МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Карачаево-Черкесский государственный университет имени У.Д. Алиева»
(КЧГУ)

Утверждаю
И.о. ректора КЧГУ
_____ Т.А. Узденов
«__06_____ 2025 г.

ПОЛОЖЕНИЕ

О применении многофакторной аутентификации

1. Общие положения

1.1. Настоящее Положение устанавливает порядок и условия применения многофакторной аутентификации (далее — МФА) для обеспечения информационной безопасности при доступе к информационным системам КЧГУ имени У.Д. Алиева (далее — Учреждение).

1.2. Многофакторная аутентификация представляет собой метод подтверждения личности пользователя, предусматривающий использование как минимум двух независимых факторов аутентификации из следующих категорий:

- знание (например, пароль, PIN-код);
- владение (например, смартфон, USB-ключ);
- принадлежность (например, биометрические данные, графический ключ).

- PIN-код (англ. PIN — personal identification number) — персональный идентификационный номер, являющийся секретным кодом карты. Его длина варьирует от 4 до 12 цифр. ПИН-код может состоять также из букв.

- USB-ключ (также аппаратный токен, криптографический токен) — компактное устройство, предназначенное для обеспечения информационной безопасности пользователя. USB-ключи используют для идентификации владельца, безопасного доступа к информационным ресурсам и других целей.

- Графический ключ — это один из методов аутентификации, основанный на воспроизведении пользователем заранее заданного рисунка, последовательности точек или геометрических фигур.

- Биометрические данные — это уникальные физические и поведенческие характеристики человека, которые используются для аутентификации, в том числе для доступа к ПК. Некоторые методы биометрической аутентификации: Распознавание лица (инфракрасная камера проверяет уникальные черты лица, распознавая их даже в темноте); Сканирование отпечатка пальца (специальный датчик считывает узор на пальце и сравнивает его с ранее сохранённым образцом); Распознавание радужной оболочки глаза (камера сканирует радужную оболочку глаза человека, изображение которой используется для аутентификации); Распознавание голоса (идентификация и аутентификация личности происходит с помощью микрофона, который подключён к записывающему устройству).

1.3. Положение разработано в соответствии с:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 28.11.2019 № 678 «Об утверждении Требований к защите информации».

1.4. Целью использования МФА является повышение уровня защиты информационных систем Учреждения от несанкционированного доступа и обеспечение конфиденциальности персональных данных.

1.5. Ответственность за организацию и контроль применения МФА возлагается на руководителя Учреждения и сотрудников, ответственных за информационную безопасность.

2. Порядок применения многофакторной аутентификации

2.1. МФА применяется при доступе к следующим информационным системам и ресурсам Учреждения.

2.2. Для аутентификации используется комбинация следующих факторов:

- первый фактор: текстовый пароль или PIN-код;
- второй фактор: графический ключ, или одноразовый код, отправляемый на мобильное устройство, или биометрическая аутентификация.

2.3. Графический ключ может быть реализован через специализированное программное обеспечение, установленное на устройствах пользователей, или через встроенные функции операционных систем.

2.4. Пользователи обязаны соблюдать следующие требования:

- не передавать свои учетные данные третьим лицам;
- регулярно обновлять пароли и графические ключи;
- сообщать о любых подозрительных действиях в системе.

2.5. В случае утраты доступа к одному из факторов аутентификации (например, потеря мобильного устройства) пользователь должен незамедлительно обратиться к сотруднику, ответственному за информационную безопасность Учреждения.

3. Ответственность сторон

3.1. Сотрудники Учреждения несут персональную ответственность за сохранность своих учетных данных и соблюдение требований настоящего Положения.

3.2. Администрация Учреждения обязана:

- обеспечить техническую возможность применения МФА;
- проводить обучение пользователей правилам работы с системой аутентификации;
- осуществлять мониторинг и анализ инцидентов, связанных с нарушением требований информационной безопасности.

3.3. За нарушение требований настоящего Положения предусмотрена дисциплинарная или административная ответственность в соответствии с действующим законодательством РФ.

4. Заключительные положения

4.1. Настоящее Положение вступает в силу с момента его утверждения руководителем Учреждения.

4.2. Изменения и дополнения в Положение вносятся приказом руководителя Учреждения.

4.3. Контроль за исполнением настоящего Положения возлагается на ответственного за информационную безопасность Учреждения.

Приложение

РЕГЛАМЕНТ

применения многофакторной аутентификации с использованием графического ключа

1. Общие положения

1.1. Регламент определяет порядок использования графического ключа в рамках многофакторной аутентификации (МФА) для доступа к информационным системам Учреждения.

1.2. Регламент является обязательным для всех пользователей информационных систем Учреждения, на компьютерах которых обрабатываются персональные данные.

2. Процесс регистрации графического ключа

2.1. Для регистрации графического ключа пользователь должен выполнить следующие шаги:

- войти в свою учетную запись на компьютере Учреждения;
- перейти в раздел «Настройки безопасности»;
- выбрать опцию «Добавить графический ключ»;
- создать уникальный рисунок, соединив не менее 4 точек на экране;
- подтвердить создание ключа путем повторного ввода рисунка.

2.2. Графический ключ должен соответствовать следующим требованиям:

- минимальная длина — 4 точки;
- запрещено использование простых геометрических фигур (например, прямые линии или квадрат);
- рекомендуется использовать сложные комбинации точек.

2.3. После регистрации графического ключа система автоматически активирует его как второй фактор аутентификации.

3. Процесс входа в систему с использованием графического ключа

3.1. Для входа в информационную систему пользователь должен выполнить следующие действия:

- ввести свой логин и пароль;
- подтвердить личность с помощью графического ключа, воспроизведя ранее зарегистрированный рисунок.

3.2. В случае трехкратного неверного ввода графического ключа доступ к системе блокируется, и пользователь должен обратиться в центр информационных технологий.

4. Безопасность и защита данных

4.1. Графический ключ хранится в зашифрованном виде.

4.2. Пользователи обязаны:

- не демонстрировать процесс ввода графического ключа посторонним лицам;
- не использовать один и тот же рисунок для других систем аутентификации;
- регулярно менять графический ключ (**не реже одного раза в 3 месяца**).

4.3. В случае подозрения на компрометацию графического ключа пользователь должен немедленно изменить его в настройках безопасности.

5. Ответственность за нарушение регламента

5.1. Нарушение требований настоящего Регламента влечет за собой:

- временную блокировку доступа к информационным системам;
- проведение служебного расследования;
- привлечение к дисциплинарной или административной ответственности.

5.2. В случае выявления систематических нарушений доступ к информационным системам может быть полностью прекращен.

6. Заключительные положения

6.1. Настоящий Регламент является неотъемлемой частью Положения о применении многофакторной аутентификации.

6.2. Изменения и дополнения в Регламент вносятся приказом руководителя Учреждения.