

**КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ИМЕНИ ПЕРВОГО ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ
Б.Н.ЕЛЬЦИНА**

П Р И К А З

от 28 августа 2026

№ 444-П

**Об утверждении
Положения о порядке
использования сети интернет
и электронной почты в КРСУ**

В целях обеспечения информационной безопасности и соответствия требованиям Политики обеспечения информационной безопасности в Межгосударственной образовательной организации высшего образования Кыргызско-Российский Славянский университет имени первого Президента Российской Федерации Б.Н.Ельцина

1. Утвердить Положение о порядке использования сети интернет и электронной почты в Межгосударственной образовательной организации высшего образования Кыргызско-Российский Славянский университет имени первого Президента Российской Федерации Б.Н.Ельцина (далее – Положение).

2. Управлению по работе с персоналом, в срок до 01.10.2026 ознакомить работников университета с Положением.

3. Управлению по взаимодействию с обучающимися, ознакомить обучающихся университета с Положением.

4. Департаменту по развитию цифровой инфраструктуры, обеспечить размещение Положения на официальном сайте университета в информационно-коммуникационной сети «Интернет».

5. Контроль за исполнением настоящего Приказа возложить на директора департамента по развитию цифровой инфраструктуры Юдина А.Н.

Приложение 1 на 10 л. в 1 экз.

Ректор КРСУ



Волков С.Ю.

Лист согласования

Документ "Об утверждении Положения о порядке использования сети интернет и электронной почты в КРСУ (врем. № Проект_9225)"

ФИО, Должность	Результат	Дата	Замечание, комментарий
Чотонов Айбек Озубекович (Административно-правовой департамент, Директор (АУП))	Согласовано	29.08.2026 12:09	
	ПОДПИСАНО ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ Чотонов Айбек Озубекович (Административно-правовой департамент, Директор (АУП))		

ПОЛОЖЕНИЕ
О ПОРЯДКЕ ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ И ЭЛЕКТРОННОЙ
ПОЧТЫ В МЕЖГОСУДАРСТВЕННОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ КЫРГЫЗСКО-РОССИЙСКИЙ
СЛАВЯНСКИЙ УНИВЕРСИТЕТ ИМЕНИ ПЕРВОГО ПРЕЗИДЕНТА
РОССИЙСКОЙ ФЕДЕРАЦИИ Б.Н.ЕЛЬЦИНА

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Положении о порядке использования сети интернет и электронной почты в Межгосударственной образовательной организации высшего образования Кыргызско-Российский Славянский университет имени первого Президента Российской Федерации Б.Н.Ельцина (далее – КРСУ, Положение) применены термины, указанные в Федеральном законе РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и законом КР от 17 июля 2024 года № 121 «О кибербезопасности Кыргызской Республики», в том числе следующие определения:

1.1. Услуга – услуга по предоставлению доступа к сети Интернет (в том числе посредством Wi-Fi) в инфраструктуре Университета на безвозмездной основе для решения задач деятельности.

1.2. Wi-Fi – один из форматов передачи цифровых данных по радиоканалам, обеспечивающий беспроводное подключение оборудования пользователя к сети доступа к телематическим услугам связи.

1.3. БСПД – беспроводная сеть передачи данных, развернутая Кыргызско-Российским Славянским университетом (далее – КРСУ).

1.4. Устройство пользователя – находящееся пользовательское (оконечное) оборудование, обеспечивающее пользователю доступ к услуге Университета посредством подключения данного оконечного оборудования к БСПД.

1.5. Сеть – сеть доступа к сети Интернет по технологии Wi-Fi Университета.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящее Положение регулирует условия и порядок использования сети Интернет, в том числе посредством сети Wi-Fi, и электронной почты работниками, обучающимися и иными пользователями указанных ресурсов Университета (далее – пользователи).

2.2. Настоящее Положение разработано в соответствии с Федеральным законом РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных

технологиях и о защите информации», законом КР от 17 июля 2024 года № 121 «О кибербезопасности Кыргызской Республики», Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», иными федеральными законами, приказом Федеральной службы по техническому и экспортному контролю от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», Политикой обеспечения информационной безопасности в КРСУ, Уставом Университета.

2.3. Настоящее Положение расширяет и уточняет требования Политики обеспечения информационной безопасности в КРСУ и является ее неотъемлемой частью.

3. ДОСТУП К СЕТИ ИНТЕРНЕТ

3.1. Использование сети Интернет в Университете направлено на решение задач учебной, научной, организационно-управленческой и хозяйственной деятельности.

3.2. Доступ пользователей к ресурсам сети Интернет предоставляется исключительно в целях исполнения ими должностных и функциональных обязанностей, а также обеспечения учебного процесса, включая поиск информации, сбор данных, повышение квалификации и т.п.

3.3. Доступ пользователей к ресурсам сети Интернет осуществляется с компьютеров, расположенных на рабочих местах пользователей, в компьютерных классах, корпоративных и персональных мобильных устройств.

3.4. Компьютеры и корпоративные мобильные устройства, с которых предоставляется доступ к сети Интернет, должны быть оборудованы корпоративными средствами антивирусной защиты.

3.5. Доступ предоставляется только после прохождения идентификации. Доступ без идентификации не предоставляется.

3.6. Доступ к ресурсам сети Интернет для пользователей, осуществляющих работу с конфиденциальной информацией, может быть ограничен в целях обеспечения информационной безопасности Университета. Объем ограничений определяется исходя из характера обрабатываемой информации и необходимости доступа к ресурсам сети Интернет для выполнения должностных обязанностей. Ограничение доступа осуществляется ДРЦИ на основании представления руководителя соответствующего структурного подразделения и (или) требований по обеспечению информационной безопасности Университета.

3.7. Доступ к ресурсам сети Интернет может быть заблокирован без предварительного уведомления в случае возникновения нештатных ситуаций,

связанных с наличием угрозы безопасности Университета либо осуществлением атаки со стороны сети Интернет.

3.8. Доступ к сети Интернет может быть ограничен работникам Университета, не прошедшим обучение навыкам информационной безопасности в установленном порядке.

3.9. Для ограничения доступа к сети Интернет в Университете применяются средства антивирусной защиты, межсетевые экраны, прокси-серверы, системы контентной фильтрации, средства, предоставляемые третьими лицами (в том числе режим «Семейный» Яндекс.DNS и другие). Настройка, сопровождение, контроль работоспособности и своевременное обновление указанных средств осуществляются Департаментом по развитию цифровой инфраструктуры.

3.10. Руководители структурных подразделений и филиалов Университета по запросу департамента по развитию цифровой инфраструктуры (далее – ДРЦИ) предоставляют перечни ресурсов сети Интернет, ресурсов локальной сети Университета, необходимых для выполнения должностных обязанностей работникам данных структурных подразделений.

3.11. По представлению руководителей структурных подразделений ДРЦИ может ограничить доступ к ресурсам локальной сети Университета, сети Интернет, отдельным ресурсам сети Интернет для всех или отдельных работников данных структурных подразделений.

3.12. Посредством проведения мероприятий по организации и проведению защиты от компьютерных атак, направленных на отказ в обслуживании, исключена возможность блокирования авторизованным пользователям доступа к информационным системам и (или) содержащейся в них информации вследствие несанкционированных воздействий на интерфейсы, порты, сервисы, к которым должен быть обеспечен постоянный доступ из сети Интернет.

3.13. Обеспечение доступности из сети Интернет интерфейсов и сервисов информационных систем, подлежащих защите от компьютерных атак, направленных на отказ в обслуживании, осуществляется в соответствии с внутренними регламентами по защите информации по согласованию с отделом информационной безопасности ДРЦИ КРСУ после принятия мер по контролю и фильтрации исходящего и входящего сетевого трафика.

4. БЕСПРОВОДНОЙ ДОСТУП К СЕТИ ИНТЕРНЕТ

4.1. В Университете доступны для подключения четыре основных БСПД для доступа к сети Интернет посредством технологии Wi-Fi:

- «KRSU» – сеть для работников Университета;
- «KRSU.STUDY» – сеть для обучающихся Университета;
- «KRSU.FREE» – гостевая сеть.

4.2. Для подключения к сети Интернет с помощью БСПД каждому пользователю необходимо пройти процедуру аутентификации:

- для пользователей сети «KRSU» – по паролю и логину корпоративной учетной записи работника Университета;

- для пользователей сети «KRSU.STUDY» – по паролю и логину корпоративной учетной записи обучающегося Университета.

- для пользователей гостевой сети «KRSU.FREE » – с авторизацией по номеру мобильного телефона путем совершения звонка с номера мобильного телефона пользователя на номер, определенный Университетом.

- По запросу отдельных подразделений Университета при обосновании и согласовании с руководителем группы цифрового развития, директором Департамента по развитию цифровой инфраструктуры (далее – директор ДРЦИ) могут быть созданы специализированные БСПД для доступа в сеть Интернет. Аутентификация в таких сетях осуществляется по паролю.

4.3. Отношения между Университетом, предоставляющим услугу, и пользователями ДРЦИ определяют:

- для пользователей сети «KRSU» – Правила использования сети «KRSU», утверждаемые директором ДРЦИ;

- для пользователей сети «KRSU.STUDY» – Правила использования сети «KRSU.STUDY», утверждаемые директором ДРЦИ;

- для пользователей гостевой сети «KRSU.FREE» – Правила использования гостевой сети «KRSU.FREE», утверждаемые директором ДРЦИ.

4.4. Университет посредством проведения мероприятий по защите информации обеспечивает:

- исключение возможности несанкционированного доступа (воздействия) к информационным системам и содержащейся в них информации за счет несанкционированного подключения к точкам беспроводного доступа и доступа к беспроводным каналам передачи данных, подмены взаимодействующих с ними программно-аппаратных средств или доступа к ним;

- защиту беспроводных каналов передачи данных и программно-аппаратных средств, с использованием которых осуществляется беспроводной доступ;

- исключение возможности подключения к точкам беспроводного доступа лиц, не имеющих прав доступа к информационным системам Университета.

4.5. Все точки беспроводного доступа Университета имеют уникальный идентификатор и размещаются в соответствии с Планом расположения точек беспроводного доступа в Университете. План расположения точек беспроводного доступа в Университете утверждается директором ДРЦИ.

5. ПОРЯДОК ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТЫ

5.1. Корпоративная электронная почта используется для обмена в рамках локальной сети Университета и общедоступных сетей информацией в виде электронных сообщений и документов в электронном виде, направленной на решение задач учебной, научной, организационно-управленческой и хозяйственной деятельности.

5.2. Доступ пользователей к корпоративной электронной почте предоставляется с компьютеров, расположенных на рабочих местах пользователей, в компьютерных классах, корпоративных и персональных устройств.

5.3. Для обеспечения функционирования корпоративной электронной почты на компьютерах пользователей допускается использование браузера или почтового клиента, рекомендованного к использованию в Университете.

5.4. Обеспечение функционирования корпоративной электронной почты осуществляется специалистами ДРЦИ.

5.5. Все электронные сообщения и документы в электронном виде, передаваемые посредством корпоративной электронной почты, подлежат обязательной проверке на отсутствие вредоносного программного обеспечения.

5.6. Адрес корпоративной электронной почты работника Университета имеет вид i.o.familia@krsu.kg, где «i» и «o» – первые буквы имени и отчества, соответственно, «familia» – фамилия пользователя, написанная транслитерацией (написание русских слов латиницей). Изменение формата осуществляется только по решению Департамента по развитию цифровой инфраструктуры Университета с обязательным предварительным уведомлением пользователей о порядке и сроках изменений.

5.7. Адрес корпоративной электронной почты обучающегося Университета имеет вид stud0000000000@study.krsu.kg, где 0000000000 – уникальный идентификатор обучающегося. Изменение формата осуществляется только по решению Департамента по развитию цифровой инфраструктуры Университета с обязательным предварительным уведомлением пользователей о порядке и сроках изменений.

5.8. Для отдельных целей на основании заявки «На предоставление/отмену доступа к электронным ресурсам» в системе электронного документооборота по согласованию с директором ДРЦИ могут создаваться служебные адреса корпоративной электронной почты.

5.9. Доступ к электронной почте уволенного работника предоставляется руководителю структурного подразделения на основании заявки «На предоставление/отмену доступа к электронным ресурсам» в системе электронного документооборота по согласованию с директором ДРЦИ и администратором информационной безопасности (далее – администратор ИБ).

5.10. При оформлении электронного сообщения необходимо в обязательном порядке заполнять следующие поля: адрес получателя, тема электронного сообщения, текст электронного сообщения, подпись отправителя.

5.11. Рекомендуется использовать подпись отправителя следующего вида:

С уважением,
[Фамилия] [Имя] [Отчество],
Тел.: +996 (312) [XX-XX-XX], доб. [XXXXXX]
[Наименование должности]
[Наименование подразделения]

6. ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ

6.1. Пользователь имеет право:

- получать доступ к сети Интернет с компьютеров Университета и личных мобильных устройств для выполнения своих должностных и функциональных обязанностей, обеспечения учебного процесса;
- использовать корпоративную электронную почту для выполнения своих должностных и функциональных обязанностей, обеспечения учебного процесса;
- в случае возникновения проблем при подключении к сети Интернет или использовании корпоративной электронной почты получить консультацию, обратившись в диспетчерскую службу ДРЦИ it@krsu.kg +996 312 988 948 (доб 11999).

6.2. Пользователю запрещается:

- предоставлять другим пользователям или третьим лицам доступ к своему корпоративному электронному почтовому ящику;
- передавать свои реквизиты доступа к БСПД (логин, номер телефона, пароль, код подтверждения) третьим лицам;
- использовать для доступа к БСПД и корпоративному электронному почтовому ящику учетные данные (реквизиты доступа) третьих лиц;
- допускать к работе на своем рабочем компьютере посторонних лиц для доступа в сеть Интернет;
- загружать файлы со сторонних ресурсов;
- переходить по ссылкам и открывать вложенные файлы, полученные от неизвестных отправителей;
- посылать, публиковать, хранить, передавать, воспроизводить и распространять в сети Интернет или по электронной почте любым способом конфиденциальную информацию, в том числе персональные данные;
- ограничивать доступ других пользователей или препятствовать другим пользователям в использовании услуги;
- нарушать правила использования любых ресурсов сети Интернет, установленные Университетом и (или) владельцами этих ресурсов;
- в рабочее время использовать сайты социальных сетей, если это не обусловлено необходимостью выполнения должностных обязанностей или обеспечением учебного процесса;

– использовать личную электронную почту для выполнения своих должностных и функциональных обязанностей или обеспечения учебного процесса;

– использовать адрес корпоративной электронной почты для оформления подписки или регистрации в сервисах сети Интернет, если это не обусловлено выполнением должностных или функциональных обязанностей или обеспечением учебного процесса;

– использовать сайты трансляции потокового видео и аудио (трансляция TV, Интернет-радио, музыкальных программ, веб-камер и т.п.), если это не обусловлено необходимостью выполнения должностных обязанностей или обеспечением учебного процесса;

– публиковать адрес корпоративной электронной почты в общедоступных источниках в сети Интернет, если это не обусловлено выполнением должностных или функциональных обязанностей или обеспечением учебного процесса;

– производить массовую рассылку электронных сообщений, рекламных, информационных и других материалов, не связанных с выполнением должностных или функциональных обязанностей, обеспечением учебного процесса, другим пользователям сети Интернет;

– предпринимать в сети Интернет какие-либо действия и размещать какую-либо информацию, способную ущемлять имущественные и неимущественные права третьих лиц, а также носящую оскорбительный характер или противоречащую действующему законодательству Российской Федерации и законодательству Кыргызской Республики;

– использовать информационные ресурсы и сервисы сети Интернет, находящиеся под запретом действующего законодательства и иных нормативных актов Российской Федерации, законодательством Кыргызской Республики или запрещенные локальными нормативными актами Университета;

– посылать, передавать, воспроизводить или распространять материалы, распространение которых запрещено или ограничено законодательством Российской Федерации и законодательством Кыргызской Республики, в том числе порнографические материалы, материалы, оскорбляющие человеческое достоинство, пропагандирующие насилие или экстремизм, разжигающие расовую, национальную или религиозную вражду, преследующие хулиганские или мошеннические цели, направленные на дискредитацию Вооруженных Сил Российской Федерации, органов государственной власти Российской Федерации, законодательством Кыргызской Республики включенные в Федеральный список экстремистских материалов, полностью или частично защищенные нормами законодательства об охране авторского права и интеллектуальной собственности без разрешения владельца таких материалов или его полномочного представителя, иные материалы, распространение

которых запрещено или ограничено законодательством Российской Федерации, законодательством Кыргызской Республики;

- посылать, передавать, воспроизводить, предоставлять или в любом виде использовать в коммерческих целях информацию, программное обеспечение, или другие материалы, полностью или частично, полученные посредством услуги (если это явно не разрешено поставщиком подобной информации, программного обеспечения или другой продукции);

- использовать услугу в коммерческих целях путем ее перепродажи;

- использовать для подключения к сети Интернет, а также при пользовании сетью Интернет или корпоративной электронной почтой нелицензионное программное обеспечение;

- использовать на корпоративных устройствах программное обеспечение и сервисы, предназначенные для доступа к ограниченным или заблокированным ресурсам сети Интернет;

- устанавливать на компьютер и запускать загруженные из сети Интернет или полученные по электронной почте любые программы и исполняемые файлы, в том числе вредоносное программное обеспечение, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств;

- передавать любую информацию или программное обеспечение, которое содержит в себе вирусы или другие вредные компоненты;

- самостоятельно изменять любые системные, программные и сетевые настройки рабочих станций, настройки установленных систем безопасности (антивирусы, персональные межсетевые экраны и т.п.);

- проводить сканирование и иные нештатные действия в отношении средств информационной безопасности и локальной сети Университета;

- использовать пользовательское (оконечное) оборудование в качестве прокси-серверов, роутеров для каких-либо других подключенных через них компьютеров и иных устройств;

- использовать смартфон в режиме «точки доступа» для подключения к Сети иных устройств;

- подключаться к виртуальным частным сетям, не принадлежащим Университету, если это не обусловлено выполнением их должностных или функциональных обязанностей и не согласовано с директором ДРЦИ;

- подключать рабочий компьютер к внешним сетевым ресурсам с использованием стороннего канала связи (модем, сотовый телефон, коммерческие беспроводные сервисы Wi-Fi, WiMAX и др.) в обход либо дополнительно к действующему подключению;

- производить самовольное (несанкционированное) проникновение в любые технологические компоненты (узлы), программы, базы данных и иные составляющие элементы сети Университета, сеть Интернет, имея в виду действия, совершение или покушение на совершение которых предусматривает

установленную в Российской Федерации, законодательством Кыргызской Республики уголовную ответственность за такие деяния;

- использовать программное обеспечение, производящее автоматическую авторизацию пользователя в целях получения услуги, за исключением программного обеспечения, предоставленного либо одобренного Университетом;

- осуществлять попытки несанкционированного доступа к ресурсам сети, проведение или участие в сетевых атаках и сетевом взломе, за исключением случаев, когда атака на сетевой ресурс проводится с явного разрешения владельца или администратора этого ресурса.

6.3. Пользователь несет ответственность:

- за содержание передаваемой и принимаемой посредством сети Интернет и по электронной почте информации и правомерность ее распространения;

- за соблюдение локальных нормативных актов Университета и действующего законодательства Российской Федерации, а также Кыргызской Республики при работе с ресурсами сети Интернет и корпоративной электронной почтой;

- за вред, причиненный Университету или третьим лицам вследствие нарушения требований настоящего Положения.

6.4. Университет оставляет за собой право:

- доступа к электронным сообщениям пользователей с целью их архивирования и централизованного хранения, а также мониторинга выполнения требований настоящего Положения и иных локальных нормативных актов Университета, в том числе с помощью системы предотвращения утечек конфиденциальной информации;

- результаты проверок могут использоваться не только в целях обеспечения информационной безопасности, но также для анализа нагрузки на информационно-телекоммуникационную сеть Университета, выявления проблем с производительностью и оптимизации работы информационных систем и сервисов;

- ведения мониторинга, протоколирования и проведения выборочных проверок характера использования ресурсов сети Интернет-пользователями, в том числе с использованием системы предотвращения утечек конфиденциальной информации;

- вести учет подключений к Сети и сетевого трафика пользователей;

- отслеживать проходящую через Сеть информацию и раскрывать любые сведения, если это необходимо в соответствии с законом, требованиями уполномоченных государственных органов, учреждений, либо для нормального функционирования услуги, либо для защиты Университета и других его пользователей, а равно третьих лиц, чьи законные права и интересы были нарушены;

– отказать в пересылке или удалять со своих серверов любую информацию или материалы полностью, или частично, если они, исключительно с точки зрения Университета, являются неприемлемыми, нежелательными или нарушают настоящее Положение, а также ограничивать доступ к развлекательным и иным ресурсам сети Интернет;

– осуществлять идентификацию пользователей в порядке, установленном Университетом, в том числе путем установления абонентского номера, назначенного оператором связи пользователю в соответствии с договором об оказании услуг подвижной радиотелефонной связи, и осуществлять обработку и хранение идентификационных данных пользователя, а также информации об идентификаторах устройства пользователя в целях оказания услуги;

– ограничивать доступ к сети в целях обеспечения корректного функционирования сети и (или) обеспечения информационной безопасности Университета;

– ограничивать доступ к ресурсам сети Интернет, не связанным с исполнением должностных и функциональных обязанностей, обеспечением учебного процесса, а также к ресурсам, доступ к которым должен быть ограничен в соответствии с законодательством Российской Федерации, законодательством Кыргызской Республики в том числе к информации, которая может причинить вред здоровью и (или) развитию детей.

6.5. Университет не будет преднамеренно просматривать или разглашать любые частные сообщения, в том числе электронной почты или иных электронных способов обмена сообщениями (за исключением случаев, предусмотренных законом).

6.6. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную и/или уголовную ответственность в соответствии с законодательством Российской Федерации, законодательством Кыргызской Республики, а также локальными нормативными актами Университета.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. В настоящее Положение могут быть внесены изменения, дополнения в соответствии с действующим законодательством Российской Федерации, а также Кыргызской Республики и локальными нормативными актами Университета. Инициатива может исходить от структурных подразделений, а окончательное решение принимает ректор по согласованию с Департаментом по развитию цифровой инфраструктуры и службой безопасности.

7.2. Внесение изменений и дополнений в настоящее Положение осуществляется приказом ректора Университета.