**Министерство науки и высшего образования Российской Федерации**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«Самарский государственный экономический университет»**

# ПРИКАЗ

Самара

№ 84- ОВ «04» марта 2019 года

По общим вопросам

ПРИКАЗЫВАЮ:

1. Утвердить Положение о корпоративной компьютерной сети ФГБОУ ВО « СГЭУ».

И.о. ректора В.В. Болгова

Федеральное государственное бюджетное образовательное учреждение высшего образования
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

**Положение о корпоративной компьютерной сети ФГБОУ ВО СГЭУ**

УТВЕРЖДЕНО
приказом и.о. ректора
ФГБОУ ВО «СГЭУ»

№84-ОВ от «4» марта 2019 г.

## 1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Положение о корпоративной компьютерной сети ФГБОУ ВО СГЭУ (далее – Положение, Университет) определяет основные принципы и правила функционирования корпоративной компьютерной сети Университета, а также права, обязанности и ответственность участников корпоративной компьютерной сети.

1.2. Настоящее положение предназначено для создания нормативной основы регулирования информационных процессов в корпоративной компьютерной сети Университета, организации совместной работы в корпоративной компьютерной сети структурных подразделений Университета и отдельных пользователей.

1.3. Соблюдение требований настоящего положения отвечает интересам Университета и является обязательным для всех участников корпоративной компьютерной сети.

## 2. НОРМАТИВНЫЕ ССЫЛКИ

2.1. ГОСТ Р 54623-2011 «Информационно-коммуникационные технологии в образовании. Системы зданий образовательного назначения технологические информационно-коммуникационные. Термины и определения».

2.2. ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

2.3. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ (в редакции от 27.12.2018 № 529-ФЗ).

2.4. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (в редакции от 18.12.2018 № 472-ФЗ).

2.5. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (в редакции от 31.12.2017 № 498-ФЗ).

2.6. Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ (в редакции от 05.10.2015 N 285-ФЗ).

2.7. Нормативно-правовые акты и организационно-распорядительные документы Министерства науки и высшего образования России.

2.8. Устав Университета.

2.9. Иные локальные нормативные акты Университета.

## 3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

3.1. Данные – информация, представленная на электронном носителе в цифровой форме, пригодной для автоматизированной обработки.

3.2. Идентификационные данные – это данные, которые уникальным образом характеризуют работника, учащегося, сотрудника или объект инфраструктуры.

3.3. Информационная система – совокупность содержащейся в базах данных информации и информационных технологий и технических средств, обеспечивающих ее обработку.

3.4. Информационная технология – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления этих процессов и методов.

3.5. Информационно-коммуникационная технологическая система – совокупность инженерного оборудования и информационных технологий, предназначенных для комплексного управления технологическими процессами с применением средств вычислительной техники и телекоммуникаций.

3.6. Информационно-коммуникационная технология – информационные процессы и методы работы с информацией, осуществляемые с применением средств вычислительной техники и средств телекоммуникации.

3.7. Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

3.8. Информационные ресурсы – переведенная в цифровой код информация в форме данных, баз данных и программно-информационных продуктов, которая обрабатывается с использованием средств вычислительной техники.

3.9. Информационный процесс – процесс создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.

3.10. Кабельная система – совокупность физических каналов, предназначенных для передачи электрических и оптических сигналов, включающих телекоммуникационные кабели и элементы коммутации.

3.11. Локальная сеть – объединение терминального, сетевого и периферийного оборудования помещения или комплекса помещений с помощью кабельной системы и радиоканалов с целью совместного использования аппаратных и сетевых ресурсов и периферийного оборудования.

3.12. Несанкционированный доступ – доступ к информации или к ресурсам информационной системы, осуществляемый с нарушением установленных прав и/или правил доступа.

3.13. Рабочее место – часть помещения, оснащенная терминальным оборудованием и интерфейсом структурированной кабельной системы и предназначенная для работы одного пользователя.

3.14. Структурированная кабельная система – кабельная система здания, предназначенная для передачи телекоммуникационных сигналов, построенная по общепринятым стандартам, составляющая телекоммуникационную инфраструктуру указанного здания.

3.15. Телекоммуникационная розетка – окончание кабеля, оснащенное гнездовым разъемом и предназначенное для подключения терминального или периферийного оборудования (оконечное оборудование).

3.16. Оконечное оборудование данных или терминальное оборудование (DTE – англ. Data Terminal Equipment) – оборудование, преобразующее пользовательскую информацию в данные для передачи по линии связи, и осуществляющее обратное преобразование.

3.17. Оконечное оборудование данных (ООД) – это обобщенное понятие, используемое для описания оконечного прибора пользователя или его части. ООД может являться источником информации, ее получателем или тем и другим одновременно. ООД передает и (или) принимает данные посредством использования аппаратуры канала данных (АКД) и канала связи.

3.18. Терминальное оборудование – оборудование, подключенное к информационно-телекоммуникационной сети, являющееся источником и потребителем информации, преобразующее информацию в данные и осуществляющее обратное преобразование.

3.19. Узел связи – совокупность аппаратных и программных средств, обеспечивающих маршрутизацию трафика и присоединение корпоративной компьютерной сети к сетям общего пользования.

## 4. ОБЩИЕ ПОЛОЖЕНИЯ

4.1. Корпоративная компьютерная сеть является технологической основой функционирования ИТ-среды Университета, обеспечивающей информационную поддержку учебной, научной и административной деятельности.

4.2. ККС Университета выполняет функции объединения структурных подразделений университета в единую информационно-коммуникационную технологическую систему, способствует формированию единого научно образовательного пространства университета и его интеграцию в мировое информационное пространство.

4.3. ККС представляет собой организационно-технологический комплекс, на основе технологий Ethernet и стека протоколов TCP/IP, объединяющий локальные компьютерные сети, отдельные рабочие места, серверы, прочее терминальное оборудование, связанные между собой проводным или беспроводным способом с использованием сетевого оборудования, в единую сеть. Указанные составляющие ККС могут располагаться как в

зданиях (сооружениях), помещениях, на территории университета, так и в объектах, принадлежащих иным лицам, находящихся в законном пользовании Университета.

4.4. Для объединения территориально удаленных составляющих ККС университета и обеспечения доступа из ККС в глобальную сеть Интернет могут быть использованы каналы связи, предоставляемые операторами связи.

4.5. Доступ в ККС предоставляется работникам, обучающимся университета с оборудованных рабочих мест при условии регистрации.

4.6. Управление ККС и ее развитие осуществляется под руководством ректора Университета, управлением информационных систем и технологий в лице начальника управления и работников отдела технического администрирования управления информационных систем и технологий в соответствии с их должностными инструкциями.

## 5. ОСНОВНЫЕ ЗАДАЧИ КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

5.1. ККС университета предназначена для решения следующих основных задач:

- обеспечение информационного взаимодействия структурных подразделений университета, отдельных работников и обучающихся;
- обеспечение надежного и эффективного доступа к глобальной сети Интернет;
- обеспечение эффективного сбора, обработки, хранения, распространения, поиска, передачи и защиты информации;
- создание условий развития и внедрения новых информационно коммуникационных технологий в основные направления деятельности университета;
- интеграция различных информационных ресурсов и систем университета на основе современных информационно-коммуникационных технологий.

## 6. СТРУКТУРА КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

6.1. Основными компонентами ККС являются:

- узлы связи университета;
- базовая информационно-телекоммуникационная сеть (ИТС) университета;
- локальные компьютерные сети подразделений;
- информационные системы.

6.2. Узлы связи университета обеспечивают интеграцию компонентов ККС, а также маршрутизацию трафика в глобальную сеть Интернет. В состав узлов входит активное сетевое и серверное оборудование, в том числе коммутаторы, маршрутизаторы, межсетевые экраны.

6.3. Базовая ИТС университета обеспечивает коммутацию и передачу данных между отдельными компонентами ККС. В ее состав входят кабельные линии связи, коммутационное оборудование, в том числе коммутаторы уровня агрегации и уровня доступа, а также каналы связи, арендуемые у операторов связи на основании договоров или организованные через общие сети связи, точки подключения рабочих мест и компонентов ККС в виде телекоммуникационных розеток.

6.4. Беспроводные сети в Университете организуются в соответствии с настоящим положением.

6.5. Информационные системы, размещаемые на серверах Университета, могут быть:

- публично доступные – системы и сервисы, доступные пользователям внешних сетей, такие как web-сайты, электронная почта и т. д.;
- корпоративные – системы и сервисы, доступные для различных групп пользователей университета, такие как внутренний информационный портал, внутренняя электронная почта, система документооборота и т. д.;
- ресурсы подразделений – системы и сервисы, доступные работникам отдельных подразделений, такие как файловые серверы, сервисы совместной разработки и т. д.

## 7. УЧАСТНИКИ КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

7.1. Участниками ККС являются:

- ответственное руководство ККС;
- администраторы ККС университета;
- администраторы ИС;
- пользователи ККС университета.

7.2. Ответственное руководство ККС в составе ректора, первого проректора по учебной и воспитательной работе, начальника управления информационных систем и технологий и заместителя начальника управления информационных систем и технологий определяет стратегию развития ККС, требования к ее компонентам с целью обеспечения высокого уровня информатизации университета.

7.3. Администраторы ККС университета – работники отдела технического администрирования управления информационных систем и технологий, осуществляющие контроль, поддержание работы, обеспечение безопасности, развитие и модернизацию узлов связи и базовой информационно телекоммуникационной сети университета.

7.4. Администраторы информационных систем - осуществляют контроль, обслуживание, обеспечение безопасности ИС. Администраторами ИС являются работники подразделения, разработавшего или внедрившего соответствующую систему, обладающие необходимыми навыками, назначаемые распоряжением руководителя структурного подразделения.

7.5. В случае неназначения администратора, ответственность за функционирование ИС возлагается на руководителя подразделения.
7.6. Пользователи ККС – работники, обучающиеся и иные лица, использующие услуги, предоставляемые компонентами ККС университета.

## 8. ПОРЯДОК ПОДКЛЮЧЕНИЯ К КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

8.1. Подключение рабочих мест, серверов информационных систем к ККС заключается в монтаже кабельной системы и телекоммуникационной розетки, подключенной к базовой ИТС, осуществляется проводным способом и производится работниками отдела технического администрирования управления информационных систем и технологий.
8.2. На основании служебной записки на подключение к ККС сотрудники управления информационных систем и технологий определяют технические условия подключения и составляют техническое задание. После согласования задания с начальником управления информационных систем и технологий и приобретения необходимых оборудования и материалов, сотрудники отдела технического администрирования выполняют необходимые работы.
8.3. При подключении ИС к ККС данная ИС подлежит регистрации в управлении информационных систем и технологий. При регистрации определяются функции, назначение и состав ИС, размещение ИС, администратор ИС, сетевые настройки для работы в ККС, доступность из других сетей, необходимость и ограничения использования сети Интернет, другие необходимые для подключения параметры, подтверждаемые руководителем подразделения.
8.4. Регистрации в управлении информационных систем и технологий подлежат пользователи при получении доступа к сети Интернет через ККС. При регистрации определяются идентификационные данные пользователя, сетевые настройки для работы в ККС, необходимость и ограничения использования сети Интернет, другие параметры, необходимые для подключения.
8.5. Настройка рабочих мест для работы в ККС осуществляется пользователями. В случае использования одного рабочего места несколькими пользователями, настройка осуществляется ответственным лицом, назначаемым распоряжением руководителя этого структурного подразделения.

## 9. БЕЗОПАСНОСТЬ В КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

9.1. Политика обеспечения информационной безопасности в ККС университета строится руководством ККС совместно с администраторами ККС и администраторами ИС в соответствии с

законодательством РФ и локальными нормативными актами Университета.

9.2. Обеспечение информационной безопасности предусматривает комплекс организационных, технических мероприятий, направленных на исключение или существенное затруднение противоправных деяний, злоупотреблений в отношении компонентов ККС.

9.3. К организационным мероприятиям относятся:

- ознакомление участников ККС с настоящим положением и контроль соблюдения требований настоящего положения;
- разработка локальных нормативных актов в области регулирования ИТ-среды Университета и их исполнение;
- организация взаимодействия администраторов ККС и администраторов ИС;
- ограничение доступа работников, обучающихся и посетителей в помещения, в которых расположены серверы и телекоммуникационное оборудование; регистрация пользователей ИС с назначением прав доступа.

9.4. К техническим мероприятиям относятся:

- логическое и физическое сегментирование ККС университета с разграничением доступа между сегментами;
- применение межсетевых экранов и контентных фильтров;
- ограничение функционирования отдельных сетевых протоколов;
- применение парольной и антивирусной защиты;
- приобретение и использование сертифицированного оборудования, гарантирующего надежную работу самого оборудования и информационных систем;
- размещение серверов ККС в специально оборудованном помещении, исключающем несанкционированный доступ и обеспечивающем требуемый режим работы оборудования;
- приобретение и использование лицензионного программного обеспечения;
- своевременное обновление программного обеспечения;
- регулярное резервное копирование критичной для функционирования информации;
- мониторинг действий пользователей в ККС Университета.

9.5. Запрещается использовать для обработки, передачи и хранения служебной информации личные устройства.

9.6. Запрещается использовать для обработки, передачи и хранения служебной информации публичные облачные сервисы.

## 10. ТРЕБОВАНИЯ К РАБОТЕ В КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

10.1. При работе в ККС запрещается:

- самовольное подключение к ККС;

- организация точек доступа к ККС для третьих лиц, а также организация удаленного доступа без согласования с руководством ККС;
- установка точек беспроводного доступа без согласования с руководством ККС;
- физическое повреждение компонентов ККС;
- установка на рабочем месте сетевых служб без согласования с администраторами ККС, к которой рабочее место подключено;
- разглашение идентификационных данных;
- сканирование сети и подбор паролей других пользователей;
- использование чужих сетевых атрибутов (в частности IP-адресов, MAC-адресов) и/или идентификационных данных;
- подмена адреса отправителя при использовании электронной почты;
- массовая рассылка электронных сообщений (спам);
- разработка или распространение вредоносного программного обеспечения;
- проведение сетевых атак;
- несанкционированный доступ или попытки несанкционированного доступа к информации;
- использование ККС в личных и коммерческих целях;
- необоснованная производственной необходимостью загрузка сети;
- распространение информации, запрещенной законодательством РФ;
- распространение информации, противоречащей нормам морали и нравственности, порочащей честь и достоинство граждан, рассылка обманных или угрожающих сообщений;
- нарушение авторских прав, модификация, повреждение, удаление не принадлежащих пользователю данных;
- использование ККС в деятельности, противоречащей законодательству РФ.

10.2. При выявлении нарушений необходимо принять меры по их пресечению, проинформировать руководство ККС о нарушении и принятых мерах.

10.3. Нарушители частично или полностью отстраняются от пользования ККС и несут ответственность в соответствии с законодательством РФ и локальными нормативными актами Университета.

10.4. Общая политика Университета заключается в том, что при обнаружении нарушений, проблем или сбоев в сети, а также больших потоков трафика, производится временное отключение пользователя или компонента ККС до выяснения и устранения причин.

10.5. При возникновении в структурном подразделении Университета проблем в работе с ККС, требующих выяснения внутренних причин, поиска внутренних нарушителей или проведения внутренних расследований, эти действия осуществляются работниками этого подразделения.

10.6. В случае необходимости организации больших потоков трафика, в том числе в пределах ККС, во избежание отключения необходимо предварительное согласование с руководством ККС.

## 11. ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ УЧАСТНИКОВ ККС

11.1. Права, обязанности и ответственность руководства ККС университета:

- Обязанности руководства ККС:
  - знать и выполнять требования законодательства РФ, настоящего положения и других локальных нормативных актов в области регулирования ИТ-среды университета;
  - определять стратегию и осуществлять планирование развития ККС и её отдельных компонентов;
  - осуществлять организацию работы в ККС в соответствии с законодательством РФ и локальными нормативными актами Университета;
  - взаимодействовать с руководством университета и внешними организациями в вопросах работы и развития ККС Университета;
  - доводить до сведения заинтересованных участников ККС информацию о решениях руководства ККС и руководства университета, об изменениях в работе ККС;
  - осуществлять руководство деятельностью администраторов ККС и ИС университета;
  - оказывать информационную и материально-техническую помощь администраторам ККС в исполнении их обязанностей.
- Права руководства ККС:
  - осуществлять контроль деятельности администраторов ККС и ИС университета;
  - запрашивать отчеты по работе ККС и отдельных ее компонентов;
  - издавать обязательные к исполнению участниками ККС распоряжения, направленные на развитие и улучшение функциональности ККС университета;
  - требовать от участников ККС исполнения требований настоящего положения;
  - получать и принимать предложения по развитию и улучшению функциональности ККС или отдельных ее компонентов.
- Ответственность руководства ККС:
  - функционирование ККС в целом;
  - обеспечение информационной безопасности ККС;
  - соответствие ККС требованиям законодательства и локальных нормативных актов университета;
  - соответствие ККС современному уровню развития ИТ.

11.2. Права, обязанности и ответственность администраторов ККС.

- Администратор ККС обязан:
  - знать и выполнять требования настоящего положения и других локальных нормативных актов в области регулирования ИТ-среды Университета;
  - обеспечивать установку, настройку и обновления программных и аппаратных элементов узлов связи и базовой информационно-телекоммуникационной сети Университета;
  - обеспечивать информационную безопасность программных и аппаратных элементов узлов связи и базовой информационно-телекоммуникационной сети университета;
  - обеспечивать резервное копирование критичной для функционирования узлов связи и базовой информационно-телекоммуникационной сети информации;
  - ограничивать доступ работников и посетителей в помещения узлов связи Университета;
  - проводить работы, связанные с внедрением новых технологий и развитием узлов связи и базовой информационно-телекоммуникационной сети Университета;
  - проводить периодический контроль работы узлов связи и базовой информационно-телекоммуникационной сети Университета;
  - в случае отказа работоспособности программных и аппаратных элементов узлов связи и базовой информационно-телекоммуникационной сети университета принимать меры по их восстановлению и выявлению причин, приведших к отказу;
  - информировать руководство ККС об отказах работоспособности и нарушениях или попытках нарушений информационной безопасности узлов связи и базовой информационно-телекоммуникационной сети университета;
  - оповещать участников ККС об изменениях в работе узлов связи и базовой информационно-телекоммуникационной сети, влияющих на их работу;
- Администратор ККС имеет право:
  - давать участникам ККС обязательные к исполнению указания и рекомендации по вопросам работы и соблюдения информационной безопасности в ККС;
  - осуществлять контроль информационных потоков в ККС;
  - отключать от ККС ИС, отдельные рабочие места и пользователей, нарушающих ее работу, а также в случаях злоупотребления сетью, нарушений требований настоящего положения и других локальных нормативных актов Университета;
  - запрашивать и получать от руководителей и специалистов структурных подразделений университета информацию и материалы, необходимые для организации своей работы;

- запрашивать и получать от руководства ККС информационное и материально-техническое обеспечение деятельности, а также оказание содействия в исполнении своих обязанностей;
- вносить на рассмотрение руководства ККС предложения по развитию и улучшению функциональности ККС.

– Ответственность администратора ККС:
- функционирование узлов связи и базовой информационно-телекоммуникационной сети;
- обеспечение информационной безопасности элементов узлов связи и базовой информационно-телекоммуникационной сети;
- выполнение требований настоящего положения.

– Администратор ККС не несет ответственность за:
- содержание проходящих по сети данных;
- информацию, находящуюся в ИС, на компьютерах пользователей и другом терминальном оборудовании;
- работоспособность ИС, компьютеров пользователей и другого терминального оборудования.

11.3. Права, обязанности и ответственность администраторов ИС Университета.

– Администратор ИС обязан:
- знать и выполнять требования настоящего положения и других локальных нормативных актов в области регулирования ИТ-среды Университета;
- организовывать работу ИС таким образом, чтобы она не нарушала работоспособности других компонентов ККС;
- осуществлять контроль устанавливаемого и/или разрабатываемого программного обеспечения ИС на предмет соответствия законодательству РФ, в том числе на предмет соблюдения авторских прав;
- обеспечивать информационную безопасность программных и аппаратных элементов ИС;
- обеспечивать резервное копирование критичной для функционирования ИС информации;
- ограничивать доступ работников и посетителей к программным и аппаратным элементам ИС;
- проводить контроль работы ИС;
- в случае нарушения работоспособности ИС принимать меры по ее восстановлению и выявлению причин, приведших к нарушению;
- информировать непосредственного руководителя об отказах работоспособности и нарушениях или попытках нарушений информационной безопасности ИС;
- оповещать участников ККС об изменениях в работе ИС, влияющих на их работу;

– содействовать администраторам и руководству ККС в организации работы ККС.

– Администратор ИС имеет право:
  – давать пользователям ИС обязательные к исполнению указания и рекомендации по вопросам работы и соблюдения информационной безопасности в ИС;
  – осуществлять контроль информационных потоков в ИС;
  – отключать от ИС пользователей, нарушающих ее работу, а также в случае нарушений требований настоящего положения и других локальных нормативных актов университета;
  – развивать и модернизировать ИС в соответствии с общим развитием ИТ-среды университета;
  – запрашивать и получать от администраторов ККС консультативную помощь в вопросах организации правильной работы ИС в ККС университета;
  – вносить на рассмотрение руководства и администраторов ККС предложения по развитию и улучшению функциональности ККС.

– Ответственность администраторов ИС:
  – за функционирование ИС;
  – за обеспечение информационной безопасности ИС;
  – в случае нарушения работоспособности компонентов ККС в результате некорректной настройки и управления ИС;
  – за выполнение требований настоящего положения.

11.4. Права, обязанности и ответственность пользователей ККС.

– Пользователь обязан:
  – знать и выполнять требования настоящего положения и других локальных нормативных актов в области регулирования ИТ-среды Университета;
  – использовать ККС только в профессиональных, служебных и учебных целях;
  – обеспечивать информационную безопасность рабочего места, в том числе парольную и антивирусную защиту;
  – хранить в тайне свои идентификационные данные;
  – препятствовать несанкционированному и недобросовестному использованию ККС;
  – об изменении конфигурации рабочего места сообщать администратору ККС или ЛКС, к которой рабочее место подключено;
  – не устанавливать на рабочем месте сетевые сервисы без согласования с администратором ККС или ЛКС, к которой рабочее место подключено;
  – не устанавливать оконечное оборудование (роутеры, wi-fi точки, персональные вычислительные устройства) к ККС.

– Пользователь имеет право:

- получать доступ к информационным ресурсам ККС в профессиональных и служебных целях;
- получать доступ во внешние сети, в том числе в глобальную сеть Интернет в профессиональных и служебных целях;
- запрашивать и получать от администраторов ККС консультативную помощь в вопросах правильной организации работы в ККС Университета.

– Пользователь ККС несет ответственность:
- за любые действия, совершенные с использованием его идентификационных данных или с закрепленного за ним рабочего места;
- за соблюдение информационной безопасности рабочего места, в том числе парольной и антивирусной защиты;
- в случае нарушения работоспособности компонентов ККС в результате некорректной настройки рабочего места или действий пользователя;
- за (не) выполнение требований настоящего положения.

## 12. БЕСПРОВОДНЫЕ СЕТИ В УНИВЕРСИТЕТЕ

12.1. Беспроводные сети в университете представлены беспроводными сетями структурных подразделений и публичными беспроводными сетями.

12.2. Беспроводные сети структурных подразделений не являются публичными и должны быть защищены паролем и доступны лишь зарегистрированным пользователям.

12.3. Рекомендации к организации беспроводных сетей:
- имя сети (SSID) состоит из сокращенного названия подразделения и номера аудитории, в которой размещена точка доступа (например, SSEU_403D);
- SSID сети не должен транслироваться;
- длина пароля составляет не менее 8 символов;
- в числе символов пароля обязательно присутствуют буквы латинского алфавита в верхнем и нижнем регистре и цифры или специальные символы;
- пароль не должен записываться или передаваться открытым текстом в электронных сообщениях;
- смена пароля производится не реже одного раза в 3 месяца;
- новый пароль должен отличаться от предыдущего не менее чем в 5 позициях;
- пароль для доступа к беспроводной сети должен отличаться от пароля для настройки точки доступа;
- протокол безопасности WPA2;
- применяется фильтр MAC-адресов для разрешения доступа с ограниченного количества устройств; служба WPS отключена.

12.4. В случае компрометации либо подозрения на компрометацию пароля необходимо сообщить об этом администратору беспроводной сети. Администратор в свою очередь должен немедленно изменить пароль.

12.5. При организации беспроводной сети структурного подразделения точки беспроводного доступа должны быть зарегистрированы в управлении информационных систем и технологий.

12.6. Публичные беспроводные сети в университете организуются оператором связи на основании договора и в соответствии с законодательством РФ. Публичные беспроводные сети не интегрируются в ККС и используются для доступа к сети Интернет.

Начальник управления информационных систем и технологий — (подпись) С.В. Горбатов

СОГЛАСОВАНО:

Начальник управления кадров — (подпись) О.Н. Лебедева

Начальник правового управления — (подпись) О.Е. Девяткина