бюджетное профессиональное образовательное учреждение Вологодской области «Великоустюгский многопрофильный колледж»

УТВЕРЖДЕНЫ
приказом директора колледжа
от 24.05.2022 г. № 236

ПРАВИЛА

«24» 05 2022 г. № 15

г. Великий Устюг

управления доступом к ресурсам локальной сети и обеспечения безопасности при работе пользователей

1. Общие правила работы

1.1. Работа в локальной вычислительной сети (ЛВС) производится сотрудниками учреждения с целью получения необходимой информации для выполнения возложенных на них должностных обязанностей.

1.2. Работа в ЛВС учреждения производится с помощью базового компьютера и иных дополнительных устройств.

1.3. Запрос на установку базового компьютера, его настройку и установку сетевого программного обеспечения осуществляется работником учреждения по предварительной письменной заявке, написанной на имя директора учреждения.

1.4. Для идентификации пользователя ЛВС работнику выдается имя (учетная запись) и пароль. Имя и пароль необходимы для идентификации в ЛВС учреждения и получения доступа к ресурсам сети (сетевым дискам, принтерам и программам). Имя и пароль работника должны быть уникальны в сети. За уникальность и сохранность пароля отвечает пользователь. Пароль – информация конфиденциальная, конфиденциальность обеспечивается самим пользователем и средствами операционных систем.

1.5. Запрещается сообщать пароль другим пользователям ЛВС и работать под чужим паролем.

1.6. Пользователи ЛВС обязаны ознакомиться с данными правилами.

2. Технические нормы и правила

2.1. Для каждого работника выделено дисковое пространство на сервере в соответствии с текущими квотами, для хранения документов, связанных с выполнением должностных обязанностей.

2.2. При входе в ЛВС под своим именем и паролем происходит автоматическое подключение сетевого диска. Никто, кроме программиста и работника учреждения, не имеет доступ к информации, хранящейся на сетевом диске.

2.3. Для обмена информацией между работниками доступен общий ресурс – автоматически подключаемый сетевой диск. Доступ к этому сетевому диску имеют абсолютно все зарегистрированные пользователи сети. Хранить документы на общем ресурсе не рекомендуется, т.к. он автоматически очищается в ночь на первое число каждого месяца. За удаление информации на нем программист ответственности не несёт.

2.4. Категорически запрещается выкладывать важную информацию на общих ресурсах ЛВС. За размещение на общем ресурсе сети важной информации персональную ответственность несет пользователь, выложивший ее.

2.5. При нарушении нормальной работы сети и в случае обнаружения неисправности любого компьютерного и сетевого оборудования, а также при сбое или неправильной работе программного обеспечения пользователь обязан немедленно сообщить программисту учреждения.

2.7. Поддержка и сопровождение установленного системного и сетевого программного обеспечения осуществляется программистом.

2.8. При необходимости использования нового программного обеспечения, пользователь обязан согласовать его использование с системным администратором.

2.9. По первому требованию программиста пользователь обязан освободить компьютер для контроля или выполнения регламентных работ.

2.10. Все действия, связанные с установкой программного обеспечения, а также предоставлением доступа к конкретным ресурсам сети, осуществляются по предварительной письменной заявке, написанной на имя директора учреждения.

2.11. Ответственность за работоспособность пользовательского программного обеспечения рабочих станций сети подразделения несёт программист учреждения.

2.12. В ЛВС учреждения установлено ограничение на объем отправляемой и принимаемой корреспонденции.

3. Права и обязанности пользователей сети

3.1. Пользователь, использующий носители информации, несет ответственность за антивирусную чистоту содержащихся на них данных.

3.2. В случае получения носителя информации из сомнительного источника пользователь обязан проверить его на «вирусы». Если у него возникли сомнения, то он вправе пригласить инженера или программиста для повторной проверки.

3.3. Пользователю категорически запрещается открывать подозрительные почтовые сообщения и вложенные в них файлы.

3.4. Пользователь обязан немедленно прекратить работу за компьютером, и обратится к инженеру или программисту учреждения для выяснения причин и выработки мер восстановления нормального функционирования сети в случаях:

- подозрения на заражение вирусами;
- обнаружения заражения вирусами;
- нарушением безопасности работы сети.

3.5. Каждый пользователь в индивидуальном порядке отвечает за понимание и правильное отношение к правилам безопасности систем, которые они используют.

3.6. В программах, использующих парольную защиту, пользователи обязаны выбирать качественные пароли и периодически самостоятельно менять их.

3.7. В целях защиты от подбора системного пароля пользователя наложено ограничение: при неправильном вводе пароля более 5 раз, учетная запись пользователя блокируется. Блокировку может снять только инженер или программист учреждения.

3.8. Для надежной и безопасной работы основных сервисов функционирующих в сети, а также информации пользователей, инженеры и программист обязаны проводить полное или частичное резервное копирование баз данных.

4. Ответственность пользователей сети

4.1. Пользователи, нарушившие нормальное (безопасное) функционирование сети, повлекшее за собой материальный и моральный ущерб учреждению, должностным лицам и пользователям сети, несут ответственность.

4.2. Ответственность пользователей сети определяется действующим законодательством.

5. Пользователям запрещается

5.1. Самостоятельно переставлять и передвигать, а также подключать компьютерную технику в помещении (в том числе при проведении генеральных уборок, перестановке мебели и пр.).

5.2. Самостоятельно производить установку, настройку, модификацию и тестирование сетевого аппаратного или программного обеспечения.

5.3. Передавать по сети информацию, оскорбляющую честь и достоинство других абонентов сети, содержащую призывы к насилию, разжиганию межнациональной розни, информацию в зашифрованном виде, а также передавать информацию за пределы учреждения, если это не входит в должностные обязанности пользователей.

5.4. Использовать ресурсы сети для осуществления любого рода личной или посторонней коммерческой деятельности.

5.5. Предпринимать какие-либо действия прямо или косвенно направленные на нарушение нормальной работы сетевого оборудования и разрушение общих информационных ресурсов.

5.7. Передавать кому-либо свой пароль, работать под чужим регистрационным именем, а так же осуществлять любые действия, связанные с получением паролей и регистрационных записей.

6. Безопасность и устойчивость сети

6.1. Составляющие безопасности сети:

- конфиденциальность - защита от несанкционированного получения информации;

- целостность - защита от несанкционированного изменения информации;
- доступность - защита от несанкционированного удержания информации и ресурсов.

6.2. Системный администратор, инженеры и программист обязаны:

- обеспечивать и поддерживать безопасность всех компонентов ЛВС;
- обеспечивать антивирусную защиту программного обеспечения.

6.3. Для обеспечения устойчивости и безопасности сети системный администратор, инженеры и программист обязаны проводить регулярные регламентные работы.

Рассмотрено
Советом Учреждения
Протокол № 22
«24» 05 20 22 г.

В дело № 01-14
«24» 05 20 22 г.