Областное государственное бюджетное профессиональное образовательное учреждение «Ряжский колледж имени Героя Советского Союза А.М. Серебрякова»

Рассмотрено на заседании
Педагогического Совета
протокол № 2
от «30» 10 2019 г.

УТВЕРЖДАЮ
Директор
_____ А.В. Ухвачев
«30» 10 2019 г.

ПОРЯДОК ДОСТУПА ПЕДАГОГИЧЕСКИХ РАБОТНИКОВ
к информационно - телекоммуниционным сетям и базам данных учебных и методическим материалам, материально-техническим средствам

2019

1. Общие положения

1.1 Настоящий порядок разработан на основе Федерального закона от 29 декабря 2012 г. N 273-ФЗ "Об образовании в Российской Федерации" и определяет порядок доступа педагогических работников Областного государственного бюджетного профессионального образовательного учреждения «Ряжский колледж имени Героя Советского Союза А.М. Серебрякова» (далее - колледж)

- к информационно-телекоммуникационным сетям,
- к базам данных,
- к учебным и методическим материалам,
- к материально-техническим средствам обеспечения образовательной деятельности.

1.2. Доступ педагогических работников к вышеперечисленным ресурсам осуществляется в целях получения ими информации и качественного осуществления педагогической, научной, методической или исследовательской деятельности.

1.3. Настоящий Порядок доводится руководителями структурных подразделений до сведения педагогических работников при приеме их на работу.

2. Порядок доступа педагогических работников

2.1. **к информационно-телекоммуникационной сети (Интернет, корпоративной информационно-телекоммуникационной сети колледжа):**

2.1.1 Серверное и сетевое оборудование корпоративной информационно-телекоммуникационной сети работает круглосуточно.

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

2.1.3. В нерабочие дни и с 17.00 до 8.15 в рабочие дни, ресурсы доступны без гарантии их непрерывной работы, то есть системный администратор оставляет за собой право отключать пользователей от ресурсов без предупреждения и не несет ответственность за возможную потерю несохраненных данных.

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

2.1.5. Доступ педагогических работников к информационно-телекоммуникационной сети Интернет осуществляется;

- с персональных компьютеров (ПК) подразделений, кабинетов ВТ

подключенных к сети Интернет, в пределах установленного лимита на входящий трафик для сотрудников колледжа.

2.1.6. Доступ педагогических работников к корпоративной информационно-телекоммуникационной сети колледжа осуществляется;

- с ПК подразделений, кабинетов ВТ, подключенных к корпоративной информационно-телекоммуникационной сети колледжа без ограничения и потребленного трафика;

2.2. к базам данных (внешние базы данных, базы данных колледжа):

2.2.1. Педагогические работники имеют право к полнотекстовым электронным базам данных (например, электронные библиотечные системы) на условиях, указанных в договорах, лицензионных соглашениях заключенных колледжем с правообладателем электронных ресурсов (внешние базы данных).

В зависимости от условий, определенных в договорах и лицензионных соглашениях с правообладателями информационных ресурсов, работа с электронными документами и изданиями возможна в локальной сети колледжа, с ПК подразделений и кабинетов ВТ.

2.2.2. Доступ к электронным базам данных, правообладателем которых является колледж, осуществляется с ПК, подключенных к сети колледжа, в порядке и правилах определенных в пункте 2.1 настоящего положения.

2.3. к учебным и методическим материалам:

Педагогические работники имеют право доступа к учебным и методическим материалам (далее материалы) (учебники, учебные пособия, методические разработки, документы учебно-методических комплексов по дисциплинам, фонды, рекомендации и иные материалы), в том числе и к учебным и методическим материалам разработчиками и авторами которого являются сотрудники колледжа.

Руководители подразделений, в которых обеспечивается хранение учебных и методических материалов (методический кабинет, библиотека), обязаны по обращению педагогического работника выдать их (или копию) во временное пользование.

Работники данных подразделений должны оказать содействие педагогическому работнику в поиске испрашиваемого материала.

Выдача материалов во временное пользование, перечень основных и дополнительных услуг и условия их предоставления осуществляется в порядке и правилах установленных в подразделениях (например, положение о библиотеке).

Доступ педагогических работников к материалам, размещенным на сайтах, электронных страницах подразделений осуществляется в соответствии с пунктом 2.1. настоящего порядка.

2.4. к музейным фондам:

Доступ педагогических работников, а также организованных групп студентов

под руководством педагогического работника (работников) к музейным фондам колледжа осуществляется безвозмездно.

2.5. к материально-техническим средствам обеспечения образовательной деятельности:

2.5.1. Доступ педагогических работников к материально-техническим средствам обеспечения образовательной деятельности осуществляется;

- по заявке согласно приказа директора, если помещение оснащено электронной системой контроля доступа к аудиториям, лабораториям, мастерским, тренировочным залам и иным помещениям и местам проведения занятий во время определенное в расписании занятий;

- без ограничения к аудиториям, лабораториям, мастерским, тренировочным залам и иным помещениям и местам проведения занятий во время определенное в расписании занятий;

- к аудиториям, лабораториям, мастерским, тренировочным залам и иным помещениям и местам проведения занятий во время вне определенного расписанием занятий по согласованию с должностным лицом, ответственным за данную аудиторию, мастерскую, лабораторию и иное помещение.

- к движимым (переносным) материально-техническим средствам обеспечения образовательной деятельности (видеопроекторы, измерительное оборудование и др. имущество) по согласованию с руководителем структурного подразделения, на балансе которого числится данное имущество.

3. Порядок оформления доступа к информационным ресурсам

3.1. На новые подключения к ресурсам оформляется заявка, в которой указывается фамилия, имя, отчество, наименование сетевого ресурса, буква подключаемого диска, срок использования ресурса, уровни доступа сотрудников, подключаемых к ресурсу, обоснование такого подключения и подписывается ответственным пользователем информационного ресурса. Ответственный пользователь информационных ресурсов - это сотрудник колледжа, который в силу своих полномочий, должностных обязанностей или на основании указаний руководства колледжа, 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. Каждому пользователю выдается уникальный идентификатор (логин) и пароль.

4. Порядок подключения компьютеров к сети

4.1. За каждым ПК, подключенным к сети, назначается ответственный технический работник, 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 инженером по АСУ колледжа;
- недопущение переключения компьютера в другую розетку сети (за исключением компьютерных классов, где допускается переключение компьютеров в розетки сети в пределах одного помещения).

5. Обязанности и права пользователей

Пользователь – это сотрудник или студент колледжа, который в силу своих должностных обязанностей или с целью выполнения учебной программы должен получать доступ к компьютерному оборудованию и оргтехнике колледжа.

5.1. **пользователи обязаны:**

5.1.1. Ознакомиться с инструкциями по работе сотрудников или студентов в локальной вычислительной сети колледжа 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. 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.

5.1.6. Сообщать о замеченных неисправностях компьютерного оборудования и недостатках в работе программного обеспечения инженеру по АСУ колледжа.

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

5.1.8. Выполнять требования инженера по АСУ колледжа, а также лиц, назначенных ответственными за эксплуатацию конкретного оборудования, в части,

касающейся безопасности работы в сети.

5.1.9. Выполнять инструкции по работе сотрудников или студентов в локальной вычислительной сети колледжа.

5.1.10. Выполнять обязательные рекомендации ответственных лиц по защите информации.

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

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

5.1.13. Незамедлительно сообщать инженеру по АСУ колледжа 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 инженером по АСУ колледжа.

5.2.2. Разделение ресурсов своего компьютера без согласования с инженером по АСУ колледжа.

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

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

5.2.5. Использование информационно-вычислительных ресурсов в личных целях.

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

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

5.2.8. 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.

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

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

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

5.2.12. Удаление файлов других пользователей на серверах общего пользования.

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

5.2.14. 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.

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

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

5.2.17. Предоставление доступа к компьютерному оборудованию незарегистрированным пользователям.

5.2.18. 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.

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

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

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

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

5.2.23. Производить замену IP адресов и других сетевых параметров.

5.2.24. Создание и поддержка с использованием ресурсов корпоративных АРМ персональных WEB-страниц на серверах, не входящих в состав ЛВС колледжа, 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 инженера по АСУ колледжа 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 инженера по АСУ колледжа. Оборудование персонального пользования закрепляется за работником, берущим на себя ответственность за его эксплуатацию. Передачей оборудования считается только передача, оформленная по правилам материального учета.

7. Обязанности и права системного администратора.

7.1. **системный администратор колледжа обязан:**

7.1.1. Совершенствовать работу оборудования и программного обеспечения для повышения эффективности выполнения пользователями их служебных обязанностей.

7.1.2. Следить за стабильной работой серверов, установленных на них программ и информационных систем.

7.1.3. Предоставлять пользователям информацию, необходимую для работы на компьютерном оборудовании общего пользования.

7.1.4. Доводить до сведения пользователей информацию об изменении правил или режима работы оборудования общего пользования.

7.1.5. Минимизировать время простоя оборудования из-за неполадок и сервисных работ.

7.2. **системный администратор колледжа имеет право:**

7.2.1. Делать предупреждения пользователям, нарушившим установленные правила работы, а также информировать руководство о произошедшем инциденте.

7.2.2. Требовать от пользователя подробного отчета о работе, если во время этой работы произошел отказ или сбой оборудования или программного обеспечения общего пользования.

7.2.3. Требовать обоснования необходимости выделения пользователю ограниченных ресурсов или расходных материалов сверх запланированного уровня.

7.2.4. Проверять исправность компьютеров, подключенных к сети, правильность настройки сетевых программ и соблюдение правил работы с использованием, при необходимости, административного доступа к ПК на время проверки.

7.2.5. Оперативно отключать от сети, блокировать работу или выводить из эксплуатации оборудование в случае нарушения компьютерной безопасности, по причине неисправности или грубого нарушения правил работы.

7.2.6. Осуществлять экстренное отключение оборудования в отсутствие ответственного лица или пользователя и без предварительного уведомления, для обеспечения бесперебойной работы сети и компьютеров общего пользования.

7.2.7. Удалять без предупреждения файлы пользователей, содержащие игровые программы и программы, предназначенные для нарушения компьютерной безопасности, файлы, зараженные компьютерными вирусами, или содержащие мультимедиа-информацию, не имеющую отношения к деятельности колледжа.

8. Общие правила работы.

8.1. **требования к паролям пользователей и порядок работы с ними:**

8.1.1. 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 (" ~ ! @ # $ % ^ & * ( ) - + _ = \ ! / ?).

8.1.2. 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.

8.2 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.).

8.3 хранение пароля

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

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

8.3.3. Запрещается пересылать пароль открытым текстом в сообщениях электронной почты.

8.4 смена паролей

8.4.1. Плановая смена паролей должна проводиться не реже одного раза в год или по требованию политики программного обеспечения.

8.4.2. 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.

8.4.3. 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.

8.5. действия в случае утери или компрометации пароля.

8.5.1. В случае утери или компрометации пароля Пользователь обязан незамедлительно поставить в известность системного администратора колледжа и

предпринять меры по смене пароля: сменить его самостоятельно, либо оформить заявку на смену пароля в адрес инженера по АСУ колледжа.

9. Ответственность.

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

9.2. 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.

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

9.4. Колледж 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 колледжа.

9.5. Колледж также не несет ответственности за самостоятельную установку пользователем программного обеспечения, не входящего в утвержденный перечень, а также за ненадлежащую и некачественную работу данного ПО.

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

9.7. Колледже несет ответственности за самостоятельное размещение пользователем учебных материалов на информационных ресурсах колледжа, за их качество и соблюдение пользователем авторских прав.