Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.422.81

Шуманский
Дмитрий Игоревич

Единая идентификация пользователей в государственных системах на основе технологии OpenID connect

Автореферат диссертации
на соискание степени магистра технических наук
по специальности 1-98 80 01 «Информационная безопасность»

_____
(подпись магистранта)

Научный руководитель
Пулко Татьяна Александровна
кандидат технических наук, доцент

_____
подпись научного руководителя)

г. Минск, 2021

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Исследования на тему магистерской диссертации выполнялись в рамках выполнения опытно-конструкторской работы «Разработка компонентов Белорусской интегрированной сервисно-расчетной системы (Единая система идентификации физических и юридических лиц, Клиентская программа)» (далее – ОКР) выполненной в рамках мероприятия 12 «Создание Белорусской интегрированной сервисно-расчетной системы» (Этап 2 – Создание информационно-коммуникационной инфраструктуры Белорусской интегрированной сервисно-расчетной системы (внедрение пилотной зоны)) подпрограммы 2 «Инфраструктура информатизации» Государственной программы развития цифровой экономики и информационного общества на 2016 – 2020 годы) (в редакции постановления Совета Министров Республики Беларусь от 9 ноября 2018 г. № 806).

Исследования по теме магистерской диссертации проводились с целью разработки механизма предоставления информационным системам различных государственных органов и иных организаций Республики Беларусь сервиса строгой идентификации/аутентификации.

Для достижения для достижения целей исследования решены следующие задачи:

– выполнен аналитический обзор способов аутентификации в веб-приложениях;

– разработаны протоколы аутентификации CAUTH и SAUTH;

– проведена экспертная оценка стойкости разработанных протоколов аутентификации в экспертной организации, осуществляющей прикладные математические исследования;

– выполнена ОКР;

– проведены испытания средств защиты, разработанные в ходе выполнения ОКР, в аккредитованной испытательной лаборатории по требованиям безопасности информации.

Научная новизна проведенных исследований заключается в расширении спецификации Open ID Connect [11] криптографическими алгоритмами, стандартизованными в Республике Беларусь, в разработке и реализации новых протоколов аутентификации.

Соискатель ученой степени в соответствии с приказом директора научно-производственного республиканского унитарного предприятия «Научно-исследовательский институт технической защиты информации» от 25.07.2019 № 64 выполнял роль руководителя проекта, главного конструктора ОКР.

Основные результаты диссертации реализованы в разработанных в рамках ОКР ЕС ИФЮЛ, КП, КПСИС. Результаты ОКР являются составной частью БИСРС.

Полный объем диссертации составляет 81 страницу, в том числе 20 рисунков и 3 таблицы. Список литературы содержит 14 наименований.

Описание представляемого исследования включает введение, шесть глав, заключение, библиографический список и приложение.

Во Введении обсуждается актуальность работы, цели и задачи исследования.

В главе 1 описываются существующие способы аутентификации в веб-приложениях. В разделе 1.1 описываются методы аутентификации по паролю. Раздел 1.2 содержит описание аутентификации с использованием сертификатов открытых ключей. В разделе 1.3 изложен способ прохождения процедуры аутентификации с использованием одноразовых паролей. Раздел 1.4 содержит описание аутентификации с использованием ключей доступа. В разделе 1.5 описываются методы и стандарты аутентификации с использованием различных токенов.

В главе 2 исследуются возможности протокола Open ID Connect, описываются механизмы регистрации, подготовки запроса, получения токенов, проверки их действительности, проверки подписи, запрос информации об аутентифицированных пользователях.

Глава 3 содержит описание подсистем разработанной Единой системы аутентификации физических и юридических лиц, содержит описание применяемых механизмов, структуру модифицированных токенов, схемы взаимодействия прикладных информационных систем с ЕС ИФЮЛ.

Главы 4 и 5 содержат описание разработанных протоколов аутентификации CAUTH и SAUTH. Изложено описание шагов протокола и структур, передаваемых между сторонами протокола сообщений.

В главе 5 содержится описание применяемых в ЕС ИФЮЛ механизмов безопасности.

В заключении сформулированы основные результаты диссертации.

В приложении 1 приведена копия экспертного заключения о стойкости протоколов аутентификации CAUTH и SAUTH.

ОСНОВНАЯ ЧАСТЬ

Цифровые технологии меняют нашу действительность. Развитие современной экономики во многом базируется на процессах цифровой трансформации.

Цифровизация является неотъемлемой частью инновационного развития Республики Беларусь, приоритеты которого определены в Государственной программе инновационного развития Республики Беларусь.

Ключевую роль играет возможность строгой аутентификации граждан Республики Беларусь в электронном мире.

Стойкость протокола аутентификации и достоверная уверенность в подлинном соответствии электронного представителя действительному физическому лицу, находящемуся «по ту сторону экрана», являются гарантом соблюдения интересов граждан при оказании электронных услуг и получении административных процедур. Применение современных методов защиты при использовании электронных средств аутентификации дают гарантию защиты передаваемых и хранимых в электронном виде персональных данных.

ЕС ИФЮЛ разработана с целью формирования единых подходов к обеспечению идентификации гражданина с использованием информационно-коммуникационных технологий и обеспечения юридически значимого электронного взаимодействия между гражданами и государством (за счет реализации возможности совершения юридически значимых действий посредством ЭЦП) и предназначена для предоставления информационным системам различных государственных органов и иных организаций Республики Беларусь сервиса идентификации/аутентификации.

ЕС ИФЮЛ состоит из следующих подсистем:

– подсистемы серверов идентификации и ресурсов;

– подсистемы пользователя;

– подсистемы управления, настройки и конфигурирования.

Схема функционирования ЕС ИФЮЛ приведена на рисунок 1.

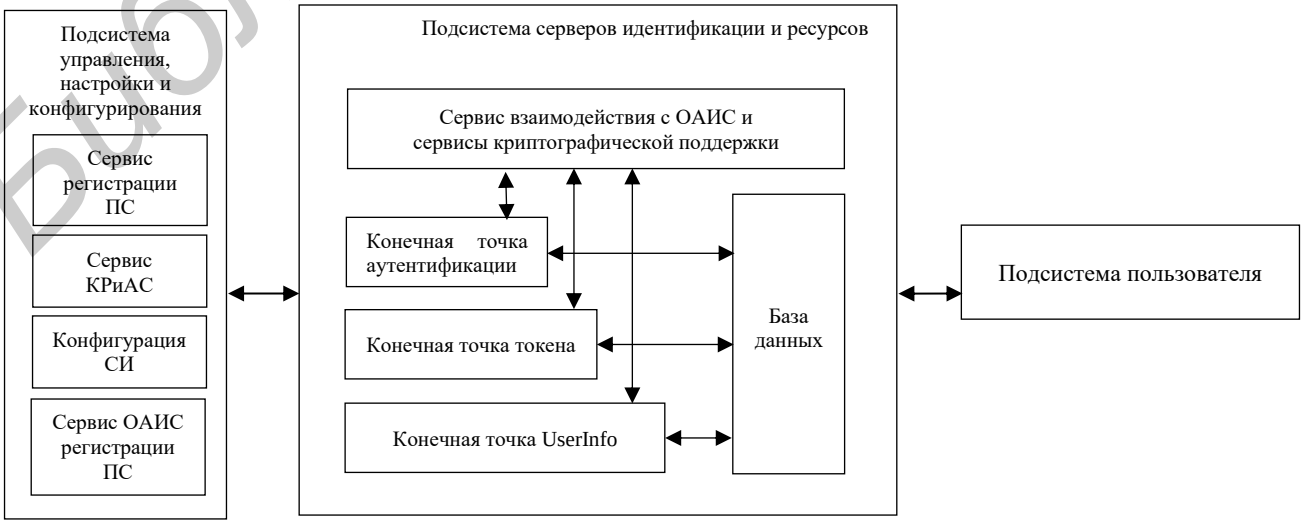

Рисунок 1 – Схема функционирования ЕС ИФЮЛ

Коммуникационная схема взаимодействия ЕС ИФЮЛ в рамках БИСРС изображена на рисунке 2.

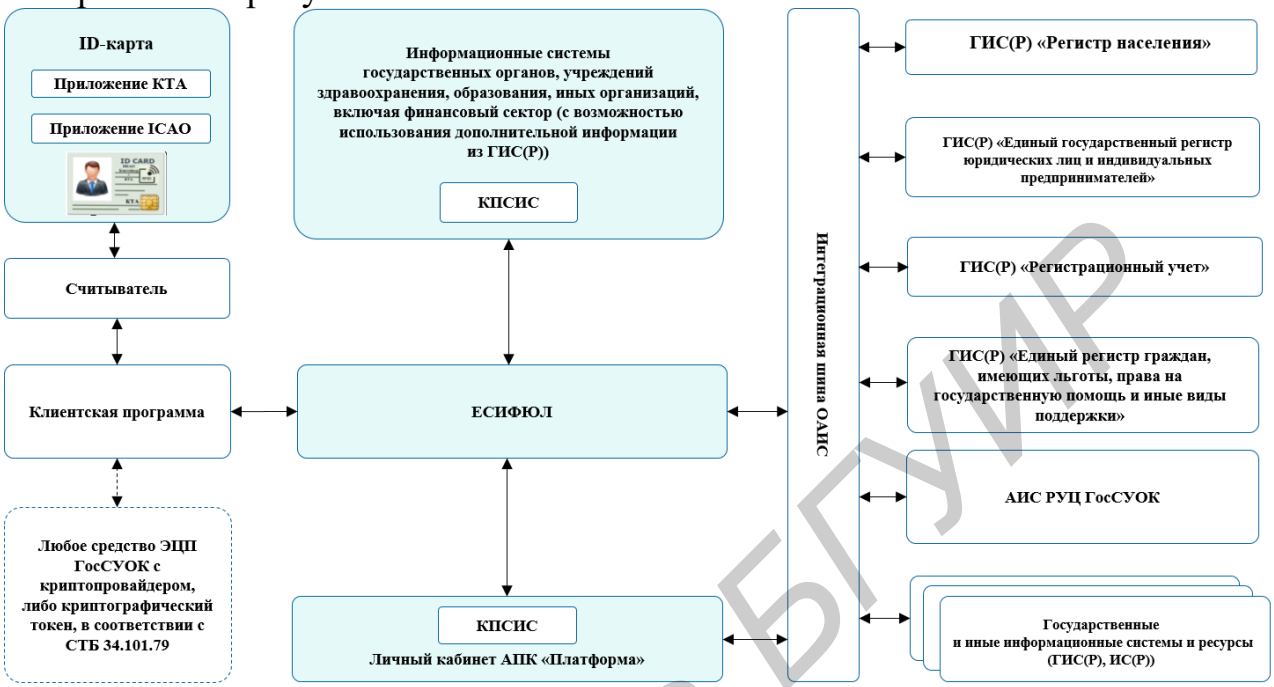

Рисунок 2

Схема взаимодействия ЕС ИФЮЛ с внешними ПС изображена на рисунке 3.

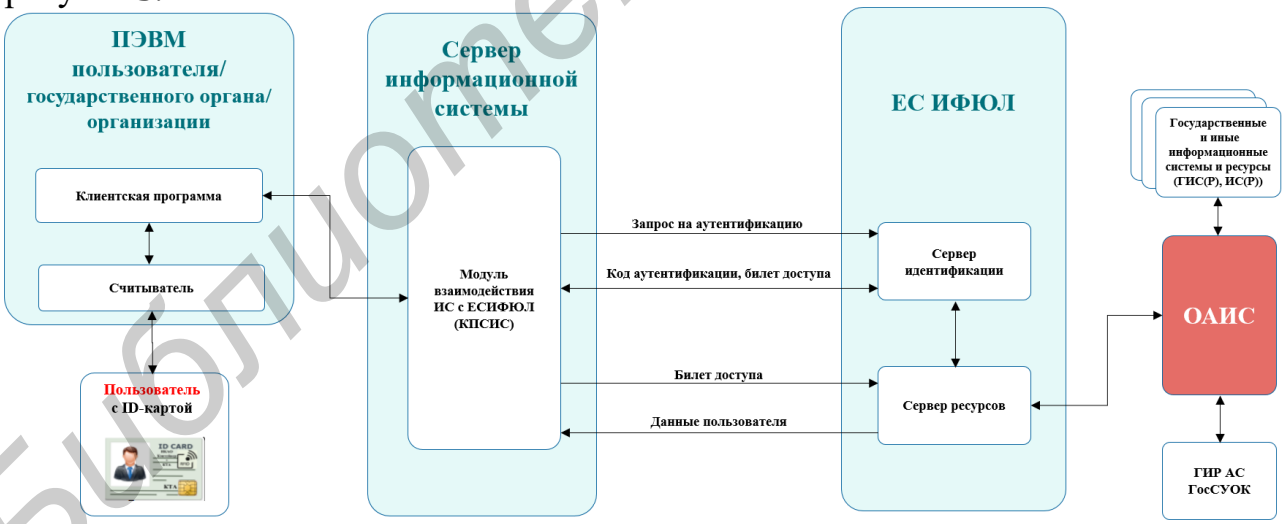

Рисунок 3

Протокол аутентификации CAUTH

Протокол аутентификации CAUTH используется для взаимной аутентификации физического лица, владеющего идентификационной картой (КТА), и СИ.

В ходе протокола стороны проводят аутентификацию друг друга и дополнительно СИ формирует для ПС код авторизации.

Физическое лицо в ходе аутентификации использует КП и КТА.

КП взаимодействует с КТА путем обмена APDU-командами в соответствии с Профилем КТА.

Аутентификация и выпуск кода авторизации проводятся СИ ЕС ИФЮЛ по запросу ПС при помощи КП и с согласия владельца.

Порядок взаимодействия ЕС ИФЮЛ и ПС соответствует схеме Authorization Code Flow спецификации OpenID Connect Core 1.0.

В протоколе аутентификации используются утверждения Scope_ПС, которые могут быть получены из СОК конечного пользователя (Scope_token) или дополнительно запрошены посредством сервисов ОАИС (Scope_ОАИС).

При использовании открытых каналов связи атрибуты передаются в формате конвертованных данных в соответствии с СТБ 34.101.23 (9), для шифрования используется СТБ 34.101.31 (6.4).

Входные данные протокола аутентификации – запрос аутентификации, сформированный КПСИС, подписанный личным ключом ПС и сконвертованный на открытом ключе СИ.

Выходные данные протокола аутентификации – код авторизации.

Протокол аутентификации SAUTH

Протокол аутентификации SAUTH используется для взаимной аутентификации физического лица, владеющего сертификатом открытого ключа, и СИ.

В ходе протокола стороны проводят аутентификацию друг друга и дополнительно СИ формирует для ПС код авторизации.

Физическое лицо в ходе аутентификации использует КП и программно-аппаратное средство ЭЦП, реализующее функцию выработки ЭЦП.

Средство ЭЦП должно иметь сертификат соответствия Национальной системы подтверждения соответствия требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность», включать криптопровайдер, реализующий интерфейс CryptoAPI для ОС семейства Windows. Сертификат открытого ключа физического лица должен храниться в средстве ЭЦП.

КП взаимодействует со средством ЭЦП следующими способами:

1) посредством криптопровайдера, работающего по интерфейсу CryptoAPI – для ОС семейства Windows;

2) посредством интерфейса обмена информацией с аппаратно-программным носителем ключевой информации (токеном), определенному в СТБ 34.101.21 с уточнениями, определенными в СТБ 34.101.78 (12) – для ОС семейства Windows, Linux, MacOS.

Аутентификация и выпуск кода авторизации проводятся СИ ЕС ИФЮЛ по запросу ПС при помощи КП и с согласия владельца.

Порядок взаимодействия ЕС ИФЮЛ и ПС соответствует схеме Authorization Code Flow спецификации OpenID Connect Core 1.0.

В протоколе аутентификации используются утверждения Scope_ПС, которые могут быть получены из СОК конечного пользователя (Scope_token)

или дополнительно запрошены посредством сервисов ОАИС (Scope_ОАИС).

При использовании открытых каналов связи атрибуты передаются в формате конвертованных данных в соответствии с СТБ 34.101.23 (9), для шифрования используется СТБ 34.101.31 (6.4).

Входные данные протокола аутентификации – запрос аутентификации, сформированный КПСИС, подписанный личным ключом ПС и сконвертованный на открытом ключе СИ.

Выходные данные протокола аутентификации – код авторизации.

Механизм PKCE

The Proof Key for Code Exchange (PKCE) – дополнение для Authorization Code Flow, используется для усиления безопасности и предотвращения атак, направленных на перехват кода авторизации.

Механизм PKCE включает следующие объекты:

– code_verifier – хэш-значение, вычисленное в соответствии с СТБ 34.101.31 по алгоритму *belt-hash256* от сгенерированной псевдослучайной числовой последовательности в соответствии с СТБ 34.101.47 по алгоритму *brng-crt-hbelt*, которое закодировано в соответствии с правилами BASE64URL;

– code_challenge – хэш-значение от значения code_verifier по алгоритму *belt-hash256*;

– code_challenge_method – значение идентификатора алгоритма преобразования, используемого для получения code_challenge (используется метод «HBELT», который указывает на использование алгоритма *belt-hash256)*.

Порядок работы механизма PKCE:

1) КПСИС делает запрос аутентификации (/authz), включая code_challenge и code_challenge_method;

2) СИ ЕС ИФЮЛ проверяет запрос аутентификации, сохраняет code_challenge и code_challenge_method;

3) СИ ЕС ИФЮЛ проводит аутентификацию пользователя;

4) СИ ЕС ИФЮЛ возвращает код авторизации конечному пользователю с его перенаправлением в ПС;

5) при необходимости получения БД, ПС посредством КПСИС запрашивает его в конечной точке токена СИ ЕС ИФЮЛ. В запрос включается code_verifier;

6) СИ проверяет запрос, вычисляет code_challenge, используя алгоритм, указанный в code_challenge_method;

7) СИ сравнивает code_challenge, полученный во время авторизации, и вычисленный ранее. Если они совпадают, то СИ ЕС ИФЮЛ выдает БД для ПС.

Защищенные соединения

В соответствии с рекомендациями, изложенными в спецификации OpenID Connect core 1.0, защита каналов между ПС и СИ должна осуществляться с применением TLS.

Могут быть использованы иностранные криптонаборы, удовлетворяющие следующим требованиям:

– версия протокола TLS не ниже 1.2;

– для выработки общих ключей должны использоваться алгоритмы на основе алгоритма Диффи-Хеллмана с эфемерными ключами, такие, как DHE_RSA, ECDHE_ECDSA, ECDHE_RSA;

– для шифрования и имитозащиты должен использоваться алгоритм AES-GCM, либо связка алгоритмов ChaCha20 и Poly1305;

– для вычисления хэш-значения должны использоваться функции семейств SHA-2 или SHA-3;

– должно быть запрещено шифрование в режиме CBC;

– битовая длина модуля RSA должна быть не меньше 2048;

– битовая длина порядка группы точек эллиптической кривой должна быть не меньше 256;

– битовая длина ключей шифрования и имитозащиты должна быть не меньше 128;

– должны быть запрещены 64-битовые блочные криптосистемы;

– битовая длина хэш-значений должна быть не меньше 256.

Должны использоваться криптонаборы, определенные в СТБ 34.101.65, или криптонаборы из следующего списка:

1) ECDHE-ECDSA-AES128-GCM-SHA256;
2) ECDHE-ECDSA-AES256-GCM-SHA384;
3) ECDHE-ECDSA-CHACHA20-POLY1305.

Схема защиты передаваемых сообщений

Сообщения, направляемые между ПС и ЕС ИФЮЛ защищаются с применением механизмов CMS. Используется схема Enveloped-then-Signed.

Сообщения от ПС к СИ имеют формат: Signed_ПС(Enveloped_СИ(Req)). Обратные сообщения от СИ к ПС передаются в формате Signed_СИ(Enveloped_ПС(Resp)).

Алгоритмы генерации псевдослучайных чисел

Для генерации кода авторизации применяется алгоритм генерации псевдослучайных чисел в режиме HMAC *brng-hmac-hbelt* согласно СТБ 34.101.47.

Алгоритмы шифрования и контроля целостности

Для защиты информации при ее передаче и обработке в соответствии с требованиями СТБ 34.101.31 применяются следующие алгоритмы:

– *belt-cfb256* – алгоритм шифрования в режиме гаммирования с обратной связью (6.4);

– *belt-hash256* – алгоритм хэширования (6.9).

Выработка и проверка электронной цифровой подписи

Для контроля целостности и подлинности сообщений в соответствии с требованиями СТБ 34.101.45 применяют алгоритмы выработки и проверки ЭЦП, алгоритмы транспорта ключа.

Выработка ЭЦП осуществляется по алгоритму *bign-with-hbelt* в соответствии с СТБ 34.101.45-2013 (7.1).

Транспорт ключа осуществляется по алгоритму *bign-keytransport* в соответствии с СТБ 34.101.45-2013 (7.2).

Синтаксис криптографических сообщений

Для обеспечения конфиденциальности, контроля целостности и подлинности данных при их передаче и хранении применяются требования СТБ 34.101.23 [3], который устанавливает синтаксис криптографических сообщений и определяет форматы криптографических сообщений, а также правила создания и обработки сообщений. При описании форматов используется абстрактно-синтаксическая нотация версии 1.

Форматы данных

Подписанные данные – это произвольные данные, дополненные несколькими ЭЦП, выработанными одной или несколькими сторонами.

Тип подписанных данных согласно СТБ 34.101.23 (8) [3] задается следующим идентификатором:

id-signedData OBJECT IDENTIFIER::={iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 2}

Формат подписанных данных в обязательном порядке содержит компоненты:

– certificate – сертификат подписанта;

– атрибут время подписания с идентификатором

id-signingTime OBJECT IDENTIFIER ::= (iso(l) member-body(2) us(840) rsadsi(113549) pkcs(l) pkcs9(9) 5}.

Конвертованные данные – это зашифрованные данные вместе с зашифрованными для получателя ключом шифрования данных.

Тип конвертованных данных задается следующим идентификатором:

id-EnvelopedData OBJECT IDENTIFIER ::={iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 3}

ЗАКЛЮЧЕНИЕ

В ходе выполнения магистерской диссертации выполнен анализ способов аутентификации в веб-приложениях, изучена спецификация OIDC, выполнена модернизация OIDC с использованием криптографических механизмов и протоколов, стандартизованных в Республике Беларусь, разработана Единая система идентификации физических и юридических лиц, разработаны протоколы аутентификации CAUTH и SAUTH. Выполнен анализ стойкости разработанных протоколов в НИИ ППМИ БГУ (копия экспертного заключения изложена в приложении 1).

ЕС ИФЮЛ является компонентом БИСРС и предназначена для предоставления гражданам Республики Беларусь сервисов строгой цифровой аутентификации для получения электронных услуг в информационных системах электронного правительства.

Разработка и внедрение ЕС ИФЮЛ позволит использовать идентификационную карту гражданина Республики Беларусь для получения допуска к миру электронных услуг и формирования электронной цифровой подписи для подтверждения для осуществления юридически-значимых действий в электронном мире.

Используемые в ЕС ИФЮЛ механизмы защиты позволяют с высокой степенью вероятности утверждать о безопасности разработанной системы и надежности способов защиты персональных данных граждан в соответствии с законодательством Республики Беларусь.

СПИСОК СОБСТВЕННЫХ ПУБЛИКАЦИЙ

1. Д.И.Шуманский. Единая идентификация физических лиц / 56-я научная конференции аспирантов, магистрантов и студентов БГУИР: материалы научной конференции, Минск, 18-20 мая, 2020 г. – Минск: БГУИР, 2020.

2. Д.И.Шуманский. Безопасность при аутентификации физических лиц посредством Единой системы идентификации физических и юридических лиц / XIX Белорусско-российская научно-техническая конференция: материалы научно-технической конференции, Минск, 8 июня 2021 г. – Минск: БГУИР, 2021.