КОПИЯ

Автономная некоммерческая организация высшего образования
«Российский новый университет»
(АНО ВО «Российский новый университет»)

ПРИКАЗ

«01» 03 2019 г. № 73/о

Москва

Об утверждении Инструкции об управлении безопасностью и правами доступа к информационным ресурсам АНО ВО «Российский новый университет»

В целях обеспечения конфиденциальности коммерческой, финансовой и технической информации Автономной некоммерческой организации высшего образования «Российский новый университет» (далее, Университет), для упорядочивания рабочего времени сотрудников и увеличения отказоустойчивости и эффективности работы технических и информационных систем Университета, с учетом требований Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных», методических документов Федеральной службы по техническому и экспортному контролю Российской Федерации и в соответствии со «Специальными требованиями и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденными приказом Государственной технической комиссии при Президенте Российской Федерации от 30 августа 2002 г. № 282, а также в целях обеспечения соблюдения иных нормативных актов Российской Федерации-

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Инструкцию об управлении безопасностью и правами доступа к информационным ресурсам АНО ВО «Российский новый университет» (приложение к настоящему приказу).

2. Начальнику Управления информатизации Гуськову Б.Л.:

2.1. Предоставлять доступ к информационным ресурсам строго в

соответствии с Инструкцией об управлении безопасностью и правами доступа к информационным ресурсам АНО ВО «Российский новый университет».

2.2. При увольнении или переводе работников осуществлять блокировку прав доступа к информационным ресурсам в соответствии с Инструкцией об управлении безопасностью и правами доступа к информационным ресурсам АНО ВО «Российский новый университет».

3. При выполнении работ руководствоваться Инструкцией об управлении безопасностью и правами доступа к информационным ресурсам АНО ВО «Российский новый университет», Положением о защите персональных данных и Положением об использовании сети «Интернет» в научно-образовательных целях и защите обучающихся от информации, причиняющей вред их здоровью и развитию.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Ректор В.А. Зернов

СОГЛАСОВАНО:

Проректор по учебной работе Г.А. Шабанов

Проректор по учебной работе И.В. Дарда

Проректор по информационным технологиям Д.В. Растягаев

Проректор по развитию Е.В. Лобанова

Проректор по научной работе Е.А. Палкин

Начальник Управления информатизации Б.Л. Гуськов

Начальник юридической службы Ю.Г. Рогачев

Главный бухгалтер Г.М. Страусова

Начальник отдела кадров Н.В. Соломатина

Юрист отдела кадров В.В. Бехтина

Нач. общего отдела

ВЕРНО:

Приложение к приказу
от 01.03.2019 № 73/о.

1. Общие положения

1.1. Инструкция об управлении безопасностью и правами доступа к информационным ресурсам АНО ВО «Российский новый университет» (далее – Инструкция) регулирует порядок предоставления, изменения, прекращения работникам Университете (далее – Сотрудник) права доступа к информационным системам и ресурсам АНО ВО «Российский новый университет» (далее – информационные ресурсы Университета).

1.2. Целью Инструкции является обеспечение защиты информации, содержащейся в информационных ресурсах Университета, от несанкционированного доступа.

1.3. Право доступа к информационным ресурсам Университета предоставляется Сотруднику в требуемом объеме и на время, необходимое для выполнения своих должностных обязанностей.

1.4. Для предоставления Сотруднику доступа к информационным ресурсам Университета создаются учетные записи (имя и пароль), которые однозначно идентифицируют Сотрудника при использовании информационных ресурсов Университета.

1.5. Сотрудник несет ответственность за нарушение требований настоящей Инструкции в соответствии с действующим законодательством Российской Федерации и должностной инструкцией.

2. Порядок предоставления доступа к информационным ресурсам Университета

2.1. Целью работы Сотрудника в информационных системах и сети интернет является сбор, обработка, хранение общедоступной и служебной информации, обмен электронными сообщениями в служебных целях.

2.2. Доступ к ресурсам информационных систем и сервисам сети интернет предоставляется Пользователям только в том случае, если это не противоречит требованиям по защите информации (требованиям настоящей Инструкции и иными нормативными документами в области защиты информации).

2.3. Для получения доступа Сотруднику к информационным ресурсам Университета оформляется заявка на предоставление (изменение) доступа к информационным ресурсам Университета (далее – заявка, оформленная в соответствии с установленной в Приложение 1 формой) и после введения необходимой информации по работнику отделом кадров головного университета или территориального подразделения в информационную систему.

Для получения доступа Сотруднику к информационным ресурсам Управления бухгалтерского учета, отчетности и контроля содержащим данные коммерческого и финансового характера заявка визируется начальником или заместителем начальника Управления бухгалтерского учета, отчетности и контроля в соответствии с правилами, утверждаемыми начальником Управления бухгалтерского учета, отчетности и контроля. .

Доступ Сотруднику к информационным ресурсам, содержащим персональные данные, заявка визируется работником кадровой службы (отдела кадров) на предмет включения в список лиц имеющих доступ к персональным данным и ознакомления работника с нормативной базой.

2.4. Заявка подписывается руководителем подразделения Университета, в подчинении которого находится Сотрудник, нуждающийся в предоставлении доступа к информационным ресурсам Университета.

2.5. Согласованная заявка направляется в адрес начальника Управления информатизации, в соответствии с которой Управление информатизации в течение двух рабочих дней создает необходимые учетные записи и производит назначение пользовательских полномочий Сотруднику.

2.6. Руководитель подразделения, запросивший доступ к ресурсам информационных систем и сервисам сети интернет, определяет ответственного за информационную безопасность, во вверенном ему подразделении.

3. Порядок изменения доступа к информационным ресурсам Университета

3.1. В случае изменения должностных обязанностей Сотрудника, которые повлекут за собой изменения полномочий доступа к информационным ресурсам Университета, руководитель подразделения подает на имя начальника Управления информатизации заявку с уточнением полномочий доступа к информационным ресурсам Университета вышеуказанного сотрудника.

3.2. Если Сотрудник переведен в другое подразделение, руководитель этого подразделения подает на имя начальника Управления информатизации заявку на изменение полномочий доступа к информационным ресурсам Университета.

3.3. В заявке указывается дата изменения прав доступа, перечень требуемых информационных ресурсов Университета и при необходимости делается отметка об отмене пользовательских полномочий, ранее назначенных Сотруднику.

3.4. Дальнейшая работа с заявкой (в случаях изменения должностных обязанностей или перевода Сотрудника) проводится Управлением информатизации в соответствии с пунктами 2.1-2.3 Инструкции. Если полномочия Сотрудника, ранее установленные, не подтверждены в новой заявке, Управление информатизации удаляет все неподтвержденные пользовательские полномочия.

3.5. Изменение доступа Сотрудника к информационным ресурсам Управления бухгалтерского учета, отчетности и контроля осуществляется в соответствии с правилами, утверждаемыми начальником Управления бухгалтерского учета, отчетности и контроля.

Изменение доступа Сотрудника к информационным ресурсам, содержащим персональные данные осуществляется Управлением информатизации в соответствии с Инструкцией по обработке персональных данных.

4. Порядок прекращения доступа к информационным ресурсам Университета

4.1. Основанием для отключения Сотрудника от информационных систем и сервисов сети интернет являются следующие события:

- нарушение инструкций и иных локальных нормативных актов в области защиты информации Университета;
- в случае нарушения Сотрудником действующего законодательства в сфере компьютерной информации;
- увольнение Сотрудника, либо переводе его в другое подразделение.

4.2. При увольнении Сотрудника в течение одного рабочего дня после издания соответствующего распоряжения Общий отдел (кадровые подразделения территориальных подразделений) передает копию приказа (выписку из приказа) в Управление информатизации.

Ответственный – начальник Общего отдела, руководитель территориального подразделения.

Срок – не позднее даты увольнения.

4.3. Подразделения Управления информатизации выполняют блокировку к информационным ресурсам университета в следующем порядке:

4.3.1 Отдел поддержки и администрирования информационных систем (ОПиАИС) на основании полученного распоряжения (выписки) осуществляет блокировку доступа ко всем предоставленным ранее ресурсам ИС и сообщает о приказе в следующие подразделения:

Отдел эксплуатации информационно-технических средств и сетей (ОЭИТСиС);

Отдел снабжения и технического обслуживания (ОСТО);

Центр мультимедийных технологий в образовании (ЦМТО).

Ответственный – начальник ОПиАИС.

Срок – в течение одного рабочего дня.

4.3.2. Центр мультимедийных технологий в образовании на основании полученного распоряжения блокирует пропуск в системе контроля и управления доступа (СКУД) и блокировки доступов к учебным материалам в СДО.

Ответственный – начальник ЦМТО.

Срок – в течение одного рабочего дня.

4.3.3. Отдел эксплуатации информационно-технических средств и сетей на основании полученного распоряжения блокирует доступы к сетевым ресурсам и корпоративной электронной почте.

Ответственный – начальник ОЭИТСиС.

Срок – в течение одного рабочего дня.

4.3.4. Отдел снабжения и технического обслуживания проверяет рабочее место работника на предмет сохранности аппаратных, программных средств и передачи локально размещённых данных.

Ответственный – начальник ОСиТО.

Срок – в течение одного рабочего дня.

4.4. Пункт 4.2 Инструкции, может быть выполнены заранее при подписании обходного листа, до получения приказа.

4.5. Права доступа Сотрудника на основании заявки (служебной записки) руководителя подразделения могу передаваться другому работнику (со сменой пароля) в срок до получения приказа на увольнение.

4.6. Подключение оборудования к локальной вычислительной сети университета осуществляется на основании заявки (служебной записки по форме Приложение 2) от руководителя структурного подразделения, с указанием ответственного лица по каждой единице оборудования.

Срок – в течение двух рабочих дней (при необходимости проведения монтажных работ, срок может быть продлен).

4.7. Срок исполнения заявок на предоставление прав доступа и подключения к сетевым информационным ресурсам один рабочий день с момента получения заявки.

Срок – в течение двух рабочих дней (при необходимости проведения монтажных работ, срок может быть продлен).

5. Обязанности Работника – пользователя информационных ресурсов Университета

5.1. Знать и выполнять требования законодательных актов Российской Федерации, настоящей Инструкции и других внутренних документов, регламентирующих работу с информационными ресурсами Университета.

5.2. Выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры работы с информационными ресурсами данных, которые определены для него должностной инструкцией.

5.2. При обработке персональных данных знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных. Использовать для хранения персональных данных только определенные места хранения и учтенные носители персональных данных. Не разглашать персональные данные, которые будут доверены или станут известны в ходе рабочего процесса во время выполнения должностных (договорных) обязанностей. Не сообщать устно или письменно, не передавать в каком либо виде третьим лицам и не раскрывать публично персональные данные без соответствующего разрешения непосредственного руководителя. Незамедлительно, в кратчайшие сроки, сообщать непосредственному руководителю об утрате или недостаче носителей информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению персональных данных.

5.3. При обработке данных, составляющих коммерческую или финансовую информацию знать и соблюдать установленные требования по режиму данных, учету, хранению и пересылке носителей информации, обеспечению безопасности данных. Использовать для хранения таких данных только определенные места хранения и учтенные носители персональных данных. Не разглашать информацию, которая будет доверена или станет известна в ходе рабочего процесса во время выполнения должностных (договорных) обязанностей. Не сообщать устно или письменно, не передавать в каком либо виде третьим лицам и не раскрывать публично данные, составляющие коммерческую или финансовую информацию, без соответствующего

разрешения непосредственного руководителя. Незамедлительно, в кратчайшие сроки, сообщать непосредственному руководителю об утрате или недостаче носителей информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению данных, составляющих коммерческую или финансовую информацию.

5.4. Использовать информационные ресурсы Учреждения и переданные в распоряжение технические средства хранения, обработки и передачи информации исключительно для выполнения порученных работ, должностных (договорных) обязанностей.

5.5. Соблюдать требования антивирусной защиты.

5.6. Пользователи, имеющие выход в интернет, обязаны соблюдать правила при работе в сетях связи общего пользования и (или) сетях международного информационного обмена – интернет.

5.7. Пользователи, работающие с электронной подписью или использующие шифрование, обязаны соблюдать соответствующие инструкции.

5.8. Пользователям запрещается:

5.8.1. Нарушать установленные в Университете правила работы с информационными ресурсами.

5.8.2. Использовать компоненты программного и аппаратного обеспечения Университета в неслужебных целях.

5.8.3. Записывать и хранить конфиденциальную информацию (в том числе персональные данные) на неучтенных носителях информации.

5.8.4. Самовольно изменять состав и конфигурацию используемых программных, аппаратных, программно-аппаратных средств, самовольно устанавливать программное обеспечение, отключать/подключать оборудование или изменять режимы его работы.

5.8.5. Самовольно подключать компьютер к ЛВС Университета, изменять IP-адрес, MAC-адрес и иные настройки сети компьютера.

5.8.6. Производить действия, направленные на получение несанкционированного доступа к АРМ и серверам, равно как и любым другим узлам сети интернет, в том числе:

- действия, направленные на нарушение нормального функционирования элементов сети (компьютеров, другого сетевого оборудования или программного обеспечения);
- установка программного обеспечения, осуществляющего перехват информации (информационных пакетов), адресованной другим пользователям;
- действия, направленные на получение несанкционированного доступа к информационным ресурсам, в последующем использовании такого доступа;
- уничтожение, модификация программного обеспечения или данных без согласования с непосредственным руководителем или владельцами этого ресурса;
- попытки подбора паролей к любым информационным ресурсам методом перебора всех возможных вариантов паролей, либо атак по словарю;
- умышленные действия по созданию, использованию и распространению вредоносных программ, в том числе направленных на получение несанкционированного доступа к любым информационным и служебным ресурсам, либо на нарушение целостности и работоспособности этих систем;
- действия по сканированию локальной сети с целью определения ее внутренней структуры, списков открытых портов, наличия существующих сервисов и уязвимостей.

5.8.7. Самовольно изменять параметры средств защиты информации (в том числе и средств антивирусной защиты), а также завершать их работу и (или) самостоятельно их устанавливать.

5.8.8. Самостоятельно разрабатывать или использовать нерегламентированные (без разрешения непосредственного руководителя, не относящиеся к производственному процессу) программы.

5.8.9. Разрешать посторонним лицам работать под своей учетной записью на АРМ.

5.8.10. Пересылать конфиденциальную информацию (в том числе персональные данные) по каналам связи в открытом виде, в том числе интернет, по телефону, факсу, электронной почте и т.п. (без использования средств шифрования или шифрования и электронной подписи).

5.8.11. Самовольно создавать совместно используемые сетевые ресурсы (папки общего доступа) на своих компьютерах и файловых серверах, несанкционированно удалять или изменять права доступа к ним.

5.8.12. В случае возникновения любых механических неисправностей в оборудовании осуществлять самостоятельные попытки их устранения.

5.8.13. Препятствовать должностным лицам при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации.

5.8.14. Удалять или искажать программы и файлы с конфиденциальной информацией (в том числе персональных данных) и иной важной информацией (например, системной, необходимой для функционирования информационных систем).

5.8.15. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению внештатной ситуации. Об обнаружении такого рода ошибок – ставить в известность руководителя своего подразделения и сотрудников, ответственных за установку и (или) сопровождение программного обеспечения.

5.8.16. Подключать к вычислительной сети Университета личные средства вычислительной техники: ноутбуки, карманные компьютеры, смартфоны и т.п., а так же личные носители и накопители информации. В случае необходимости переноса информации с личных носителей информации обращаться к системному администратору.

6. Антивирусная защита

6.1. В случае отсутствия штатных функций антивирусной программы, предусматривающих автоматическую проверку файлов, Пользователь обязан осуществлять проверку файлов получаемых:

- по электронной почте;
- через сеть интернет;
- на магнитном, оптическом диске, флеш–накопителе;
- ином съемном носителе информации;
- полученные иным способом.

6.2. Пользователю запрещается:

6.2.1. Осуществлять действия, направленные на выключение антивирусной программы.

6.2.2. Самостоятельно устанавливать на АРМ программное обеспечение.

6.2.3. Запускать файлы, полученные по сетям связи (электронной почте, интернет), со съемных носителей, даже если они получены проверенного адресата, без предварительной их проверки антивирусной программой.

6.2.4. 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.). Пользователь самостоятельно или вместе с сотрудниками Управления информатизации должен провести внеочередной антивирусный контроль своего рабочего места.

6.3. В случае обнаружения при проведении антивирусной проверки вирусного заражения Пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вирусного заражения сотрудника Управления информатизации, ответственного за антивирусную защиту;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь ответственного за антивирусную защиту).

7. Порядок работы в сети интернет

7.1. Использование Сотрудниками сети Интернет должно осуществляться исключительно для выполнения должностных обязанностей.

7.2. Информация, образованная (образующаяся) в процессе трудовой деятельности Сотрудника является собственностью Университета и не подлежит использованию (в том числе использованию в сети Интернет или с помощью сети Интернет) в личных целях и (или) в корыстных интересах других лиц (организаций).

7.3. При проведении технических работ, связанных с настройкой оборудования (коммуникационное оборудование, прокси-сервера, маршрутизаторы и т.п.); в случае обнаружения попыток несанкционированного доступа к Интернет-шлюзу, АРМ Сотрудника может проводиться временное отключение Сотрудников от сервисов сети Интернет (в случае планового отключения Пользователи уведомляются об этом заблаговременно).

7.4. При работе в сети интернет Пользователям запрещается:

- умышленное распространение и получение материалов в/из сети интернет, противоречащих законодательству Российской Федерации, в том числе материалов, пропагандирующих насилие или экстремизм; разжигающих расовую, национальную или религиозную вражду; разъясняющих порядок изготовления и/или применения наркотиков, взрывчатых веществ, оружия и т.п.; материалов порнографического характера; компьютерных вирусов и других вредоносных программ;
- передавать в сеть интернет информацию, к которой в соответствии с законодательством ограничен доступ (персональные данные, коммерческая тайна) без соответствующего разрешения;
- фальсифицировать IP-адрес, MAC-адрес, иные адреса, используемые в сетевых протоколах, а также прочую служебную информацию при передаче данных через сеть интернет.
- предоставлять доступ в сеть интернет со своей рабочей станции кому-либо, в том числе программно-техническими способами через локальную вычислительную сеть Университета (например: путем несанкционированной установки локального интернет-шлюза на рабочую станцию);
- получать доступ к сети интернет любыми способами, не предусмотренными действующими локальными документами (Инструкциями, положениями, регламентами);
- осуществлять несанкционированный доступ к ресурсам и сервисам сети интернет.
- выполнять действия (взлом, DoS (отказ в обслуживании), ARP-spoofing атаки, сканирование локальной вычислительной сети) направленные на нарушение функционирования элементов сети интернет (коммуникационного оборудования, серверов, рабочих станций, программного обеспечения).

8. Правила работы Пользователей с электронной почтой:

8.1. Пользователи обязаны использовать электронную почту только для выполнения служебных обязанностей.

8.2. Запрещается массовая рассылка почтовых сообщений (более 10) внешним адресатам без согласования с руководством (спама).

8.3. Запрещается использовать не свой обратный адрес при отправке электронной почты.

8.4. Запрещается отправлять по электронной почте исполняемые файлы (обычно имеют расширения exe, com, bat). В случае необходимости отправки таких файлов, помещать их в архив.

8.5. Присоединяемые файлы рекомендуется упаковывать в архив при помощи программ-архиваторов.

9. Порядок работы с носителями информации

9.1. Под использованием носителей информации в информационных системах Учреждения понимается их подключение к инфраструктуре информационных систем с целью

обработки, приема/передачи информации между информационными системами и носителями информации.

9.2. Допускается использование только учтенных носителей информации, которые являются собственностью Университета и подвергаются регулярной ревизии и контролю.

9.3. При использовании носителей информации необходимо:

- использовать носители информации исключительно для выполнения своих служебных обязанностей;
- бережно относится к носителям конфиденциальной информации.
- обеспечивать физическую безопасность носителей информации всеми разумными способами.

9.4. При использовании носителей конфиденциальной информации запрещено:

- использовать носители конфиденциальной информации в личных целях;
- передавать носители конфиденциальной информации другим лицам (за исключением администраторов);
- хранить съемные носители с конфиденциальной информацией (персональными данными) на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съемные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т. д.

10. Права Сотрудника – пользователя информационных ресурсов Университета

10.1. Использовать информационные системы Университета для выполнения служебных обязанностей.

10.2. Обращаться к системным администраторам для консультаций по поводу использования программного обеспечения и АРМ.

10.3. Направлять предложения по установке новых версий существующего программного обеспечения (с обоснованием необходимости замены).

10.4. Направлять предложения по модернизации программного обеспечения, разрабатываемого по заказу Университета.

10.5. Направлять предложения по установке нового (а также дополнительного) программного обеспечения (с указанием цели использования, преимуществ перед существующими аналогами).

10.6. Направлять предложения по модернизации АРМ (замены на новые аналоги) с обязательным обоснованием замены и указанием преимуществ перед существующими аналогами).

11. Ответственность

11.1. Пользователь несет персональную ответственность за свои действия или бездействие, которые повлекут за собой разглашение конфиденциальной информации (в том числе, персональных данных), а также за нарушение нормального функционирования информационных систем или ее отдельных компонентов, несанкционированный доступ к информации в соответствие с законодательством Российской Федерации и локальными нормативными актами Университета.

12. Заключительные требования безопасности при работе с информационными ресурсами Университета

12.1. К работе с информационными системами могут быть допущены работники, ознакомленные с действующими инструкциями и положениями в части неразглашения данных и использования систем.

12.2. При подключении к ИС и сетям допускается использование только личных, полученных от Управления информатизации учётных записей, применение чужих учётных записей недопустимо.

12.3. Допускается применение оборудование и программных средств установленных по заявке работниками Управления информатизации, самостоятельная установка и применение иного оборудования и программных продуктов не допустима.

12.4. Любое плановое или внеплановое перемещение оборудования, подключенного к информационным ресурсам Университета, согласуется с работниками Управления информатизации.

Приложение 1
к инструкции

Форма заявки на предоставление (изменение) доступа к информационным ресурсам

Начальнику Управления
информатизации РосНОУ

Прошу Вас открыть/закрыть доступ работникам «наименование структурного/ территориального подразделения» с «дата-год» к «наименование ИС или ресурса»

№	Фамилия И.О.	Контакты (тел., e-mail №комнаты)	Доступ к функцион. разделам	Уровень доступа

Выше названные работники ознакомлены с инструкцией по работе с названной системой и нормативными документами в части доступа к информационным ресурсам и предупреждён об ответственности за разглашение сведений.

Руководитель «структурного/ территориального подразделения»

Дата, Подпись

Об ответственности за разглашении персональных данных предупреждён. Обязательство о неразглашении персональных данных названными работниками подписано и хранится в Отделе кадров.

Виза работника Отдела кадров.

Об ответственности за разглашении данных коммерческого и финансового характера работник предупреждён.

Виза начальника Управления бухгалтерского учета, отчетности и контроля.

Составил или подготовил ФИО и номер телефона

Приложение 2
к инструкции
Форма заявки на подключение оборудования к локальной вычислительной сети университета

Начальнику Управления
информатизации РосНОУ

Список оборудования *Наименование подразделения* подключаемого к локальной вычислительной сети Университета, необходимого для выполнения должностных обязанностей работниками.

№	Ответственный ФИО	Размещение (комната)	Наименование оборудования	MAC адрес*	Контакты телефон и почта ответственного

Названные ответственные работники ознакомлены с нормативными документами в части использования сети и безопасности информационных ресурсов Университета.

Дата и подпись руководителя

Составил или подготовил ФИО и номер телефона

* графу MAC адрес при необходимости заполняет работник осуществляющий подключение.