МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования «Санкт-Петербургский государственный
университет ветеринарной медицины»

УТВЕРЖДАЮ
Ректор ФГБОУ ВО СПбГУВМ

А.А. Стекольников

«18» мая 2020 г.

Положение
о компьютерной сети ФГБОУ ВО СПбГУВМ

Обсуждено и принято Ученым советом университета
30 апреля 2020 г. (протокол № 4)

г. Санкт-Петербург
2020 год

1. Основные положения

1.1 Настоящее Положение определяет основные принципы и правила функционирования компьютерной сети (далее КС) ФГБОУ ВО "Санкт-Петербургский университет ветеринарной медицины" (далее Университет), а также права, обязанности и ответственность всех участников сети.

1.2 КС Университета представляет собой организационно-технологический комплекс, обеспечивающий учебный процесс, научно-исследовательскую деятельность, функционирование информационно-управленческой системы Университета.

1.3 КС Университета является корпоративной сетью передачи данных и выполняет функции объединения подразделений Университета в единую информационно-коммуникационную систему, способствует формированию единого научно-образовательного пространства Университета и его интеграцию в мировое информационное пространство.

1.4 Доступ в КС предоставляется преподавателям, сотрудникам, студентам, аспирантам и докторантам Университета.

1.5 Управление компьютерной сетью Университета, согласно Положению о сети Университета, осуществляется отделом информационных технологий (далее ОИТ).

1.6 КС Университета предоставляет индивидуальным абонентам и коллективным пользователям, подразделениям Университета, сервис сети Интернет.

1.7 КС Университета является некоммерческой сетью (извлечение прибыли не является целью эксплуатации сети). Однако это не запрещает в соответствии с Уставом Университета и действующим законодательством предоставлять сетевые услуги для частных лиц на платной основе с реинвестицией прибыли на поддержание и развитие КС.

1.8 Целями настоящего Положения являются создание основы регулирования информационных процессов в КС, организация совместной согласованной работы подразделений, факультетов и отдельных пользователей сети Университета.

1.9 Положение призвано обеспечить надежную и эффективную работу сети и каналов доступа к Internet.

1.10 Соблюдение пунктов данного Положения обязательно для всех пользователей КС Университета.

1.11 Положение о КС утверждается приказом ректора Университета.

2. Основные задачи

Компьютерная сеть Университета предназначена для решения следующих задач:

2.1 совершенствование системы управления вузом в его основных направлениях деятельности (образовательной, научной, инновационной) за счет информатизации и интегрирования информационно-вычислительных ресурсов в единую информационную научно-образовательную среду;

2.2 создание условий внедрения новых информационных технологий и педагогических инноваций в основные направления деятельности Университета;

2.3 поддержка обмена информацией с корреспондентами регионального, федерального и международного уровня;

2.4 интегрирование информационных ресурсов Университета на основе

INTERNET/INTRANET-технологий.

3. Организационно-правовые основы функционирования КС Университета

3.1 Функционирование КС Университета осуществляется в соответствии с Уставом Университета, законами Российской Федерации:

- гражданский кодекс Российской Федерации;
- закон РФ «Об образовании»;
- федеральный Закон РФ "О связи" от 07.07.2003 № 126-ФЗ,
- федеральный Закон РФ "Об информации, информационных технологиях и защите информации" от 27.07. 2006 г № 149-ФЗ;
- организационно-распорядительными и нормативно-правовыми актами Министерства образования и науки Российской Федерации;
- организационно-распорядительными актами Университета.

3.2 КС Университета является корпоративной сетью передачи данных, включающей базовую сеть, предназначенную для информационного обмена между структурными подразделениями Университета (INTRANET) и предоставляющей возможности для информационного обмена в адресном пространстве глобальной сети INTERNET.

3.3 Техническое и организационное управление и эксплуатацию КС Университета осуществляется отделом информационных технологий.

3.4 Порядок управления и администрирования КС определяются руководителем ОИТ.

3.5 Оперативное управление КС, рабочими станциями и отдельными ПК, входящими в КС Университета, осуществляют администраторы ОИТ.

3.6 Администраторы КС осуществляют свою деятельность в соответствии с обязанностями, перечисленными в приложении к настоящему положению.

3.7 Пользователи КС Университета обязаны выполнять правила работы в КС Университета. Несоблюдение правил работы пользователей в КС Университета может повлечь за собой отключение от сети. Несоблюдение правил работы в КС Университета, связанное с нарушением законов РФ, наказывается в соответствии с законодательством РФ.

3.8 Развитие и эксплуатация КС Университета осуществляется за счет централизованных средств Университета и его подразделений, научно-технических программ, грантов и т.д.

3.9 Для предотвращения нерационального использования ресурсов КС Университета администрацией сети могут вводиться лимиты на пропускную способность каналов, на объем трафика и использование сетевых ресурсов (размеры почтовых ящиков, WWW страниц и т.д.).

4. Функциональная структура КС Университета

4.1 Основными компонентами КС Университета являются:

- базовая сеть;
- коммуникационный узел КС Университета;
- локальные вычислительные сети (далее ЛВС) факультетов, подразделений Университета; отдельные персональные компьютеры подразделений, факультетов;
- информационно-вычислительные ресурсы.

4.2 Базовая сеть - опорная сеть Университета, включающая магистральные каналы, распределенный узел связи с сетями провайдера интернета, точки доступа к ЛВС и

отдельным ПК подразделений, факультетов Университета.

4.3 Коммуникационный узел (КУ) является основным системообразующим звеном КС Университета, интегрирующим ресурсы КС. КУ обеспечивает передачу трафика между ЛВС и отдельными ПК подразделений и факультетов, базовой сетью Университета и Интернет.

4.4 В КС Университета поддерживается стандартный для IP-сетей информационный сервис:

- удаленный доступ к информационным ресурсам в адресном пространстве сети INTERNET в режиме "on-line" на базе протоколов HTTP, FTP;
- целевой обмен сообщениями по сети электронной почты (E-mail) с адресацией сообщений в адресном пространстве сети INTERNET на базе протоколов SMTP, POP3;
- поддержка локальных, региональных (федеральных) телеконференций;
- другие информационные сервисы сети INTERNET.

На серверах установлено программное обеспечение, поддерживающее функционирование DNS, WWW, FTP, прокси-серверов, серверов электронной почты, серверов баз данных, серверов аудио- и видеотрансляций, системы дистанционного образования, электронной библиотеки и др.

4.5 Отдельные ПК подразделений, факультетов могут объединяться в более крупные единицы - сети коллективного пользования различного уровня (корпусные сети, факультетские сети и т.д.).

4.6 Перечень и назначение уровней КС Университета:

- уровень вуза - предназначен для информационного обмена между подразделениями, факультетами Университета;
- внутренний уровень - предназначен для информационного обмена между пользователями КС;
- внешний уровень - предназначен для информационного обмена в адресном пространстве сети INTERNET.

4.7 Правила настоящего положения не распространяются на средства вычислительной техники (СВТ) и локальные вычислительные сети подразделений и факультетов, не имеющих соединения с КС Университета.

5. Обязанности ИТО по организации и поддержке КС Университета

5.1 В обязанности ОИТ входит контроль состояния технических средств магистрали сети, телекоммуникационного узла, административно-технического сегмента и их соединения с другими сетями.

5.2 Проектирование и монтаж базовой сети КС Университета производится ОИТ.

5.3 ОИТ производит подключение к КС Университета локальных сегментов и отдельных персональных компьютеров подразделений, факультетов.

5.4 В обязанности отдела ИТ входит ввод в действие средств аппаратного и системного программного обеспечения базовой сети КС Университета, их обслуживание, восстановление при отказах, администрирование адресного пространства и сбор статистики о работе ПК подразделений, факультетов в КС Университета и загрузке

каналов связи (трафике), межсетевая маршрутизация.

5.5 Развитие, эксплуатация, восстановление оборудования после сбоев и настройка сетевого сервиса на факультетах и подразделениях производится администраторами ОИТ.

6. Порядок подключения к сети

6.1 Подключение ЛВС, отдельных ПК к КС Университета производится на основании заявки в ОИТ, подписанной и утвержденной ректором. На основании заявки начальник ОИТ выдает техническое задание (ТЗ) администраторам ОИТ на подключение.

6.2 После выполнения необходимых работ, объект подключается к сети и передается пользователю для эксплуатации.

7. Порядок обмена служебной информацией в КС Университета

7.1 Информация, предназначенная для администраторов ОИТ, отправляется электронной почтой. При таком способе передачи информация автоматически попадает к тем администраторам КС, которым она предназначена и тем самым обеспечиваются минимальные задержки при передаче информации, и достигается наибольшая эффективность работы всех административных групп КС.

7.2 При необходимости замены ранее подключенного к КС компьютера, переноса подключенного к КС компьютера в другое помещение или передаче его в другое подразделение Университета, для регистрации новых IP-адресов и для получения сетевых сервисов, находящихся в ведении ОИТ (DNS, mail, proxy, видеоконференции и т.д.) составляется заявка за подписью ректора на имя начальника ОИТ.

8. Ответственность ОИТ

8.1 ОИТ в рамках настоящего положения несет ответственность за функционирование КС Университета:

- работоспособность оборудования телекоммуникационного узла, магистрали сети, административно-технического сетевого сегмента и компьютерных классов управления информатизации;
- обеспечение маршрутизации в сети; функционирование базовых сервисов сети.

8.2 ОИТ несет ответственность за:

- работоспособность Интернет- и Интранет-серверов управления информатизации;
- учет трафика каналов связи и мониторинг его использования;
- безопасность на уровне TCP/IP протокола совместно с администраторами или ответственными лицами факультетов, подразделений;
- поддержку и сопровождение сетевых программных средств, обеспечивающих функционирование сетевых служб;

8.3 ОИТ не несет ответственности за:

- содержание проходящих по сети данных;
- информацию, находящуюся на компьютерах подразделений, факультетов, входящих в КС Университета;
- действия пользователей, имеющих полномочия самостоятельно назначать права

доступа своим сотрудникам
- деятельность сотрудников, ведущуюся на компьютерах на рабочих местах сотрудников;
- состояние компьютеров и оборудования подразделений и факультетов, на балансе которых числится указанное оборудование.

9. Безопасность в сети.

Организация защиты информации в КС Университета возложена на руководителей подразделений, факультетов, которые эксплуатируют средства вычислительной техники (СВТ).

Политика защиты информации в КС Университета устанавливается отделом ОИТ совместно с лицами, ответственными за компьютеры подразделений и факультетов, в соответствии с действующим законодательством, нормативными актами и руководящими документами ФСТЭК России, путем реализации организационных и технических мероприятий.

Организационные мероприятия включают в себя:

- организацию постоянного контроля соблюдения «Правил пользования КС Университета» реализацию антивирусной политики в КС Университета;
- ограничение доступа сотрудников и посетителей в помещения, в которых установлены серверы и коммутационное оборудование КС Университета;
- контроль структуры сети и пресечение несанкционированных подключений средств вычислительной техники к КС Университета.

Технические мероприятия включают в себя:

- регулярную смену сетевых паролей;
- антивирусный контроль;
- регулярное резервное копирование информации;
- физическое отделение от базовой сети сегментов сети, в которых передается конфиденциальная информация;
- отслеживание запуска и пресечение использования программного обеспечения, затрудняющего или нарушающего нормальную работоспособность сети, компьютеров и коммуникационного оборудования в ней и нарушающего безопасность сети;

10. Злоупотребление в сети.

10.1 Возможные злоупотребления.

К злоупотреблениям в сети, в первую очередь, относится деятельность, нарушающая действующее законодательство (гражданское и уголовное, а также несанкционированный доступ к сети.

К злоупотреблениям в КС Университета кроме того относятся:

- использование КС в коммерческих целях без согласования с администрацией Университета;
- организация точек доступа в сеть по коммутируемым, выделенным и физическим линиям, через фиктивные адреса, транслирующий прокси-сервер или любыми другими способами без письменного разрешения ректора Университета;
- доступ к данным и программам без разрешения их владельцев;
- уничтожение или изменение данных и программ без разрешения их собственника;

- незапланированная и не обоснованная производственной необходимостью загрузка сети;
- установка сетевого оборудования и настройка сетевых сервисов без согласования с отделом ИТ.

10.2 Пресечение злоупотреблений.

Ответственные лица отдела ИТ при выявлении злоупотреблений должны немедленно принять меры по пресечению злоупотребления.

В случае злоупотребления сетью нарушители частично или полностью отстраняются от пользования сетью и несут ответственность в соответствии с действующим законодательством Российской Федерации и иными нормативными актами.

При обнаружении факта злоупотребления сетью администраторы отдела ИТ обязаны немедленно принять меры к локализации нарушения, выявлению нарушителя, ограничению его работы в сети (вплоть до его полного отключения и выяснения всех обстоятельств) и получению документального объяснения нарушителя и его руководителя.

Приложение 1

Обязанности администраторов КС Университета

На администраторов КС Университета в рамках настоящего Положения возлагаются следующие обязанности:

- оперативно-административное руководство сетью;
- решение административных и технических вопросов взаимодействия с пользователями при подключении к КС Университета, изменении предоставляемых услуг и отключении от сети;
- разработка и реализация адресной и маршрутной политики сети;
- проведение работ, связанных с внедрением новых технологий и развитием сети;
- организация работ по мониторингу сети;
- организация и проведение мероприятий по обеспечению безопасности в сети;
- управление маршрутизаторами и магистралью сети;
- локализация и устранение сбоев в работе сети;
- руководство работой по сопровождению технических и программных средств сети;
- управление разделяемыми сетевыми ресурсами;
- заполнение журналов профилактических, аварийных и экстренных работ на КС;
- регистрацию, подключение и отключение рабочих мест.

Приложение 2

Правила пользования компьютерной сетью Университета

1. Общие положения

1.1 Все пользователи, при получении первичного доступа к ресурсам КС Университета, обязаны ознакомиться с требованиями настоящего Положения.

1.2 Каждый пользователь несет персональную ответственность за свои действия и обязан строго соблюдать установленные правила по работе с программными и техническими средствами КС.

1.3 Ресурсы КС предоставляются пользователям для осуществления ими своих обязанностей, связанных с научной, образовательной, производственной деятельностью Университета. При этом соблюдаются принципы разумной достаточности и минимальной необходимости.

1.4 Пользователи не имеют права получать доступ к информационным ресурсам КС, не пройдя процедуру официального разрешения на доступ к ресурсам в соответствии с процедурой, установленной в Университета.

1.5 Пользователи не должны разглашать информацию о процедурах и технической реализации защиты информации, принятых в Университета.

1.6 Пользователи должны информировать руководителя отдела ИТ обо всех фактах нарушения данной политики.

2. Рабочее место пользователя.

2.1 Для доступа к информационным ресурсам КС Университета ПК пользователя подключается к вычислительной сети университета в установленном порядке. Самовольное подключение к сети строго запрещено!

2.2 Все сетевые параметры (конфигурация протокола TCP/IP, настройка прокси-сервера, фильтрация и шифрование трафика различными программными и аппаратными средствами и т.п.) настраиваются только в соответствии с требованиями отдела ОИТ. Самовольная настройка этих параметров пользователями запрещена! Запрещается также устанавливать нелицензионное программное обеспечение (ПО) и ПО, угрожающее функционированию сети или ее безопасности, например, программы сканирования сетей, подбора паролей, и т.п.

2.3 Оставляя рабочее место в классе, пользователь обязан заблокировать доступ к работающему ПК.

2.4 При необходимости обеспечить сохранность информации, хранящейся на жестком диске ПК, пользователь должен периодически создавать резервные копии, сохраняя важную информацию на сменных носителях.

3 Пользователям запрещается:

3.1 Несанкционированно изменять параметры доступа к ресурсам КС.

3.2 Подключать к КС Университета несанкционированное оборудование (активное сетевое оборудование, незарегистрированные компьютеры и т.д.).

3.3 Использовать ПК как средство обеспечения сетевого взаимодействия между внешними сетями.

3.4 Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты.

3.5 Осуществлять действия, направленные на преодоление систем безопасности, получение несанкционированного доступа к ресурсам КС, ухудшение рабочих характеристик корпоративных информационных систем, перехват информации, циркулирующей в КС Университета.

3.6 Допускать к работе на ПК лиц, не имеющих прав доступа в КС Университета.

4 Пароли

4.1 Для предотвращения несанкционированного доступа к ресурсам КС используются пароли и/или аппаратные средства аутентификации.

4.2 Пользователи обязаны обеспечить безопасное хранение пароля и/или средств аутентификации, исключающее их утерю или разглашение.

4.3 Запрещается сообщать кому-либо, даже администраторам сети, свой пароль для доступа к информационным ресурсам КС.

4.4 В случае подозрения на разглашение пароля, необходимо немедленно изменить пароль и проинформировать администратора КС.

4.5 При выборе пароля рекомендуется придерживаться следующих правил:

- длина пароля должна быть не менее 8 символов;
- пароль не должен быть легко угадываемым (пароль не должен включать повторяющуюся, последовательность каких-либо символов (например, "111111", "aaaaaa", "12345", "qwerty", "йцукен" и т.п);
- пароль не должен включать в себя легко подбираемые сочетания символов (имена, фамилии, наименования, клички домашних животных, даты рождения и т.д.) и общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.));

5 Электронная почта

5.1 Запрещается отправлять сообщения противозаконного, враждебного или неэтического содержания.

5.2 При получении электронных сообщений сомнительного содержания и/или из незнакомого источника не следует открывать файлы, вложенные в сообщение, так как они с большой вероятностью могут содержать вирусы.

5.3 Не следует отвечать на подозрительные письма и, тем более, сообщать любые данные о себе, если Вы не доверяете отправителю письма или незнакомы с ним.

5.4 Не следует выполнять инструкции по установке или настройке программного обеспечения, полученные по электронной почте.

6 Интернет

6.1 Запрещается посещать ресурсы Интернет, содержащие материалы противозаконного или экстремистского характера.

6.2 Запрещается использовать Интернет для несанкционированной передачи (выгрузки) или получения (загрузки) материалов, защищенных авторским правом.

6.3 Запрещается несанкционированно загружать неподписанные программы из сети Интернет и запускать их, поскольку они могут содержать вирусы и программы-трояны.

Приложение 4

1 Порядок антивирусной защиты

1.2 К работе в КС Университета допускаются ПК только с установленным антивирусным программным обеспечением. К использованию в КС Университета допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков указанного средства, или свободно распространяемые антивирусные программы.

1.3 Установка средств антивирусного контроля на серверах корпоративной компьютерной сети Университета осуществляется отделом ИТ.

1.4 Ежедневно в начале работы при загрузке компьютера (для серверов - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и служб ПК.

1.5 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD/DVD-дисках, картах памяти и т.п.).

Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема ПК. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

1.6 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения, факультета самостоятельно или вместе с ответственным лицом подразделения, факультета должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь специалистов отдела ИТ для определения ими факта наличия или отсутствия компьютерного вируса и выбора формы лечения ПК.

1.7 В случае обнаружения, при проведении антивирусной проверки, зараженных компьютерными вирусами файлов, пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения, факультета, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.