УТВЕРЖДЕНО
Генеральный директор

_____А.П. Бадаев
Приказ № 260-09/10-01 от «09» октября 2026 г.

ПОЛОЖЕНИЕ

О СПОСОБАХ ИДЕНТИФИКАЦИИ И (ИЛИ) АУТЕНТИФИКАЦИИ ОБУЧАЮЩИХСЯ ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

МОСКВА 2026

1. Общие положения

1.1. Настоящее Положение о способах идентификации и (или) аутентификации обучающихся при использовании электронного обучения и дистанционных образовательных технологий (далее – Положение) устанавливает способы идентификации и (или) аутентификации обучающихся в Обществе с ограниченной ответственностью «Киберпротект» (далее – Компания, образовательная организация) при реализации образовательных программ с применением электронного обучения (далее – ЭО) и дистанционных образовательных технологий (далее – ДОТ) посредством электронной информационно-образовательной среды (далее – ЭИОС).

1.2. Настоящее Положение разработано в соответствии с Федеральным законом от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», Постановлением Правительства Российской Федерации от 11 октября 2023 г. № 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ», ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 10 апреля 2020 г. № 159-ст, иными нормативными правовыми актами, регламентирующими деятельность в сфере образования с применением ДОТ и ЭО, локальными нормативными актами Компании.

2. Термины и определения

2.1. **Администратор ЭИОС** - ответственное лицо, осуществляющее функции централизованного управления и информационно-технологического сопровождения ЭИОС.

2.2. **Аттестационное мероприятие** - организованная процедура оценки результатов освоения образовательной программы (её части или этапа), направленная на установление уровня знаний, умений, навыков и компетенций обучающихся.

2.3. **Аутентификация** - процедура проверки подлинности субъекта (подтверждение того, что субъект является тем, за кого себя выдаёт) посредством предъявления учётных данных (пароль, иные факторы).

2.4. **Дистанционные образовательные технологии (ДОТ)** - образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и преподавателей.

2.5. **Дополнительные профессиональные программы (ДПО, образовательная программа)** - образовательные программы в рамках ДПО, направленные на совершенствование имеющихся или получение новых профессиональных компетенций.

2.6. **Журнал событий ЭИОС** - встроенный механизм фиксации действий пользователей и системных событий в ЭИОС.

2.7. **Защита от несанкционированного доступа** - комплекс организационных, технических и правовых мер, направленных на предотвращение или существенное затруднение получения защищаемой информации (а также работы с ней: ознакомления, копирования, модификации, уничтожения) лицами, не имеющими на это установленных прав или действующих в обход утверждённых правил.

2.8. **Идентификация** - процедура распознавания субъекта по его идентификатору (имя пользователя / логин) с целью установления его личности в системе.

2.9. **Идентификационные данные** - сведения, которые позволяют прямо или косвенно установить (идентифицировать) конкретное физическое или юридическое лицо.

2.10. **Контрольные мероприятия** - текущий контроль успеваемости и аттестационные мероприятия.

2.11. **Компрометация учетных данных** - ситуация, при которой сведения, используемые для аутентификации и получения доступа к информационным системам, ресурсам или учётным записям (логины, пароли, токены, ключи доступа, ответы на контрольные вопросы), становятся известны лицам, не имеющим на это права, либо используются для несанкционированного доступа.

2.12. **Методист** - педагогический работник, осуществляющий профессиональную деятельность по разработке, внедрению и контролю эффективности образовательных программ, учебно-методических материалов и технологий обучения.

2.13. **Образовательный процесс** - целенаправленная, организованная деятельность по обучению, реализуемая в рамках образовательной программы и направленная на формирование знаний, умений, навыков, компетенций.

2.14. **Обучающийся** - физическое лицо, осваивающее образовательную программу.

2.15. **Педагогический работник** - физическое лицо, которое состоит в трудовых отношениях с Компанией, осуществляющей образовательную деятельность, и выполняет обязанности по обучению обучающихся и (или) организации образовательной деятельности.

2.16. **Пользователь** - участник образовательного процесса, который зарегистрирован в ЭИОС и имеет учетную запись с определенным набором прав и функций.

2.17. **Политика паролей** - внутренний нормативный документ Компании, который устанавливает обязательные правила создания, использования, хранения и смены паролей для обеспечения информационной безопасности.

2.18. **Преподаватель** - педагогический работник, который осуществляет обучение по определённой учебной дисциплине (предмету) в Компании, осуществляющей образовательную деятельность.

2.19. **Проктор** - лицо, осуществляющее наблюдение за ходом прокторируемого испытания.

2.20. **Прокторинг** - комплекс мер и технических решений, направленных на обеспечение объективности и самостоятельности выполнения контрольного задания обучающимся в дистанционном формате, включающий идентификацию личности и наблюдение за ходом испытания.

2.21. **Текущий контроль успеваемости** - систематическая проверка учебных достижений обучающихся, которая проводится педагогическим работником в ходе образовательной деятельности в соответствии с рабочей программой учебного предмета, курса, дисциплины (модуля).

2.22. **Центр дополнительного образования Киберпротект** - структурное подразделение Компании, занимающееся образовательной деятельностью Компании.

2.23. **Электронная информационно-образовательная среда (ЭИОС)** - совокупность информационных и телекоммуникационных технологий, соответствующих технологических средств и сервисов, обеспечивающих организацию и реализацию образовательного процесса в электронной среде, включая платформу дистанционного обучения.

2.24. **Электронное обучение (ЭО)** - организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также

информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников.

3. Способы идентификации обучающихся

3.1. Первичная (организационная) идентификация

3.1.1. Первичная идентификация осуществляется при регистрации обучающегося в ЭИОС:

1) Администратор ЭИОС или уполномоченный работник Центра дополнительного образования Киберпротект создаёт учётную запись обучающегося на основании официальных документов (договор об оказании образовательных услуг, приказ о зачислении на обучение), содержащих ФИО обучающегося.

2) Обучающемуся присваивается уникальный логин.

3) Сведения об обучающемся (ФИО, группа, электронная почта, мобильный телефон) вносятся в профиль ЭИОС и являются его идентификационными данными.

3.1.2. Самостоятельная регистрация обучающихся через форму ЭИОС допускается только при включённом тесте, позволяющим отличить реального пользователя от компьютерной программы (CAPTCHA) и последующем подтверждением Администратором ЭИОС полноты и аутентичности учётных данных методом сверки по спискам лиц, допущенных до обучения. Неподтверждённые учётные записи не имеют доступа к образовательным материалам Компании.

4. Идентификация при текущем контроле успеваемости и аттестационных мероприятиях (базовая идентификация)

4.1.1. Базовая идентификация при проведении контрольных мероприятий в ЭИОС осуществляется посредством локальной аутентификации, описанной в разделе 3 Положения. Для повышения достоверности идентификации при аттестационных мероприятиях применяются следующие методы:

— Визуальная идентификация по документу, удостоверяющему личность: применяется при проведении прокторируемых испытаний через систему видеоконференцсвязи (далее – ВКС). Проктор визуально сверяет изображение в документе с изображением обучающегося на экране веб-камеры. Метод не предполагает сбора и хранения биометрических данных.

— Дополнительная проверка активности в профиле ЭИОС: Администратор ЭИОС или преподаватель вправе проверить, что вход в ЭИОС в период испытания осуществлялся с устройства и из местоположения (по IP), соответствующих обычному профилю обучающегося, используя журнал событий ЭИОС.

4.1.2. Единая биометрическая система (ЕБС) и Единая система идентификации и аутентификации (ЕСИА/ Госуслуги) для идентификации обучающихся в ЭИОС Компании не применяются.

4.1.3. В случае возникновения сомнений в идентичности личности обучающегося преподаватель или роктор вправе приостановить испытание и запросить дополнительное подтверждение личности очным способом, дополнительным телефонным звонком по голосовой связи или посредством иной системы ВКС, установленной на мобильный телефоне и отличной от той, с которой проводится оценочная процедура, с включенной камерой и микрофоном, для параллельной проверки образа и голоса обучающегося.

5. Способы аутентификации обучающихся в ЭИОС

5.1. Основной метод аутентификации

5.1.1. Аутентификация в ЭИОС осуществляется методом локальной аутентификации: введение логина (имени пользователя) и пароля, хранимых в базе данных ЭИОС в зашифрованном виде

(хеширование с солью), а также дополнительного сгенерированного кода – второго фактора аутентификации.

5.1.2. Интеграция с внешними системами аутентификации (Active Directory, LDAP, SSO) в текущей конфигурации ЭИОС не применяется. Техническая архитектура ЭИОС допускает добавление таких интеграций в будущем без изменения основной структуры системы.

5.2. Требования к паролям

5.2.1. В целях обеспечения безопасности аутентификации устанавливаются следующие обязательные требования к паролям учётных записей ЭИОС:

— минимальная длина пароля — 8 символов;

— обязательное наличие символов не менее трёх из четырёх категорий: строчные буквы, прописные буквы, цифры, специальные символы;

— запрет использования пароля, совпадающего с логином;

— плановая смена пароля не реже одного раза в 6 месяцев (рекомендательно; может устанавливаться как обязательное требование решением Администратора ЭИОС);

— запрет повторного использования последних 5 паролей.

5.2.2. Политика паролей настраивается Администратором ЭИОС в разделе Администрирование → Безопасность → Настройки безопасности.

5.3. Защита от несанкционированного доступа

5.3.1. В ЭИОС применяются следующие механизмы защиты:

— CAPTCHA при регистрации новых пользователей через форму самостоятельной регистрации (Плагины → Аутентификация → Самостоятельная регистрация → Использовать reCAPTCHA);

— блокировка учётной записи после нескольких последовательных неудачных попыток входа (количество неудачных попыток входа и период блокировки устанавливаются Администратором ЭИОС, рекомендуется: не более 10 попыток, блокировка не менее 2 часов, но не более 24 часов), Администратор ЭИОС имеет право вручную снять блокировку при запросе от обучающегося в техническую поддержку с почтового адреса, указанного при регистрации;

— принудительный выход по тайм-ауту неактивной сессии (рекомендуется: не более 60 минут);

— возможность сброса пароля через подтверждённый e-mail обучающегося.

5.3.2. Все попытки входа (успешные и неуспешные) фиксируются в Журнале событий ЭИОС и хранятся в нем 356 дней.

6. Обязанности участников образовательного процесса

6.1. Обязанности обучающегося

— Не передавать логин и пароль от учётной записи ЭИОС третьим лицам.

— Незамедлительно сообщать администратору ЭИОС о подозрении в компрометации учётных данных. Признаками компрометации учетных данных могут быть время, IP-адрес последнего посещения, если сам Пользователь не входил в систему, любые активные действия в системе, которые Пользователь не совершал (отправленные сообщения, попытки выполнения заданий в курсе и др.), иные аномалии, причиной которой могли стать действия в системе от имени обучающегося.

— Использовать учётную запись исключительно для освоения назначенных образовательных программ.

6.2. Обязанности Администратора ЭИОС

— Создавать учётные записи обучающихся на основании официальных документов.

— Деактивировать учётные записи обучающихся, завершивших обучение или отчисленных, в течение пяти рабочих дней после завершения обучения или отчисления.

— Контролировать соответствие Политики паролей требованиям настоящего Положения.

— Обеспечивать хранение идентификационных данных обучающихся в соответствии с действующим законодательством и локальными нормативными актами Компании.

7. Защита персональных данных при идентификации и аутентификации

7.1. Обработка персональных данных обучающихся в рамках процедур идентификации и аутентификации осуществляется в соответствии с действующим законодательством, локальными нормативными актами Компании, на основании согласия обучающегося, полученного при зачислении на обучение.

7.2. Биометрические персональные данные при базовом способе аутентификации в ЭИОС не обрабатываются и не хранятся. Визуальная идентификация при прокторинге производится в режиме реального времени без сохранения биометрического шаблона.

7.3. Пароли обучающихся хранятся в базе данных ЭИОС исключительно в виде хеш-значений (bcrypt или аналоговый алгоритм), открытое хранение паролей запрещено.

8. Заключительные положения

8.1. Настоящее Положение вступает в силу с момента его утверждения приказом Генерального директора и действует до введения нового Положение. Все изменения в Положение вносятся приказом Генерального директора.

8.2. Настоящее Положение подлежит пересмотру не реже одного раза в три года, а также при изменении нормативных правовых актов в сфере образования. Актуализация настоящего Положения инициируется руководителем Центра дополнительного образования Киберпротект.

8.3. Настоящее Положение обязательно для исполнения работниками подразделений Компании, участвующих в образовательной деятельности Компании и обучающимися, осваивающими образовательные программы с использованием ЭИОС.

8.4. Настоящее Положение подлежит доведению до сведения работников Компании, участвующих в образовательной деятельности Компании, посредством кадрового электронного документооборота, а также располагается на Внутреннем портале Компании в разделе «Все ЛНА компании».

8.5. Настоящее Положение доводится до сведения обучающихся при приеме на обучение посредством размещения его в подразделе «Документы» специального раздела «Сведения об образовательной организации» официального сайта Компании. Факт ознакомления с Порядком фиксируется подписью в специальном разделе заявления о приеме.