техники были открыты для циркуляции воздуха;

е) проводить мероприятия по обеспыливанию рабочего места не реже одного раза в неделю с соблюдением требований техники безопасности и инструкции по эксплуатации оборудования;

ж) незамедлительно сообщать о замеченных неисправностях компьютерного оборудования и недостатках в работе программного обеспечения в ЦИТ;

з) рационально пользоваться ограниченными разделяемыми (общими) ресурсами (дисковой памятью компьютеров общего пользования, пропускной способностью локальной сети) и расходными материалами;

и) выполнять требования сотрудников ЦИТ, а также лиц, назначенных ответственными за эксплуатацию конкретного оборудования, в части, касающейся работы в сети;

к) выполнять правила работы в вычислительной сети;

л) выполнять обязательные рекомендации ответственных лиц по защите информации и персональных данных;

м) по запросу сотрудников ЦИТ предоставлять корректную информацию об используемых сетевых программах, о пользователях, имеющих доступ к ПК или зарегистрированных в многопользовательских операционных системах;

н) предоставлять доступ к ПК сотрудникам ЦИТ для проверки исправности и соответствия установленным правилам работы, содействовать им в выполнении служебных обязанностей;

о) незамедлительно сообщать в ЦИТ о замеченных случаях нарушения

компьютерной безопасности (несанкционированный доступ к оборудованию и информации, несанкционированное искажение или уничтожение информации).

2. Пользователям запрещается:

а) устанавливать и настраивать какие-либо серверные сервисы общего пользования (DHCP, FTP, DNS, HTTP, DS и т.п.) без согласования с ЦИТ;

б) разделение ресурсов своего компьютера без согласования с ЦИТ;

в) шифрование сетевого трафика без разрешения ЦИТ;

г) несанкционированная установка шлюзов в другие локальные и глобальные сети;

д) использование на компьютерах, подключенных к сети, беспроводных устройств и/или интерфейсов (Wi-Fi, GSM, и др.) для получения доступа одновременно в сеть академии и любые другие сети;

е) использование информационно-вычислительных ресурсов и оборудования академии для деятельности, не обусловленной производственной необходимостью и должностной инструкцией;

ж) создание помех в работе других пользователей, компьютеров и сети;

з) включать, выключать, переключать, перемещать, разбирать, изменять настройки оборудования общего пользования, кроме прямого указания ответственного лица и случаев пожарной опасности, дыма из оборудования, или других угроз жизни и здоровью людей и сохранности имущества;

и) подключать к локальной сети новые компьютеры и оборудование без участия сотрудников ЦИТ.

к) передача другим лицам своих личных атрибутов доступа (логин и пароль) к оборудованию, сети и информационным системам;

л) осуществление доступа к оборудованию и сети с использованием чужих личных атрибутов доступа, или с использованием чужого сеанса работы;

м) удаление файлов других пользователей на серверах общего пользования;

н) осуществление попыток несанкционированного доступа к компьютерному оборудованию и информации, хранящейся на компьютерах и передаваемой по сети;

о) использование, распространение и хранение ПО, предназначенного для осуществления несанкционированного доступа, взлома паролей, для нарушения функционирования компьютерного оборудования и компьютерных сетей, а также компьютерных вирусов и любых файлов, ими инфицированных;

п) использование, распространение и хранение программ сетевого управления и мониторинга без специального разрешения сотрудников ЦИТ.

р) нарушение правил работы на удаленных компьютерах и удаленном оборудовании, доступ к которым осуществляется через оборудование или сеть подразделения;

с) предоставление доступа к компьютерному оборудованию незарегистрированным пользователям;

т) использование съемных накопителей и прочих устройств без их проверки на возможные угрозы (проникновение вирусов, вредоносные программы, вероятность физических неисправностей); в случае, когда пользователь не может самостоятельно оценить ситуацию и удостовериться в отсутствии угроз, он может привлечь для анализа сотрудников ЦИТ;

у) изменение аппаратной конфигурации ПК (вскрывать ПК, менять, добавлять, удалять узлы и детали);

ф) удаление или замена установленного программного обеспечения (ПО);

х) самостоятельная установка на свой компьютер любого ПО;

ц) выполнение действий и команд, результат и последствия которых пользователю не известны;

ч) самостоятельная замена IP адресов и других сетевых параметров компьютеров и оборудования.

3. Пользователи имеют право при наличии технической возможности и обоснования руководителем подразделения:

а) на получение автоматизированного рабочего места, технически исправного и соответствующего непосредственно выполняемым функциональным обязанностям;

б) на подключения к оборудованию общего пользования;

в) на получение и модернизацию компьютерного оборудования персонального пользования;

г) на получение и (или) увеличение квот на компьютерные ресурсы и удовлетворение потребностей в расходных материалах (при превышении средних норм должно представляться обоснование руководителем подразделения);

д) вносить предложения по приобретению компьютерного оборудования;

е) вносить предложения по установке бесплатного и приобретению коммерческого программного обеспечения, включая программное обеспечение общего пользования;

ж) вносить предложения по улучшению настроек оборудования и программного обеспечения общего пользования, по улучшению условий труда;

з) получать консультацию у системного администратора по работе с компьютерным оборудованием и программным обеспечением общего пользования, по вопросам компьютерной безопасности;

и) получать уведомления об изменениях настоящего Порядка и правил работы на конкретном оборудовании.

VII. Общие правила обеспечения информационной безопасности при работе с информационными ресурсами и сетями академии

1. Требования к паролям пользователей и порядок работы с ними:

а) Пароли должны генерироваться специальными программными средствами либо выбираться самостоятельно пользователями, а при необходимости – сотрудниками ЦИТ с учетом следующих требований:

длина пароля пользователя должна составлять не менее 6 символов, если не предъявляются специфические требования программным обеспечением;

в составе символов пароля обязательно должны присутствовать буквы и цифры;

в составе символов пароля желательно использовать знаки пунктуации, специальные символы (" ~ ! @ # $ % ^ & * ( ) - + _ = \ ! / ?);

б) пароль не должен содержать:

фамилии, имени, отчества пользователя ни в каком виде, т.е. написанными в строчном, прописном, смешанном виде, задом наперед, два раза и т.д.;

фамилий, имен, отчеств родных и близких пользователя ни в каком виде;

кличек домашних животных, номеров автомобилей, телефонов и других значимых сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

известных названий, словарных и жаргонных слов;

последовательности символов и знаков (111, qwerty, abcd и т.д.);

общепринятых сокращений и аббревиатур (ЭВМ, ЛВС, USER и т.д.);

наименования учетной записи пользователя;

в) при вводе пароля пользователю необходимо исключить возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерам и т.п.);

г) запрещается записывать пароли на бумаге, в файлах, электронных записных книжках и других носителях информации, в том числе на каких либо предметах;

д) запрещается сообщать пароли другим пользователям, обслуживающему персоналу информационных автоматизированных систем и регистрировать их в системах под своей учетной записью;

е) запрещается пересылать пароль открытым текстом в сообщениях электронной почты;

ж) хранение своего пароля на бумажном носителе допускается только в личном сейфе владельца пароля.

2. Смена паролей.

а) Плановая смена паролей должна проводиться не реже одного раза в 6 месяцев или по требованию политики программного обеспечения.

б) Для автоматизированных систем (АС), позволяющих настраивать политику парольной защиты и доступа пользователей, используются следующие

принципы смены паролей:

при создании учетной записи администратор устанавливает опцию, регулирующую период смены пароля;

смена пароля производится пользователем самостоятельно в соответствии с предупреждением системы, возникающим при приближении к сроку окончания действия текущего пароля.

в) Для автоматизированных систем, в которых отсутствует возможность настройки политики парольной защиты и доступа пользователей, смена паролей осуществляется администратором, путем генерации нового пароля. Передача созданного пароля пользователю осуществляется способом, исключающим его компрометацию.

3. Действия в случае утери или компрометации пароля.

а) В случае утери или компрометации пароля Пользователь обязан незамедлительно поставить в известность ЦИТ и предпринять меры по смене пароля: сменить его самостоятельно, либо оформить заявку на смену пароля в адрес системного администратора ЦИТ.

б) Устная заявка Пользователя на смену пароля не является основанием для проведения таких изменений.

VIII. Ответственность

1. Пользователь несет дисциплинарную ответственность:

а) за сохранение в секрете своих паролей. Пользователям запрещается действием или бездействием способствовать разглашению своего пароля.

б) за нарушение корректности технологического процесса подсистемы или автоматизированного рабочего места и (или) правил доступа к информационным ресурсам, влекущее за собой искажение информации в ресурсах.

в) за достоверность, актуальность, полноту и соответствие вводимой и отчетной информации в базы данных информационных ресурсов.

2. Руководитель подразделения несет дисциплинарную ответственность за достоверность, полноту и своевременность обновления информации о подразде-

лении на официальном сайте академии в соответствии с действующими локальными актами.

3. За утрату или повреждение технических средств Пользователь несет материальную ответственность в установленном нормами ТК РФ порядке.

4. СГАКИ не несет ответственности за противоправные или неэтичные действия в сфере компьютерных или телекоммуникационных технологий, если таковые действия совершены во внеслужебное время и с территории и посредством оборудования, не находящихся под юрисдикцией СГАКИ. В данной ситуации ссылки такого лица (лиц) на принадлежность к СГАКИ не могут служить основанием для судебного преследования СГАКИ.

5. СГАКИ также не несет ответственности за самостоятельную установку пользователем какого-либо программного обеспечения или технических средств, а также за их ненадлежащую и некачественную работу.

6. Устранение всех возможных неполадок и сбоев в работе компьютерных ресурсов академии и оборудования, возникших по причине ненадлежащего их использования, осуществляется за счет собственных средств работника.

IX. Заключительные положения

1. В данный Порядок могут вноситься изменения и дополнения в том же порядке, в котором принят данный Порядок.