РОСЖЕЛДОР

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Ростовский государственный университет путей сообщения»
(ФГБОУ ВО РГУПС)

УТВЕРЖДАЮ
Ректор ФГБОУ ВО РГУПС
В.Д. Верескун
07.04.2017

ПОЛОЖЕНИЕ
об использовании информационных, вычислительных и сетевых ресурсов ФГБОУ ВО РГУПС

1. **Общие положения**

1.1. Настоящее Положение определяет порядок доступа работников ФГБОУ ВО РГУПС (далее – университет) к информационно-телекоммуникационным сетям, базам данных, учебным и методическим материалам, материально-техническим средствам обеспечения образовательной деятельности, необходимым для качественного осуществления деятельности ФГБОУ ВО РГУПС.

1.2. Настоящее Положение разработано на основании:

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

– Федерального закона от 23.08.1996 N 127-ФЗ "О науке и государственной научно-технической политике";

– Устава ФГБОУ ВО РГУПС.

1.3. Доступ работников к вышеперечисленным услугам и ресурсам осуществляется в целях качественного исполнения ими трудовых обязанностей, предусмотренных должностной инструкцией.

1.4. Действие настоящего Положения распространяется на пользователей любого компьютерного оборудования (компьютеры, компьютерная периферия, коммуникационное оборудование), локальной сети университета, информационным ресурсам и базам данных, включая информационные музейные фонды (далее - ресурсам), а также на пользователей, осуществляющих удаленный

доступ к оборудованию локальной сети, информационным ресурсам и базам данных, из других локальных сетей и Интернет.

1.5. В Положении определены права и обязанности пользователей информационно-вычислительной техники, информационных ресурсов и баз данных вне зависимости от прав доступа.

1.6. Несоблюдение требований настоящего Положения работниками университета признается нарушением трудовой дисциплины и может служить основанием для применения дисциплинарного взыскания, в установленном законом порядке.

1.7. Настоящее Положение доводится руководителями структурных подразделений до сведения работников при приеме их на работу.

2. Доступ к сетевым ресурсам

2.1. Серверное и сетевое оборудование локальной вычислительной сети университета (далее – сети) работает круглосуточно.

2.2. Гарантированный доступ пользователей к информационным и вычислительным ресурсам - с 8.15 до 17.00 в рабочие дни. В случае сокращения рабочего дня приказом по университету доступ к ресурсам прекращается за один час до времени завершения рабочего дня.

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

2.4. При необходимости 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 УИ письменную заявку, утвержденную руководителем подразделения.

2.5. При профилактиках сетевого оборудования, переходе на новую системную платформу, версию СУБД или сайта и т.п. режим доступа регламентируется приказом по университету.

3. Порядок оформления доступа к информационным ресурсам

3.1. 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. Ответственный пользователь

информационных ресурсов - это сотрудник ФГБОУ ВО РГУПС, который, в силу своих полномочий, должностных обязанностей или на основании указаний руководства университета, несет ответственность за содержание информационного ресурса или базы данных.

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

3.3. Каждому пользователю выдается уникальный идентификатор (логин) и пароль.

4. Порядок подключения компьютеров к сети

4.1. За каждым ПК, подключенным к сети, распоряжением руководителя структурного подразделения назначается ответственный (копия распоряжения направляется в УИ), в должностные обязанности которого входит:

– установка, настройка и обновление антивирусного программного обеспечения (ПО);

– недопущение замены параметров сетевого подключения компьютера или сетевого оборудования без согласования с УИ;

– недопущение переключения компьютера в другую розетку сети (за исключением компьютерных классов, где допускается переключение компьютеров в розетки сети в пределах одного помещения).

4.2. В случае увольнения ответственного за ПК руководитель подразделения назначает нового ответственного.

4.3. На период временного отсутствия ответственного за ПК руководитель подразделения временно назначает другого ответственного.

5. Обязанности и права пользователей

5.1. Пользователи обязаны:

5.1.1. Ознакомиться с Положением до начала работы на компьютерном оборудовании.

5.1.2. Пройти регистрацию, инструктаж и получить личные атрибуты доступа (имя, пароль) для работы с информационными системами и оборудованием с установленными полномочиями.

5.1.3. Устанавливать личный пароль доступа в соответствии с требованиями к паролям пользователей и порядком работы с ними.

5.1.4. Использовать компьютерное оборудование исключительно для деятельности, предусмотренной производственной необходимостью и

должностными инструкциями.

5.1.5. Использовать сеть Интернет и ресурсы, а также компьютерную и иную оргтехнику университета, закрепленную за работником, исключительно в целях исполнения своих должностных обязанностей.

5.1.6. Устанавливать компьютерное оборудование 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.

5.1.7. Протирать оборудование от пыли не реже одного раза в две недели с соблюдением требований ТБ и инструкции по эксплуатации оборудования.

5.1.8. Сообщать о замеченных неисправностях компьютерного оборудования и недостатках в работе программного обеспечения в УИ.

5.1.9. Рационально пользоваться ограниченными разделяемыми ресурсами (дисковой памятью компьютеров общего пользования, пропускной способностью локальной сети) и расходными материалами.

5.1.10. Выполнять требования системного администратора, а также лиц, назначенных ответственными за эксплуатацию конкретного оборудования, в части, касающейся безопасности работы в сети.

5.1.11. Выполнять правила работы в вычислительной сети.

5.1.12. Выполнять обязательные рекомендации ответственных лиц по защите информации.

5.1.13. По запросу системного администратора предоставлять корректную информацию об используемых сетевых программах, о пользователях, имеющих доступ к ПК или зарегистрированных в многопользовательских операционных системах.

5.1.14. Предоставлять доступ к ПК системным администраторам для проверки исправности и соответствия установленным правилам работы.

5.1.15. Содействовать системным администраторам в выполнении ими своих служебных обязанностей.

5.1.16. Незамедлительно сообщать в УИ о замеченных случаях нарушения компьютерной безопасности (несанкционированный доступ к оборудованию и информации, несанкционированное искажение или уничтожение информации).

5.2. **Пользователям запрещается:**

5.2.1. Устанавливать и настраивать какие-либо серверные сервисы общего пользования (DHCP, FTP, DNS, HTTP, DS и т.п.) без согласования с УИ.

5.2.2. Разделение ресурсов своего компьютера без согласования с УИ.

5.2.3. Шифрование сетевого трафика без разрешения УИ.

5.2.4. Несанкционированная установка шлюзов в другие локальные и глобальные сети.

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

5.2.6. Использование информационно-вычислительных ресурсов в личных целях.

5.2.7. Использование оборудования для деятельности, не обусловленной производственной необходимостью и должностной инструкцией.

5.2.8. Создание помех в работе других пользователей, компьютеров и сети.

5.2.9. 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.

5.2.10. Подключение к локальной сети новых компьютеров и оборудования без участия системного администратора УИ.

5.2.11. Передача другим лицам своих личных атрибутов доступа (логин и пароль) к компьютерному оборудованию, сети и информационным системам.

5.2.12. Осуществление доступа к оборудованию и сети с использованием чужих личных атрибутов доступа, или с использованием чужого сеанса работы.

5.2.13. Удаление файлов других пользователей на серверах общего пользования.

5.2.14. Осуществление попыток несанкционированного доступа к компьютерному оборудованию и информации, хранящейся на компьютерах и передаваемой по сети.

5.2.15. 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.

5.2.16. Использование, распространение и хранение программ сетевого управления и мониторинга без специального разрешения системного администратора УИ.

5.2.17. Нарушение правил работы на удаленных компьютерах и удаленном оборудовании, доступ к которым осуществляется через оборудование или сеть подразделения.

5.2.18. Предоставление доступа к компьютерному оборудованию незарегистрированным пользователям.

5.2.19. 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 удостовериться в отсутствии угроз, он может привлечь для анализа системного администратора УИ.

5.2.20. Изменение аппаратной конфигурации ПК (вскрывать ПК, менять, добавлять, удалять узлы и детали).

5.2.21. Удаление или замена установленного программного обеспечения (ПО).

5.2.22. Установка на свой компьютер ПО, не предназначенного для выполнения производственных задач.

5.2.23. Выполнение действий и команд, результат и последствия которых пользователю не известны.

5.2.24. Производить замену IP адресов и других сетевых параметров.

5.2.25. Создание и поддержка с использованием ресурсов корпоративных АРМ персональных WEB-страниц на серверах, не входящих в состав ЛВС РГУПС, за исключением случаев, согласованных с руководством подразделений.

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

5.3.1. На получение АРМа, технически исправного и соответствующего непосредственно выполняемым функциональным обязанностям.

5.3.2. На подключения к оборудованию общего пользования.

5.3.3. На получение и модернизацию компьютерного оборудования персонального пользования.

5.3.4. На получение и(или) увеличение квот на компьютерные ресурсы и удовлетворение потребностей в расходных материалах. (При превышении средних норм должно представляться обоснование руководителем подразделения.)

5.3.5. Вносить предложения по приобретению компьютерного оборудования.

5.3.6. Вносить предложения по установке бесплатного и приобретению коммерческого программного обеспечения, включая программное обеспечение общего пользования.

5.3.7. Вносить предложения по улучшению настроек оборудования и программного обеспечения общего пользования, по улучшению условий труда.

5.3.8. Получать консультацию у системного администратора по работе с компьютерным оборудованием и программным обеспечением общего пользования, по вопросам компьютерной безопасности.

5.3.9. Получать уведомления об изменениях настоящего Положения и правил работы на конкретном оборудовании.

6. Регистрация пользователей и оборудования.

6.1 Регистрация нового оборудования, подключаемого к сети, производится у системного администратора УИ. Оборудование персонального пользования закрепляется за работником, берущим на себя ответственность за его эксплуатацию. Ответственное лицо обязано сообщать системному администратору УИ, ведущему учет, о перемещении оборудования в иное помещение, об

изменении комплектации, о сдаче в ремонт, о передаче ответственности за оборудование другому лицу.

6.2 Передачей оборудования считается только передача, оформленная по правилам материального учета.

6.3 Регистрация пользователей производится системным администратором, ответственным за предоставление доступа к конкретному оборудованию или ресурсу, по заявке оформленной соответствующим образом.

7 Общие правила работы

7.1 Требования к паролям пользователей и порядок работы с ними:

7.1.1 Пароли должны генерироваться специальными программными средствами либо выбираться самостоятельно пользователями, а при необходимости - администраторами 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 (" ~ ! @ # $ % ^ & * ( ) - + _ = \ ! / ?).

7.1.2 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.

7.2 Ввод пароля

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.).

7.3 Хранение пароля

7.3.1 Запрещается записывать пароли на бумаге, в файлах, электронных записных книжках и других носителях информации, в том числе на каких либо предметах.

7.3.2 Запрещается сообщать пароли другим пользователям, обслуживающему персоналу информационных автоматизированных систем и регистрировать их в системах под своей учетной записью.

7.3.3 Запрещается пересылать пароль открытым текстом в сообщениях электронной почты.

7.3.4 Хранение своего пароля на бумажном носителе допускается только в личном сейфе владельца пароля.

7.4 Смена паролей

7.4.1 Плановая смена паролей должна проводиться не реже одного раза в 40 дней или по требованию политики программного обеспечения.

7.4.2 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.

7.4.3 Для АС, 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.

7.5 Действия в случае утери или компрометации пароля.

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

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

8 Ответственность

8.1 Пользователь несет ответственность за сохранение в секрете своих паролей. Пользователям запрещается действием или бездействием способствовать разглашению своего пароля.

8.2 Пользователь несет ответственность за нарушение корректности технологического процесса подсистемы или АРМа и (или) правил доступа к информационным ресурсам, влекущее за собой искажение информации в ресурсах.

8.3 Пользователь несет ответственность за достоверность, актуальность, полноту и соответствие вводимой и отчетной информации в базы данных информационных ресурсов.

8.4 Руководитель подразделения несет ответственность за достоверность, полноту и своевременность обновления информации о подразделении на официальном сайте университета.

8.5 ФГБОУ ВО РГУПС 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 ФГБОУ ВО РГУПС. В данной ситуации ссылки такого лица (лиц) на принадлежность к ФГБОУ ВО РГУПС не могут служить основанием для судебного преследования ФГБОУ ВО РГУПС.

8.6 ФГБОУ ВО РГУПС также не несет ответственности за самостоятельную установку пользователем программного обеспечения, не входящего в утвержденный перечень, а также за ненадлежащую и некачественную работу данного ПО.

8.7 Устранение всех возможных неполадок и сбоев в работе компьютерных ресурсов университета, возникших по причине самостоятельной установки работником ПО, не входящего в утвержденный перечень, или в результате нерационального использования техники, осуществляется за счет собственных средств пользователя.

8.8 ФГБОУ ВО РГУПС не несет ответственности за самостоятельное размещение пользователем учебных материалов на информационных ресурсах университета (Образовательном портале РГУПС, Сайте подразделения, и т.д.), за их качество и соблюдение пользователем авторских прав.

9 Заключительные положения

9.1. Положение об использовании информационных, вычислительных и сетевых ресурсов ФГБОУ ВПО РГУПС, утвержденное 06.10.2014, признать утратившим силу.

РАЗРАБОТАНО

Начальник УИ Б.Х. Кульбикаян

СОГЛАСОВАНО:

Проректор по научной работе А.Н. Гуда

Начальник юридической службы Е.В. Дараселия