Личный кабинет читателя библиотеки. Интеграция с ЕСИА

Галина Арноси

Для чего библиотеке?

- Вход в «Личный кабинет читателя», не имея читательского билета
- Удаленная самостоятельная и самодостаточная регистрация читателя. Не требует подтверждения. Данные пользователя подтверждены и достоверны.

Этапы интеграции с ЕСИА

Организационный этап — регистрация информационной системы в Министерстве цифрового развития

Технический этап — подключение информационной системы к ЕСИА

Библиотеке не дадут промышленный доступ к ЕСИА, в отличие от тестового …

А кому дадут?

- органу государственной власти (министерства, ведомства на всех уровнях)
- органу местного самоуправления (администрация города, района и т.д.)

Выход

- СРАЗУ договориться с ОГВ или ОМСУ о том, что регистрация ИС в ЕСИА будет проходить от их имени.

Владельцем ИС становится ОГВ или ОМСУ,

а БИБЛИОТЕКА как организация - оператор этой ИС.

Организационный этап

1. Создание учетной записи организации на портале Госуслуг

- Создает подтвержденный сотрудник, имеющий КЭП юридического лица
- Если КЭП юридического лица не принадлежит сотруднику, назначенному за работу с тех.порталом ЕСИА, то необходимо добавить сотрудника через Госуслуги в организацию и наделить ролью для работы с тех.порталом

2. Регистрация ИС на технологическом портале ЕСИА

- Заполнение всех данных и адреса личного кабинета в сети Интернет. Присваивается мнемоника - буквенно-цифровой код системы. Перечень требуемых scope: fullname, birthdate, gender, email, contacts или какие кому еще необходимы
- Загружается сертификат – открытая часть КЭП. Необходимо для обмена зашифрованными данными между личным кабинетом и ЕСИА (Сертификат КЭП так же загружается и используется по договоренности или ОГВ или ОМСУ или организации)

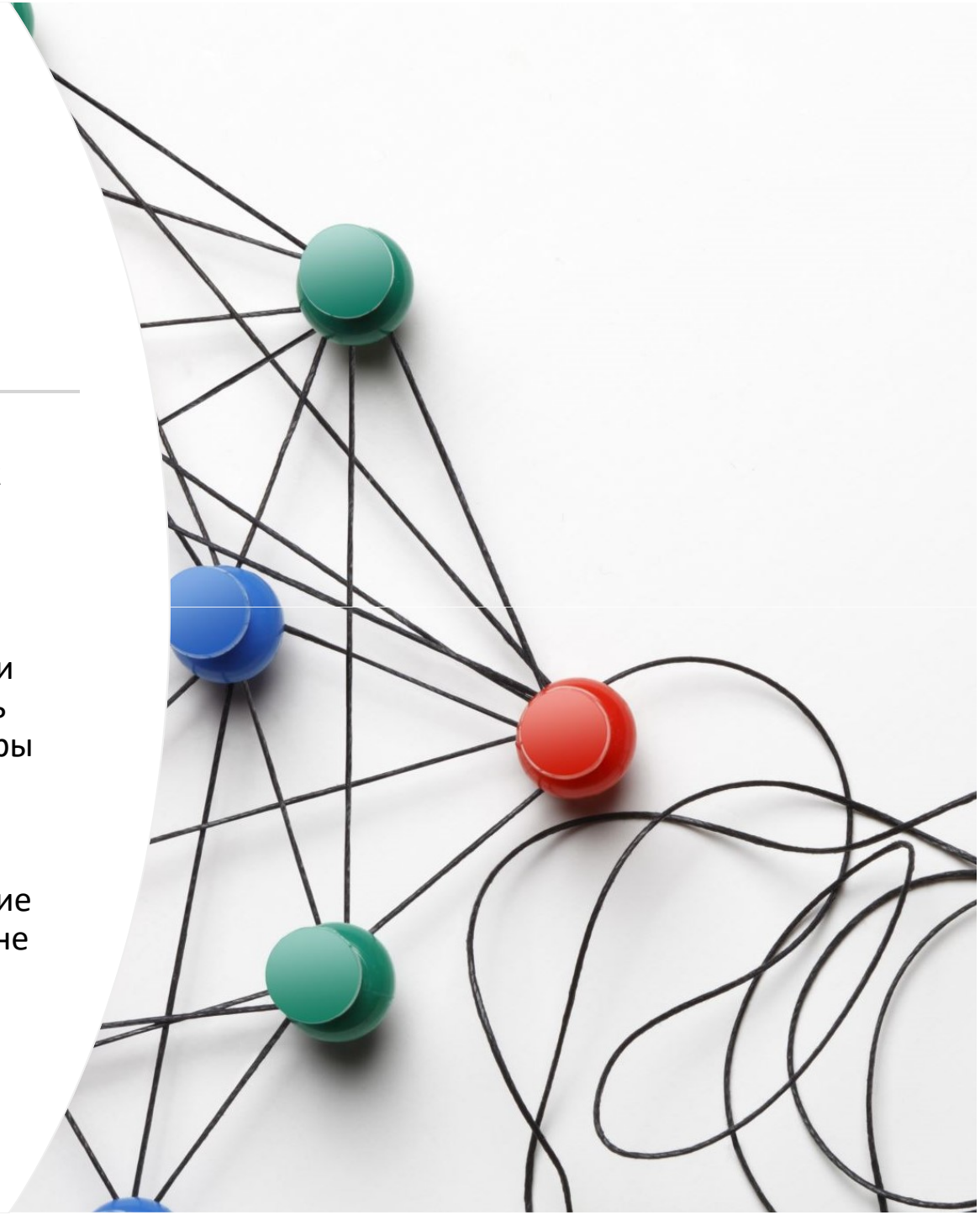
Организационный этап

3. Отправка заявки на подключение к тестовому контуру ЕСИА

- Заполнение заявки от имени организации и отправка вместе с открытым сертификатом КЭП и документами, подтверждающими возможность и целесообразность подключения к ЕСИА на Минцифры РФ

4. Получение доступа к тестовому контуру ЕСИА

- Доработка, отладка и тестирование модуля авторизации ИС на стороне организации



Организационный этап

5. Отправка заявки на подключение к промышленному контуру ЕСИА
   - Заполнение заявки от имени организации и отправка вместе с открытым сертификатом КЭП и документами, подтверждающими возможность и целесообразность подключения к ЕСИА на Минцифры РФ, а так же номером заявки на тестовый доступ
6. Получение доступа к промышленному контуру ЕСИА
   - Запуск модуля авторизации в личном кабинете в промышленную эксплуатацию

Документация

Руководство пользователя технологического портала:
https://digital.gov.ru/ru/documents/6190/

Регламент информационного взаимодействия Участников с Оператором ЕСИА и Оператором инфраструктуры электронного правительства:
https://digital.gov.ru/ru/documents/4244/
Содержит формы заявок для отправки в Минцифру

Методические рекомендации по использованию ЕСИА:
https://digital.gov.ru/ru/documents/6186/

Статья по сборке криптопровайдера OpenSSL+Gost
https://cyber01.ru/kak-dobavit-podderzhku-gost-34-10-2012-v-centos-redhat-7/

Статья Сборка модуля ГОСТ для веб-сервера XAMPP в сборнике КРЫМ 2021
https://www.gpntb.ru/win/inter-events/crimea2021/sbor-docl21.pdf

Технический этап

Подключение к тестовому контуру

- **Взаимодействие с ЕСИА осуществляется с использованием протокола OAuth 2.0 и расширения OpenID Connect 1.0**

- *OAuth 2.0* — протокол авторизации, позволяющий выдать одному сервису (приложению) права на доступ к ресурсам пользователя на другом сервисе. Протокол избавляет от необходимости доверять приложению логин и пароль, а также позволяет выдавать ограниченный набор прав, а не все сразу.

- *OpenId Connect* - простой слой учетных данных поверх протокола OAuth 2.0. Данный протокол является протоколом системы единого входа, позволяющей использовать пользователю одну учётную запись для авторизации на различных интернет ресурсах

- **Сценарий аутентификации при интеграции по OpenIDConnect1.0**

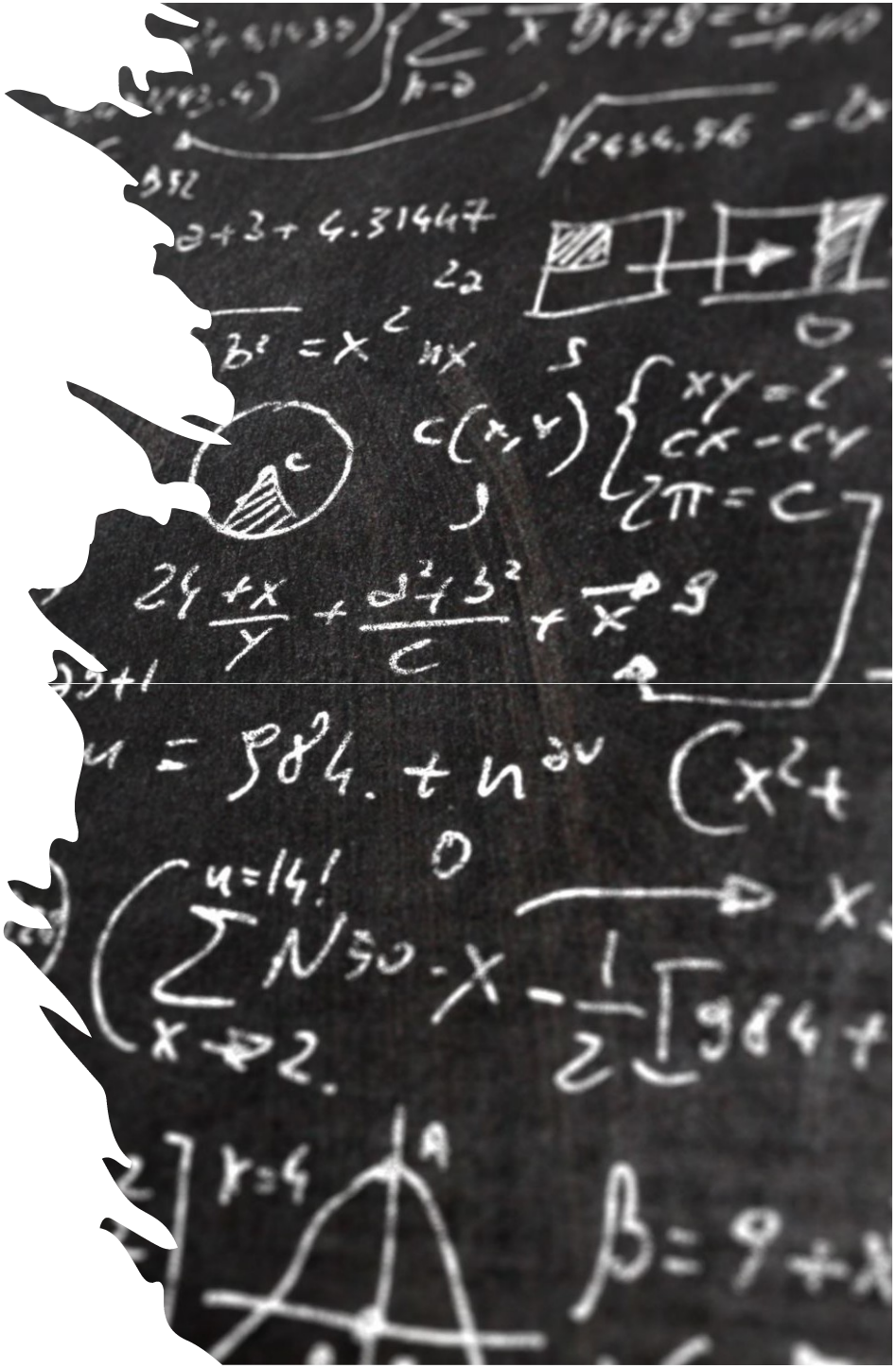
Рекомендуется использовать модель контроля на основе делегированного принятия решения, когда система-клиент при доступе к ресурсу должна получить разрешение на это действие со стороны владельца ресурса – зарегистрированного пользователя портала Госуслуг.

Требования к программному обеспечению для поддержки авторизации пользователей АБИС с использованием ЕСИА

- веб-сервер должен поддерживать протокол https с зарегистрированным и действительным сертификатом SSL
- требуется наличие PHP версии не ниже 7.2.31 с подключенными функциями (extensions): curl, dom, libxml, openssl, session
- на веб-сервере должна быть включенной поддержка синхронизации системного времени через интернет
- необходимо сформировать отдельный сертификат для подписи запросов к ЕСИА

Сертификат для подписи запросов к ЕСИА

- Сообщения, отправляемые на сервис ЕСИА требуется снабжать цифровой подписью, сделанной с помощью сертификата с ГОСТ алгоритмом
- Такие ЭЦП распространяются на «Флешке» в виде закрытого контейнера приватного ключа и открытого сертификата.
- Для встраивания в ИС на стороне «Личного кабинета читателя» **НЕ ПОДХОДИТ. ЭЦП должен быть с возможностью экспортировать сертификат** экспортировать вместе с приватным ключом. Для этого , понадобится купить ПО (P12FromGostCSP от Lissy они платные)
- Чтобы работать с экспортированным сертификатом ГОСТ без покупки специализированного ПО понадобится специальная сборка openssl, которая публично не распространяется, а существует только в виде исходных кодов



Сертификат для подписи запросов к ЕСИА

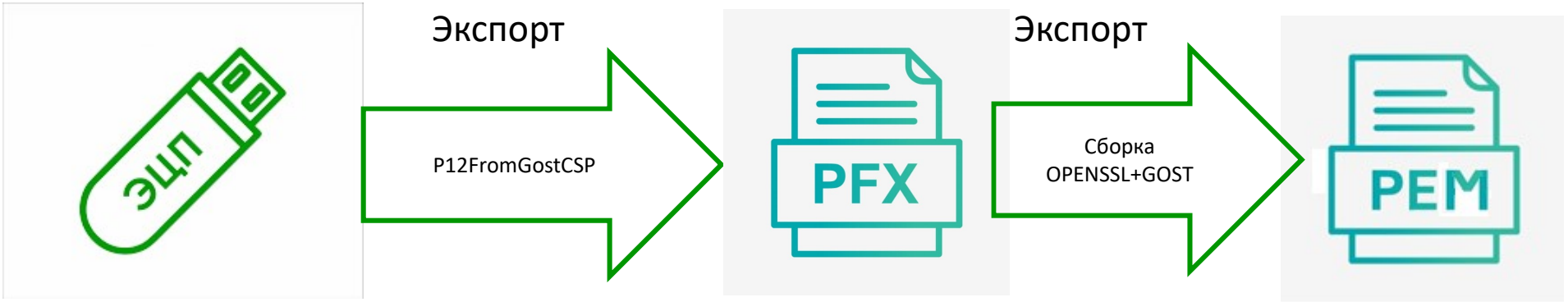
Что же делать с КЭП ?

Такие ЭЦП распространяются на «Флешке» в виде закрытого контейнера приватного ключа и открытого сертификата.

Для встраивания в ИС на стороне «Личного кабинета читателя» **НЕ ПОДХОДИТ. ЭЦП должен быть с возможностью экспортировать сертификат**

Конвертировать !

Существуют различные варианты, один из:



Закрытый контейнер
(приватный ключ)
+
открытый сертификат
в отдельных файлах
7 файлов

Формат ключа
PKCS # 12
Закрытый
+
открытый ключ
в одном файле,
зашифрован

Формат ключа
PEM
Закрытый
+
открытый ключ
в одном файле,
текстовый

Этапы взаимодействия с ЕСИА

на сайте вашей ИС формируется запрос к ЕСИА с использованием цифровой подписи, которую вы делаете с помощью выгруженного сертификата

после прохождения авторизации на ваш сайт приходит запрос от ЕСИА с данными пользователя в виде JSON с теми полями, которые вы запросили

далее вы должны либо найти пользователя, либо создать его у себя

Пример данных приходящих с ЕСИА

```
$personInfo =
Array
(
    'stateFacts' => Array('EntityRoot'),
    'firstName' => ‘имя',
    'lastName' => ‘фамилия',
    'middleName' => ‘отчетсво',
    'birthDate' => ‘дд.мм.гггг',
    'gender' => 'M',
    'trusted' => '1',
    'updatedOn' => '1664801576',
    'rfgUOperatorCheck' => false,
    'status' => 'REGISTERED',
    'verifying' => false,
    'rIdDoc' => '15839750',
    'containsUpCfmCode' => false,
    'eTag' => '58F951C6FA45BF1A9C5D4F78AE9E28EE9B5F1229'
);
```

Пример данных приходящих с есиа

```
$addressInfo =
Array
(
   Array
      (
         'stateFacts' => Array('Identifiable'),
         'id' => '63894966',
         'type' => 'PRG',
         'addressStr' => ‘региона, населенный пункт, улица',
         'fiasCode' => '86626fac-3d49-4134-9e33-9cc9c727e53d',
         'flat' => ‘квартира',
         'countryId' => 'RUS',
         'house' => ‘дом',
         'zipCode' => ‘почтовый индекс',
         'city' => ‘НП',
         'street' => ‘улица',
         'region' => ‘регион',
         'eTag' => '0CD3CFC9540A36A380E28CCEAECEFDE41F4EF50B'
      )
);
```

Пример данных приходящих с есиа

```
$contactInfo =
Array
(
   Array
      (
         'stateFacts' => Array('Identifiable'),
         'id' => '58626785',
         'type' => 'EML',
         'vrfStu' => 'VERIFIED',
         'value' => ‘имя_ящика@адрес почтового сервера',
         'otpCodeLength' => '4',
         'eTag' => '21111D023D8D91980570B5C54676838C84B4540C',
      ),
   Array
      (
         'stateFacts' => Array('Identifiable'),
         'id' => '241848496',
         'type' => 'MBT',
         'vrfStu' => 'VERIFIED',
         'value' => '+7(999)9999999',
         'otpCodeLength' => '4',
         'eTag' => '2E8BBB01449B0B16E459F7841F2483E902CB4863'
      )
);
```

Компонент для авторизации через ЕСИА

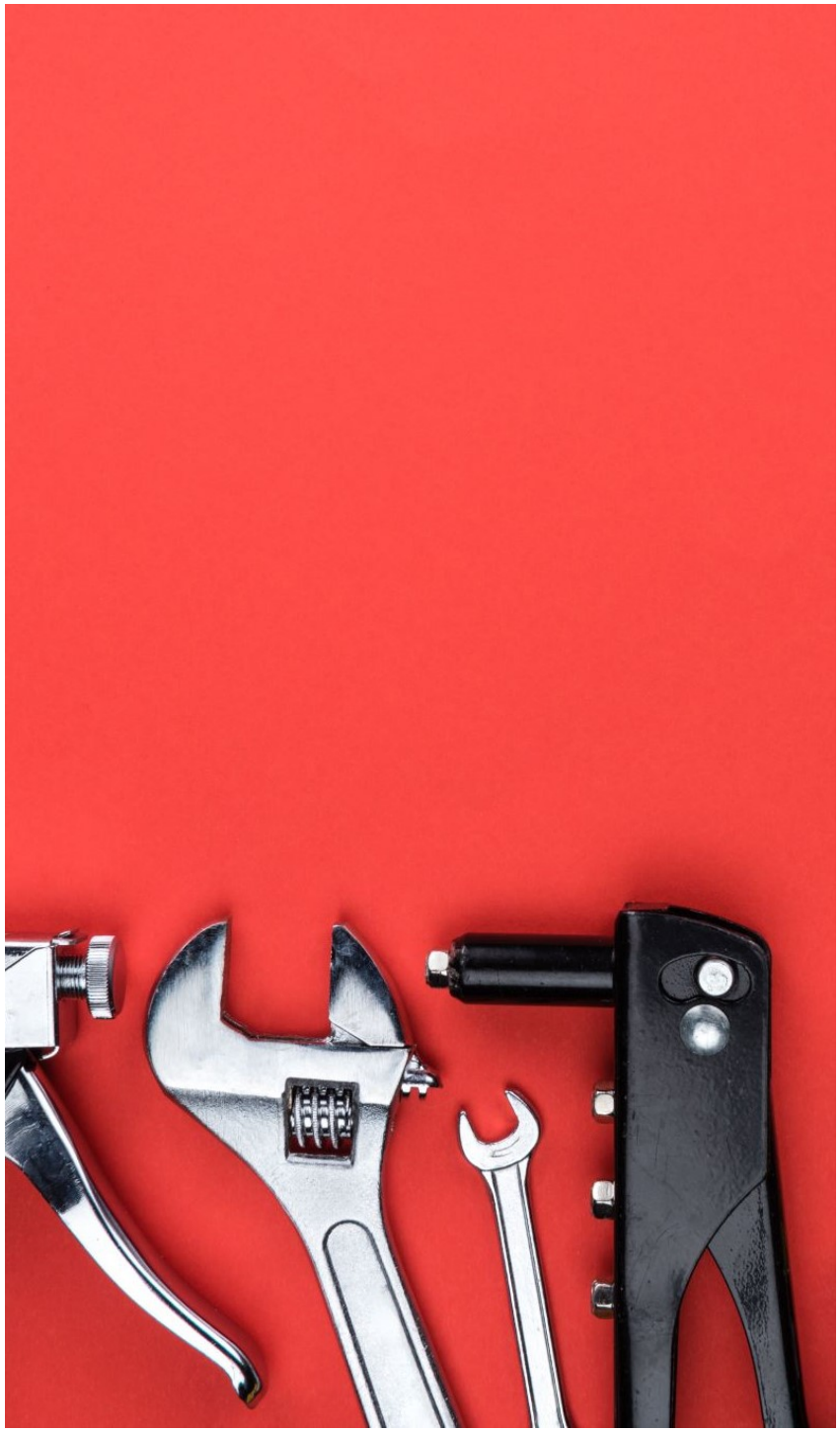
1. Установить composer:

https://getcomposer.org/

2. Установить пакет:

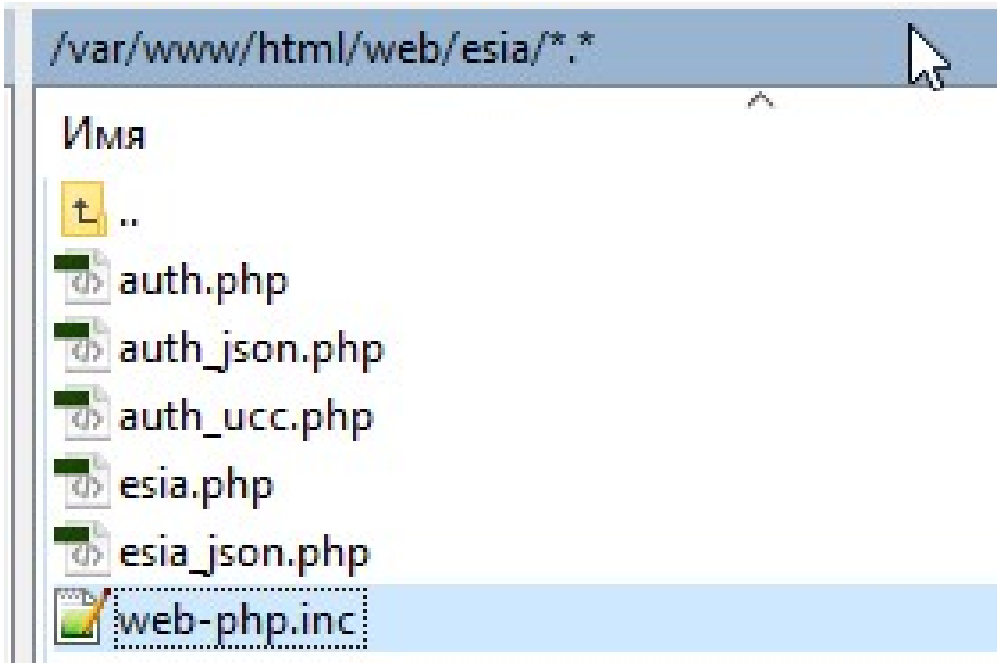
https://github.com/fr05t1k/esia

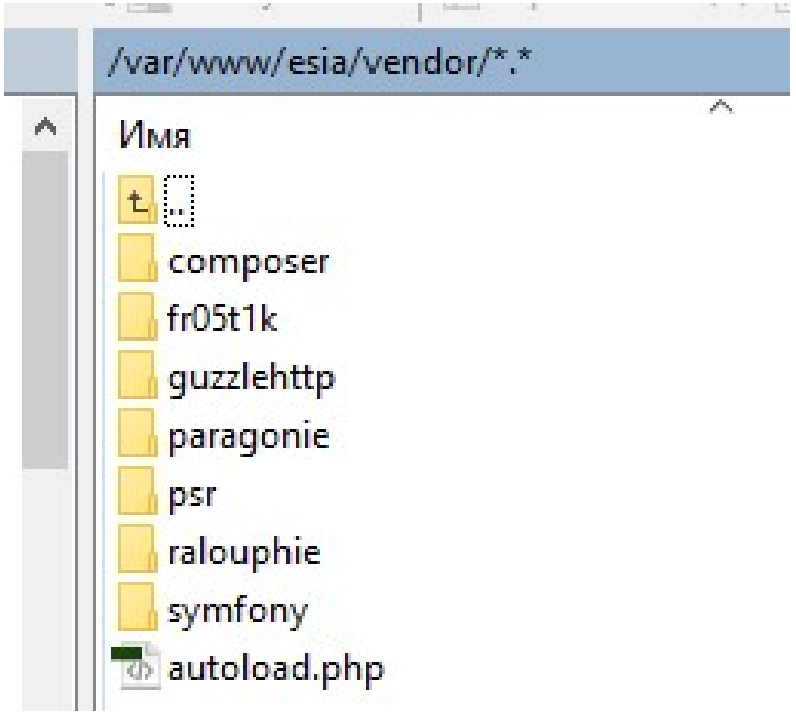
3. Инструкция по установке composer и установки необходимых пакетов - https://www.hostinger.ru/rukovodstva/kak-ustanovit-composer



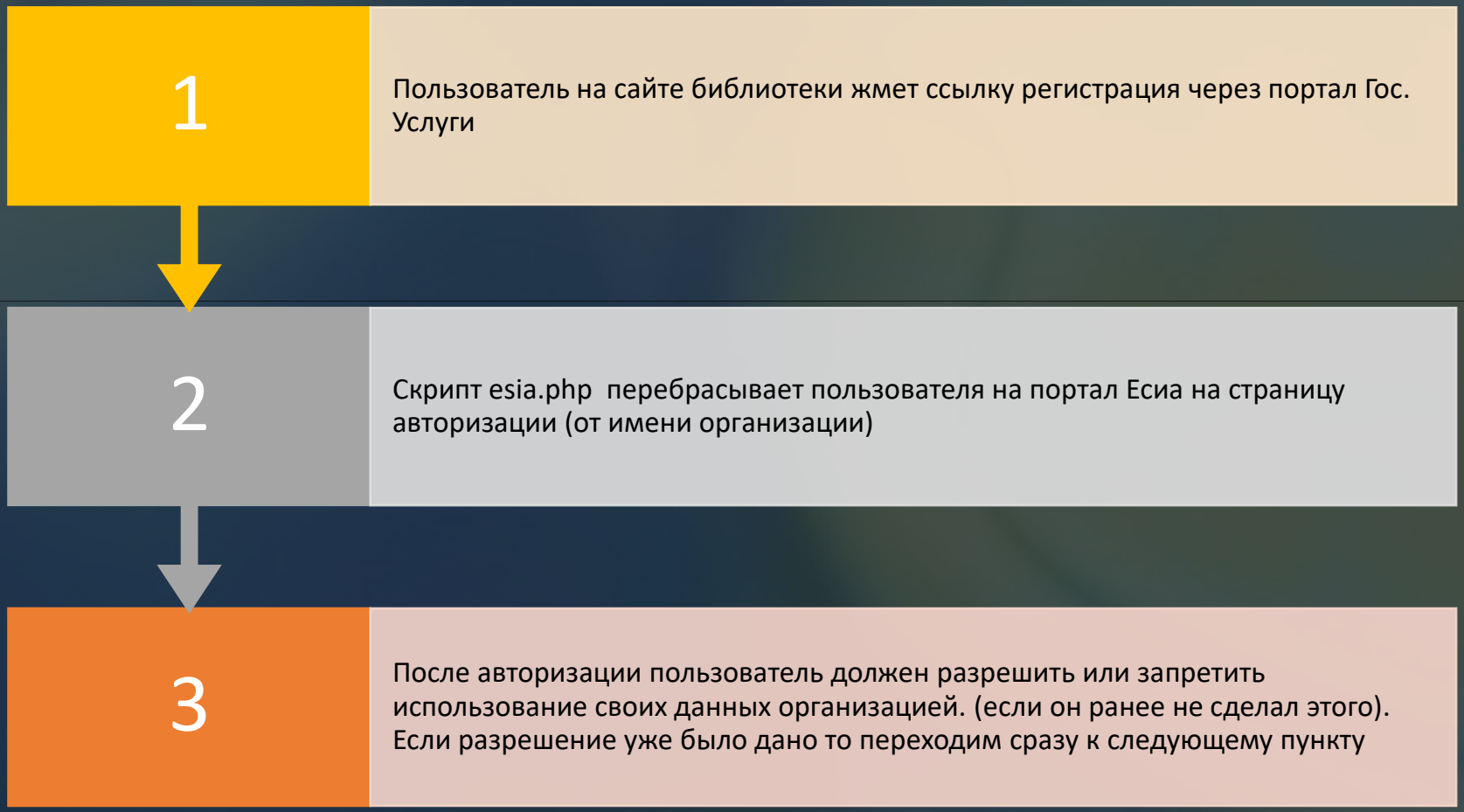
Модуль авторизации через ЕСИА для WEB-ирбис

- устанавливается как набор скриптов php на той же платформе веб-сервера, на которой работает портал WEB ИРБИС
- Начальный вариант был предоставлен Ассоциацией ЭБНИТ и в поставке он скрипты работают с сервером ИРБИС64+ через Z-сервер (*Колосов Кирилл Анатольевич*)
- В научной библиотеке вся работа идет с БД Читателей через скрипты разработанные для модуля WEB-Ирбис64+ php





Последовательность действий



Последовательность действий

4

Если пользователь дал согласие, то портал ЕСИА переадресует пользователя на сайт библиотеки на скрипт auth.php (с кодом для получения токена)

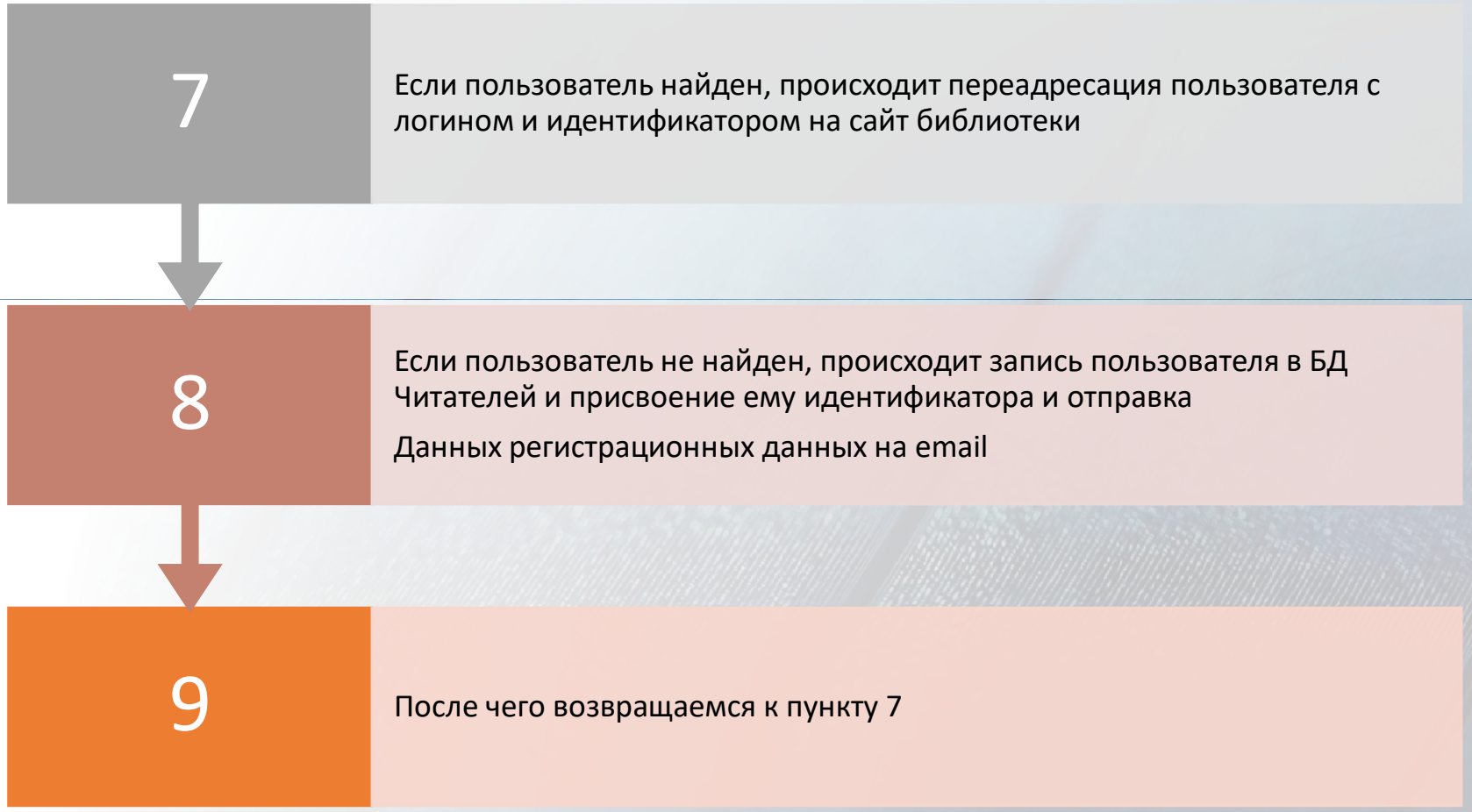
5

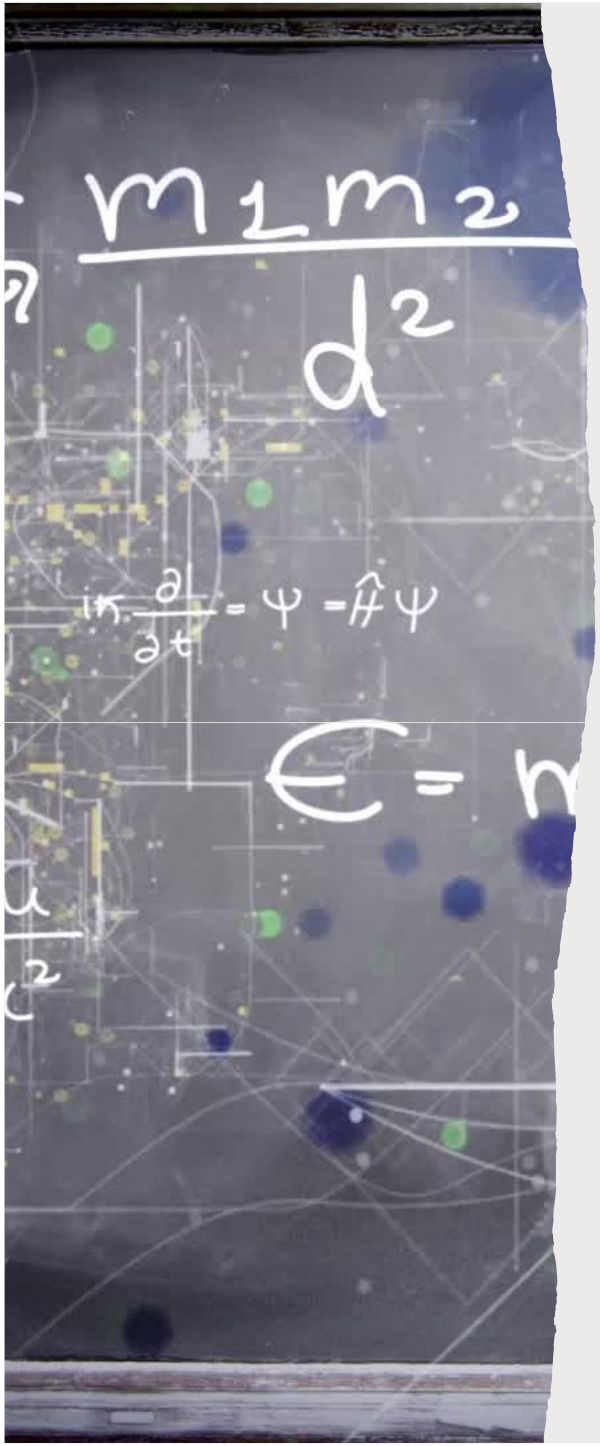
Скрипт auth.php запрашивает токен пользователя и его данные через компонент fr05t1k/esia

6

После получения запрошенных данных скрипт auth.php пытается найти пользователя в БД Читателей

Последовательность действий

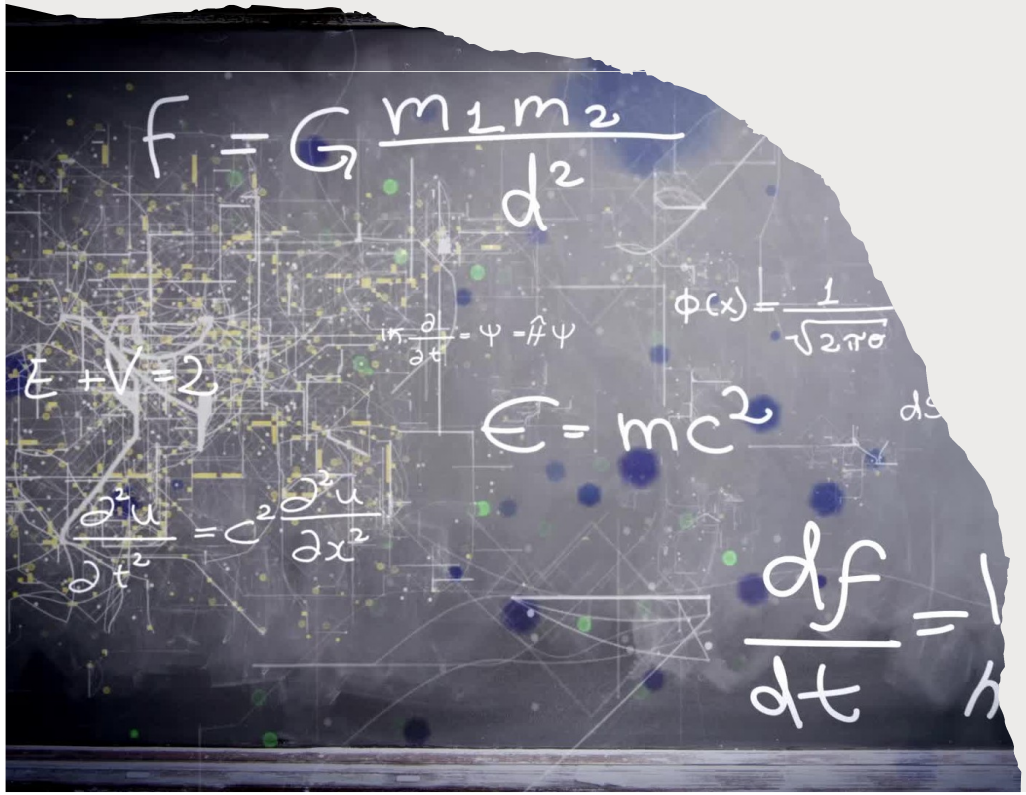




Config в файле esia.php

- **'clientId'** => мнемоника - буквенно-цифровой код системы
- **'redirectUrl'** => Адрес на сайте куда переадресовывать после авторизации
- **'portalUrl'** => 'https://esia-portal1.test.gosuslugi.ru/’ - адрес портала ЕСИА тестовый контур
- **'privateKeyPath'** => Путь до ключа pem
- **'privateKeyPassword'** => Пароль ключа pem
- **'certPath'** => Путь до ключа pem
- **'scope'** => ['fullname','birthdate','gender','email','contacts'] - Перечень требуемых scope

Config в файле auth.php



- 'clientId' => мнемоника - буквенно-цифровой код системы
- 'redirectUrl' => Адрес на сайте куда переадресовывать после авторизации
- 'portalUrl' => 'https://esia-portal1.test.gosuslugi.ru/' - адрес портала ЕСИА тестовый контур
- 'privateKeyPath' => Путь до ключа pem
- 'privateKeyPassword' => Пароль ключа pem
- 'certPath' => Путь до ключа pem
- 'scope' => ['openid'] - уникальный идентификатор владельца токена

Подключение компонента fr05t1k

- Оба скрипта подключают компонент fr05t1k в начале скрипта

  require __DIR__ . '/vendor/autoload.php';
- Пришлось немного доработать сам компонент fr05t1k

  esia\vendor\fr05t1k\esia\src\Esia\Signer SignerPKCS7.php
- Были закомментированы строки с 22 по 40, а так же с 45 по 59
- И добавлена строчки для подписи сообщении при общении с порталом есиа

- **$cmd**="set OPENSSL_CONF=путь до конфига сборки openssl /openssl_gost/openssl.cnf && путь до самой сборки сборки/openssl_gost/openssl smime -sign -in ".$messageFile." -out ".$signFile." -noattr -passin pass:".$this->privateKeyPassword." -binary -signer ".$this->certPath;

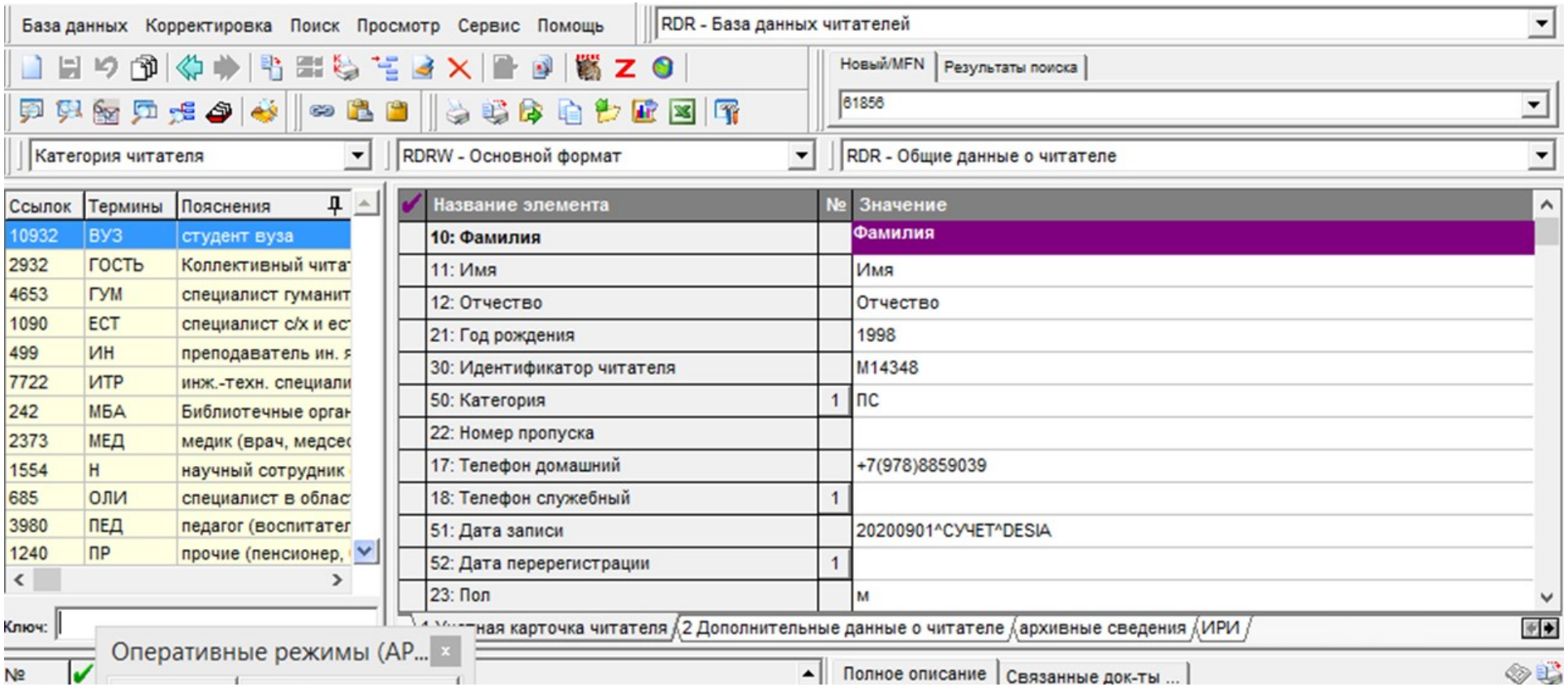
- **exec($cmd);**

Вся работа с БД Читателей осуществляется через модуль WEB-Ирбис64+ php

```
REP
10
1
if ' ':&uf('Av10*',f(rsum(&uf('+95'v10),'-1'),0,0),'.1#1') then &uf
('+v',f(rsum(&uf('+95'v10),'-1'),0,0),'#',v10) else v10 fi
XXXXXXXXXXXXXXXXXX
IF
if a(v30) and a(v22) and &uf('av51^d#1'):'ESIA' then '1' else '0' fi
XXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXX
ADD
30
XXXXXXXXXXXXXXXXXX
if v13^C='Красноярск' then &uf('++C303#1') else &uf('++C302#1')   fi
XXXXXXXXXXXXXXXXXX
```

Генерация идентификатора

Для генерация идентификатора используется БД счетчиков (COUNT) и сценарий технической глобальной корректировки autoing.gbl БД RDR



Результат записи читателя в БД RDR

Что корректировать в самом WEB-Ирбис

- В директории фреймов WEB-Ирбис64 корректировке подвергаются лишь два файла для **старого интерфейса**/директория DEFAULT/

- В **файле Not_author_3.frm** прописываем ссылку вида:

 Войти через Гос. Услуги

- В файле **author_3.frm** ссылка на выход меняется :

Выход

- В директории фреймов WEB-Ирбис64+ корректировке подвергаются лишь два файла для **нового интерфейса** /директория DEFAULT/

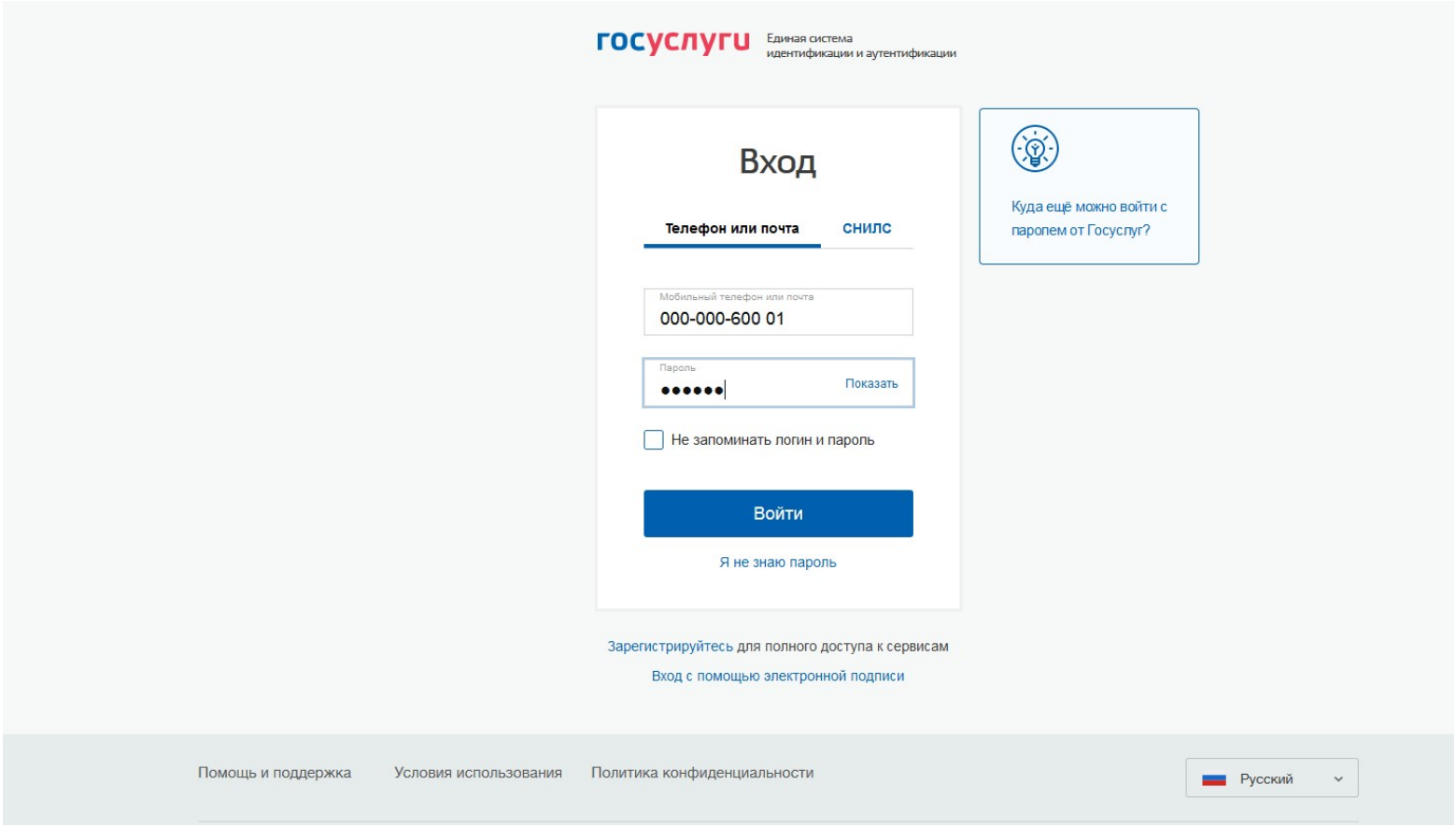
- В файле **header_ft.frm** ссылка ссылка на выход меняется :

Выход

- В файле **author.frm** прописываем ссылку вида:

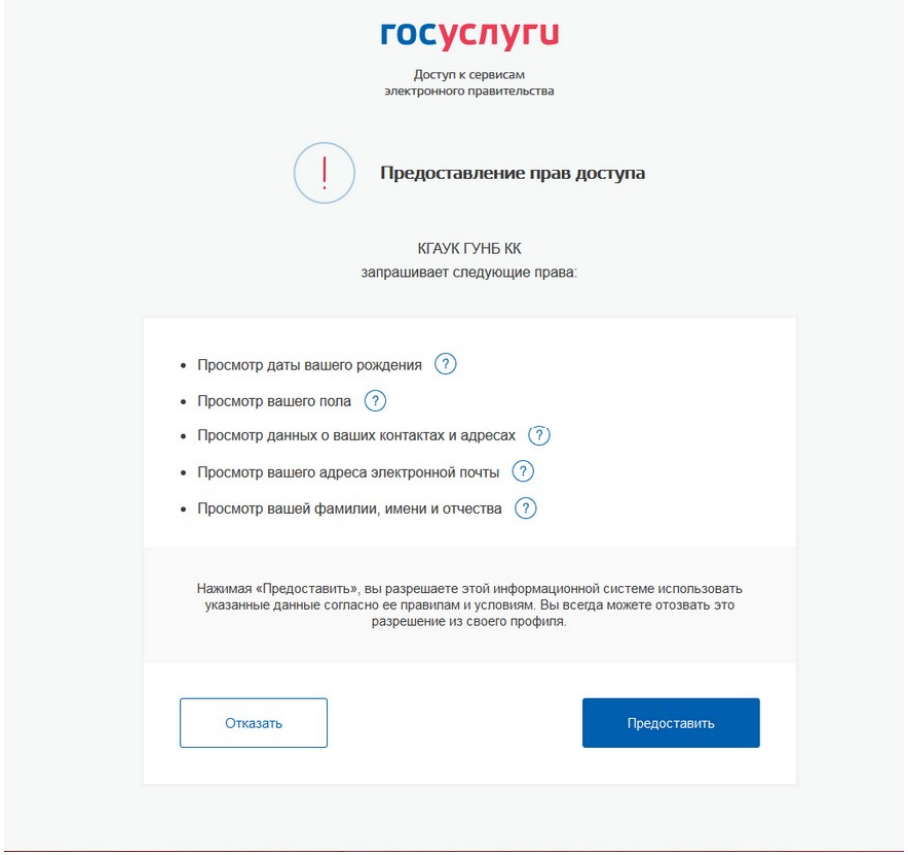
 Войти через Гос. Услуги

Ссылка в моем примере ведет на тестовый контур ЕСИА (в реальной работе здесь должна быть ссылка на промышленную среду ЕСИА)

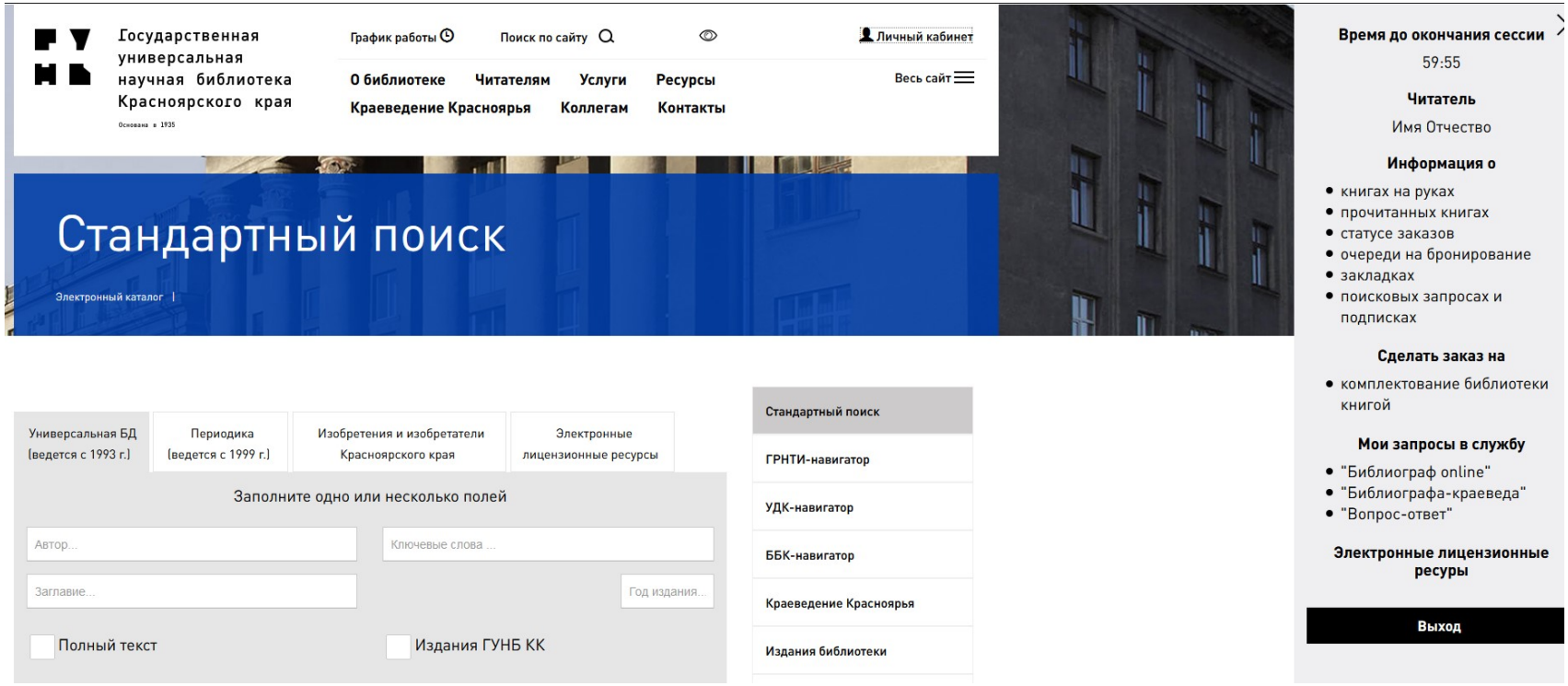


Окно авторизации на портале госуслуг

Запрос разрешения на использование учетных данных



Результат авторизации



Спасибо за внимание

arnosi@mail.ru