Приложение
к приказу и.о. ректора
РХТУ им. Д.И. Менделеева
от 06.02.2024 № 8 01

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский химико-технологический университет имени Д.И. Менделеева» (РХТУ им. Д.И. Менделеева)

РЕГЛАМЕНТ

предоставления корпоративной учетной записи в Федеральном государственном бюджетном образовательном учреждении высшего образования "Российский химико-технологический университет имени Д.И. Менделеева"

Москва
2024 г.

Оглавление

1. Область применения

1.1. Настоящий Регламент определяет правила предоставления, отключения и политику безопасности корпоративных учетных записей Федерального государственного бюджетного образовательного учреждения высшего образования "Российский химико-технологический университет имени Д.И. Менделеева" (далее – Университет), а также его филиалов и представительств.

1.2. Регламент разработан для соблюдения требований информационной безопасности при работе с корпоративной учетной записью в корпоративной информационной среде Университета и применяется для защиты информации, обеспечения её целостности и предотвращения любых несанкционированных действий с данными.

1.3. Регламент устанавливает требования по предоставлению и использованию корпоративной учетной записи для следующих категорий пользователей, которым необходим доступ к корпоративным информационным системам:

- **работнику** для выполнения трудовых функций;
- **обучающемуся** в рамках учебной программы;
- **третьему лицу** в период выполнения договорных или иных обязательств.

1.4. Регламент устанавливает требования к следующим процедурам:

- формирование корпоративной учетной записи;
- способы активации и деактивации корпоративной учетной записи;
- требования к параметрам пароля и использованию корпоративной учетной записи;
- способы информирования пользователя об окончании действия пароля;
- способы изменения пароля корпоративной учетной записи.

1.5. Регламент не распространяется на корпоративные информационные системы, не поддерживающие сквозной механизм аутентификации с использованием корпоративной учетной записи.

1.6. Регламент разработан в соответствии с действующим законодательством Российской Федерации, Уставом и действующими локальными нормативными актами Университета.

2. Термины, определения и сокращения

2.1. **Автоматизированное рабочее место (АРМ)** – программно-технический комплекс, предназначенный для автоматизации деятельности пользователей Университета.

2.2. **Аутентификация** – проверка принадлежности пользователю предъявленного им идентификатора, подтверждение подлинности.

2.3. **Департамент информационных технологий (ДИТ)** – структурное подразделение Университета, отвечающее за организацию и обеспечение комплексной защиты информации в соответствии с Положением о Департаменте информационных технологий.

2.4. **Единый центр поддержки пользователей**, support@muctr.ru – служба единого окна в ДИТ для приема, регистрации и обработки обращений пользователей.

2.5. **Корпоративная информационная среда** – совокупность информационных систем и информационной инфраструктуры, обеспечивающая сбор, обработку, хранение, защиту и передачу информации.

2.6. **Корпоративная учетная запись (КУЗ)** – совокупность идентификационных данных для аутентификации и определенного набора полномочий для выполнения действий в корпоративной информационной среде Университета, предоставляемой пользователю.

2.7. **Корпоративная электронная почта (КЭП)** – компонент корпоративной информационной среды Университета, предоставляющий возможность обмена электронными письмами и совместной работы с календарями и задачами.

2.8. **Корпоративный домен (muctr.ru)** – компонент корпоративной информационной среды Университета, отвечающий за хранение, обработку и предоставление данных о корпоративных учетных записях пользователей, программном и аппаратном обеспечении для работы с информационными системами.

2.9. **Несанкционированный доступ –** доступ к информации, осуществляемый с нарушением установленных прав и/или правил доступа.

2.10. **Обработка информации** – действие (операция) или совокупность действий (операций), совершаемых с информацией с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, восстановление, блокирование, удаление, уничтожение информации.

2.11. **Информационная безопасность** – состояние защищенности корпоративной информационной среды Университета от несанкционированного доступа, использования, раскрытия, искажения, изменения или уничтожения данных.

2.12. **Идентификационные данные корпоративной учетной записи (идентификационные данные)** – уникальные данные пользователя: пароль и логин пользователя. Правила генерации логина пользователя устанавливаются Приложением 1 настоящего Регламента.

2.13. **Информационная система (ИС)** – совокупность информации, которая содержится в базах данных, обеспечивающих ее обработку с использованием информационных технологий и технических средств.

2.14. **Обучающийся** – физическое лицо, осваивающее образовательную программу в Университете.

2.15. **Операционная система** – комплекс программ, предназначенных для управления ресурсами АРМ и организации взаимодействия с пользователем.

2.16. **Работник** – физическое лицо, состоящее в трудовых отношениях с Университетом.

2.17. **Третьи лица** – любые физические лица, не являющиеся работниками или обучающимися Университета; любые юридические лица, их объединения; должностные лица, органы государственной власти и местного самоуправления; иные лица, с которыми Университет вступает в какие-либо правоотношения.

2.18. **Угроза информационной безопасности (ИБ-угроза)** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение информации, а также иных неправомерных действий при её обработке в информационной системе Университета.

3. Требования и процедуры предоставления или отзыва доступа к корпоративной учетной записи

3.1. КУЗ обеспечивает доступ к корпоративной информационной среде Университета с помощью идентификационных данных.

3.2. КУЗ позволяет получать доступ к корпоративной информационной среде Университета:

- корпоративный портал РХТУ им. Д.И. Менделеева;
- корпоративная электронная почта;
- автоматизированные рабочие места в корпоративном домене;
- сервис централизованной печати и сканирования;
- корпоративная сеть беспроводной передачи данных;
- сервис файлового хранилища;
- иные корпоративные информационные системы, разработанные или интегрированные ДИТ (поддерживающие механизм аутентификации с использованием КУЗ).

3.3. КУЗ предоставляется на основании:

- заключения трудовых отношений между работником и Университетом (КУЗ создается автоматически, способы активации КУЗ приведены в Приложении 2 настоящего Регламента);
- приказа о зачислении обучающегося в Университет (КУЗ создается автоматически);
- обращения в Единый центр поддержки пользователей от работника Университета, ответственного за третье лицо, (по согласованию с руководителем структурного подразделения) в рамках исполнения договорных обязательств или законодательных требований.[1]

3.4. Пользователю предоставляется минимальный набор полномочий, необходимых для выполнения вверенных задач. Применение этого принципа позволяет разграничивать права доступа пользователей к элементам корпоративной информационной среды Университета, минимизируя возможные риски информационной безопасности от ошибочного или несанкционированного доступа.

---

[1] Срок действия КУЗ третьего лица определяется ответственным работником в обращении, но не более 12 месяцев с даты создания. Ответственный работник имеет право направить обращение в Единый центр поддержки пользователей для продления срока действия КУЗ, в таком случае КУЗ продлевается с новым паролем. На работника Университета возлагается ответственность за действия третьего лица в корпоративной информационной среде.

3.5. Выдача дополнительного набора полномочий пользователю предоставляется по согласованию с руководителем его структурного подразделения после обращения в Единый центр поддержки пользователей.

3.6. Для своевременного выявления и предупреждения ИБ-угроз работники ДИТ вправе применять средства автоматизированного мониторинга и анализа действий пользователя в периметре корпоративной информационной среды Университета.

3.7. Деактивация доступа пользователя к корпоративной информационной среде Университета проводится:

- с даты увольнения работника согласно приказу о прекращении (расторжении) трудового договора с работником;
- по обращению руководителя структурного подразделения в Единый центр поддержки пользователей;
- с даты окончания срока действия КУЗ третьего лица, указанного в обращении ответственного за него лица в Единый центр поддержки пользователей.

3.8. Изменение доступа к корпоративной информационной среде Университета проводится:

- с даты перевода работника на другую должность и/или в другое подразделение в Университете согласно приказу;
- с даты отчисления обучающегося согласно приказу об отчислении;[2]
- по обращению руководителя структурного подразделения в Единый центр поддержки пользователей;
- обращению ответственного за третье лицо работника в Единый центр поддержки пользователей.

3.9. В случае возникновения внештатных ситуаций или подозрительных действий, выполняемых от имени КУЗ пользователя, работники ДИТ имеют право:

- выполнить блокировку КУЗ;
- ограничить права доступа к корпоративной информационной среде Университета;
- изменить пароль от КУЗ.

Для последующего восстановления доступа к КУЗ пользователю необходимо обратиться в Единый центр поддержки пользователей.

4. Требования и процедуры организации парольной защиты

4.1. Пароль пользователя является конфиденциальной информацией и должен быть известен только пользователю. Пользователь несет персональную ответственность за конфиденциальность сгенерированного им пароля.

4.2. При создании КУЗ устанавливается одноразовый пароль, который пользователь меняет при аутентификации в одной из систем корпоративной информационной среды Университета:

- корпоративный портал РХТУ им. Д.И. Менделеева (portal.muctr.ru);
- веб-версия сервиса корпоративной электронной почты (post.muctr.ru);

---

[2] Ограничиваются права в корпоративной информационной среде Университета. За исключением корпоративного портала и сайта электронной информационно-образовательной среды.

- автоматизированное рабочее место в корпоративном домене Университета.

4.3. Требования КУЗ определены базовыми параметрами:

- ограничение длины пароля КУЗ;
- срок действия пароля КУЗ;
- сложность пароля КУЗ;
- неповторимость пароля КУЗ;
- лимит неудачных попыток аутентификации;
- способ аутентификации;
- время блокировки сеанса при неактивности пользователя;
- время блокировки учетной записи при достижении лимита неудачных попыток аутентификации.

Детальные требования к параметрам пароля и КУЗ представлены и регулируются Приложением 3 настоящего Регламента.

4.4. При отсутствии визуального контроля над АРМ доступ к операционной системе должен быть немедленно заблокирован. Для этого пользователь обязан нажать одновременно комбинацию клавиш Win + L или Ctrl + Alt + Del и выбрать опцию «Заблокировать».

4.5. Заблаговременно до истечения срока действия текущего пароля пользователь информируется о необходимости его изменения. Способы информирования приведены в Приложении 4 настоящего Регламента.

4.6. В случае компрометации, утери или истечения срока действия пароля, пользователь обязан немедленно изменить его с помощью одного из способов, указанных в Приложении 5 настоящего Регламента.

4.7. Правила генерации пароля:

- запрещается использовать в качестве пароля логин, простые пароли (например – «1234567890», «1111111111», «password» и им подобные, а также имена и даты рождения, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно вычислить, основываясь на информации о пользователе);
- запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию символов (например - «fffffff», «aabaabaab» и т.п.);
- запрещается использование средств упрощенной аутентификации в операционной системе (например – «Windows Hello» или иных способов упрощенной аутентификации);
- запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например – «1qaz2wsx», «qwerty», «1q2w3e» и т.п.).

4.8. Правила хранения пароля:

- запрещается сообщать другим пользователям пароль и аутентифицировать их в корпоративных системах под КУЗ;
- запрещается использование пароля КУЗ на сторонних ресурсах, не входящих в периметр корпоративной информационной среды Университета;

- запрещается записывать пароль на бумаге, в файле, мобильном телефоне и других носителях информации, в том числе на предметах.

4.9. Правила ввода пароля:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;
- во время ввода пароля необходимо исключить произнесение его вслух, возможность подсматривания посторонними лицами, в том числе с использованием технических средств. При аутентификации ИС обеспечивается исключение отображения для пользователя действительного значения пароля, вводимые символы могут отображаться условными знаками «*», «•» или иными знаками.

5. Внесение изменений в Регламент

5.1. Плановая актуализация настоящего Регламента проводится 1 раз в 2 года с даты утверждения с целью обновления в соответствии с реальными условиями и текущими требованиями к защите информации.

5.2. Внеплановая актуализация Регламента проводится в обязательном порядке в следующих случаях:

- при изменении указов и законов Российской Федерации в области защиты информации;
- при изменении законодательных норм, действующих на территории иностранных государств, в которых присутствуют филиалы и/или представительства Университета в области защиты информации;
- при изменении локальных нормативных актов (инструкций, положений, руководств), касающихся информационной безопасности Университета;
- при происшествии и выявлении инцидента по нарушению информационной безопасности, влекущего ущерб для Университета.

5.3. В ряде случаев, требующих оперативного вмешательства, связанного с инцидентом информационной безопасности (несанкционированный доступ, угроза или разглашение конфиденциальной информации, превышение полномочий определенными лицами) вносятся изменения в настоящий Регламент и принимаются меры по ликвидации и последующему предупреждению инцидента информационной безопасности в срочном одностороннем порядке директором ДИТ без согласований.

5.4. Изменения и дополнения в Регламент выносятся на рассмотрение ректора директором ДИТ и утверждаются приказом ректора Университета.

5.5. Изменения и дополнения в Приложения настоящего Регламента утверждаются директором ДИТ. В случае внесения изменений проводится информирование пользователей, которых затронули исправления.

6. Ответственность

6.1. Пользователь обязан знать и строго выполнять требования настоящего Регламента и других локальных нормативных актов или иных документов Университета.

6.2. Пользователь обязан незамедлительно сообщать в Единый центр поддержки пользователей об утере, компрометации и несанкционированном изменении пароля.

6.3. Пользователь несет персональную ответственность за все действия и последствия, совершенные от имени его КУЗ.

6.4. Руководитель подразделения обязан своевременно информировать ДИТ обо всех изменениях, связанных с определением прав доступа пользователя. Ответственность за возникновение инцидента, связанного с непредоставлением или предоставлением недостоверной информации в ДИТ, несет Руководитель подразделения.

Приложение 1

Правила формирования корпоративной учетной записи пользователя

Корпоративная учетная запись работника

Логин КУЗ работника имеет вид:

[1].[2].[3]@[4], где:

[1] – транслитерированная фамилия работника;
[2] – транслитерированный инициал имени работника;
[3] – транслитерированный инициал отчества работника;
[4] – наименование корпоративной доменной зоны – **muctr.ru**.

Пример обозначения КУЗ работника Иванова И.И.:

ivanov.i.i@muctr.ru

***Важно**: в случае, если такой логин уже существует, к инициалу отчества работника добавляется вторая (а, при необходимости и последующие), транслитерированные буквы из отчества.*

Пример обозначения КУЗ работников однофамильцев с одинаковыми инициалами имени и отчества: **ivanov.i.iv@muctr.ru** – КУЗ работника однофамильца Университета Иванов И.И. в muctr.ru. Аналогично следующая КУЗ будет иметь вид:

ivanov.i.iva@muctr.ru, **ivanov.i.ivan@muctr.ru** и т.д.

Корпоративная учетная запись обучающегося

Логин КУЗ обучающегося имеет вид:

[1]@[2], где:

[1] – номер зачетной книжки обучающегося (2 цифры года поступления + 4 цифры уникального порядкового номера при записи данных в информационной системе);
[2] – наименование корпоративной доменной зоны – muctr.ru.

Пример обозначения КУЗ обучающегося, поступившего в 2023 году:

231572@muctr.ru

Учетная запись третьего лица

Логин КУЗ третьего лица имеет вид:

[1].[2]@[3], где:

[1] – константный индекс третьего лица – guest;
[2] – уникальный порядковый номер (4 разряда 0001…9999);
[3] – наименование корпоративной доменной зоны – muctr.ru.

Пример обозначения КУЗ третьего лица с уникальным порядковым номером 3215:

guest.3215@muctr.ru

Приложение 2

Способы активации корпоративной учетной записи работника

Активация КУЗ работника выполняется при личном обращении с документом, удостоверяющим личность, в один из пунктов приёма Единого центра поддержки пользователей:

- помещение 182 Миусского комплекса Университета (г. Москва, Миусская площадь, д. 9, стр. 1);
- помещение 341 Тушинского комплекса Университета (г. Москва, ул. Героев Панфиловцев, д. 20);
- помещение 4 Культурно-спортивного комплекса Студенческого городка Университета (г. Москва, ул. Вилиса Лациса, д. 21);
- помещение 350 Лабораторного корпуса Новомосковского института Университета (Тульская обл., г. Новомосковск, ул. Дружбы, д.8).

Дополнительная информация расположена на сайте «База знаний РХТУ» (wiki.muctr.ru) в разделе Обращение в Единый центр поддержки пользователей.

Приложение 3

Требования к параметрам пароля и использованию корпоративной учетной записи

Параметр / Категория	Работник	Обучающийся	Третье лицо
Минимальная длина пароля	**12** символов		
Максимальная длина пароля	**255** символов		
Минимальный срок действия пароля	**1** календарный день		
Максимальный срок действия пароля	**75** календарных дней		
Сложность пароля	В пароле должны использоваться минимум **3** типа символов из следующего списка: цифры, символы английского алфавита в верхнем регистре, символы английского алфавита в нижнем регистре, спец. символы		
Требования к неповторимости	Новое значение пароля должно отличаться от предыдущего, не менее чем в **3** последовательных символах		
Количество старых паролей, которые хранятся в информационной системе, запрещая пользователю повторно использовать старый пароль	**5** шт.		
Количество неудачных попыток входа в систему до блокировки КУЗ	**5** шт.		
Время блокировки КУЗ при неоднократных неудачных попытках аутентификации	**15** мин.		
Время автоблокировки сеанса доступа на АРМ	**10** минут		
Время разблокировки КУЗ через единый центр поддержки пользователей	От **15** мин.		
Способ аутентификации	Логин и пароль		
Символы, допустимые для использования в пароле	A – Z, a – z, 0 – 9 , ! # % & * + - . : < = > ? @ ^ _ | ~		

Приложение 4

Способы и формат информирования пользователя об окончании действия пароля

1. Информирование пользователя о необходимости плановой смены пароля проводится путем отправки электронного сообщения в КЭП с адреса ДИТ (info@muctr.ru). Первое информирование происходит за 10 календарных дней до окончания срока действия пароля. В случае, если пользователь не сменил пароль от КУЗ, на корпоративный электронный адрес Пользователя направляются дополнительные информационные сообщения посредством КЭП по следующему графику:

- за 3 календарных дня до окончания срока действия пароля;
- за 1 календарный день до окончания срока действия пароля.

Текст направляемого сообщения:

Уважаемый(ая) [Ф.И.О. Пользователя].

Действие пароля Вашей учетной записи в корпоративной домене muctr.ru заканчивается через [число] дней.

Для предотвращения потери доступа к информационным системам РХТУ им. Д.И. Менделеева, пожалуйста, обновите пароль до истечения указанного срока.

Инструкция по смене пароля расположена на сайте «База знаний РХТУ» в разделе «Корпоративные системы и сервисы», подраздел Корпоративная учетная запись РХТУ им. Д.И. Менделеева (wiki.muctr.ru).

Процедура смены пароля.

На рабочем месте: нажмите одновременно сочетание клавиш Ctrl + Alt + Del, из появившегося списка выберите «Сменить пароль…».

В окне смены пароля проверьте корректность написания Вашего логина, в строке «Старый пароль» необходимо указать текущий пароль, в строке «Новый пароль» следует ввести новый пароль. В строке «Подтверждение пароля» введите новый пароль для подтверждения. После этого нажмите на клавиатуре клавишу «Enter» или на стрелку «Отправить».

Обращаем внимание, пароль должен отвечать следующим требованиям:

- длина не менее 12 символов;
- содержать буквы, цифры и специальные символы (#, @, %, ^ и т.д.);
- новый пароль не должен совпадать с пятью предыдущими;
- допускается не более 5 неудачных попыток ввода пароля (в случае неверного ввода, учетная запись будет заблокирована на 15 мин.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования автоматизированных рабочих мест и т.д.).

Если Вы находитесь вне корпоративной сети, сменить пароль можно в веб-интерфейсе корпоративной электронной почты (post.muctr.ru) в разделе «Параметры». Дополнительная информация расположена на сайте «База знаний РХТУ» (wiki.muctr.ru) в

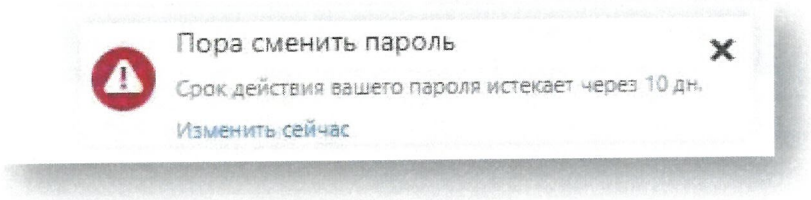
разделе «Корпоративные системы и сервисы» - «Корпоративная учетная запись РХТУ им. Д.И. Менделеева».

При возникновении вопросов Вы можете обратиться в Единый центр поддержки пользователей по адресу support@muctr.ru.

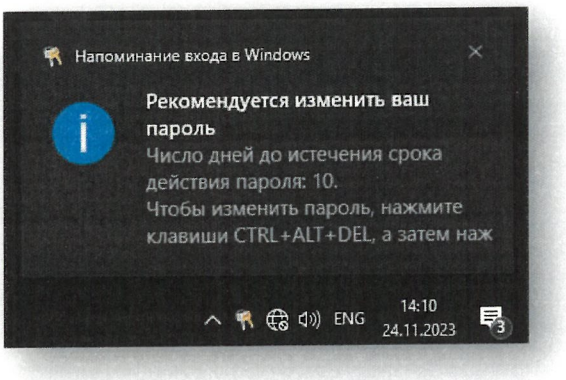
С уважением,

Департамент информационных технологий
РХТУ им. Д.И. Менделеева
125047, г.Москва, Миусская площадь, д.9
Тел: +7 (499) 2502765
E-mail: support@muctr.ru
WEB: www.muctr.ru/dit

2. Информирование об окончании срока действия пароля в веб-интерфейсе КЭП проводится в формате всплывающего уведомления. Пользователь получает уведомление об истечении срока действия пароля за 10 дней до окончания срока его действия. Оповещение повторяется каждый день с обратным счетчиком до момента смены пароля.



3. Информирование об окончании срока действия пароля на АРМ проводится в формате всплывающего уведомления. Пользователь получает уведомление об истечении срока действия пароля за 10 дней до окончания срока его действия. Оповещение повторяется каждый день с обратным счетчиком до момента смены пароля.



Приложение 5

Способы изменения пароля корпоративной учетной записи пользователя

Для изменения пароля КУЗ пользователю необходимо воспользоваться одним из способов:

1. В корпоративном портале РХТУ им. Д.И. Менделеева (portal.muctr.ru) и выбрать «Изменить пароль»;
2. В веб-интерфейсе КЭП (post.muctr.ru) в разделе «Параметры»;
3. На рабочем столе АРМ в корпоративном домене Университета нажать одновременно сочетание клавиш Ctrl + Alt + Del, в появившемся списке выбрать «Изменить пароль…»;
4. Лично обратиться в один из пунктов приема Единого центра поддержки пользователей:

- помещение 182 Миусского комплекса Университета (г. Москва, Миусская площадь, д. 9, стр. 1);
- помещение 341 Тушинского комплекса Университета (г. Москва, ул. Героев Панфиловцев, д. 20);
- помещение 4 Культурно-спортивного комплекса Студенческого городка Университета (г. Москва, ул. Вилиса Лациса, д. 21);
- помещение 350 Лабораторного корпуса Новомосковского института Университета (Тульская обл., г. Новомосковск, ул. Дружбы, д. 8).

В случае окончания срока действия пароля КУЗ при аутентификации в корпоративном портале, КЭП или АРМ, пользователю потребуется изменить пароль на новый. Возможно личное обращение в один из пунктов приема Единого центра поддержки пользователя для смены пароля.

Подробная информация и пошаговые инструкции по каждому из вышеописанных вариантов расположены на сайте «База знаний РХТУ» (wiki.muctr.ru) в разделе «Корпоративные системы и сервисы» – «Корпоративная учетная запись РХТУ им. Д.И. Менделеева».