ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «АКАДЕМИЯ КИБЕРЁЖ»

ООО «АКАДЕМИЯ КИБЕРЁЖ»

ОГРН: 1257700486702 ИНН: 7735212702 КПП: 773501001

Лицензия на осуществление образовательной деятельности: рег. № Л035-01298-77/03866463
Орган, выдавший лицензию: Департамент образования и науки города Москвы
Приказ о предоставлении/внесении изменений: от 28.11.2025 № ПР/УГНК-2965/25

Утверждаю
Генеральный директор

01.01.2026 г.

_____/ Денисенко Павел Андреевич

РЕГЛАМЕНТ ФУНКЦИОНИРОВАНИЯ ЭЛЕКТРОННОЙ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ (ЭИОС) / ЛМС

г. Москва, 2026 г.

1. Общие положения

1.1. Настоящий Регламент определяет состав, принципы функционирования, правила доступа, администрирования, журналирования (логирования), резервного копирования, восстановления, а также меры обеспечения доступности и безопасности **электронной информационно-образовательной среды (ЭИОС) / системы управления обучением (ЛМС)** ООО «Академия Киберёж» (далее - «Организация»).

1.2. Регламент применяется при реализации образовательных программ Организации по направлениям:
- дополнительное образование (ДО) для лиц от 18 лет;
- дополнительное профессиональное образование (ДПО);
- профессиональное обучение (ПО),
которые реализуются **исключительно** с применением электронного обучения и дистанционных образовательных технологий (ЭО/ДОТ).

1.3. Регламент обязателен для исполнения работниками Организации, привлечёнными преподавателями/экспертами/кураторами (при наличии доступа к ЭИОС), а также для обучающихся в части правил использования доступа и допустимого поведения в цифровой среде (в увязке с Правилами внутреннего распорядка обучающихся и условиями договора/оферты).

1.4. Регламент разработан с учетом требований к применению ЭО/ДОТ и обязательной фиксации действий и результатов в цифровой среде, включая требования Правил применения ЭО/ДОТ, утвержденных Постановлением Правительства РФ от 11.10.2023 № 1678.

1.5. Регламент является локальным нормативным актом Организации по вопросам организации и осуществления образовательной деятельности и действует совместно с иными ЛНА Организации. Основание по компетенции принятия ЛНА: ст. 30 Федерального закона № 273-ФЗ.

2. Термины и целевое назначение ЭИОС/ЛМС

2.1. **ЭИОС/ЛМС** - совокупность программно-технических средств и информационных ресурсов, обеспечивающих:
а) размещение учебных материалов и предоставление доступа к ним;
б) проведение обучения в дистанционном формате;
в) контроль и фиксацию результатов обучения/аттестации (если предусмотрено программой);
г) учет обучающихся и событий обучения;
д) хранение «цифрового следа» образовательного процесса и доказательств исполнения обязательств Организации.

2.2. **Учетная запись** - персонализированный профиль пользователя ЭИОС (обучающийся/преподаватель/администратор), с которым связаны права доступа и события (логи).

2.3. **Средства доступа** - логин/пароль, коды подтверждения, токены, ссылки или иные механизмы, применяемые для аутентификации и авторизации в ЭИОС.

2.4. **Цифровой след** - совокупность технических событий и данных, формируемых ЭИОС: входы, открытия модулей, попытки тестов, загрузки работ, выставление оценок, комментарии проверяющего, статусы завершения, подтверждения личности (если применимо), журналы администрирования, а также метаданные времени и сессий.

3. Состав ЭИОС и границы ответственности

3.1. ЭИОС Организации включает (в зависимости от текущей технической архитектуры):
а) официальный сайт Организации (информационная часть и вход в личный кабинет);
б) ЛМС/личный кабинет обучающегося (доступ к курсам, модулям, материалам, заданиям, тестированию);
в) сервисы коммуникации, интегрированные в обучение (встроенные сообщения/чаты/уведомления), если они используются как элемент образовательного процесса;
г) сервисы приема оплаты/выдачи доступа (если технически связаны с ЭИОС);
д) хранилища контента и резервные хранилища (бэкапы);
е) подсистемы учета и выгрузки данных (реестры выдачи документов, отчеты по успеваемости/аттестации, выгрузка для ФИС ФРДО - если реализовано технически).

3.2. В целях проверяемости при проверках Организация фиксирует в едином «контуре ЭИОС»:
- какие системы относятся к ЭИОС;
- какие системы являются вспомогательными (например, внешние мессенджеры) и на каких условиях они применяются;
- где хранятся первичные данные «цифрового следа» и результаты обучения.

3.3. Ответственность за функционирование ЭИОС включает:
а) доступность среды (работоспособность);
б) сохранность данных;
в) корректность распределения прав доступа;
г) защиту персональных данных;
д) соблюдение требований к применению ЭО/ДОТ, включая идентифицируемость результатов и возможность подтверждения фактов обучения.

4. Роли, полномочия и разграничение доступа

4.1. В ЭИОС устанавливаются роли (минимально необходимый набор):

4.1.1. Администратор ЭИОС (системный администратор/ответственный специалист):
- управляет настройками ЭИОС, учетными записями и правами доступа;
- обеспечивает журналирование действий администраторов;
- организует резервное копирование и восстановление;
- ведет учет инцидентов и устранения сбоев;
- обеспечивает обновления и контроль уязвимостей (в пределах компетенции).

4.1.2. Методист/куратор программы (при наличии):
- управляет структурой курса (модули, задания, контрольные точки) в рамках утвержденной образовательной программы;
- имеет доступ к данным обучающихся только в объеме, необходимом для сопровождения обучения.

4.1.3. Преподаватель/эксперт/проверяющий (при наличии):
- проверяет работы, выставляет оценки/статусы, оставляет комментарии;
- не имеет доступа к административным настройкам и данным, не относящимся к его группе/программе.

4.1.4. Обучающийся:
- имеет доступ только к собственным курсам/материалам в рамках оплаченного/предоставленного доступа;
- не имеет доступа к чужим данным и административным разделам.

4.2. Принцип разграничения доступа: **минимально необходимый доступ** (только то, что нужно для выполнения функций).

4.3. Назначение ответственных лиц и распределение ролей оформляется распорядительным актом Организации (приказами о назначении ответственных за ЭО/ДОТ и функционирование ЭИОС/ЛМС, а также утверждением перечня администраторов).

5. Порядок регистрации, аутентификации и управления учетными записями

5.1. Создание учетной записи обучающегося осуществляется:
а) автоматически при регистрации/оплате (если предусмотрено архитектурой); или
б) вручную уполномоченным лицом Организации на основании данных, предоставленных обучающимся/заказчиком.

5.2. Идентификатор учетной записи должен обеспечивать однозначную связь учетной записи с обучающимся (ФИО и контактные данные) и возможность последующей верификации данных для выдачи документов (при применимости).

5.3. Требования к средствам доступа:
а) пароли должны иметь достаточную сложность (длина, разные классы символов) и не храниться в открытом виде;
б) рекомендуется (и при наличии технической возможности применяется) дополнительная защита (2FA/коды подтверждения);
в) восстановление доступа осуществляется через подтвержденный канал (e-mail/телефон) с фиксацией события в журнале.

5.4. Ограничение совместного использования доступа:
а) учетная запись является персональной;
б) передача логина/пароля третьим лицам запрещена;
в) при выявлении совместного использования Организация вправе применить меры защиты результата обучения и доказуемости аттестации (в том числе блокировку сессий, ограничение доступа, назначение повторной идентификации).

5.5. Блокировка/удаление учетных записей:
а) учетная запись может быть временно заблокирована при выявлении угроз безопасности, попытках взлома или нарушениях правил;
б) удаление учетной записи осуществляется в соответствии с требованиями к хранению учебной документации и персональных данных (приоритет - сохранение обязательных данных учета обучения в пределах законных сроков хранения).

6. Журналирование (логирование) и хранение «цифрового следа»

6.1. Организация обеспечивает журналирование событий ЭИОС, достаточное для подтверждения:
- факта предоставления доступа;
- факта входа/использования материалов;
- факта выполнения контрольных мероприятий;
- факта выставления оценок/статусов и формирования результатов;
- действий администраторов (изменения прав доступа, структуры курсов, настроек оценивания, выгрузок данных).
Это необходимо как для качества и управляемости процесса, так и для проверяемости применения ЭО/ДОТ.

6.2. Минимальный состав логов (рекомендуемый для проверок и споров):
а) лог аутентификации: дата/время, учетная запись, IP/устройство (если фиксируется), результат попытки;
б) лог доступа к курсу/модулю: событие открытия/просмотра, дата/время;
в) лог выполнения заданий/тестов: попытка, вариант/идентификатор задания, время, результат;
г) лог загрузки/проверки работ: факт загрузки, версия файла/ответа, комментарии проверяющего, итог;
д) лог административных действий: кто, что изменил, когда, результат.

6.3. Синхронизация времени: для доказуемости логов в ЭИОС должна применяться единая настройка времени (серверное время) и единый часовой пояс фиксации событий.

6.4. Сроки хранения логов устанавливаются Организацией исходя из:
а) требований к подтверждению результатов обучения (особенно для ДПО и ПО);
б) требований к хранению учебной документации;
в) сроков претензионной работы и судебной защиты.
Рекомендуемо устанавливать срок хранения ключевых логов **не менее 3 лет** после завершения обучения по конкретной программе, если иной срок не установлен внутренним контуром хранения.

6.5. Доступ к логам предоставляется строго уполномоченным лицам. Выдача логов обучающемуся возможна только в части, относящейся к нему, и с учетом ограничений по защите персональных данных и информации о безопасности системы.

7. Резервное копирование, восстановление и отказоустойчивость

7.1. Организация обеспечивает резервное копирование данных ЭИОС, включая:
а) базы данных пользователей и прогресса;
б) контент (материалы, задания, тесты);
в) загруженные работы и результаты проверок;
г) логи и технические журналы;
д) настройки системы и шаблоны курсов (при наличии).

7.2. Минимальная политика резервного копирования (для проверяемости и устойчивости):
а) регулярные бэкапы (ежедневно - инкрементальные/дифференциальные; еженедельно - полный);
б) хранение копий в изолированном хранилище (отдельная зона/облако), защищенном от несанкционированного доступа;
в) контроль целостности резервных копий;
г) периодическое тестовое восстановление (не реже 1 раза в квартал) с фиксацией результата.

7.3. Восстановление после инцидента:
а) Организация фиксирует регламент действий при утрате доступа/сбое: выявление причины, ограничение ущерба, восстановление, уведомление ответственных;
б) критичные данные (результаты аттестации, реестры, ключевые логи) восстанавливаются в приоритетном порядке.

7.4. Планируемые технические работы:
- допускаются при условии уведомления пользователей через доступный канал (внутренние уведомления/сайт/почта), если такие работы могут повлиять на доступ к оценочным мероприятиям.

8. Информационная безопасность, персональные данные и конфиденциальность

8.1. Организация обеспечивает защиту персональных данных пользователей ЭИОС в пределах требований законодательства и внутренних документов Организации (политики обработки ПДн, согласия, регламенты доступа). Настоящий Регламент определяет технически-организационные меры в части ЭИОС.

8.2. Минимальные меры защиты:
а) разграничение прав доступа;
б) учет и контроль административных учетных записей;
в) запрет передачи учетных данных;
г) применение защищенных протоколов передачи данных (https и аналоги);
д) обновление программных компонентов и устранение критических уязвимостей в разумные сроки;
е) защита резервных копий (шифрование/доступ по ролям).

8.3. Конфиденциальность материалов обучения и объектов авторского права:
а) материалы, размещенные в ЭИОС, предназначены исключительно для личного обучения обучающегося;
б) Организация вправе применять технические ограничения (ограничение скачивания, водяные знаки, ограничения сессий и др.) в пределах функционала ЭИОС;

в) выявленные факты копирования/распространения фиксируются (логи, скриншоты, служебные записки) и рассматриваются в порядке, установленном внутренними документами и условиями договора.

8.4. Инциденты безопасности:
а) при выявлении подозрительных действий Организация вправе временно ограничить доступ, инициировать проверку и запросить подтверждение личности;
б) результаты проверки оформляются внутренней записью (служебной запиской/актом) и являются основанием для мер реагирования.

9. Достоверность результатов обучения и идентификация при аттестации (особенно ДПО/ПО)

9.1. Организация обеспечивает возможность подтверждения достоверности результатов контроля и аттестации в ЭИОС, что критично для ДПО и ПО (в том числе в контуре последующего оформления документов и внесения сведений в государственные информационные системы).

9.2. Минимальный набор мер для повышения достоверности результатов:
а) персональная учетная запись обучающегося;
б) фиксация попыток и результатов в логах;
в) фиксация действий проверяющих/экспертов;
г) при необходимости - дополнительные процедуры идентификации (по правилам, установленным в локальных актах и программе).

9.3. Для ДПО при организации обучения учитываются требования Порядка, утвержденного приказом Минобрнауки России от 24.03.2025 № 266 (с 01.09.2025).

9.4. Для ПО учитываются требования Порядка, утвержденного приказом Минпросвещения России от 26.08.2020 № 438.

10. Контроль актуальности, изменения и ответственность

10.1. Регламент пересматривается:
а) при существенных изменениях технической архитектуры ЭИОС/ЛМС;
б) при изменениях требований законодательства к применению ЭО/ДОТ;
в) при выявлении недостатков по итогам внутреннего контроля/самообследования.

10.2. Ответственность за исполнение Регламента:
а) общий контроль - Генеральный директор (либо назначенное лицо);
б) операционное обеспечение - администратор ЭИОС/ответственный за ЭО/ДОТ;
в) соблюдение правил доступа - каждый пользователь в пределах своей роли.

10.3. Нарушение настоящего Регламента рассматривается как нарушение локальных нормативных актов Организации и может повлечь:
- ограничение доступа к ЭИОС;
- дисциплинарные меры в рамках образовательных отношений (для обучающихся - по правилам внутреннего распорядка и положениям об отчислении);

- меры по гражданско-правовой ответственности в рамках договора (оферты), если нарушены условия использования материалов и доступа.