

	Министерство спорта Российской Федерации
	Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет физической культуры»
	Политика
	7.4. КОММУНИКАЦИИ
СК-Пол-057.14-25	Политика информационной безопасности в Федеральном государственном бюджетном образовательном учреждении высшего образования «Уральский государственный университет физической культуры»

УТВЕРЖДАЮ
Ректор ФГБОУ ВО «УралГУФК»
С. Г. Сериков
«18» февраля 2025 г.



ПОЛИТИКА
информационной безопасности в Федеральном государственном бюджетном
образовательном учреждении высшего образования «Уральский
государственный университет физической культуры»

СК-Пол-057.14-25

Версия 1.0

Дата введения: 28 февраля 2025 г.

Челябинск
2025

	Должность	Фамилия/Подпись	Дата
Разработал	Начальник центра информационно-образовательных технологий	С.А. Белоногов/ 	24.02.2025
Согласовано	Проректор по планированию, стандартизации и цифровизации образовательного процесса	О.А. Клестова/ 	24.02.2025
	Начальник юридического отдела	И.Ю. Павлова/ 	24.02.2025
Версия: 1.0	Без подписи документ действителен 8 часов после распечатки. Дата и время распечатки: 24/02/2025, 10:00 AM		КЭ: _____ УЭ № _____ Стр. 1 из 9



Федеральное государственное бюджетное образовательное учреждение
высшего образования «Уральский государственный университет физической
культуры»

Политика

СК-Пол-057.14-25

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящая Политика информационной безопасности (далее – «Политика») предназначена для установления единых норм, правил и требований к информационной безопасности в Федеральном государственном бюджетном образовательном учреждении высшего образования «Уральский государственный университет физической культуры» (далее по тексту - Университет).

1.2 Целью настоящего Положения являются защита конфиденциальности информационных ресурсов Университета, защита целостности существенной информации, обеспечение непрерывного авторизованного доступа к информационным ресурсам Университета для поддержки основной деятельности, повышение осведомленности работников Университета и их понимания рисков, связанных с информационными ресурсами Университета, повышение их квалификации в области информационной безопасности.

1.3 Область применения настоящего Положения распространяется на все структурные подразделения Университета, в том числе и филиалы, и является обязательным для исполнения всеми работниками Университета, обучающимися, а также к любой третьей стороне, имеющей доступ к информационным ресурсам Университета.

2 НОРМАТИВНЫЕ ССЫЛКИ

Настоящее Положение разработано в соответствии со следующими нормативными документами:

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации» с последующими изменениями.
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
- Указ Президента РФ от 05 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности РФ».
- Указ Президента РФ от 09 мая 1997 г. № 188 «О Стратегии развития информационного общества в РФ на 2017-2030 годы».
- Указ Президента РФ от 06 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».
- Указ Президента РФ от 01 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности РФ».
- ГОСТ Р ИСО/МЭК 27001-2021. «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

3 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящей Политике используются следующие определения:

3.1 Информационная безопасность – комплекс мер, направленных на защиту информации от несанкционированного доступа, утраты, модификации и других угроз.

3.2 Аутентификация – процедура проверки подлинности пользователя или устройства для предоставления доступа к информационным ресурсам.

3.3 Разграничение доступа – механизм установления прав доступа пользователей к различным информационным ресурсам.

3.4 Информационные ресурсы – данные, технические средства, программное обеспечение и

	Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет физической культуры»
	Политика
	СК-Пол-057.14-25

услуги (сервисы) информационных систем Университета.

3.5 Учетная запись пользователя – персональная запись, содержащая идентификационные данные и права доступа пользователя.

3.6 Криптографическая защита информации – методы защиты данных путем шифрования.

3.7 Брандмауэр – программное или аппаратное средство защиты, ограничивающее доступ к сети или ресурсам.

3.8 Пароль – последовательность символов, используемая для аутентификации пользователя.

3.9 Токен — это ключевой носитель для записи сертификата и ключей электронной подписи.

3.10 Компрометация пароля – ситуация, при которой пароль стал известен третьим лицам.

3.11 Программное обеспечение (ПО) – совокупность программ, используемых в Университете.

3.12 Лицензионное программное обеспечение (ПО) – программное обеспечение, приобретенное или используемое на основании официальных соглашений с правообладателями.

3.12 Свободное ПО – программное обеспечение, распространяемое с открытым исходным кодом по свободным лицензиям (GNU, GPL, LGPL, BSD, Apache и аналогичным).

3.13 Нелицензионное ПО – программное обеспечение, используемое без разрешения правообладателя.

3.14 Интернет – глобальная сеть, используемая для передачи данных.

3.15 Конфиденциальная информация – данные, доступ к которым ограничен и защищен законодательством или внутренними нормативными актами.

3.16 Электронная почта – сервис для передачи сообщений между пользователями через сеть Интернет.

3.17 Корпоративная почта – электронная почта Университета, работающая в едином почтовом домене.

3.18 Вредоносное программное обеспечение (вирусы, трояны, шпионские программы и т. д.) – программы, предназначенные для нанесения ущерба системам и данным.

3.19 Антивирусное ПО – программные средства защиты от вредоносного ПО.

3.20 Беспроводной доступ (Wi-Fi) – технология связи, обеспечивающая подключение устройств к сети без проводов.

3.21 Гостевая сеть Wi-Fi – отдельная сеть с ограниченным доступом для временных пользователей.

3.22 Физическая защита – меры по защите оборудования и помещений, где хранятся или обрабатываются данные.

3.23 Серверное оборудование – технические средства для хранения и обработки данных Университета.

4 ДОСТУП К ИНФОРМАЦИОННЫМ РЕСУРСАМ

4.1 Получение пользователями доступа к информационным ресурсам основывается на аутентификации этих пользователей и разграничении доступа.

4.2 В качестве объектов доступа рассматриваются информационные ресурсы Университета: данные (информация), технические средства, программные средства, услуги (сервисы) информационные системы.

	Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет физической культуры»
	Политика
	СК-Пол-057.14-25

4.3 Каждому пользователю сопоставляется учетная запись пользователя, присваиваются права доступа с учетом их важности и ценности для деятельности Университета.

4.4 В Университете могут применяться виды аутентификации, основанные на знании пользователем пароля (базовый вид аутентификации), на владении физическим носителем (USB-ключи, токены).

4.5 Пользователи уведомляются об обязанностях по обращению с физическими носителями аутентификации и сроках истечения их действия. Передача пользователем личного физического носителя другому лицу запрещена.

4.6 Назначение прав доступа соответствует принципу «Запрещено все, что явно не разрешено» и определяется, исходя из служебных обязанностей пользователя.

4.7 Категорически запрещен доступ к ресурсам по принципу «Всем – Полный доступ». Запрещен также неавторизованный (анонимный, гостевой) доступ к любым ресурсам, кроме общедоступных страниц веб-сайтов Университета.

4.8 Управление доступом к сетевым информационным ресурсам и услугам производится, в том числе, путем разделения информационной телекоммуникационной системы Университета на отдельные логические и физические сетевые сегменты.

4.9 Служебный доступ к объектам доступа Университета, осуществляемый по внешним каналам связи, должен защищаться с применением механизмов аутентификации и криптографической защиты информации.

4.10 Доступ к общедоступным страницам веб-сайтов Университета не требует соблюдения требований раздела 4.9, достаточно обеспечить шифрование трафика.

4.11 Объекты доступа Университета должны быть защищены от внешних угроз из сети Интернет и из локальной сети сетевыми брандмауэрами и штатными средствами защиты, входящими в состав операционной системы и приложений. Число открытых для доступа сервисов и ресурсов на этих объектах должно быть минимально необходимым.

4.12 При увольнении работника обеспечивается невозможность его доступа к объектам доступа Университета.

4.13 При нарушении требований данной Политики доступ пользователя к информационным ресурсам может быть временно заблокирован до устранения нарушения.

5 ИСПОЛЬЗОВАНИЕ ПАРОЛЕЙ

5.1 Пользовательские пароли (для доступа к электронной почте, сети, компьютеру и т.д.) должны содержать не менее шести буквенно-цифровых символов (буквы латинского алфавита, цифры).

5.2 Административные пароли (административных учетных записей операционных систем, телекоммуникационного оборудования, баз данных, информационных систем и т.д.) должны содержать не менее восьми буквенно-цифровых символов и спецсимволов, если они поддерживаются программным обеспечением (буквы латинского алфавита в верхнем и нижнем регистре, цифры и специальные символы типа: ! @ # \$ % л & * _ =).

5.3 Для простоты запоминания могут быть использованы парольные фразы, разделенные спецсимволами и цифрами.

5.4 Пароль не должен совпадать с логином пользователя (наименованием учетной записи) и содержать легко угадываемые слова и числа (имена, даты рождения, номера документов и т.п.).

5.5 Пользователи лично ответственны за выбор пароля, отвечающего заданным критериям

	Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет физической культуры»
	Политика
	СК-Пол-057.14-25

сложности, и за его хранение, исключаящее ознакомление с ним третьих лиц.

5.6 Запрещается передача паролей третьим лицам.

5.7 Запрещается запись и хранение паролей в местах, где они могут быть легко доступны и прочитаны.

5.8 Доступ к общедоступным страницам веб-сайтов Университета не требует парольной защиты.

5.9 В случае компрометации пароля (утраты, хищения и т.п.), пользователь должен немедленно сменить пароль. Если пользователь не имеет возможности самостоятельно сменить пароль, администратор заменяет его пароль новым паролем, который сообщает пользователю.

5.10 Учетные записи пользователей, чьи пароли не соответствуют требованиям Политики, могут быть заблокированы

6 ИСПОЛЬЗОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

6.1 В Университете разрешается использовать следующие виды ПО:

- ПО, разработанное в Университете для обеспечения своей деятельности.
- ПО, законно приобретенное или полученное Университетом на основании договорных или лицензионных соглашений с разработчиком либо правообладателем.
- Свободное ПО, распространяемое с открытым исходным кодом (Open Source) либо под свободными лицензиями: GNU, GPL, LGPL, BSD, Apache и аналогичными.
- Бесплатное ПО, лицензия на которое явно допускает его безвозмездное использование в корпоративной среде (в коммерческих целях, на служебных компьютерах, для выполнения должностных обязанностей и т.п.).

6.2 Доступ пользователей к системному и прикладному ПО должен быть санкционирован и разрешен непосредственным руководителем только для выполнения служебных обязанностей.

6.3 Пользователям ЗАПРЕЩЕНО:

- Получать (приносить, скачивать), хранить, устанавливать и использовать нелицензионное программное обеспечение.
- Использовать программное и аппаратное обеспечение Университета в неслужебных (личных) целях.
- Использовать административные учетные записи, за исключением обстоятельств, когда без этого невозможно выполнение ими должностных обязанностей.
- Использовать административные учетные записи без пароля.
- Устанавливать и использовать программное обеспечение, которое не требуется им для выполнения должностных обязанностей.

6.4 Пользователи могут самостоятельно устанавливать и обновлять необходимое для работы ПО на своих рабочих местах после согласования с руководителем Центра информационно-образовательных технологий. При этом каждый пользователь несет персональную ответственность за ПО, установленное на его рабочей станции.

6.5 Бездействующие сеансы работы должны автоматически блокироваться после определенного периода бездействия. Если автоматическое блокирование рабочего сеанса не настроено, пользователь должен самостоятельно блокировать свой сеанс, отходя от компьютера.

6.6 Для обеспечения корректной работы ПО рекомендуется применять системы автоматического обновления ПО.

6.7 ПО, установленное или используемое в Университете в нарушение настоящей

	Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет физической культуры»
	Политика
	СК-Пол-057.14-25

Политики, может быть заблокировано или удалено.

7 ИСПОЛЬЗОВАНИЕ СЕТИ ИНТЕРНЕТ

7.1 Доступ к сети Интернет должен быть разрешен только для выполнения служебных обязанностей и не может использоваться для ненадлежащей или незаконной деятельности.

7.2 При работе в сети Интернет запрещается передавать информацию ограниченного доступа (персональные данные, коммерческая и служебная информация) без соответствующего разрешения и надлежащей защиты (шифрование, пароли, электронная подпись).

7.3 Доступ в сеть Интернет для участников конференций, семинаров, иных мероприятий возможен при наличии заявки в адрес администратора сегмента сети от лица, ответственного за проведение мероприятия.

7.4 При использовании сети Интернет в Университете необходимо соблюдать законодательные, регулирующие и контрактные требования в отношении авторских и смежных прав на интеллектуальную собственность в области программного обеспечения, а также в отношении научных, литературных, музыкальных, кинематографических и иных произведений, работ, трудов и материалов.

7.5 Запрещается посещать ресурсы сети Интернет, противоречащие законодательству РФ, в том числе: пропагандирующие насилие или экстремизм; разжигающие расовую, национальную или религиозную вражду; разъясняющие порядок изготовления и (или) применения наркотиков, взрывчатых веществ, оружия и т. п.; содержащие материалы порнографического характера; предназначенные для распространения компьютерных вирусов и других вредоносных программ; нарушающие авторские и смежные права; предназначенные для подбора паролей и серийных номеров, для взлома и иной модификации программного обеспечения.

7.6 В Университете должен проводиться мониторинг информации, принимаемой и передаваемой посредством сети Интернет с использованием информационных систем Университета.

7.7 Требования к представителям сторонних организаций, использующих в своей деятельности системы Университета для доступа в сеть Интернет, должны включаться в соответствующие договоры.

7.8 Пользователям, допустившим нарушения данной Политики, может быть временно заблокирован доступ в сеть Интернет.

8 ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ

8.1 В Университете реализована концепция единого почтового домена uralgufk.ru для служебной почты Университета, работники Университета могут использовать в служебных целях почтовые ящики на базе домена uralgufk.ru (далее – корпоративная почта, почтовый сервер).

8.2 Все входящие и исходящие сообщения электронной почты должны проверяться на наличие вредоносных программ.

8.3 При использовании электронной почты в Университете запрещается передавать информацию ограниченного доступа (персональные данные, коммерческая и служебная информация) без соответствующего разрешения и надлежащей защиты (шифрование, пароли, электронная подпись).

8.4 Запрещена отправка пользователями и пересылка почтовыми серверами Университета исполняемых, служебных и системных файлов, модулей и компонентов операционных систем и

	Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет физической культуры»
	Политика
	СК-Пол-057.14-25

приложений.

8.5 При увольнении работника доступ к его корпоративной электронной почте блокируется по заявке руководителя подразделения, в котором ранее числился сотрудник.

8.6 При пользовании электронной почты пользователи обязаны соблюдать следующие правила:

- Соблюдать общепринятые нормы и правила обмена почтовыми сообщениями.
- Не рассылать сообщения противозаконного или неэтичного содержания, а также содержащие угрозы в адрес других пользователей.
- Строго следовать ограничениям в рассылке определенных видов информации, по которым установлен особый режим доступа и использования в соответствии в Законодательством РФ, локальными нормативными актами.

8.7 При массовой рассылке работники Университета должны использовать в качестве адресатов максимально заинтересованную аудиторию, не отправлять сообщение всем пользователям.

8.8 При нарушении указанных в данной Политике правил работы с электронной почтой доступ работника к корпоративной электронной почте может быть временно приостановлен до устранения нарушения.

9 ЗАЩИТА ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

9.1 Средства защиты от вредоносного программного обеспечения должны быть установлены, настроены и активизированы на всех допускающих такую установку программно-технических средствах до начала их работы с информационными системами Университета.

9.2 Средства защиты от вредоносного программного обеспечения должны иметь все последние обновления, полученные из доверенных источников.

9.3 Контролю на предмет обнаружения вредоносного программного обеспечения должна подвергаться вся информация, создаваемая и (или) обрабатываемая программно-техническими средствами, а также принимаемая и (или) передаваемая с помощью машинных носителей или средств телекоммуникаций.

9.4 В соответствии с главой 6 настоящей Политики, в Университете разрешается использовать только лицензионные, свободные или бесплатные средства защиты от вредоносного программного обеспечения. Запрещено использовать средства защиты от вредоносного программного обеспечения, не имеющие требуемых лицензий либо модифицированные с целью снятия лицензионных ограничений.

9.5 Программно-технические средства (компьютеры, серверы, коммуникационное оборудование и т.д.), допускающие установку средств защиты от вредоносного программного обеспечения, но не имеющие таковых, могут быть временно отключены от информационных систем и сегментов локальных вычислительных сетей Университета.

9.6 Запрещено отключение или модификация антивирусного ПО.

9.7 Файлы, полученные из внешних источников, должны быть проверены антивирусной программой перед открытием.

10 ИСПОЛЬЗОВАНИЕ СРЕДСТВ БЕСПРОВОДНОГО ДОСТУПА

10.1 Беспроводной доступ к информационным системам и ресурсам Университета для работников, обучающихся Университета и лиц, работающих по договорам гражданско-правового

Версия: 1.0	Без подписи документ действителен 8 часов после распечатки. Дата и время распечатки: 24/02/2025, 10:00	КЭ: _____	УЭ № _____	Стр. 7 из 9
--------------------	--	-----------	------------	-------------

	Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет физической культуры»
	Политика
	СК-Пол-057.14-25

характера, разрешается при соблюдении требований безопасности.

10.2 Беспроводной доступ в сети Университета предоставляется через защищенные точки доступа.

10.3 Для подключения к корпоративной сети Wi-Fi пользователи должны использовать пароль, установленный для данной сети. Авторизация осуществляется путем ввода пароля при подключении к защищенной беспроводной сети.

10.4 Гостевой доступ к беспроводной сети предоставляется через отдельную сеть (гостевая Wi-Fi) с ограниченными правами доступа. Для подключения к гостевой сети каждый пользователь должен пройти регистрацию через всплывающую форму авторизации. В форме необходимо указать номер телефона, на который поступит звонок с сообщением, содержащим код для завершения регистрации. После ввода кода доступ к гостевой сети будет предоставлен на ограниченный срок.

10.5 Запрещается использование незащищенных или неподконтрольных университету точек доступа для работы с корпоративными данными.

10.6 Все беспроводные соединения должны использовать шифрование данных (WPA2/WPA3 или выше).

10.7 Запрещается передача конфиденциальной информации через открытые или общедоступные беспроводные сети.

10.8 Устройства, подключаемые к беспроводным сетям университета, должны быть защищены антивирусным ПО и иметь актуальные обновления безопасности.

10.9 В случае обнаружения подозрительной активности или нарушений, доступ пользователя к беспроводной сети может быть заблокирован до выяснения обстоятельств.

11 ФИЗИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИОННЫХ РЕСУРСОВ

11.1 Работники Университета и лица, работающие по гражданско-правовым договорам, должны постоянно помнить о необходимости обеспечения физической безопасности оборудования (предотвращение воздействий окружающей среды и возможности неавторизованного доступа), на котором хранится, передаётся или обрабатывается информация Университета.

11.2 Оборудование, поддерживающее функционирование критичных информационных систем, должно быть установлено в отдельных помещениях. Помещения должны быть доступны только уполномоченному персоналу и защищены от преднамеренного или случайного повреждения.

11.3 Все места установки и хранения компьютерного оборудования должны быть расположены и защищены таким образом, чтобы уменьшить риски от воздействий окружающей среды и возможности неавторизованного доступа.

11.4 Серверное оборудование Университета должно быть защищено от угроз, связанных с отказами и сбоями систем обеспечения.

11.5 Конфиденциальную информацию и оборудование либо программное обеспечение, предназначенное для обработки или защиты конфиденциальной информации, разрешается выносить за пределы территории Университета только на основании соответствующего разрешения.

11.6 Должен существовать процесс предоставления и блокирования физического доступа к серверным комнатам, к центрам обработки или хранения данных.

11.7 При передаче (списании) оборудования, все носители информации должны быть

Версия: 1.0	Без подписи документ действителен 8 часов после распечатки. Дата и время распечатки: 24/02/2025, 10:00	КЭ: _____	УЭ № _____	Стр. 8 из 9
--------------------	--	-----------	------------	-------------

	Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет физической культуры»
	Политика
	СК-Пол-057.14-25

проверены на предмет полного уничтожения содержащейся на них важной (конфиденциальной) информации и программного обеспечения с целью предотвращения возможности восстановления этой информации.

12 РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

12.1 Все пользователи информационных систем, услуг и ресурсов Университета должны сообщать о любых замеченных или подозреваемых недостатках безопасности в системах или услугах так оперативно, насколько это возможно.

12.2 Все пользователи обязаны сообщать своему руководству об известных им или подозреваемых ими нарушениях информационной безопасности, а также ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

12.3 В случае обнаружения пропажи информационных ресурсов или компонентов информационных систем Университета следует незамедлительно сообщить об этом руководителю своего структурного подразделения.