Приложение №2

К договору №\_\_-\_\_-\_\_/20\_\_М

От «\_\_\_» \_\_\_\_20\_\_ г.

**Технический РЕГЛАМЕНТ Проекта АРБИКОН**

**«ФЕдерация Доступа к Удаленным Ресурсам Учебной Среды (ФЕДУРУС)»**

1. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**ФЕДУРУС** (Далее - Федерация)- единая информационная система, объединяющая и согласовывающая сервисы аутентификации участников на основе утвержденных правил и политик, и позволяющая эффективно использовать электронные ресурсы через глобальные сети передачи данных.

**Домашняя организация** – учебная, научная или иная организация, использующая в своей учебной и научной деятельности электронные ресурсы.

**Правообладатель** - учебная, научная или коммерческая организация, владеющая правами на один или несколько электронных ресурсов и предоставляющая к нему/к ним доступ на определенных условиях.

**Пользователь** – физическое лицо, являющееся студентом или сотрудником **Домашней организации** (аффилировано с **Домашней организацией**).

**Сервис Провайдер/Service Provider (SP)** – информационная система, управляющая доступом **Пользователей** к электронному ресурсу или группе ресурсов **Правообладателя**. **SP** предоставляет доступ пользователю, аффилированному с **Домашней** организацией, если **Домашняя** организация пользователя имеет право предоставлять аффилированным с ней пользователям доступ к ресурсу на основе лицензионных и/или иных договоров с **Правообладателем**.

**Провайдер идентификации/Identity Provider (IdP)** – информационная система, отвечающая за взаимодействие системы управления учетными записями пользователей **Домашней организации** с SP и иными сервисами **ФЕДУРУС**.

**Оператор IdP, Оператор SP –** организация, принимающая на себя обязательства по развертыванию за свой счет, своими силами, соответственно, **IdP** или **SP** сервисов аутентификации на основе правил и политик **ФЕДУРУС.**

**Члены Федерации** – организация, являющаяся **Оператором IdP и/или SP** и заключившая соответствующий Договор с АРБИКОН (п. \_\_\_).

**Утверждение** - набор данных в цифровой форме, генерируемый сервисом IdP на основе информации о **Пользователе (Цифровой карты идентификации)**, получаемой от системы управления учетными записями пользователей **Домашней организации**

**Цифровая карта идентификации** – информация необходимая для аутентификации Пользователя Домашней организации, за хранение и управление которой отвечает система управления учетными записями пользователей Домашней организации.

**Оператор Федерации** – управляющий орган Проекта ФЕДУРУС.

1. ПРИНЦИПЫ РАБОТЫ ПРОТОКОЛА АВТОРИЗАЦИИ

sc1

sc2

**Доступ Пользователя к электронному ресурсу**

Когда Пользователь изъявляет желание получить доступ к электронному ресурсу (шаг 1) SP требует от Пользователя аутентифицироваться в Домашней организации (шаги 2 и 3) и посредством сервиса IdP получает Утверждение об аутентификации или отказе (4).

1. ПРАВА И ОБЯЗАННОСТИ ЧЛЕНОВ ФЕДЕРАЦИИ
   1. **Общие права и обязанности Членов Федерации**
      1. Члены Федерации имеют права и обязанности в соответствии с этим Положением и Договором между Членом Федерации и АРБИКОН о сотрудничестве в области развития библиотечно-информационных ресурсов и сервисов.
      2. Объем бесплатных и платных услуг и сервисов, получаемых Членами Федерации, определяется в Договоре между Членом Федерации и АРБИКОН о сотрудничестве в области развития библиотечно-информационных ресурсов и сервисов.
      3. Члены Федерации признают, что участие в Федерации не дает автоматического доступа к электронным ресурсам других Членов Федерации и является вопросом двусторонних Договоров с правообладателем электронного ресурса, не являющихся предметом настоящего положения.
      4. Члены Федерации воздерживаются от изменения или иного технического вмешательства в функционирование федеративных сервисов ФЕДУРУС.
      5. Каждый член Федерации развертывает за свой счет, своими силами SP и/или IdP сервисы аутентификации.
   2. **Роли членов Федерации**
      1. **Оператор Федерации**
         1. Управляет центральными компонентами инфраструктуры аутентификации и авторизации Authentication and Authorization Infrastructure (AAI), включая:
            * Реестр Федерации;
            * Тестовую федеративную среду;
            * Сервис определения/Discovery Service (WAYF Сервис «Откуда ты пришел?»/Where are You from);
            * Веб-сайт федерации по адресу fedurus.ru
         2. Поддерживает функционирование репозитория ПО Федерации.
         3. Осуществляет консультационную и организационно-техническую поддержку членов Федерации (также см. 3.6.2).
         4. Члены Федерации признают право **Оператора Федерации** использовать получаемые Метаданные IdP и SP с целью администрирования федеративных сервисов.
         5. Члены Федерации признают право **Оператора Федерации** использовать факт членства их организаций в Федерации с целью продвижения Федерации и привлечения новых членов.
      2. **Оператор IdP.**
         1. Оператор IdP обязан за свой счет, своими силами развернуть сервис IdP на основе взаимодействия с системой управления учетными записями пользователей **Домашней организации** с выпуском **Утверждений о Пользователе для SP.**
         2. Сервис считается развернутыми после прохождения процедур проверки корректной работы IdP в режиме тестовой федерации в соответствии с «Инструкцией по развертыванию и эксплуатации ПО ФЕДУРУС».
         3. Оператор IdP обязан организовать процедуру аутентификации Пользователей своей Домашней организации, включая:
            * Удаление аккаунтов Пользователей, более не аффилированных с Домашней организацией (отчисленные и закончившие обучение студенты, уволенные сотрудники).
            * Своевременное изменение атрибутов Пользователей своей Домашней организации в случае изменений Пользовательских данных (смена электронной почты, изменения в должности и пр.).
         4. Оператор IdP обязан предотвратить выпуск идентификационных данных, совпадающих с уже выпущенными для выбывшего пользователя, если с момента последнего использования идентификационных данных выбывшего пользователя прошло менее 24 месяцев.
         5. Оператор IdP обязан обеспечить поддержку Пользователей своей Домашней организации, а также квалифицированную техническую поддержку администраторам сервисов IdP. Оператор IdP обязан организовать такой уровень поддержки пользователей, чтобы избежать запросов Пользователей напрямую в Федерацию. Оператор IdP обязан обеспечить поддержку пользователей в рабочие дни и часы по своему местному времени.
      3. **Оператор SP.**
         1. Оператор SP обязан за свой счет, своими силами развернуть сервис SP.
         2. Сервис SP считается развернутыми после прохождения процедур проверки корректной работы SP в режиме тестовой федерации в соответствии с «Инструкцией по развертыванию и эксплуатации ПО ФЕДУРУС».
         3. На основании Утверждений, выпускаемых операторами IdP Членами Федурус, осуществлять управление доступами Пользователей к своему ресурсу или группе ресурсов.
         4. Оператор SP обязан использовать передаваемые ему метаданные Пользователей исключительно для организации доступа к своему ресурсу и предотвратить передачу метаданных третьей стороне.