РЕГЛАМЕНТ ФЕДЕРАЦИИ FEDURUS
Версия 2.0 • Редакция от 15.08.2026 г.
Утвержден 59 Советом АРБИКОН 14.10.2026

**1. Общие положения**

1.1. Настоящий Регламент определяет правовые, организационные и технические условия функционирования Федерации доступа FEDURUS (далее— Федерация).

1.2. Федерация представляет собой совокупность ИТ-систем, программно-технических средств и организационных мер, обеспечивающих технологию единого сквозного входа (WebSSO) к удаленным электронным ресурсам.

1.3. Оператором центральной технологической инфраструктуры Федерации выступает Некоммерческое партнерство «Ассоциация региональных библиотечных консорциумов» (НП АРБИКОН) (далее — Оператор Федерации).

1.4. Настоящий Регламент является открытым документом и обязателен для исполнения всеми Участниками и Партнерами Федерации.

**2. Термины и определения**

**Поставщик удостоверений** / Identity Provider (IdP) — программно-технический комплекс Участника (Университета, НИИ), осуществляющий аутентификацию пользователей на основе локальной базы учетных записей.

**Поставщик услуг** / Service Provider (SP) — программно-технический комплекс Веб-ресурса (ЭБС, научной базы данных), предоставляющий доступ к контенту на основании токенов авторизации Федерации.

**Метаданные** / Metadata — XML-документ, содержащий технические паспорта, адреса шлюзов и открытые криптографические ключи участников.

**MDQ Сервер** (Metadata Query) — центральный технологический сервис Федерации, осуществляющий поатомное (точечное) предоставление метаданных участников в реальном времени.

**Системные журналы (логи аудита)** — технические файлы регистрации сетевых маркеров (IP-адрес, дата, время и тип запроса к Discovery Service или MDQ Серверу), хранящиеся на серверах Оператора строго в течение 12 месяцев с момента фиксации для анализа стабильности распределенной сети.

**SAML 2.0** — стандартизированный протокол обмена данными авторизации и аутентификации, используемый в качестве единого технологического базиса Федерации.

**3. Права и обязанности участников (Вузов / IdP)**

3.1. Участник обязан поддерживать в актуальном и работоспособном состоянии локальный шлюз IdP (Shibboleth IdP, SimpleSAMLphp или аналог).

3.2. Участник самостоятельно несет ответственность за безопасность, конфиденциальность и своевременный отзыв учетных записей (при отчислении или увольнении пользователей) в своей локальной службе каталогов (Active Directory / LDAP).

3.3. Участник имеет право на включение своих метаданных в реестр Федерации и получение бесшовного доступа к ресурсам, на которые у организации оформлена коммерческая подписка.

3.4. Участник обязуется своевременно (не менее чем за 5 рабочих дней) инициировать процедуру ротации криптографических сертификатов (IdP Certificate Rollover), извещая Команду проекта.

**4. Права и обязанности поставщиков услуг (ЭБС /SP)**

4.1. Поставщик услуг обязан обеспечить корректный прием SAML-токенов от IdP-участников и разграничивать права доступа на основе переданных академических атрибутов.

4.2. Поставщик услуг гарантирует легитимный учет уникальных читателей и предоставление корректной статистики использования ресурсов вузами.

4.3. Поставщик услуг обязуется своевременно обновлять кэш метаданных с центрального MDQ-сервера Федерации.
4.4. Поставщик услуг имеет право запрашивать стандартный профиль атрибутов: eduPersonPrincipalName (ePPN) для личного кабинета и eduPersonScopedAffiliation для определения роли пользователя (student, faculty, staff).

**5. Политика безопасности и персональных данных (Матрица ФЗ-152)**

5.1. Инфраструктура Федерации спроектирована и функционирует на основе сквозного принципа технологической изоляции потоков данных (Privacy by Design). Центральные узлы Оператора (Discovery Service, MDQ Сервер) физически и технологически не запрашивают, не собирают, не хранят и не обрабатывают аутентификационные данные (логины и пароли) пользователей, их имена или иные прямые персональные данные.
5.2. Прямой обмен обезличенными SAML-атрибутами осуществляется Сторонами напрямую через веб-браузер конечного пользователя посредством HTTP-редиректов и полностью минует центральные серверы Оператора Федерации. Первоначальным Оператором ПДн своих студентов и сотрудников признается Вуз; Поставщик услуг (ЭБС) признается самостоятельным Оператором ПДн строго в рамках личного кабинета читателя.
5.3. Передача деперсонализированных академических атрибутов (eduPersonPrincipalName, eduPersonScopedAffiliation, schacHomeOrganization) признается Сторонами легитимной в рамках исполнения Федерального закона№ 152-ФЗ, не содержит трансграничных рисков и осуществляется в зашифрованном HTTPS/TLS-периметре.
5.4. В случае компрометации учетных записей пользователей на стороне внутренней инфраструктуры Вуза или несанкционированного доступа к базам данных ЭБС, локализация инцидента и оперативное уведомление Роскомнадзора осуществляются силами и за счет стороны, допустившей нарушение, без юридического и финансового привлечения Оператора Федерации.

**6. Порядок подключения, изменения реестра и финансовые условия**

6.1. Подключение новых организаций к эксплуатационной системе осуществляется на основании официального заявления-анкеты и является возмездным. Участие в проекте FEDURUS предусматривает оплату вступительного взноса в размере 25 000 рублей и ежегодного членского взноса в размере 30 000 рублей. Для организаций, являющихся действующими членами НП АРБИКОН, предоставляется скидка в размере 10% от утвержденной стоимости тарифов.
6.2. Включение метаданных в производственный фид (Production) выполняется Исполнительной командой проекта после успешного прохождения технического тестирования в утилите AttributeValidator и верификации ЭЦП.
6.3. Оператор оставляет за собой право временно исключить метаданные Участника или Поставщика услуг из центрального реестра в случае компрометации его закрытых ключей шифрования или создания критической нагрузки на инфраструктуру Федерации.

**7. Разрешение споров и технический аптайм**

7.1. Мониторинг работоспособности центральных узлов (Discovery Service, MDQ Сервер, RapidConnect) осуществляется Командой проекта АРБИКОН в режиме 24/7.
7.2. Все споры, связанные с некорректным маппингом атрибутов или блокировкой доступа, решаются путем направления технических тикетов в службу поддержки по адресу: support@fedurus.ru.
7.3. В случае проведения официальных проверок органами государственного надзора (Роскомнадзор) или расследования инцидентов ИБ, Оператор Федерации обязуется по официальному запросу Участника предоставить техническую выписку из системных журналов аудита (сетевые маркеры IP и времени доступа), если с момента фиксации инцидента не истек установленный 12-месячный срок хранения логов